UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

METODOLOGÍA DE AUDITORÍA EN SEGURIDAD INFORMÁTICA PARA REDES DE COMPUTADORAS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N :

FERNANDO GONZÁLEZ BRINGAS

MARCOS GARCÍA FRANCO

ULISES ESCALONA GONZÁLEZ

DIRECTOR DE TESIS: ING. HERIBERTO OLGUÍN ROMO

MÉXICO, D.F. 2 0 0 7

Agradecimientos generales:

A la Universidad Nacional Autónoma de México y a la Facultad de Ingeniería, en donde nos hemos desarrollado y dejado parte de nuestras vidas, pasando una etapa muy importante y especial en nuestra preparación y desarrollo como profesionistas.

Deseamos agradecerle a nuestro director de tesis, el Ing. Heriberto Olguín Romo, por su apoyo y guía para la realización del presente trabajo. Así mismo al Ing. Andrés Velázquez Olavarrieta por su valiosa colaboración en el desarrollo de esta tesis.

Un agradecimiento especial al Ing. Javier Solano Trejo al brindarnos tiempo durante su trabajo, para la aplicación de la tesis, de antemano gracias.

M.C. Eduardo Pierdant Mucharraz, Microsoft México.- por el tiempo y material proporcionado para el desarrollo de algunos capítulos, gracias.

M.C. Marco A. Vigueras Villaseñor.- por la aportación de conocimiento y tiempo para el desarrollo de este trabajo.

Lic. Lizzette Beatriz Pérez Arbesú, editora de b:Secure y Netmedia.info.- Por la invitación a las conferencias de Netmedia Publishing así como del material proporcionado sobre seguridad de Mancera.

Ing. Javier Alejandro Carmona Pérez, por su confianza en nuestro trabajo y al Consejo de la Judicatura Federal por el apoyo en la evaluación de la auditoria.

Lucio Augusto Molina Focazzio, CISA Colombia.- por su valiosa plática en la conferencia de Netmedia.

Fernando González Bringas

Marcos García Franco

Ulises Escalona González

Agradecimientos:

Gracias Dios por todo lo que me haz dado.

Agradezco eternamente a mis padres por su inagotable apoyo, sus consejos y su incondicional amor, que fueron vitales para llegar hasta donde estoy. Los amo.

A mis hermanos y hermanas que siempre me alentaron a seguir adelante, por su compañía y cariño. Les deseo lo mejor en la vida.

A mi hermano Juan por sus valiosos consejos y por la confianza que siempre puso en mi.

También agradezco a mi abuela por su incansable cariño.

A toda mi familia que ha depositado su apoyo y su confianza en mi y que siempre me han alentado a seguir adelante.

Agradezco a mis amigos Fernando y Marcos por su amistad, los momentos que pasamos juntos y por compartir sus conocimientos para la realización de este trabajo.

A todos aquellos amigos que a lo largo de la carrera me brindaron su compañía, conocimientos y más importante su amistad.

Agradezco profundamente a la Máxima Casa de Estudios que me ha brindado todo, más de lo que esperaba.

Ulises Escalona González.

Agradecimiento:

Dedico este trabajo, que se demoró un poco, al apoyo de mi familia, especialmente a la confianza de mi papá.

Indudablemente al apoyo de mi novia, Mariana, que ha visto paso a paso el desarrollo de mi carrera y de esta tesis.

No podría olvidar por escrito el agradecimiento a mis compañeros de tesis, Ulises y Fernando, que han tenido la paciencia y hasta el buen humor de llevar a término este esfuerzo.

Marcos García Franco

Agradecimiento:

Doy gracias a Dios, por darme fuerzas para concluir esta etapa de mi vida, y darles esta satisfacción a mis viejos, siempre estás conmigo...

A mi padre y madre, nunca tendré palabras para agradecerles y lo que significan para mi, sólo quisiera decirles: "lo lograron, lo logramos…".

A mis hermanos Irma, Miguel Ángel y Susana por el apoyo, el cariño y la guía que me han dado, los tres, siempre serán mi orgullo…

A mis Primos por ser amigos, compañeros en mi vida, gracias…

A al memoria de mis Abuelitos: Piedad (†), Florencio, Luis (†), y en especial a mi Abuelita Lilia, siempre estarás en mis recuerdos (Gogli)…

A mis compañeros de tesis, Ulises y Marcos, por incluirme en este gran proyecto y la paciencia que me tuvieron, de antemano gracias…

A todos mis amigos del Colegio de Bachilleres No. 17.

A todos mis compañeros y profesores, ahora amigos de la Facultad de Ingeniería.

A todos mis compañeros de Luz y Fuerza del Centro, por el apoyo brindado para la culminación de mi carrera.

A Dr. Maria Edwvigies Guillen Valenzuela, Gracias por el apoyo más que mi doctora, llegué a considerar como una gran amiga, gracias por todo (lo logramos)…

A Dr. Víctor Felipe López Devesa, en el último peldaño, usted fue el hombro que me ayudo a conseguir esto, gracias de antemano…

A Profra. Carmen Elisa Reina Delgadillo (†) , nunca olvidaré la lección de vida ni sus palabras donde quiera que este gracias …

A todas las mujeres que en partes de mi vida han llegado a ser parte de mí…

A todos mis amigos y a la vida por darme tantos amigos, y poder decir que los dedos de mis manos no alcanzan para contarlos…

Y a todas aquellas personas que han confiado en mí, gracias

Fernando González Bringas

INDICE

PREFACIO

Los sistemas de información, implementados con correspondientes tecnologías de información, son el medio de manipular uno de los bienes más importantes de una organización: la información.

Ahora bien, esta información puede ser afectada accidental o intencionalmente al ser accedida sin tener la autorización, al ser destruida, alterada o modificada; al ser revelada a personas no autorizadas o al causar daños a los sistemas que las manipulan y soportan. Todo esto es enfatizado cuando los sistemas de información comprenden redes de comunicaciones, que en realidad es lo más común ahora para casi cualquier organización.

Esto tiene como consecuencia daños variados, desde la pérdida de horas de trabajo hasta el deterioro de la organización y pérdida de dinero considerable.

La seguridad informática permite hacer frente a estas vulnerabilidades y amenazas de los sistemas de información mediante acciones, normas y técnicas que permitan que éstos logren los principios de confidencialidad, integridad y disponibilidad.

La seguridad informática en una organización debe verse reflejada inmediatamente en la implementación de las políticas de seguridad, que asimismo sólo corresponden con una instantánea de la operatividad organizacional: la seguridad debe ser parte de las acciones y procedimientos del negocio o empresa.

Es esencial, no sólo para la vida de una empresa u organización que maneje redes de datos la realización de auditorías de seguridad, sino para mejorar su eficiencia. Sin embargo, pese a que existen múltiples empresas auditoras, las empresas u organizaciones no tienen la disponibilidad de una guía que les permita por si mismos realizar una auditoría interna y explotar y aplicar la gran cantidad y variedad de estándares y procedimientos internacionales referentes tanto a seguridad en redes de datos como a auditorías en sistemas de información.

En el presente documento realizamos una revisión de los estándares y guías más usados internacionalmente y de ellos tomamos los elementos más aplicables a la seguridad de redes para una LAN gubernamental. Con estos elementos desarrollamos una metodología que permita encontrar las vulnerabilidades y mejorar la eficacia y eficiencia de las redes de datos (fin de la auditoría), para que los administradores de una red tengan una herramienta o guía que les permita realizar el proceso.

En resumen, la finalidad es que mediante un sistema de gestión de auditoria de seguridad en redes de datos, detectar las posibles fallas y/o riesgos con la finalidad de corregirlos y mejorarlos. Asimismo, fomentar la existencia de una concientización hacia una cultura de seguridad.

C A P Í T U L O

I

INTRODUCCIÓN

CAPÍTULO I

INTRODUCCIÓN

1.1 Sistemas de información.

En la mayoría de las organizaciones o negocios, los planes, las metas, su desarrollo y todos aquellos obstáculos encontrados en la actividad gerencial de las empresas, constituyen información. Por lo tanto la información es la base de todas las actividades realizadas en una organización y deben realizarse sistemas para producirlas y administrarlas. Veamos los aspectos básicos de los sistemas.

1.1.1 Definición de un sistema.

Un sistema es una unidad que funciona en un ambiente dado y tiene muchas partes que trabajan juntas para lograr una meta común. Las partes mayores del sistema son llamados subsistemas y comparten algunas o todas las características del sistema. Además, las fronteras que separan los sistemas, subsistemas y sus entornos son lógicas, no físicas. El ambiente es el contexto en el que el sistema opera. [1]

Componentes de un sistema.

Casi todos los sistemas tienen cinco componentes principales, [2] como se observa en la figura 1.1:

- Entrada: máquinas, mano de obra, materia prima, dinero, tiempo. Las entradas para cada sistema deben ser cuidadosamente definidas. La entrada de un sistema de información son los datos.
- Procesos: políticas, procedimientos y operaciones que convierten datos en información.
- Salida: información en el formato correcto, llevada en el tiempo correcto a la persona correcta.
- Retroalimentación: datos sobre los resultados del sistema. Su existencia define si se trata de un sistema abierto o cerrado. Un sistema abierto es capaz de interactuar con su entorno y recibe retroalimentación. En cambio, un sistema cerrado es incapaz de recibirla.
- Control: procesa la retroalimentación y toma la acción necesaria, como la modificación de los procesos, la entrada o la salida.

---

1 Gupta, Uma G. *Information Systems. Success in the 21st Century.* New Jersey, Prentice Hall, 2000. p. 12.

2 *Ibíd.*, p. 13.

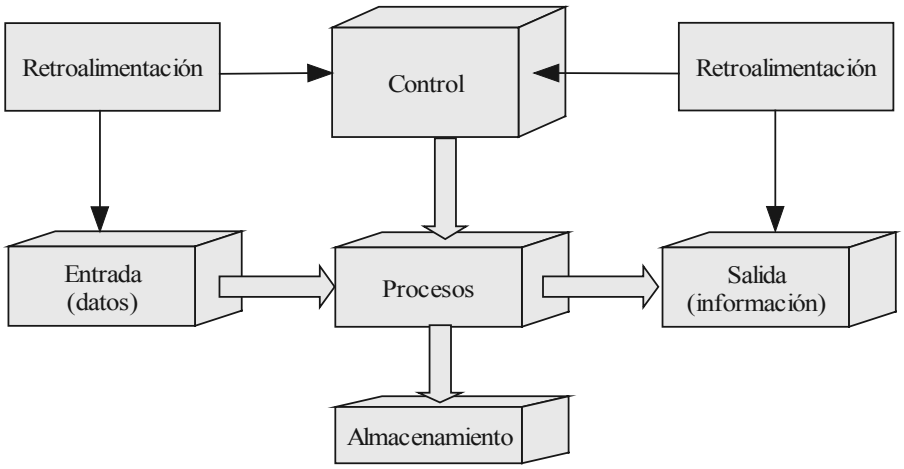


Figura 1.1 Los componentes de un sistema y su interacción

Los sistemas abiertos tienen las siguientes características: [3]

- Cada sistema tiene un propósito.
- Tienen los cinco componentes de entrada, procesamiento, salida, retroalimentación y control.
- Están construidos de subsistemas, cuyos objetivos son las submetas.
- Las metas de un sistema son más importantes que las submetas de los subsistemas.
- Los subsistemas están guiados por sus metas individuales y por su relación con otros subsistemas.
- Los subsistemas deben trabajar juntos en armonía para alcanzar los objetivos del sistema.

1.1.2 Los sistemas de información.

Definir los Sistemas de Información (SI) es una tarea complicada porque se componen de múltiples procesos que son, al mismo tiempo, actores en otros subsistemas de la organización y porque el sistema de información participa de toda actividad que se desarrolla en esa organización. Comencemos viendo la diferencia entre los datos y la información, base de los sistemas de información.

Datos.

Son flujos de hechos en bruto que representan sucesos ocurridos en las organizaciones o en el entorno físico, antes de ser organizados y acomodados de tal forma que las personas puedan entenderlos y usarlos. Pueden ser texto, números, gráficas, audio, video, imágenes o cualquier combinación de estos.

[3] *Ibíd.*, p. 14.

Los siete pasos por los que los datos se convierten en información son: 1) colección, 2) clasificación, 3) ordenación y fusión, 4) resumen, 5) almacenamiento, 6) recuperación y 7) diseminación. [4]

La información.

Son datos a los que se les ha dado una forma que tiene sentido, y es útil y significativa para la toma de decisiones. La información debe tener siete características para que sea útil para la toma de decisiones: [5]

- Valor subjetivo: el valor de la información difiere de individuo a individuo.
- Relevante: la información debe ser pertinente a la toma de decisiones.
- Oportuna: se debe recibir en el tiempo correcto.
- Precisa: libre de errores.
- Formato significativo: que pueda ser usada fácilmente.
- Integridad: la información necesaria.
- Accesibilidad: fácilmente disponible para los que la necesiten.

Sin embargo, debe haber un balance en cuanto a la accesibilidad de la información. Por un lado, no es útil cuando no es fácilmente accesible cuando es necesitada. Por otro, información con demasiada accesibilidad puede caer en manos equivocadas. Es más, demasiada información accesible puede crear sobrecarga de información.

Definición de los sistemas de información.

"El sistema de información puede ser definido como una colección de personas, procedimientos y equipos diseñados, construidos, operados y mantenidos para recoger, registrar, procesar, almacenar, recuperar y visualizar información". [6]

Un sistema de información se puede definir técnicamente como un conjunto de componentes interrelacionados que colaboran para reunir, procesar, almacenar y distribuir información para apoyar la toma de decisiones, la coordinación, el control, el análisis y la visualización en una organización. [7]

La información producida por el sistema debe tener diez características: [8]

- Accesibilidad: facilidad y rapidez con que se puede obtener la información resultante.
- Comprensibilidad: integridad del contenido de la información.
- Precisión: ningún error en la información obtenida.
- Propiedad: el contenido de la información debe ser apropiado.

---

4 *Ídem.*

5 *Ibíd.*, pp. 16-17.

6 Teichroew, D. *Information Systems. Encyclopedie of Computer science.* 1976.

7 Laudon C., Kenneth. *Sistemas de información gerencial.* México, Pearson Education, 2002. p. 7.

8 Ventura, Teodoro. *Sistema de información para el seguimiento de proyectos de agua*. Tesis Licenciatura. Universidad de las Américas-Puebla. 1999. p. 3.

- Oportunidad: la menor duración del ciclo de acceso.
- Claridad: información sin expresiones ambiguas.
- Flexibilidad: adaptabilidad de la información.
- Verificabilidad: posibilidad de que varios usuarios examinen la información y lleguen a la misma conclusión.
- Imparcialidad: no alterar la información para crear conclusiones preconcebidas.
- Cuantificabilidad: característica producida por un sistema formal de información.

1.1.3 Actividades de un sistema de información.

Un sistema de información contiene información acerca de una organización y su entorno. Cinco actividades de un sistema de información producen la información que las organizaciones necesitan y son: entrada, procesamiento, almacenamiento, salida y retroalimentación.

Entrada.
Es la captura o recolección de datos, del interior de la organización o de su entorno, para ser procesados.

Almacenamiento.
El almacenamiento es una de las actividades o capacidades más importantes que tiene una tecnología de información, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras dinámicas de información.

Procesamiento.
Es la conversión, la manipulación y el análisis de entradas brutas para darles una forma que tenga más sentido para los humanos.

Salida.
Es la distribución de la información procesada a las personas o actividades que la usarán.

Retroalimentación.
Son las salidas que se devuelven a los miembros apropiados de la organización para ayudarles a evaluar o corregir las entradas.

1.1.4 Componentes de un sistema de información.

Un sistema de información es una solución organizacional y administrativa, basada en tecnología de información, a un reto que se presenta en el entorno. Entendiendo cada elemento y cómo están interconectados nos ayuda a planear, desarrollar y usar los sistemas de información exitosamente (Figura 1.2).

Figura 1.2 Componentes de un sistema de información

Organizaciones.

Los sistemas de información forman parte de las organizaciones. Los elementos clave de una organización son su personal, la estructura, los procedimientos operativos, las políticas y la cultura. Una organización coordina el trabajo mediante una jerarquía estructurada y procedimientos operativos formales. La jerarquía acomoda al personal en una estructura de pirámide en la que la autoridad y la responsabilidad aumentan con la altura.

Los procedimientos operativos estándar son reglas formales que se han desarrollado para efectuar tareas; estas reglas guían al personal en la realización de diversos procedimientos esperados. Las organizaciones requieren muchos tipos distintos de habilidades y de personas. Además de los administradores, los trabajadores de conocimientos diseñan productos o servicios y crean conocimientos nuevos, los trabajadores de datos procesan el papeleo de la organización y los trabajadores de producción o servicio producen los bienes o servicios de la organización.

Administración.

Los administradores perciben retos en el entorno, establecen la estrategia de la organización para responder a ellos y asignan los recursos humanos y financieros para poner en práctica la estrategia y coordinar el trabajo. La tecnología de información puede desempeñar un rol crucial en la redirección y rediseño de una organización, labor también de los administradores.

Los administradores de nivel superior (directivos) toman decisiones estratégicas de largo plazo relacionadas con los bienes y servicios que se producirán. Los administradores de nivel medio (gerentes) se encargan de poner en práctica los programas y planes de los directivos. Los administradores operativos (supervisores) se encargan de monitorear las

actividades diarias de la compañía. Cada nivel administrativo tiene diferentes necesidades de información y requisitos en cuanto a sistemas de información.

Tecnología.

Es una herramienta que consta de los componentes siguientes: [9]

- El hardware es el equipo físico utilizado en un sistema de información para las actividades de entrada, procesamiento y salida.
- El software son las instrucciones preprogramadas que controlan y coordinan los componentes del hardware de la computadora en un sistema de información.
- La tecnología de almacenamiento incluye los medios físicos para almacenar datos y el software que rige la organización de los datos en esos medios físicos.
- La tecnología de comunicaciones, que consiste en dispositivos físicos y software, enlaza los diversos componentes del hardware y transfiere datos de un lugar físico a otro.

La arquitectura de información es la forma específica que la tecnología de información (TI) adopta en una organización para lograr metas o realizar funciones selectas. Es un diseño que sirve a cada especialidad funcional y nivel de la organización, y la forma específica en que cada organización los usa. La plataforma tecnológica para esta arquitectura se denomina infraestructura de tecnología de información y consiste en el hardware, software, tecnología de datos y almacenamiento, redes y recursos humanos necesarios para operar el equipo (ver Fig. 1.3).

Los sistemas de información pueden verse también como un gran rompecabezas: [10] un número de piezas deben ir juntas de una manera significativa en el sistema para ser efectivas. Las principales piezas de este rompecabezas incluyen hardware, software, datos, telecomunicaciones, procesos y reglas, gente y factores del medio ambiente (véase Figura 1.4).

[9] Laudon C., Kenneth. *Op. cit.* p. 12.
[10] Gupta, Uma G. *Op. cit.* p. 10.

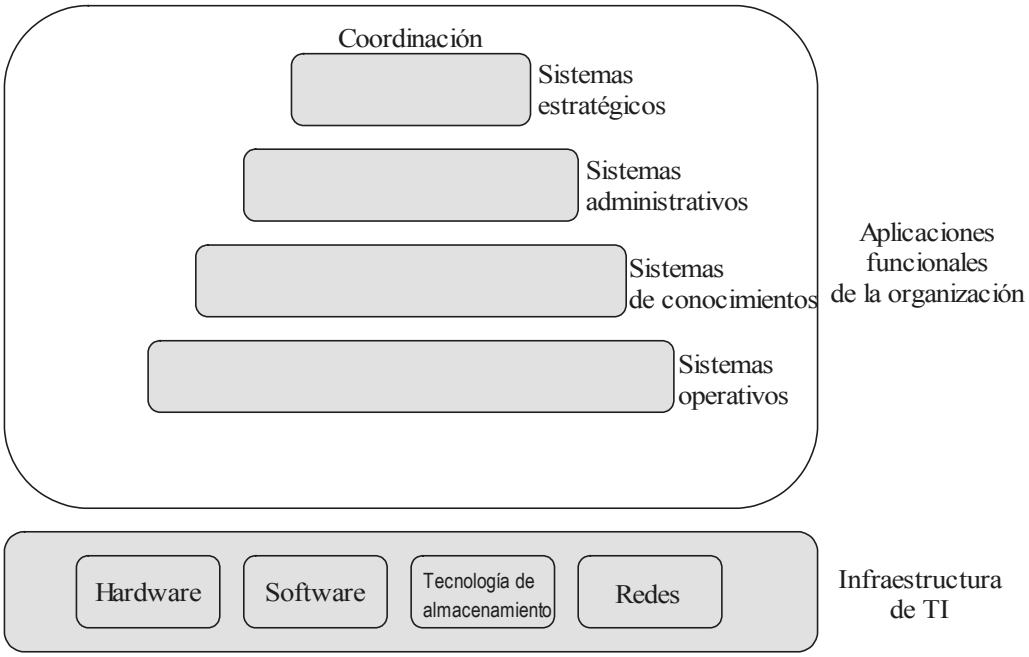


Figura 1.3 Arquitectura de la información

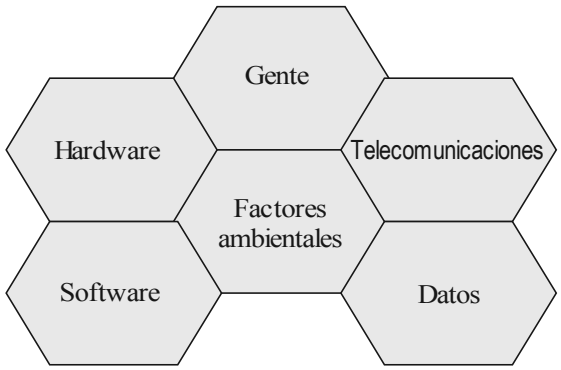


Figura 1.4 Los sistemas de información

Las computadoras y otras tecnologías de información son herramientas usadas para construir sistemas de información. La tecnología de información incluye hardware, software, bases de datos, redes y otros componentes relacionados. Los sistemas de información usan e integran tecnologías para reunir las necesidades de información de diferentes usuarios. La tecnología por sí misma no hace nada por los usuarios. Sólo cuando es aplicada de manera significativa puede ser usada efectivamente.

1.1.5 Clases y tipos de sistemas de información.

Clases de sistemas de información.

Existen cuatro tipos de sistemas de información que sirven a los diferentes niveles de una organización: [11]

- Sistemas en el nivel operativo,
- Sistemas en el nivel de conocimientos,
- Sistemas en el nivel de administración y
- Sistemas en el nivel estratégico.

SISTEMAS EN EL NIVEL OPERATIVO.

Los sistemas en este nivel apoyan a los administradores operativos siguiendo la pista a las actividades y transacciones elementales de la organización, como ventas, recibos, depósitos de efectivo, nómina, decisiones de crédito, flujo de materiales en una fábrica, etc. El propósito principal de los sistemas en el nivel operativo es responder a preguntas de rutina y rastrear el flujo de transacciones a través de la organización.

SISTEMAS EN EL NIVEL DE CONOCIMIENTOS.

Los sistemas en el nivel de conocimientos apoyan a los trabajadores de conocimientos y datos de una organización. El propósito de los sistemas en este nivel es ayudar a la empresa a descubrir, organizar e integrar conocimientos nuevos al negocio y ayudar a la organización a controlar el flujo de documentos. Esta clase de sistemas son las aplicaciones que crecen más rápidamente en los negocios hoy día, sobre todo en forma de herramientas de colaboración, estaciones de trabajo y sistemas de oficina.

SISTEMAS EN EL NIVEL DE ADMINISTRACIÓN.

Los sistemas en este nivel están diseñados para servir a las actividades de seguimiento, control, toma de decisiones y administración de los administradores de nivel medio. La pregunta principal que tratan de contestar estos sistemas es: ¿están funcionando bien las cosas? Por lo regular proporcionan informes periódicos, en lugar de información instantánea acerca de las operaciones.

SISTEMAS EN EL NIVEL ESTRATÉGICO.

Los sistemas en el nivel estratégico ayudan a los administradores de nivel superior a abordar o resolver cuestiones estratégicas y tendencias a largo plazo, tanto en la compañía como en su entorno. Su preocupación principal es la congruencia entre los cambios del entorno y las capacidades actuales de la organización.

[11] Laudon C., Kenneth. *Op. cit*. p. 38.

Tipos de sistemas de información.

Los tipos específicos de sistemas de información que corresponden a cada nivel de la organización son seis:

- ESS (*Executive Support Systems*). Sistemas de apoyo a ejecutivos, en el nivel Estratégico.
- MIS (*Management Information Systems*). Sistemas de información gerencial, en el nivel de Administración.
- DSS (*Decision-Support Systems*). Sistemas de apoyo a decisiones, también en el nivel de Administración.
- KWS (*Knowledge Work Systems*). Sistemas de trabajo de conocimientos, en el nivel de Conocimientos.
- OAS (*Office Automation Systems*). Sistemas de automatización de oficinas, también en el nivel de Conocimientos.
- TPS (*Transaction Processing Systems*). Sistemas de procesamiento de transacciones, en el nivel Operativo.

1.1.6 Relación entre sistema de información y tecnología de información.

Los sistemas de información son sistemas sociotécnicos, aunque se componen de tecnología requieren de sustanciales inversiones sociales, de organización e intelectuales, para funcionar debidamente. En esta perspectiva, el desempeño de un sistema se optimiza cuando la tecnología y la organización se ajustan recíprocamente. A veces, podría ser necesario "desoptimizar" la tecnología para lograr tal congruencia. Las personas y las organizaciones cambian para aprovechar la nueva tecnología de información. Con esto se evita un enfoque puramente tecnológico de ellos (Figura 1.5).

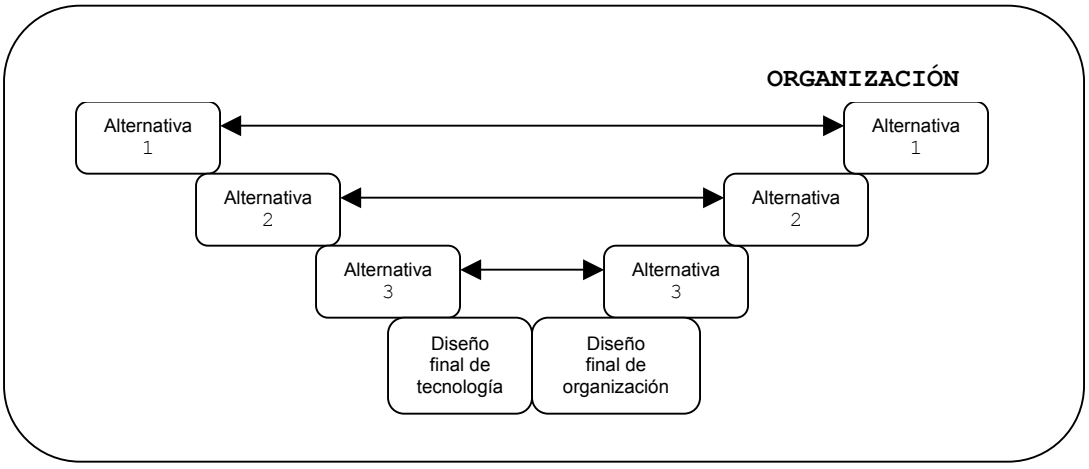


Figura 1.5 Relación sociotécnica de los SI

En cuanto a la relación entre las organizaciones y los sistemas de información, existe una interdependencia creciente de la estrategia, las reglas y los procedimientos de negocios, por un lado, y el software, el hardware, las bases de datos y las telecomunicaciones de los sistemas de información, por el otro. Un cambio en cualquiera de estos componentes a

menudo requiere cambios en otros. Esta relación se vuelve crítica cuando la administración planifica para el futuro (Figura 1.6).

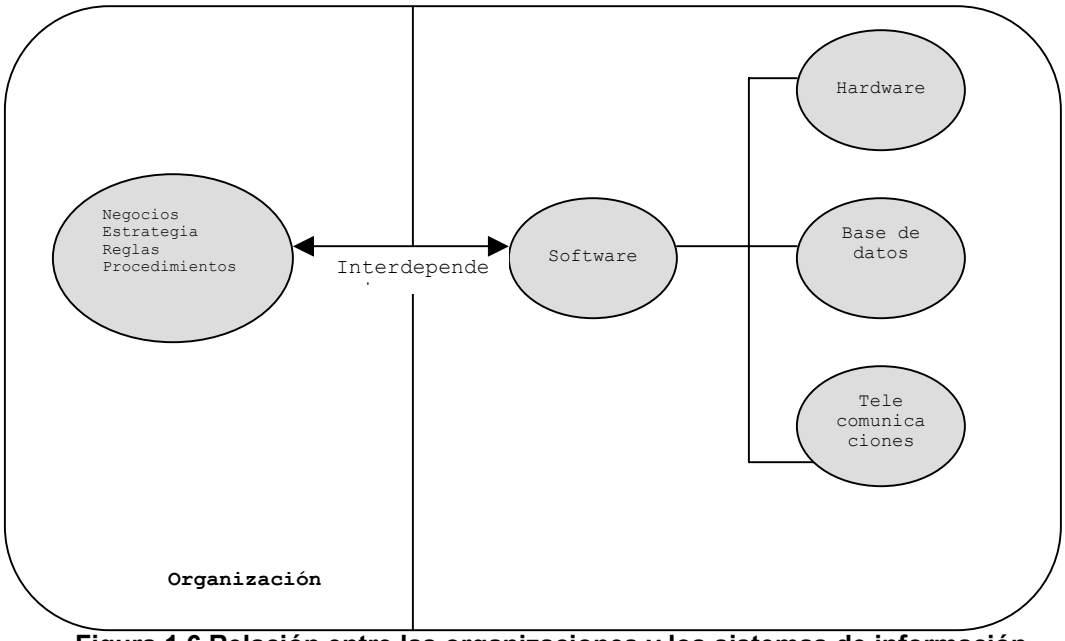


Figura 1.6 Relación entre las organizaciones y los sistemas de información

Un segundo aspecto es resultado de la complejidad creciente y el alcance de los proyectos y aplicaciones de los sistemas. Con el tiempo los sistemas de información han comenzado a desempeñar un rol más importante en la vida de las organizaciones. Los primeros sistemas implicaban cambios principalmente técnicos que eran relativamente fáciles de lograr. Los sistemas posteriores afectaron el control y el comportamiento gerencial. Actualmente, los sistemas influyen en las actividades centrales de la organización (ver figura 1.7).

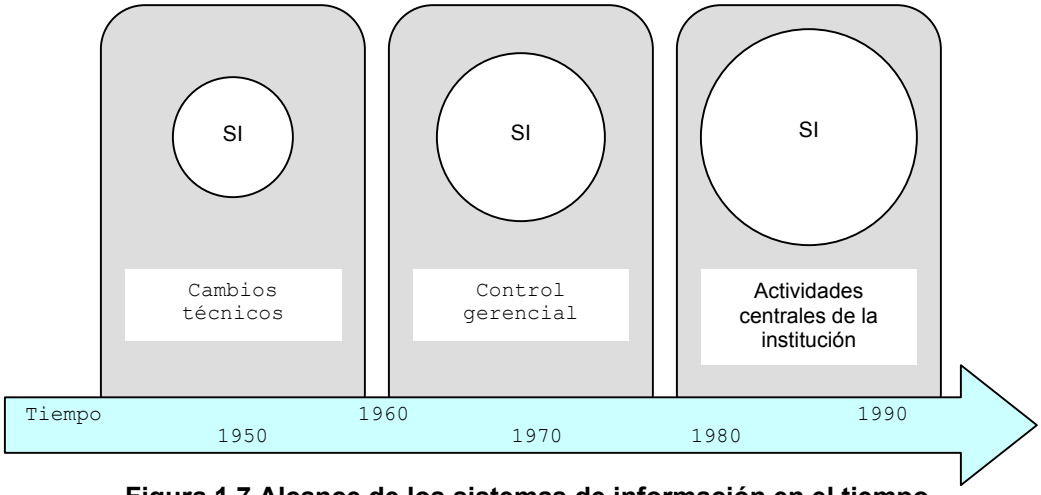


Figura 1.7 Alcance de los sistemas de información en el tiempo

1.2 La seguridad informática.

1.2.1 Definición de seguridad informática.

La seguridad informática la podemos definir como el conjunto de normas, acciones, conocimientos y técnicas que permiten a los sistemas de información cumplir con las características de disponibilidad, confiabilidad, integridad y privacidad, evitando así las posibles vulnerabilidades que provoquen robo, alteraciones o accesos no permitidos a los sistemas de información. (12)

En un entorno de redes electrónicas, hay recursos y servicios de red, así como información valiosa. Alguna persona puede accidental o intencionalmente afectarlas en:

- Acceder sin autorización a los recursos de red.
- Destruir información y recursos de red.
- Alterar o insertar información.
- Revelar información a gente no autorizada.
- Ocasionar perturbaciones o interrupciones en los servicios de red.

Algunas personas pueden afectar intencionalmente en:

- Robar información y recursos de red.
- Negar servicios recibidos e información enviada o recibida.
- Afirmar tener derechos de dar servicios que actualmente no está proporcionando y/o afirmar el enviar o recibir información que actualmente no ha sido enviada o recibida.

Estas actividades son violaciones de seguridad en el entorno de red y son llamadas *amenazas de seguridad*. Si estas amenazas son intencionales, ellas son llamadas *ataques de seguridad*. Los motivos de ataques de seguridad pueden ser tanto comerciales, espionaje político, ventaja financiera, venganza o publicidad.

1.2.2 Servicios de seguridad informática.

“Existen 3 principios clave en esta materia, los cuales pueden ser aplicados no sólo al negocio, sino desde un documento, una computadora, unas oficinas, un negocio e incluso a la persona. Estos principios son la confidencialidad, la integridad y la disponibilidad”. (13)

12 Russell y Gangemi. *Computer Security Basics.* USA, O’Reilly & Associates, 1999. p. 24.

13 Velázquez, Andrés. *Seguridad Informática: Más que una Moda.* DoDoMex - Internet Security Portal. 2005. http://www.dodomex.com/noticias2.php?id=44

Confidencialidad.

"Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados". (14)
En áreas de seguridad gubernamentales los privilegios aseguran que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad, normalmente impuestas por disposiciones legales o administrativas. Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquéllos relacionados con la defensa. En estos entornos los otros dos aspectos de la seguridad son menos críticos. Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

Integridad.

Se entiende por integridad el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad: precisión y autenticidad. El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga.

Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho el problema de la integridad no sólo se refiere a modificaciones *intencionadas*, sino también a *cambios accidentales* o no intencionados.

En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la *autenticidad*. Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos.

Disponibilidad.

Se entiende por disponibilidad:

- El grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.
- La situación que se produce cuando se puede acceder a un SI en un periodo de tiempo considerado aceptable.

Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen

[14] Heineken, Team. *Introducción a la problemática de la Seguridad Informática.* 2001. http://www.softdownload.com.ar

funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo. Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio" (*denial of service*). Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados.

Otros aspectos relacionados.

Existen otros aspectos o características de la seguridad que pueden en su mayor parte incluirse o asimilarse a uno de los tres aspectos fundamentales, pero que es importante concretar. [15]

Autenticidad: esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envíe una información haciéndose pasar por otro.

Imposibilidad de rechazo (no-repudio): esta propiedad permite asegurar que cualquier entidad que envía o recibe información no puede alegar ante terceros que no la envió o la recibió.

Consistencia: asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados. Si el software o el hardware de repente comienzan a comportarse de un modo radicalmente diferente al esperado, puede ser un desastre. Esta propiedad es amenazada, por ejemplo, por el uso de los Caballos de Troya, programas que no hacen lo que se supone que deben hacer, o que además se dedican a otras tareas.

Aislamiento: regula el acceso al sistema, impidiendo que personas no autorizadas entren en él. Este aspecto está relacionado directamente con la confidencialidad, aunque se centra más en el acceso al sistema que a la información que contiene.

Auditoría: capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, y quién y cuándo las han llevado a cabo. La única forma de lograr este objetivo es mantener un registro de las actividades del sistema, y que este registro esté altamente protegido contra modificación.

1.2.3 Política de seguridad.

La política de seguridad es una declaración de intenciones que cubre la seguridad de los SI y proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizacionales que se requerirán.

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.

[15] Pfleeger. *Security in Computing.* USA, Prentice Hall, 2000. p. 85.

Son los directivos, junto con los expertos en tecnologías de la información, quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, con lo que los procesos más importantes recibirán más protección. La seguridad debe considerarse como parte de la operativa habitual, no como un algo extraño o añadido.

La seguridad es una estrategia de negocio en la que la alta dirección debe estar plenamente involucrada, pues es ahí donde se encuentran los responsables del funcionamiento de la compañía. Dicha área es la que genera las políticas de seguridad informática, que no deben entenderse sólo como aspectos técnicos, legales o que involucran sanciones ante ciertas conductas. Si bien pueden incluirse castigos administrativos a quien no cumpla con dichas políticas, este documento es una descripción de los activos que la compañía debe proteger y que se comunica a los empleados (internos y externos) de una empresa.

Cada política de seguridad informática es una invitación que la empresa hace a sus miembros para reconocer la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Dicha invitación debe concluir en una posición consciente y alerta por parte del personal, por el uso y limitaciones de los recursos y servicios informáticos críticos de la empresa.

El compromiso de la Dirección con los SI debe tomar la forma de una política de seguridad de los SI formalmente acordada y documentada. Dicha política tiene que ser consistente con las prácticas de seguridad de otros departamentos, puesto que muchas amenazas (incendio, inundación) son comunes a otras actividades de la organización.

A la hora de establecer una política de seguridad debemos responder a las siguientes tres preguntas:

- ¿Qué necesitamos proteger?
- ¿De qué necesitamos protegerlo?
- ¿Cómo vamos a protegerlo?

Esto nos lleva a los siguientes pasos básicos:

1. Determinar los recursos a proteger y su valor.
2. Analizar las vulnerabilidades y amenazas de nuestro sistema, su probabilidad y costo.
3. Definir las medidas a establecer para proteger el sistema. Estas medidas deben ser proporcionales a lo definido en los pasos 1 y 2. Las medidas deben establecerse a todos los niveles: físico, lógico, humano y logístico. Además, debe definirse una estrategia a seguir en caso de fallo.
4. Monitorizar el cumplimiento de la política y revisarla y mejorarla cada vez que se detecte un problema. Los pasos 1 y 2 se denominan Análisis de riesgos, mientras los pasos 3 y 4 se denominan Gestión de riesgos. La política de seguridad es el conjunto de medidas establecidas en el paso 3.

Al configurar una red, ya sea una red de área local (LAN) o una LAN virtual (VLAN), es importante establecer desde el principio las políticas de seguridad. “Las políticas de seguridad son reglas electrónicamente programadas y almacenadas en equipos de seguridad para controlar áreas tales como los privilegios de acceso. Obviamente, las políticas de seguridad también consisten en reglamentaciones escritas o verbales que delimitan el funcionamiento de una organización.” [16]

Algunos elementos que deben contener son: [17]

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre los cuales aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cubren el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que cada uno tiene acceso.
- Explicar las razones de la toma de decisiones; es decir, por qué el cuidado de los servicios o recursos de información es prioritario.

Las políticas de seguridad deben mantener un lenguaje común, libre de tecnicismos y términos legales que impidan la comprensión clara del escrito, aunque no hay que sacrificar su precisión y formalidad dentro de la empresa. Asimismo, es preciso indicar quién será la autoridad responsable y el rango de correctivos y sanciones que se impondrán. No debe especificar con exactitud lo que pasará cuando alguna violación a la información sea detectada, pues no es una sentencia legal, pero siempre es bueno dar una idea de las consecuencias que podría traer no acatar las políticas.

Finalmente, las políticas de seguridad son documentos dinámicos dentro de la organización, por lo que deben seguir un proceso de actualización periódica sujeta a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura, rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc. Una parte importante en la implementación de políticas es el manejo de incidentes, que consiste en determinar qué tipo de eventos podrían estar afectando la infraestructura tecnológica para aprender a detectarlos de manera proactiva y, una vez que se identifican, saber cómo reaccionar ante tal contingencia. La idea es estar siempre preparados para responder cuando se presente un incidente y no afectar la continuidad de la operación. La información del negocio siempre debe estar disponible y ser confidencial e íntegra.

---

[16] Cisco Systems. *Op. cit*. p. 6.

[17] Olguín Romo, Heriberto. *Dirección, organización y administración de centros de tecnología de información.* México, UNAM, Facultad de Ingeniería, 2005. p. 134.

1.2.4 Vulnerabilidad.

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático. Algunos tipos de vulnerabilidad de un sistema son los siguientes:

Vulnerabilidad física: se encuentra en el nivel del edificio o entorno físico del sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruir el mismo.

Vulnerabilidad natural: se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales que pueden dañarlo, tales como el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallos eléctricos o picos de potencia. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

Vulnerabilidad del hardware y del software: desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, ciertos sistemas requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los mismos.

Vulnerabilidad de los medios o dispositivos: se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc.

Vulnerabilidad por emanación: todos los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen dispositivos y formas de interceptar estas emanaciones y descifrar o reconstruir la información almacenada o transmitida.

Vulnerabilidad de las comunicaciones: la conexión de las redes supone sin duda un enorme incremento de la vulnerabilidad del sistema. Aumenta enormemente la escala del riesgo a que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intentar tenerlo. También se añade el riesgo de intercepción de las comunicaciones:

- Se puede penetrar al sistema a través de la red, o
- Interceptar información que es transmitida desde o hacia el sistema.

Vulnerabilidad humana: la gente que administra y utiliza el sistema representa la mayor vulnerabilidad del sistema. Los usuarios del sistema suponen un gran riesgo al mismo. Ellos son los que pueden acceder al mismo, tanto físicamente como mediante conexión. Existen estudios que demuestran que más del 50% de los problemas de seguridad detectados son debidos a los usuarios de los sistemas.

1.2.5 Amenazas.

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas; depende del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios. [18]

Representan las debilidades o aspectos falibles o atacables en el sistema informático. Puede ser una persona (cracker), un programa (virus, caballo de Troya), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

Tipos de amenazas.

Según el efecto causado en el sistema. En una primera clasificación, las amenazas pueden englobarse en cuatro grandes tipos: intercepción, modificación, interrupción y generación.

Intercepción: cuando una persona, programa o proceso logra el acceso a una parte del sistema a la que no está autorizada. Son los más difíciles de detectar pues en la mayoría de los casos no alteran la información o el sistema.

Modificación: se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino, además, de cambiar en todo o en parte su contenido o modo de funcionamiento.

Interrupción: interrumpir mediante algún método el funcionamiento del sistema. Puede ser intencionada o accidental.

Generación: se refiere a la posibilidad de añadir información o programas no autorizados en el sistema.

[18] Álvarez Marañón, Gonzalo. *Amenazas deliberadas a la seguridad de la información.* CSIC. 1997-2000. http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html

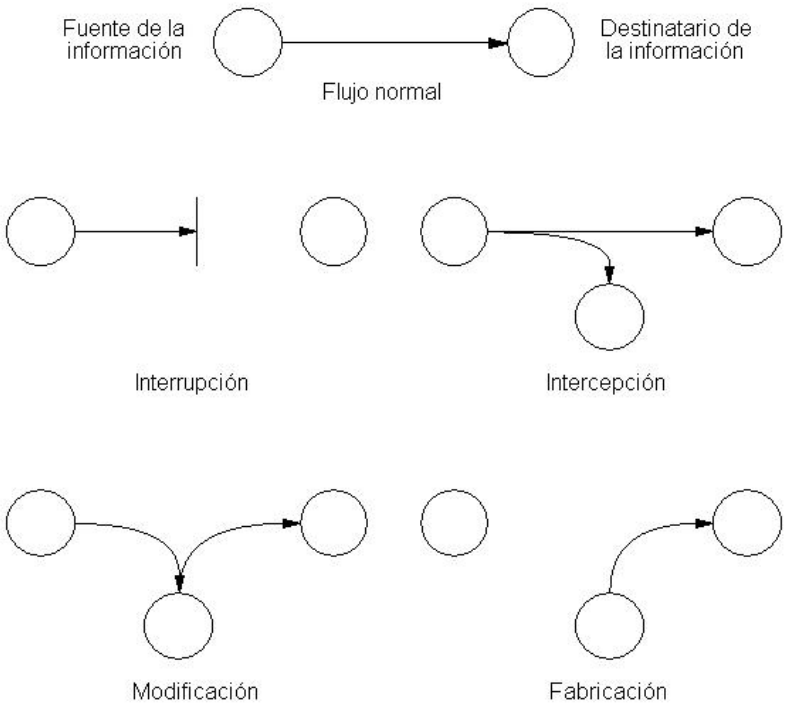


Figura 1.8 Amenazas a la seguridad de la información

Por el origen de las amenazas. Desde el punto de vista del origen de las amenazas, estas pueden clasificarse en: naturales, involuntarias e intencionadas.

Amenazas naturales o físicas: son las que ponen en peligro los componentes físicos del sistema. En ellas podemos distinguir por un lado los desastres naturales y las condiciones medioambientales.

Amenazas involuntarias: son aquellas relacionadas con el uso descuidado del equipo por falta de entrenamiento o de concienciación sobre la seguridad.

Amenazas intencionadas: son aquellas procedentes de personas que pretenden acceder al sistema para borrar, modificar o robar la información; para bloquearlo o por simple diversión.

Estos ataques se pueden clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques pasivos: En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

Ataques activos: Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo.
- **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- **Modificación de mensajes**: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, web, FTP, etc.

A continuación mencionaremos los ataques y amenazas más comunes en las redes de datos, que son casos específicos de los ya mencionados:

Eavesdropping y packet sniffing.

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

Este método es muy utilizado para capturar login IDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes.

Snooping y downloading.

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

Tampering o data diddling.

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende, alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada.

Spoofing.

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snooping o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro y en otro. Este proceso, llamado looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante.

Jamming o flooding.

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Caballos de Troya.

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (p.e. formatear el disco duro, modificar un archivo, etc.).

Bombas lógicas.

Consiste en introducir un programa o rutina que, en una fecha determinada, destruirá, modificará la información o provocará la caída del sistema.

Virus.

Si bien es un ataque de tipo tampering, difiere de éste porque puede ser ingresado al sistema por un dispositivo externo o través de la red sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse a través de una LAN rápidamente, si es que no está instalada una protección antivirus en los servidores, estaciones de trabajo y los servidores de e-mail.

1.2.6 Ataques a WLAN.

Una red de área local inalámbrica (Wireless LAN) es un sistema de comunicación de datos flexible, implementado como una extensión alternativa para la red de área local alambrada. Las LAN inalámbricas transmiten y reciben datos a través del aire usando la tecnología de la radiofrecuencia, así minimizan las conexiones cableadas. Pero una de las más preocupantes revelaciones es que las WLAN son inseguras y el envío de datos a través de ellas puede ser fácilmente roto y comprometedor. Las cuestiones de seguridad en las redes inalámbricas es mucho más crítica que en las redes cableadas.

Los principales ataques a redes de computadoras inalámbricas son:

- *Interrupción de servicio*. Aquí, los recursos del sistema son destruidos o llegan a ser no disponibles.
- *Modificación*. Éste es un ataque a la integridad del sistema. En este caso, el atacante no solamente obtiene el acceso a la red, sino que también altera datos, como cambiar los valores en una base de datos.
- *Fabricación*. Éste es un ataque sobre la autenticidad de la red. Aquí el atacante inserta objetos falsos, como insertar o grabar en un archivo.
- *Intercepción*. Éste es un ataque sobre la confidencialidad de la red como la intervención electrónica o “escuchar a escondidas” para capturar datos en una red.
- *Ataques cliente-a-cliente*. Los usuarios de redes inalámbricas necesitan defender a clientes no sólo de amenazas externas, sino también de otros usuarios. Los clientes inalámbricos que corren protocolos TCP/IP son vulnerables por la misma mala configuración de las redes inalámbricas. También la duplicación de direcciones IP o MAC, sea esto intencional o accidental, puede causar interrupción de servicio.
- *Ataques contra encriptación*. El estándar IEEE 802.11b usa un esquema de encriptación llamado Wired Equivalent Privacy (WEP) el cual ha resultado tener algunas debilidades, como se verá más adelante. Atacantes sofisticados pueden romper dicho esquema.
- *Ataques de fuerza bruta contra passwords de Access Point*. La mayoría de los AP usan un password o clave sencilla, la cual es repartida por todos los clientes conectados. Los atacantes pueden intentar romper estas claves o passwords intentando todas las posibilidades. Una vez que el atacante adivina la clave, puede obtener acceso al access point y comprometer la seguridad del sistema.
- *Ataques de inserción*. Este tipo de ataque está basado en una expansión a una nueva red inalámbrica sin seguir los procedimientos de seguridad. También, esto puede ser debido a la instalación de un dispositivo no autorizado sin la revisión apropiada de la seguridad.

Otros tipos de ataques más específicos a redes WLAN pueden ser:

- *Romper ACL's (Access Control List) basados en MAC.*
  Una de las medidas más comunes que se utilizan para asegurar una red wireless es restringir las máquinas que podrán comunicarse con el AP haciendo filtrado por dirección MAC en éste. Para esto se suele crear una tabla en el punto de acceso que contiene todas las MAC's de los clientes que están autorizados para conectarse. Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente envía y hacernos pasar por uno de los equipos que sí tienen acceso a la red. Para llevar a cabo el ataque basta con esnifear durante un momento el tráfico y fijarnos en la MAC de cualquier cliente; sólo hace falta que nos pongamos su misma MAC y ya habremos saltado la restricción.

- *Ataque de Denegación de Servicio (DoS).*
  Para realizar este ataque basta con esnifear durante un momento la red y ver cuál es la dirección MAC del AP. Una vez conocida su MAC, nos la ponemos y actuamos como si fuéramos nosotros mismos el AP. Lo único que tenemos que hacer para denegarle el servicio a un cliente es mandarle continuamente notificaciones (*management frames*) de disociación o desautenticación.

- *Ataque Man in the middle.*
  El ataque de *Man in the middle*, consiste en convencer al cliente (la víctima) de que el host que hay en el medio (el atacante) es el AP, y hacer lo contrario con el AP, es decir, hacerle creer al AP que el atacante es el cliente.

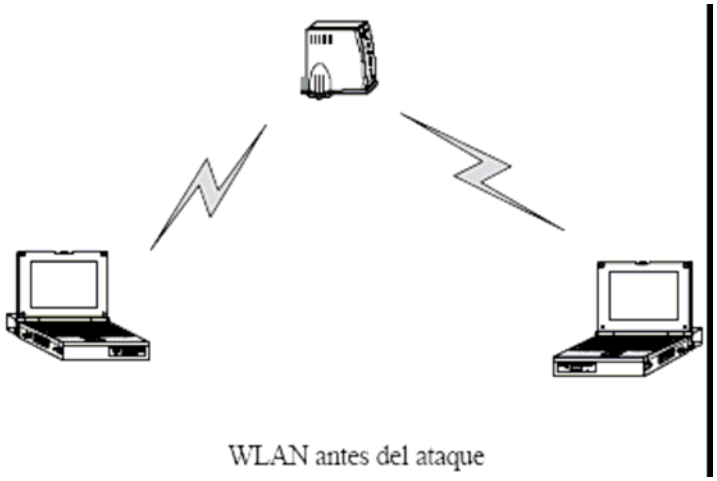


Figura 1.9

El atacante hace creer a la víctima que él es el AP real (Figura 1.10), utilizando la misma MAC y el mismo ESSID (Extended Service Set Identifier, identificador de cada WLAN) del AP al que la víctima estaba autenticada anteriormente, pero operando por un canal distinto. Por otra parte, el atacante se asocia con el AP real, utilizando la dirección MAC de la víctima.

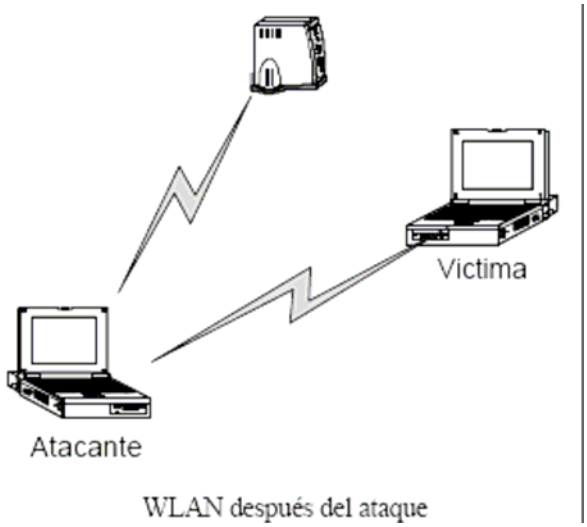


Figura 1.10

De esta manera todos los datos que viajan entre la víctima y el AP pasan a través del atacante.

- *Ataque ARP (Address Resolution Protocol) Poisoning.*
  El *ARP cache poisoning* es un ataque que sólo se puede llevar a cabo cuando el atacante está conectado a la misma LAN lógica que las víctimas, limitando su efectividad a redes conectadas con switches, hubs y bridges, pero no routers. La mayoría de los Puntos de Acceso 802.11b actúan como bridges transparentes de capa 2, lo que permite que los paquetes ARP pasen de la red wireless hacia la LAN donde está conectado el AP y viceversa. Esto permite que se ejecuten ataques de *ARP cache poisoning* contra sistemas que están situados detrás del Punto de Acceso, como por ejemplo servidores conectados a un switch en una LAN a los que se pueda acceder a través de la WLAN.

Ataques al WEP.

El nombre, *wired equivalent privacy* (WEP), o privacidad equivalente a red cableada, implica que su objetivo es proporcionar el nivel de privacidad que es equivalente para la LAN alambrada. Éste fue diseñado para proporcionar confidencialidad al tráfico de red usando protocolos inalámbricos. El algoritmo WEP es usado para proteger redes inalámbricas de “escucha a escondidas”. Está también pensado para prevenir accesos no autorizados a la red. El esquema depende de una clave secreta que es dividida entre un nodo inalámbrico y un access point. Esta clave es usada para encriptar paquetes de datos antes de ser enviados.

El protocolo WEP es débil contra los siguientes ataques:

- *Ataques activos que inyectan tráfico nuevo de estaciones móviles no autorizadas.*
  La inyección de tráfico es debido a la situación donde un atacante conoce el texto simple (plaintext) de un mensaje encriptado. Usando este conocimiento, el atacante

puede construir correctamente paquetes encriptados. Esto involucra la construcción de un nuevo mensaje, calculando el CRC-32 y realizando una inversión de bits sobre el mensaje original encriptado. Este paquete puede ahora ser enviado al access point o al nodo móvil y aceptarlo como un paquete válido.

- *Ataques activos para desencriptar tráfico basado en burlar el access point.*
  Aquí el atacante hace una adivinación del encabezado (header) del paquete, no del contenido de éste. Básicamente, todo esto es necesario para adivinar el destino de la dirección IP. El atacante puede entonces invertir bits específicos para transformar el destino de la dirección IP para transmitir el paquete a un nodo que está bajo su control, y para transmitirlo usando una estación móvil. Esto permitirá que el paquete sea adelantado a través de más firewalls.

- *Ataque de diccionario, el cual permite en tiempo real automatizar la desencriptación de tráfico después de algún análisis.*
  El atacante puede desencriptar todos los paquetes enviados sobre esa conexión inalámbrica.

1.2.7 Mecanismos de seguridad.

El principio de seguridad informática es proteger un entorno contra amenazas a través de varios servicios, mecanismos y técnicas de seguridad, e imponerlas a través de las políticas de seguridad. No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes: [19]

Identificación y autenticación.

Para ser capaz de entrar en un entorno de red, una entidad debe primero identificarse con el sistema. Esto se llama identificación. Ya sea ésta un cliente o un servidor, debe ser identificado. Usar IDs o servidores IDs son ejemplos de identificación. Lo que la identificación necesita en un sistema de red es que cada entidad debe tener un ID único. Una persona podría tener múltiples cuentas en un sistema; sin embargo, cada cuenta debe tener un ID único y cada cuenta debe ser una entidad registrada en el sistema. La *autenticación* es usada, por otro lado, para dar una prueba al sistema de que tú eres verdaderamente quien afirmas ser. El sistema verifica la información que se proporciona contra la que el sistema conoce. La identificación y la autenticación (I&A) es el punto inicial de la seguridad informática y la seguridad en redes sería efectiva sólo si la I&A es propiamente implementada.

Control de acceso.

El control de acceso responde a la siguiente pregunta: *¿Quién puede acceder, a cuál recurso y a realizar qué operaciones?* El propósito del control de acceso es limitar las

[19] Álvarez Marañón, Gonzalo. *Mecanismos de seguridad.* CSIC. 1997-2000.
http://www.iec.csic.es/criptonomicon/seguridad/mecanism.html

acciones u operaciones que un usuario o un grupo de usuarios legítimos pueden realizar en un entorno de red. El control de acceso es impuesto después de que un usuario es identificado y autentificado exitosamente.

Los componentes básicos de un mecanismo de control de acceso son los derechos o permisos que se tienen, las entidades y los recursos de red. Los derechos de acceso describen privilegios o permisos, bajo qué condiciones y cómo pueden acceder esas entidades a los recursos de red. Algunos ejemplos de esos privilegios o permisos son:

- Creación o destrucción.
- Leer, observar o escribir.
- Añadir, borrar o modificar contenido.
- Exportar o importar.
- Ejecutar.

Las entidades de red, los recursos y la información pueden ser clasificados asignándoles diferentes niveles de seguridad. El control de acceso, en particular a los recursos de red y a la información, puede ser impuesto a través de la administración de red o por una entidad individual, dependiendo de las políticas de control de acceso.

Confidencialidad.

Los servicios de confidencialidad dan protección a los recursos de red y a la información, ambos en términos de almacenamiento y transmisión, para garantizar que:

- Nadie pueda intentar leer, copiar, revelar o modificar información ni recursos de red sin autorización, y
- Nadie pueda interceptar comunicaciones o mensajes entre otras entidades de red.

Estos dos aspectos de confidencialidad son algunas veces llamados *confidencialidad de contenido* y *confidencialidad de flujo de mensaje*. La *criptografía* es usada para dar servicios de confidencialidad.

Integridad de datos.

La *integridad de datos* proporciona controles que garantizan que el contenido del dato no ha sido modificado y que la secuencia del mensaje ha sido preservada durante la transmisión. Usuarios no autorizados pueden ser o no capaces de leer un dato, pero esta protección debe prevenir que usuarios no autorizados agreguen, borren o modifiquen cualquier parte del dato. La integridad de datos es un aspecto muy importante de la seguridad en redes, sin ella una persona puede manipular los datos a su propia conveniencia.

En un entorno de red hay dos servicios de integridad de datos: *servicios de integridad de contenido* y *servicios de integridad de secuencia de mensaje*. El *servicio de integridad de contenido* proporciona una prueba de que el contenido de un recurso de red no ha sido modificado o alterado por inserción o eliminación. La *integridad de secuencia de mensaje*

proporciona una prueba del ordenamiento de una secuencia de mensajes que han sido protegidos y que son transmitidos en una red. Los servicios de integridad de datos, proporcionados a través de varios mecanismos de seguridad, son:

- *Código de detección de modificación* (Modification Detection Code).
- *Código de autenticación de mensaje* (Message Authentication Code).
- *Firma digital*.
- *Número de secuencia de mensaje.*

El código de detección de modificación (MDC) es un checksum, de un dato generado, usando un algoritmo criptográfico. El código de autenticación de mensaje (MAC) es un checksum encriptado del dato, generado por criptografía. La firma digital es una pieza de información asociada con el dato que puede sólo ser creada por el firmante y la cual puede ser verificada por cualquiera. El número de secuencia de mensaje identifica la posición del mensaje en la secuencia.

No rechazo.

Los servicios de no rechazo son los siguientes:

- No rechazo de origen, el cual da prueba de origen del dato.
- No rechazo de liberación, el cual da prueba de liberación del dato.
- No rechazo de presentación, el cual da prueba de presentación del dato.
- No rechazo de transporte, el cual da prueba de transporte del dato.

El no rechazo de origen evita que un generador de datos falsamente niegue proveer los datos. El no rechazo de liberación evita que un destinatario de datos niegue recibirlos. El no rechazo de presentación protege contra cualquier intento de negación falsa de que el dato fue presentado para entregar. El no rechazo de transporte protege contra cualquier negación falsa de que el dato fue transportado.

Administración de seguridad.

La *administración de seguridad* cubre actividades de administración de seguridad en un entorno de red, incluyendo la administración de servicios de seguridad, recursos seguros de red, mecanismos de seguridad, *auditoría de seguridad* y el establecimiento e imposición de políticas de seguridad.

La administración de servicios de seguridad, recursos seguros de red y mecanismos de seguridad involucran la administración de los servicios de seguridad individual, varios recursos seguros de red y mecanismos de seguridad que soportan los servicios de seguridad. De la *auditoría de seguridad* se hablará más ampliamente en el capitulo siguiente.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué, a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

C A P Í T U L O

I I

PROBLEMÁTICA EN SEGURIDAD INFORMÁTICA Y REDES

CAPÍTULO II

PROBLEMÁTICA EN SEGURIDAD INFORMÁTICA Y REDES

2.1 Prefacio.

La dinámica de la vida moderna se caracteriza por una necesidad creciente de administración e intercambio de datos, lo que ha dado lugar a la más extensa red de comunicación que el ser humano hubiera podido imaginar y en donde el uso intensivo de tecnología es un factor indispensable. El valor de la información ha ido tomando una posición de altísima relevancia en todos los ámbitos: en los negocios, en el gobierno, en la educación, en la vida personal. Su pérdida o el uso inadecuado de la misma, puede repercutir en daños de diversas magnitudes, desde el desperdicio de valiosas horas de trabajo, el deterioro de una reputación o la disminución de oportunidades de venta, hasta la pérdida de millones de pesos en activos o como consecuencia del espionaje industrial, por ejemplo.

Desde principios de los años 90's hasta nuestros días, con innumerables amenazas cibernéticas (propagación de programas dañinos, saturación intencional de sistemas, recopilación de información sin permiso del propietario), la Seguridad Informática sigue creciendo en importancia en un entorno social y laboral en el cual las empresas y los individuos literalmente no pueden funcionar sin conexiones electrónicas. Todos estos acontecimientos han provocado una mayor conciencia alrededor de la Seguridad Informática y de la importancia de desarrollar planes de protección de manera anticipada. Pero, ¿Qué está pasando en México? ¿Hasta dónde ha penetrado esta conciencia? ¿Qué tanto conocen los usuarios corporativos e institucionales acerca de estos riesgos y de cómo enfrentarlos?

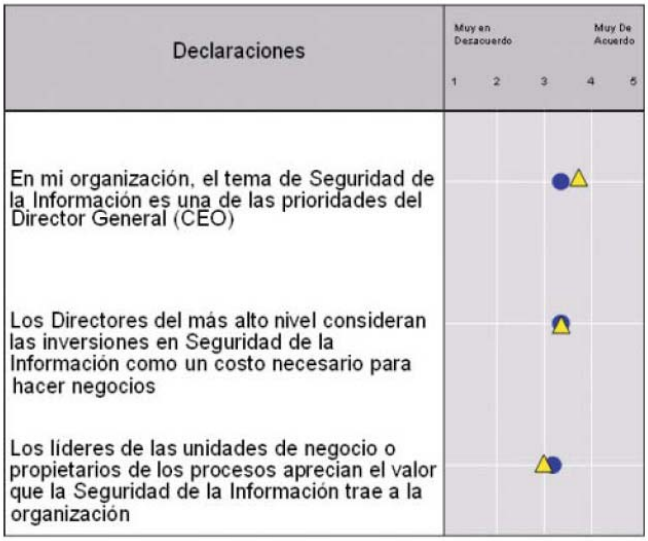
Para responder a estas y otras preguntas hemos considerado en este capítulo tres estudios importantes respecto a la Seguridad Informática a nivel mundial y con resultados enfocados hacia México. Estos estudios deben ser analizados cuidadosamente ya que, al parecer, los entrevistados no han contestado muy honestamente como se observa en el cruce de información. Al final del capítulo realizaremos una conclusión general de esta situación con algunas observaciones. Estos tres estudios mencionados son:

- *Estudio de percepción, Seguridad en Informática México 2004.* Joint Future Systems.
- *Encuesta Mundial de Seguridad IT 2004.* Information Week.
- *Encuesta global de la Seguridad de la Información 2004.* Mancera Ernst & Young.

2.2 Resultados en los usuarios de TI.

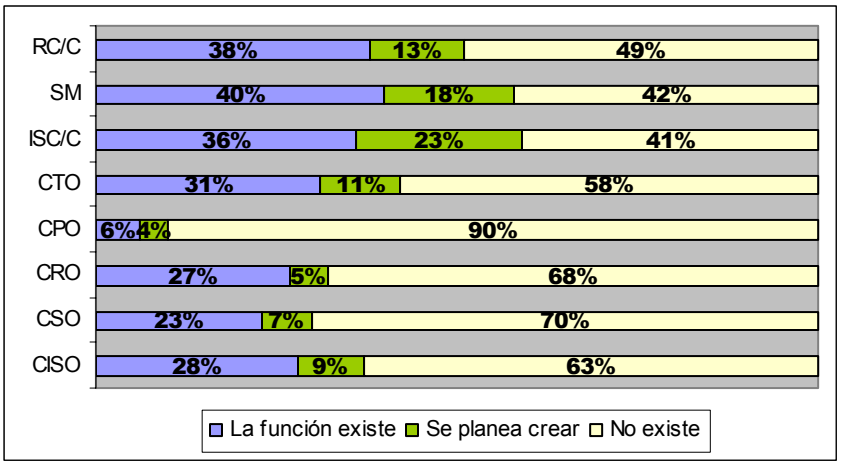
2.2.1 Actitud.

Los resultados nos permiten ver que cuando la alta dirección da su respaldo a una iniciativa, ésta se vuelve más efectiva y aporta mayor confianza. Cuando sorteamos los resultados para enfocarnos a aquellos que declararon que la seguridad de la información era muy importante para el logro de las metas y objetivos de la organización, pudimos apreciar también que la importancia que el CEO (director General) le da a este tema es mayor (gráfica 2.1). Por otra parte, donde los resultados indicaron que la alta dirección no daba su respaldo, los involucrados tienen la tendencia a hacer caso omiso de los controles, o aún peor, de evitarlos en nombre de la eficiencia, sin considerar el riesgo que esto le puede representar a la organización. Desafortunadamente, sólo el 28% de los encuestados a nivel nacional reconoce que en sus organizaciones el tema de seguridad de la información es visto con gran importancia por sus CEO's.



Gráfica 2. 1 Importancia de la Seguridad Informática en los altos mandos

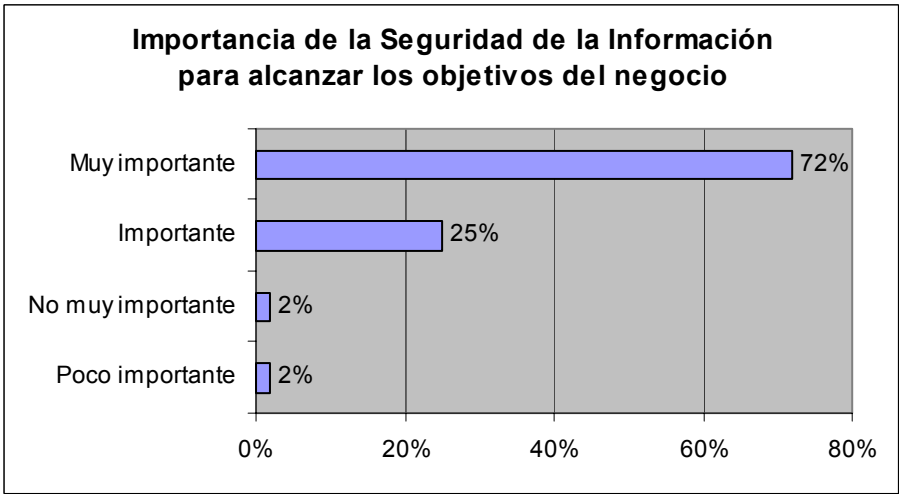
Este año, la figura del Oficial de Seguridad de la Información (CISO) o una similar, parecen existir en el 51% de ellas a nivel nacional y contrasta con el 25% del año anterior (gráfica 2.2).



Gráfica 2. 2 Organizaciones con un CISO

2.2.2 Conciencia.

Es claro que el tema de seguridad de la información sigue considerándose como "Muy Importante" para alcanzar los objetivos de la organización. Esto lo muestra la gráfica 2.3, en la que se ha dado este valor en más del 70% de los casos, cifra superior al 59% alcanzado para este mismo rubro en 2003 a nivel nacional. Sin embargo, comparando los resultados del 2004 con los de años anteriores, encontramos que muchas organizaciones aún sienten indiferencia con respecto a esta situación, solamente necesita uno ver con qué frecuencia reportan a sus consejos de administración el status de la seguridad (gráfica 2.4).



Gráfica 2. 3

	Preocupación	Transición	Conciencia
¿Con qué frecuencia su organización reporta a su consejo directivo o equivalente sobre su seguridad de la información?	59% Anual, poco frecuente o nunca	25% Trimestral y semestral	16% Mensual

Gráfica 2. 4

2.2.3 Adopción de procesos.

A nivel general, los conceptos principales asociados a Seguridad Informática son el acceso autorizado, la protección contra virus, y la integridad y confiabilidad de la información. En cuanto a "Acceso Autorizado", la mayoría de las respuestas hicieron referencia al acceso a los sistemas y a los equipos, aunque unas cuantas se refirieron al acceso a las instalaciones, con respuestas como "Contraseñas", “Control de intrusos", "Confidencialidad de la información", etc.

Es notorio que para los "informáticos" tiene más peso la integridad y confiabilidad de la información, que cualquier otro rubro, incluyendo los accesos no autorizados. De manera notoria, la protección contra virus está asociada al concepto de seguridad, con mucha mayor frecuencia entre los "no-informáticos" que entre los "informáticos", habiendo sido mencionada de manera espontánea por casi la mitad del primer grupo, contra un 17.8% del segundo. Para los "no-informáticos", la configuración correcta de los sistemas no tiene una posición relevante como factor de Seguridad Informática. Para una porción de los "no-informáticos" (3.6%), el uso de software original tiene implicaciones en beneficio de la Seguridad Informática (gráfica 2.5).

GRÁFICA 2

A	Acceso autorizado	H	Manejo adecuado de herramientas
B	Protección contra virus	I	Disponibilidad de la información
C	Integridad / Confiabilidad de la información	J	Protección contra "hackers"
D	Respaldo de información	K	Uso de software original
E	Transmisión segura de datos	L	Configuración correcta de los sistemas
F	Políticas adecuadas	M	No existe
G	Cuidado de los equipos	N	Otros

Gráfica 2. 5

Aunque muchas organizaciones en nuestro país reportan un alto nivel de adopción de mejores prácticas, creemos que reportan más acción de la que realmente ejecutan, especialmente en la identificación de riesgos, la definición de controles para aportar suficiente protección, la definición y difusión de políticas de seguridad, el manejo de contraseñas y la administración de accesos, la definición de procedimientos probados de recuperación y continuidad, así como en la ejecución de procedimientos proactivos como las pruebas de penetración recurrentes o los diagnósticos de seguridad.

Si bien la seguridad es dinámica y requiere mantenerse actualizada para seguir siendo efectiva, se sabe que más del 35% no realiza revisiones sobre el cumplimiento de sus políticas de seguridad en forma continua. La baja ocurrencia de prácticas de monitoreo es también motivo de preocupación (ver gráficas siguientes).

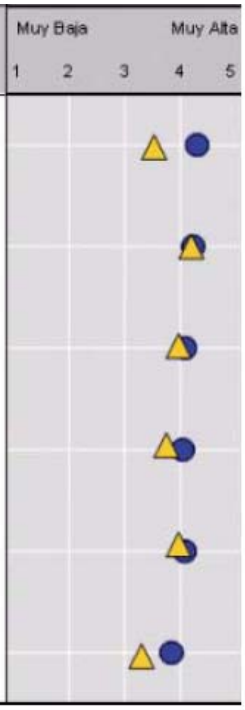
Prácticas de Control	%Sí Mx	%Sí NL	Muy Baja 1 2 3 4 5 Muy Alta
Las políticas de Seguridad han sido comunicadas	87	87	
Las políticas de seguridad son revisadas periódicamente	75	67	
Se crean nuevas prácticas de control cuando se adopta nueva tecnología	75	80	
Los usuarios dan instrucciones sobre el valor que debe darse a sus datos y la forma en la que deben clasificarse	50	53	
El responsable de la función de seguridad de la información se comunica ampliamente con sus usuarios de manera regular	43	33	
Existe un Oficial de Seguridad de Alto Nivel	42	33	
El personal recibe entrenamiento contínuo en seguridad y control	37	20	

Gráfica 2. 6 Efectividad de prácticas de control

Prácticas de Análisis de Riesgos	%Sí Mx	%Sí NL	Muy Baja 1 2 3 4 5 Muy Alta
Los sistemas que son críricos para la organización han sido identificados y se han hecho preparativos para trabajar sin ellos en caso de desastre	85	87	
Las amenazas que pueden causar daño y afectar adversamente a las operaciones críticas han sido identificadas	80	67	
Se han definido suficientes controles para proteger efectivamente contra las amenazas	77	87	
La información sensitiva o confidencial ha sido identificada	68	73	
Pruebas de penetración o vulnerabilidad son ejecutadas de Manera regular	57	40	
Las funciones y activos son identificadas y clasificadas de acuerdo a su valor, sensibilidad y la criticidad del efecto que pueda producirse si una amenaza se materializa	57	40	

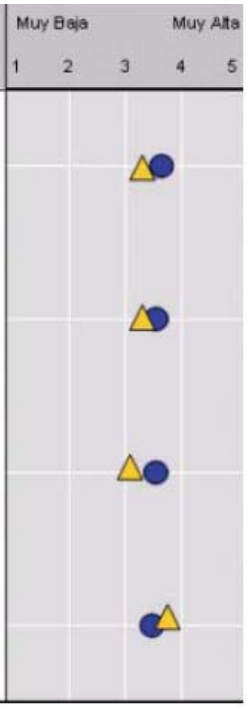
Gráfica 2. 7 Efectividad de prácticas de análisis de riesgos

Prácticas de Control	% Sí Mx	% Sí NL
Una cuenta única de usuario ha sido establecida para cada Individuo autorizado para usar el sistema	88	93
Se requiere que los usuarios cambien sus contraseñas de manera regular	82	93
El acceso de cada usuario está limitado para permitirle acceder únicamente a la información que requiere de acuerdo a sus funciones	82	87
La utilización no autorizada de cuentas de usuario es repelida por contraseñas que son difíciles de adivinar	80	87
La asistencia de la Mesa de Ayuda (Help Desk) exige una identificación positiva antes de reestablecer/cambiar contraseñas o proveer otros servicios	68	67
Los usuarios son entrenados para identificar y reportar actividades sospechosas	43	40



Gráfica 2. 8 Efectividad de prácticas de control de acceso

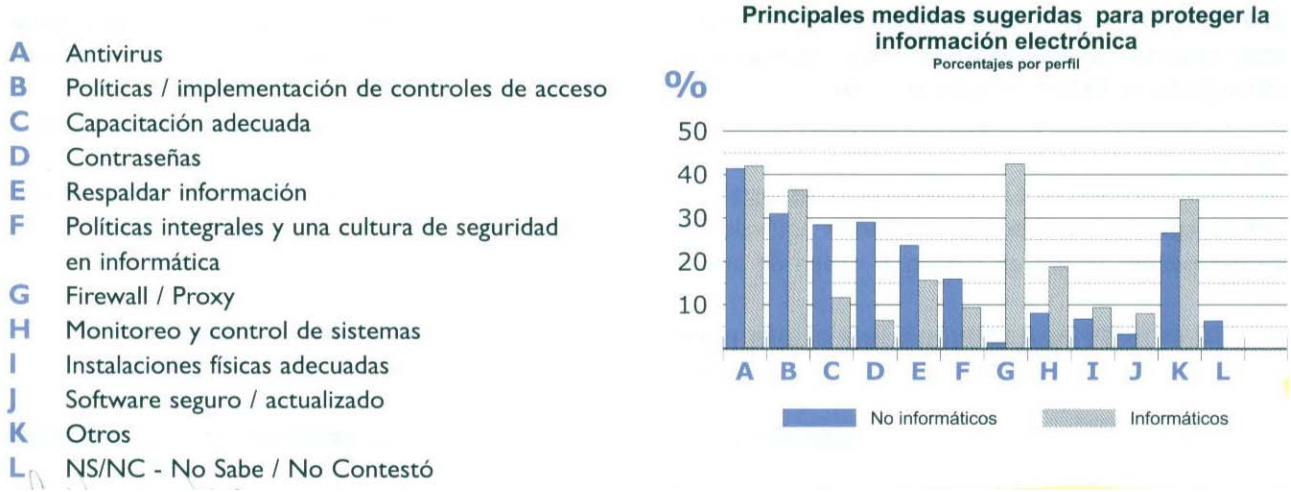
Prácticas de Monitoreo	% Sí Mx	% Sí NL
Las violaciones de seguridad generan una reacción inmediata	75	80
La ejecución de actividades sensitivas se registra en bitácoras para poder asignar responsabilidades adecuadamente	73	60
La operación de la estructura general de control es evaluada y ajustada para adaptarse a situaciones cambiantes	66	66
El cumplimiento con procedimientos de seguridad de la información es evaluado a través de revisiones periódicas de cumplimiento	63	53



Gráfica 2. 9 Efectividad de prácticas de monitoreo

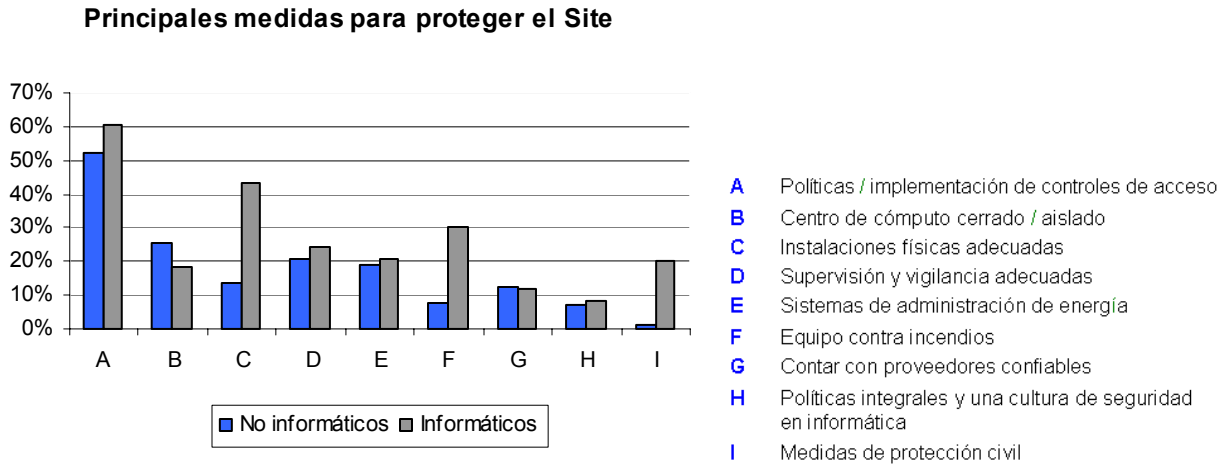
Es notorio que los 3 aspectos más importantes para los "informáticos", como medida de seguridad a implementarse, son el uso de tecnología de control y administración de las telecomunicaciones (firewalls, proxys, etc.), el uso de soluciones antivirus y la implementación de políticas y controles de acceso, entre las que se mencionaron fueron el establecimiento de privilegios, restricciones de acceso de personas a las instalaciones, turnos de trabajo bien definidos, acceso limitado a Internet para el personal, sanciones claras, creación de planes de contingencia tipo DRP, etc.

Aunque en menor proporción respecto de los "No informáticos", para los "Informáticos" también son importantes los respaldos de información y la capacitación adecuada, tanto de los administradores de los sistemas, como del personal en general. A diferencia de los “Informáticos", muy pocos de los "No informáticos" mencionaron soluciones tipo firewall. Las sugerencias más mencionadas por ellos para protección de los sistemas, giraron alrededor de soluciones antivirus, políticas y control de acceso, capacitación y uso de contraseñas, principalmente. También se observa una mayor preocupación por parte de los "Informáticos" por que existan herramientas que permitan el monitoreo y administración remota de los sistemas (gráfica 2.10).



Gráfica 2. 10

En cuanto a la protección física de las instalaciones, la principal coincidencia es que un gran número de entrevistados (más del 50% de cada grupo), mencionaron recomendaciones relacionadas con la implementación de políticas y control de acceso de personas a las instalaciones de cómputo. Después del rubro de políticas y control de acceso, para los "Informáticos" las tres recomendaciones más mencionadas correspondieron a instalaciones físicas adecuadas (aire acondicionado, cableado bien colocado, espacio suficiente, uso de plafón, etc.), equipo contra incendio y medidas de protección civil, mientras para los "No informáticos" fueron tener un Centro de Cómputo aislado, supervisión y vigilancia adecuados (cámaras de video, personal de vigilancia, etc.) y sistemas de administración de energía (gráfica 2.11).



Gráfica 2. 11

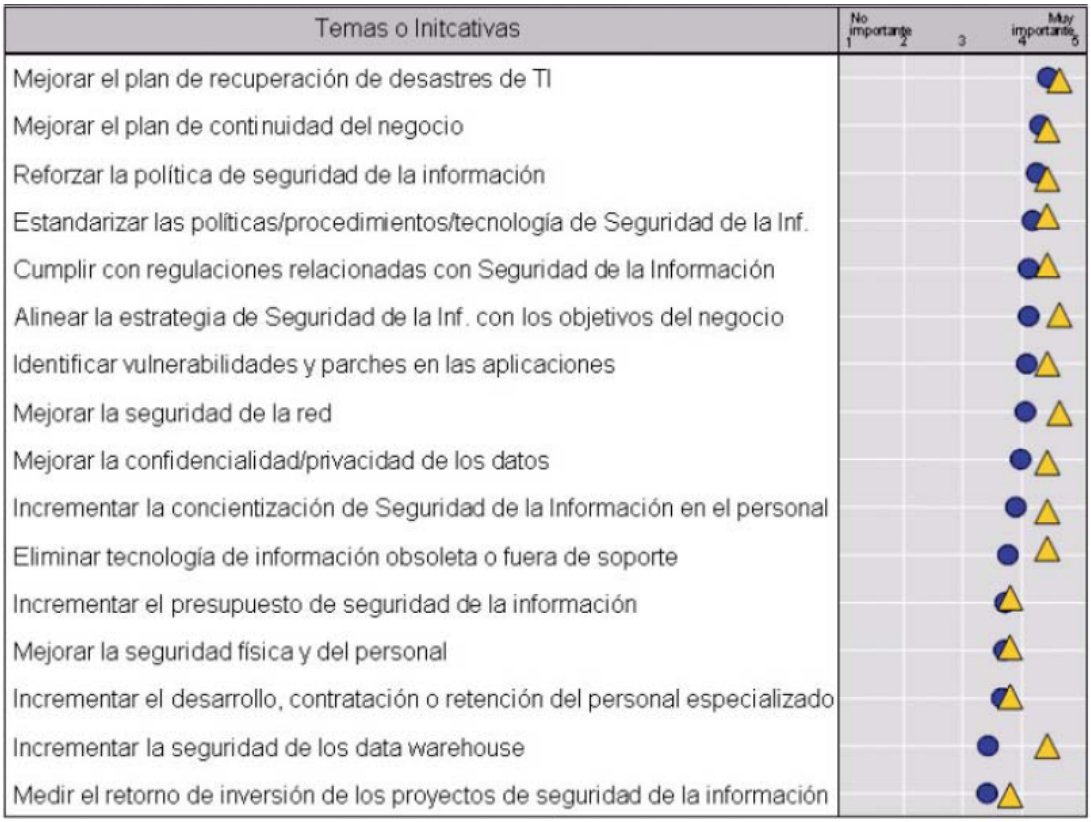
La mayoría de las compañías centran la protección de la seguridad en la red: 75% de las firmas. Ahora bien, como hay tanto ataque de código malicioso, el monitoreo de intrusiones virales es otra actividad popularizada y necesaria. El 71% de los sitios reporta usar software de detección de virus para proteger los sistemas de información. Dos de cada cinco sitios usa sistemas de detección de intrusos.

Las políticas de seguridad suelen reflejar las prioridades del negocio, que pueden ir desde simplificación de éste y preocupaciones de privacidad, a una mayor garantía de colaboración y de buen comportamiento. La administración del sistema (63%), la protección de los datos, la apertura y destrucción (56%) y el monitoreo del uso del web por parte de los empleados (47%) suelen ser frecuentes elementos de política, de acuerdo con las respuestas.

2.2.4 Prioridades y preocupaciones.

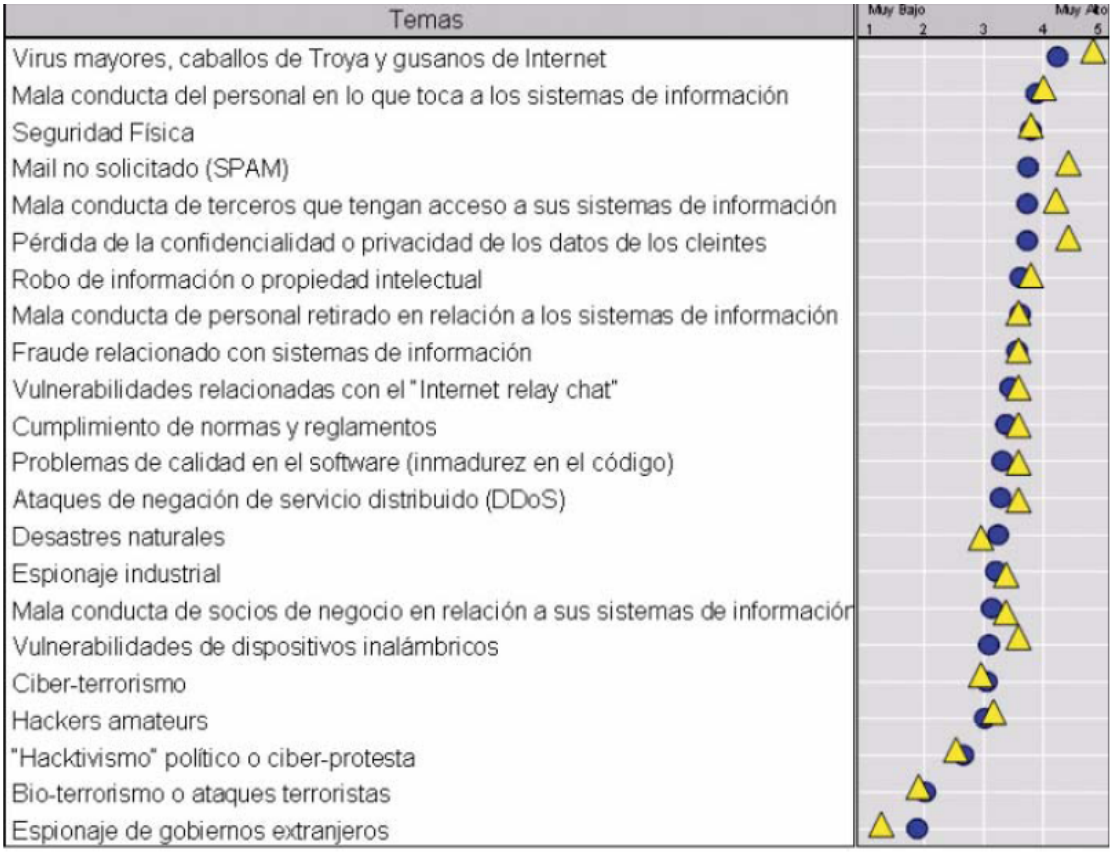
Pensamos que se mostraría más y mejor atención a la concientización y al entrenamiento de lo que vimos en los resultados. Sorprendentemente, las acciones declaradas de los participantes demuestran que siguen persistiendo deficiencias en la atención dada a estos temas. Hemos encontrado que menos de la mitad de los encuestados han establecido programas de entrenamiento y concientización, componente indispensable de una estrategia efectiva de seguridad de la información.

Esto se confirma con la insistencia en la respuesta de “falta de conciencia de seguridad por parte de los usuarios” como uno de los principales obstáculos para lograr la efectividad esperada (gráfica 2.12).



Gráfica 2. 12 Importancia de iniciativas de seguridad

Los encuestados contestaron que se siguen sintiendo más vulnerables a los ataques externos que a las violaciones internas. Los encuestados a nivel mundial y en nuestro país, identificaron a los "internos" como la segunda amenaza en importancia. No obstante, puede verse también que no se toman las medidas necesarias para contrarrestarla (gráfica 2.13).



Gráfica 2. 13 Consideraciones principales a futuro

2.2.5 Incidentes y su combate.

Las irrupciones y los ataques de códigos maliciosos han sido más amenazantes para las operaciones del negocio en 2004 que en el año pasado. Las causas de que las rupturas de seguridad y los ataques de código malicioso se consideren más amenazantes son: mayores volúmenes de ataques y las distintas maneras en que puede ocurrir. Los procedimientos inadecuados de parchado constituyen débiles ligas para la seguridad en dos de cada cinco sitios, mientras que aproximadamente un cuarto de las compañías atribuye a limitaciones presupuéstales el que se sientan amenazadas (gráfica 2.14).

Los ejecutivos de tecnología del negocio y los profesionales de la seguridad quieren ser notificados de inmediato sobre riesgos potenciales. Casi 70% de los interrogados, a nivel mundial, quiere que su proveedor de software les alerte de las vulnerabilidades de su producto inmediatamente de que sean descubiertas.

Gráfica 2. 14

La información nos indica que en algunos casos se están reforzando controles ya implantados y dedicados a áreas de alta prioridad. Sin embargo, en otros casos, la información también da amplia evidencia de que las organizaciones podrían equivocarse en la asignación de recursos a ciertos controles poco efectivos, ignorando otras iniciativas de mayor valor, de hecho, la medición del retorno de inversión de los proyectos de seguridad de la información está siendo la iniciativa con menor importancia para todos los encuestados.

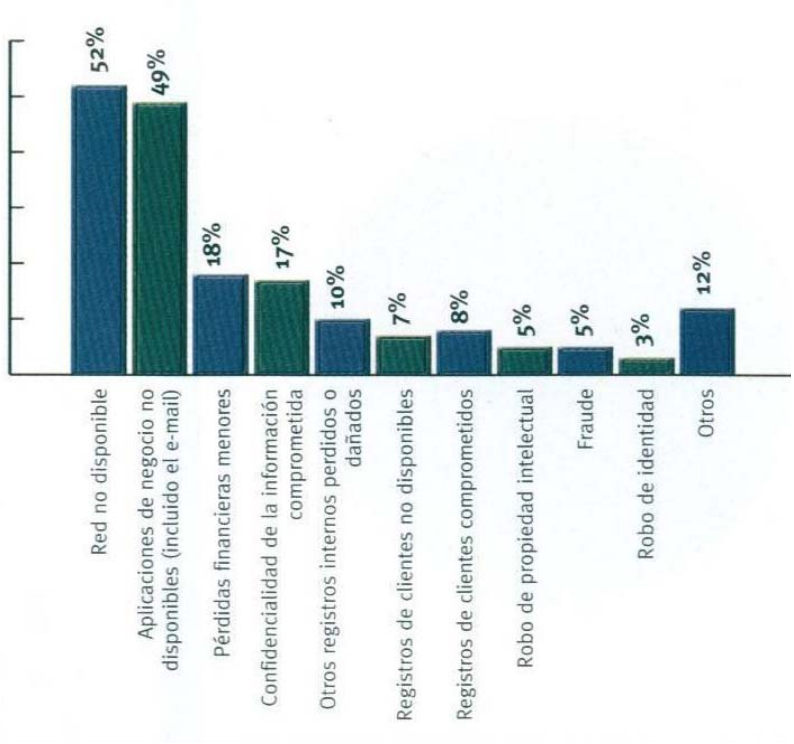
Sospechamos que algunos de los encuestados han quedado impresionados por los comentarios dramáticos de proveedores o los medios, que causan exageraciones respecto a los virus y gusanos, en lugar de enfocar su atención en sus amenazas específicas, que muy probablemente se encuentren al interior de la misma organización.

En la gráfica siguiente se observa que un peligroso 22% de las organizaciones no saben cuantificar el impacto de incidentes de seguridad.

Gráfica 2. 15

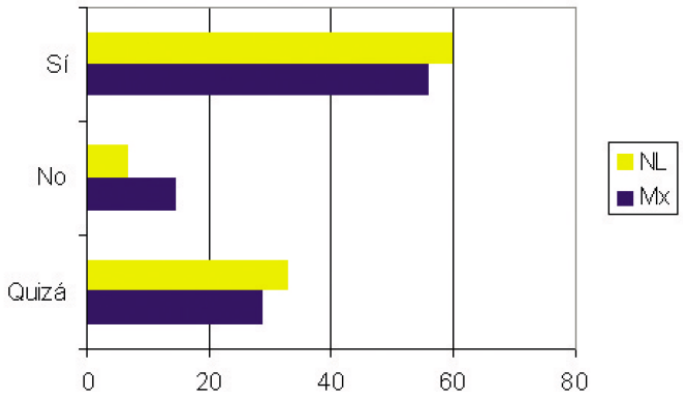
La pérdida de aplicaciones de redes y de negocio es la repercusión más común cuando un ataque a la seguridad tiene éxito (gráfica 2.16). Aproximadamente la mitad de los sitios que han reportado irrupciones en la seguridad se encontraron sin acceso a la red, y 40% afirma que sufrió una interrupción de las aplicaciones de negocio. El año pasado, 40% de los sitios informó de pérdidas de acceso a las aplicaciones de negocio, a la par que este año. Sin embargo, sólo 36% informó de interrupciones en la red, lo que confirma el aserto anterior de que ha habido más tiempos muertos en 2004.

Los métodos primarios de ataque, de que se informa a nivel mundial, han sido contra: una vulnerabilidad conocida del sistema operativo (56%), una vulnerabilidad del sistema operativo desconocida pero que fue explotada (32%) y contra una aplicación conocida, que fue explotada (28%).

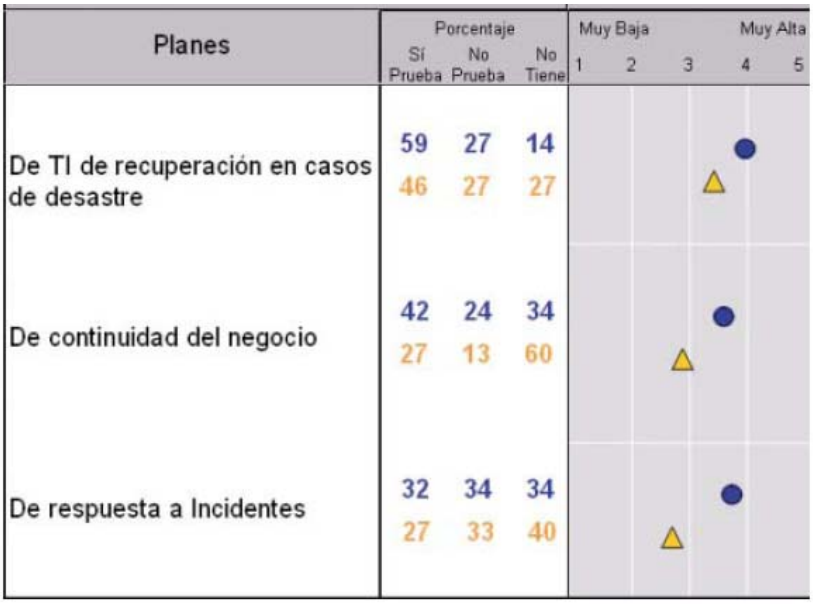


Gráfica 2. 16 Efectos del ataque

A pesar de las medidas de seguridad tomadas, la mayoría de los encuestados habían experimentado incidentes relacionados con fallas que causaron el paro de sistemas críticos por problemas con hardware o software. Aunque se ha incrementado el interés por los planes de continuidad de negocios, la encuesta sugiere que pocos de los que tienen uno, lo han puesto a prueba más allá de ejercicios de escritorio.



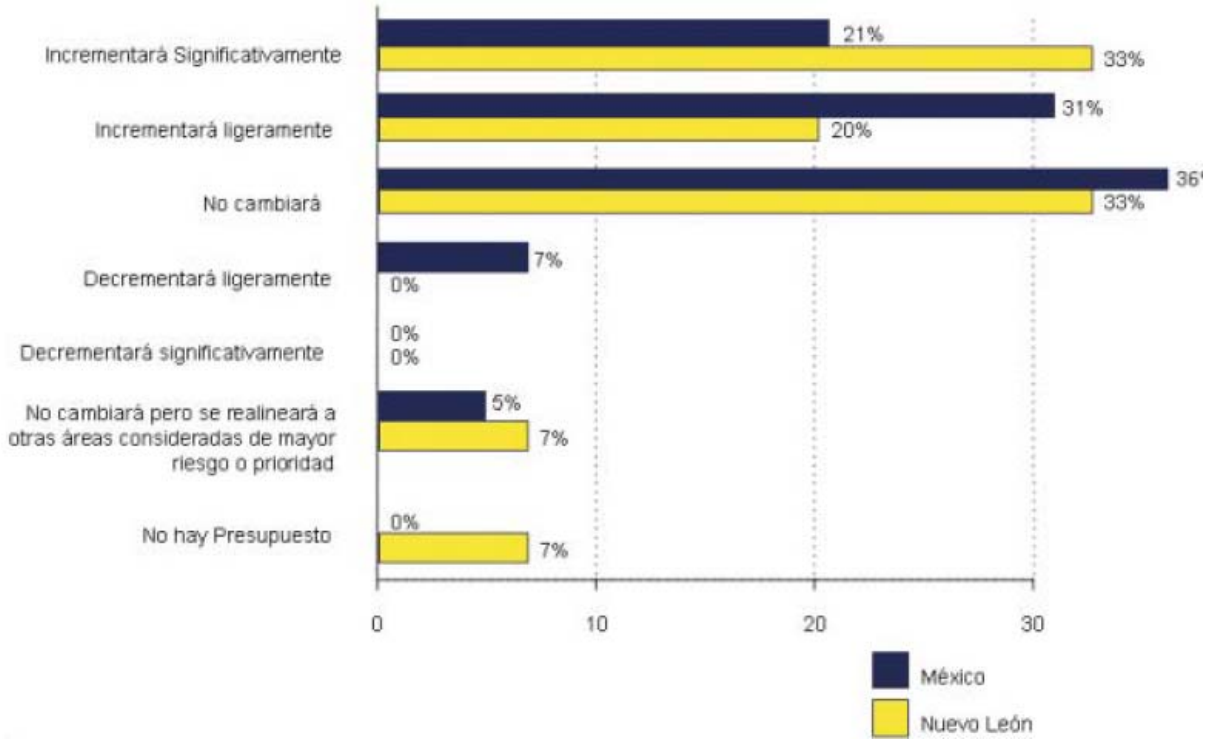
Gráfica 2. 17 ¿Se realizan pruebas de penetración?



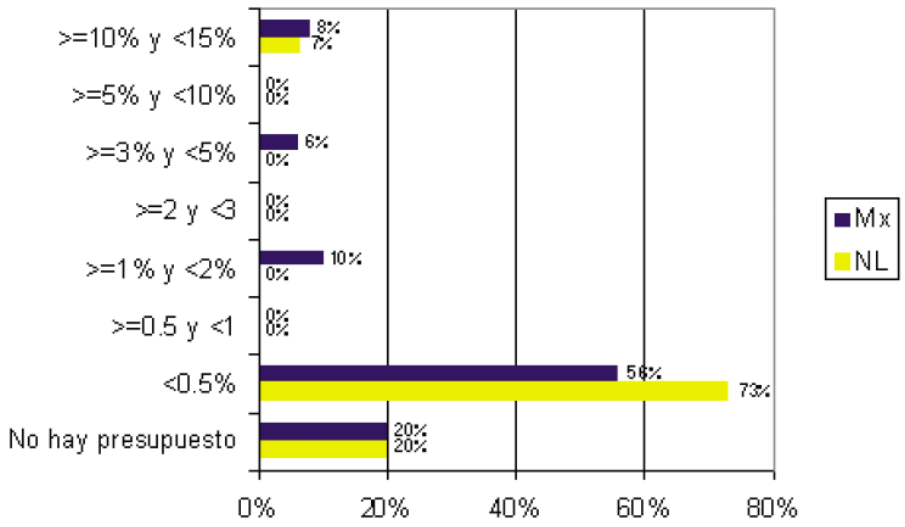
Gráfica 2. 18 ¿Se tienen y prueban estos planes?

2.2.6 Presupuestos y tendencias.

En el año 2003 se concluyó que se gastaba demasiado dinero en herramientas tecnológicas mientras que muy poco se gastaba en asuntos de procesos y de personas. En 2004, creemos que esto es más cierto que nunca.

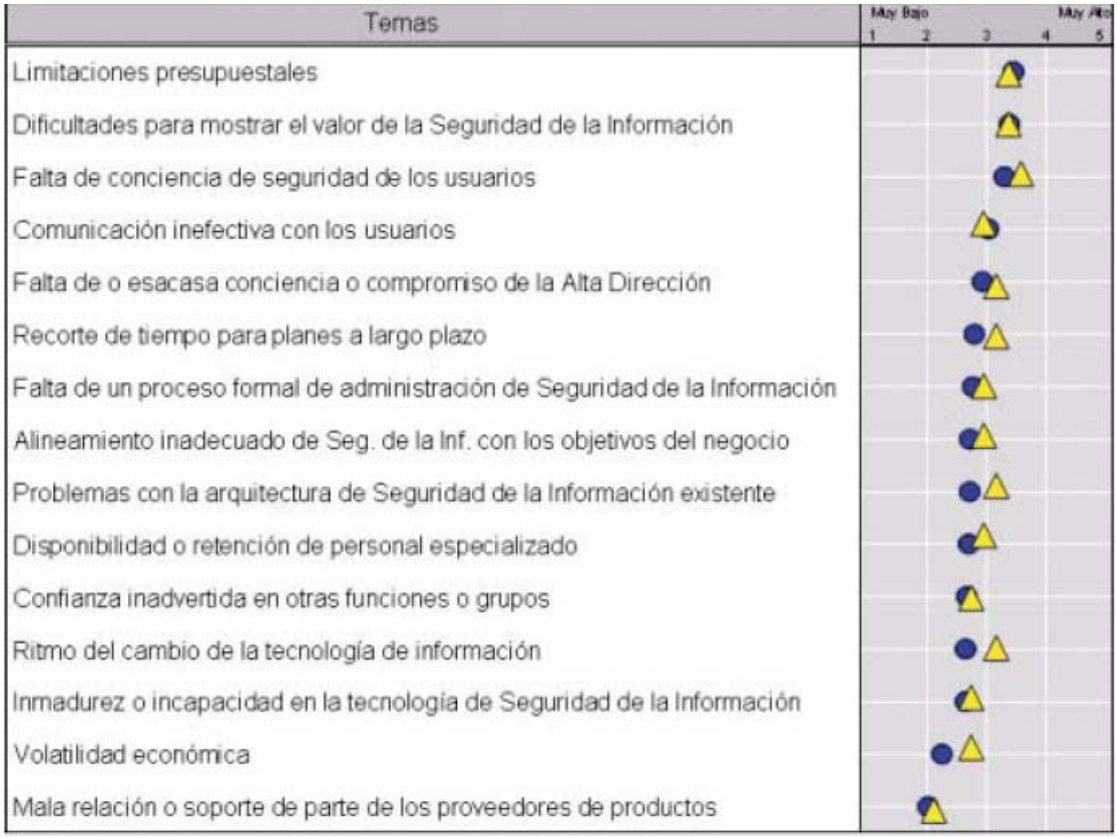


Gráfica 2. 19 Presupuesto en Seguridad respecto al año pasado



Gráfica 2. 20 Porcentaje de presupuesto invertido en seguridad

A nivel mundial encontramos que los principales obstáculos para tener un programa efectivo de seguridad de la información son: la falta de conciencia de los usuarios en torno al tema, las limitaciones presupuestales y la disponibilidad o retención de personal especializado. En nuestro país, el comportamiento es el que se muestra en la gráfica 2.21, puede apreciarse el manejo de las finanzas y la dificultad para asociar valor a las inversiones en seguridad de la información siguen siendo el dolor de cabeza de los especialistas en este campo.



Gráfica 2. 21 Obstáculos para la Seguridad en las organizaciones

2.3 Observaciones de los proveedores de TI.

2.3.1 Situación de la seguridad en México respecto a otros países.

En general, se percibe cierto rezago en nuestro país, considerando su nivel entre medio y bajo frente a los países más industrializados del mundo. Se consideran diferentes causas posibles, relacionadas, principalmente, con una baja promoción de la cultura de seguridad en general y una pobre asignación de recursos a este rubro por parte de las organizaciones, sobre todo en las de infraestructura mediana y pequeña.

Principales observaciones:

- Salvo empresas de clase mundial, existen deficiencias en la planeación e instrumentación de políticas de Seguridad Informática.
- A pesar del rezago, México está acelerando cada vez su avance en la materia.
- El nivel de conciencia respecto a la Seguridad Informática se considera bajo.
    - Hay menos conciencia en la PyME, que en los grandes corporativos.
    - Existe una mayor conciencia entre los niveles técnicos, que entre los niveles ejecutivos.
- Falta entendimiento de Seguridad Informática. Debe ser vista como parte de toma de decisión del negocio y no como un proceso tecnológico. Se está más enfocado a herramientas que a cuestiones estratégicas. Y aún así, las herramientas utilizadas suelen ser muy básicas.
- La situación económica del país y de las empresas en general, provocan que se destinen pocos recursos a la Seguridad Informática.

2.3.2 Principales retos de México, en Seguridad Informática.

Principales observaciones:

- Falta una difusión generalizada, tanto desde el punto de vista didáctico y de desarrollo profesional, como a nivel informativo.
- Se perciben huecos legales e inestabilidad jurídica a diversos aspectos relacionados con la Seguridad Informática, como son el hecho que la tecnología avanza mucho más rápido que el proceso de creación de leyes, las diversas instancias en las que se puede tener o no certeza jurídica de la validez de un documento electrónico, la forma legal de determinar el daño que una pérdida electrónica puede tener para una persona u organización y, en general, la falta de un marco jurídico sólido a estos aspectos electrónicos.
- La Cultura de Seguridad Integral debe contemplar varios rubros. La capacitación no debe limitarse a nociones básicas de seguridad para las PC’s. El tema debería estar relacionado con el ciclo de vida de la información y abarcar, desde que se genera, hasta su resguardo para fines legales, contables u operativos.
- Otros retos de importancia:
    - Lograr un comercio electrónico 100% seguro.
    - Definir y difundir estándares concretos de seguridad.

- Definición de arquitecturas adecuadas y soluciones integrales.
- Uso generalizado de herramientas de seguridad en todo el país.
- Promover la conciencia de la Seguridad Informática a nivel de individuo.
- Protección de la propiedad individual.

2.3.3 Principales retos de las organizaciones usuarias, en Seguridad Informática.

Los retos que las empresas e instituciones usuarias de la tecnología tienen en primer orden, es el de concientizar a los directivos en materia de Seguridad Informática y capacitar a sus empleados, así como establecer bases correctas y políticas claras. Se piensa que la gran mayoría de las organizaciones del país, no se han dado cuenta que invertir en Seguridad en TI es una necesidad y no un lujo.

Principales observaciones:

- Aparte de las políticas, hace falta implementar metodologías a nivel interno.
- Incorporar estándares de nivel internacional, lo exijan así a sus proveedores y cuenten con personal suficientemente especializado.
- El desarrollo de sistemas y su implementación, es un reto que la empresa debe solventar.
- Los procesos y procedimientos de Seguridad Informática deben ser continuamente revisados y actualizados, como parte de sus políticas internas.
- Otros retos de importancia:
  - Promover mayor conciencia entre los directivos de la empresa respecto de las vulnerabilidades y sus consecuencias.
  - Realmente implementar y no quedarse en el plan.
  - Asignar mayores recursos a la Seguridad Informática, haciendo una inversión inteligente.
  - Promover y exigir una legislación adecuada.
  - Simplificar el modelo de aplicación de la seguridad de la información.

2.3.4 Principales retos de los proveedores de hardware, en Seguridad Informática.

Uno de los principales retos percibidos es que se incluyan más mecanismos de seguridad en ellos y que no dejen toda la responsabilidad a los fabricantes de software. En este sentido, es importante que no reduzcan funciones de seguridad con tal de bajar sus precios; su competencia frente a otras marcas, debería ser no sólo en cuanto a precio, sino en los valores agregados que podrían existir alrededor de tecnología cada vez más segura.

Una oportunidad para la industria, en la cual se incluyen ventajas para los usuarios, es percibida en la integración de productos o herramientas de Seguridad en Informática, en la oferta de los equipos. La producción de hardware de diferentes marcas, debe estar enfocada a facilitar la integración en ambientes heterogéneos o bien a la estandarización de soluciones. Igualmente, debería haber una mayor oferta de productos específicos para Seguridad Informática.

Principales observaciones:

- Es una responsabilidad la creación de una cultura de Seguridad Informática Integral.
- Deben dimensionar adecuadamente sus productos, buscando el mejor balance costo-beneficio.
- Otros retos de importancia:
    - Crear soluciones más globales.
    - Hacer las recomendaciones óptimas de seguridad para sus productos.
    - Diseñar herramientas con más tolerancia a fallas, con mejores precios.
    - Enfocar soluciones a la administración centralizada.

2.3.5 Principales retos de los proveedores de software, en Seguridad Informática.

Uno de los principales retos de los proveedores de software es el poder facilitar la integración de soluciones en ambientes heterogéneos. Ésta es una exigencia tanto de usuarios como de integradores, en donde ambas industrias tienen que buscar coincidencias y desarrollar sus productos bajo esta perspectiva. En particular, los fabricantes de software deben incrementar las funciones de seguridad en sus productos, sin escatimar ningún aspecto por bajar precios, eliminando al máximo las vulnerabilidades. Se menciona también la formación de productos de seguridad, como una estrategia comercial adecuada. Un punto a destacar, es que los fabricantes de software deberían desarrollar aplicaciones con mayor capacidad de registro de actividades.

Principales observaciones:

- Deben compartir la responsabilidad de crear una mayor cultura de Seguridad Informática, buscar el desarrollo de aplicaciones más estandarizadas, promover soluciones con administración centralizada y mayores recursos para la investigación y el desarrollo.
- Algunos retos específicos:
    - Mayor oportunidad en la producción y liberación de actualizaciones relacionadas con seguridad.
    - Ampliar el ciclo de vida de los productos, para que sean seguros. Tenerlos perfectamente probados y establecidos, en vez de liberar “betas” todo el tiempo.
    - Desarrollar aplicaciones que por sí mismas, sean más resistentes a virus.
    - Difundir información de forma inmediata, cuando se detecten fallas.
    - Evitar el desarrollo de aplicaciones que pretendan hacer todo.
    - Que el software cuente con políticas de seguridad dentro de sí mismo.
    - Ofrecer soluciones con un buen retorno sobre la inversión.
    - Usar lenguajes seguros de programación, buscar alternativas y S.O. seguros.

2.3.6 Principales retos de las Instituciones Educativas mexicanas.

Se considera que las instituciones educativas deben preparar y desarrollar verdaderos profesionales en el campo de la Seguridad en Informática, e incluso incorporar un mayor número de carreras y materias especializadas. La Seguridad Informática debe ser una parte relevante dentro de sus programas educativos, no sólo en materias afines a la tecnología, sino también en carreras y capacitaciones de otros ramos, en donde existen futuros o actuales ejecutivos. Como corresponde a su actividad, se considera que estas organizaciones deberían ser de las principales promotoras de una Cultura de Seguridad Informática en todos los niveles, así como uno de los agentes más importantes para la creación de conciencia en la materia.

Principales observaciones:

- Promover valores de ética y responsabilidad.
- Mantener una postura neutral respecto de software libre y propietario.
- Instruir a los alumnos en el uso correcto de la TI.
- Realizar estudios para evaluar las consecuencias sociales y económicas a futuro.
- Aumentar la cantidad de carreras y cursos virtuales.
- Implementar soluciones de seguridad en sus propios sistemas.

2.3.7 Principales retos del Gobierno de México.

Existen carencias en materia de reglamentación y regulación, normas y leyes sobre la electrónica que contemplen sanciones apropiadas. En este rubro es donde el gobierno tendría su mayor reto. Asimismo, el combate a la ignorancia y la difusión de una cultura en materia de Seguridad Informática a la ciudadanía, son consideradas como prioridades.

Principales observaciones:

- Difusión de riesgos.
- Entender el entorno y promover la implementación de soluciones.
- Impulsar un gobierno digital.
- Crear y establecer políticas de fomento informático a nivel nacional (PyMEs).
- Promover programas de financiamiento para PyMEs.
- Integrar más procesos electrónicos a la ciudadanía, como usuario de sus servicios.
- Protección adecuada de sus sistemas de acceso al público en general.
- Mayor inversión en investigación y desarrollo de sistemas de Seguridad Informática.
- Mayor exigencia en el cumplimiento de estándares.
- Crear o adoptar estándares que garanticen la confidencialidad, integridad y disponibilidad de la información.
- Contar con especialistas para investigación y fallos adecuados en Seguridad Informática.
- Evitar el uso de aplicaciones que usen modelos propietarios.

2.4 Conclusiones de la situación de la Seguridad Informática en México.

En primera instancia, son notorias diversas carencias y deficiencias en difusión, capacitación y fomento a la cultura de seguridad en informática, tanto a nivel organizacional como individual, que colocan a México como un país rezagado en la materia y lo ponen en evidente desventaja frente a las vulnerabilidades actuales y latentes. La mayoría de las preocupaciones giran alrededor de los "temibles" virus y "hackers", dejando a un lado o dando menor importancia a otro tipo de riesgos, como pudieran ser una planeación deficiente, escasa o nula, la falta de políticas internas claras y comunicadas adecuadamente, la falta de educación, la negligencia y la inexperiencia, las plagas, los desastres naturales y otro tipo de contingencias, e incluso otros de difícil cuantificación como el brindar un mal servicio y la pérdida de credibilidad y confianza por parte de los clientes, por ejemplo.

Y aún en el caso de los "hackers", tan mencionados entre usuarios, es poco el conocimiento que se tiene respecto de los efectos que sus acciones pueden tener sobre cualquier tipo de empresa o institución y, por consiguiente, no conocen las medidas existentes para contrarrestarlos.

Este desconocimiento acerca de soluciones de Seguridad Informática, es generalizado entre los niveles medios de las organizaciones (principalmente PyMEs), salvo algunas excepciones entre cierto personal de alta especialización y en los grandes corporativos. En general, se percibe que la Seguridad Informática, hasta el momento, aún no forma parte importante de la cultura organizacional.

La necesidad de una mayor capacitación es percibida por una gran cantidad de personas, tanto por quienes consideran que sus subalternos requieren profundizar en el tema, como por los mismos usuarios (informáticos y no informáticos) a quienes les gustaría aprender más acerca de cómo enfrentar los riesgos que amenazan la integridad y la seguridad de la información, así como la confidencialidad de la misma. En este sentido, se percibe una conciencia general de que es necesario conocer más sobre seguridad informática, y resulta notorio que existe disposición para obtener este conocimiento.

Coincidencias y diferencias entre el usuario "informático" y el "no-informático".

Aunque la percepción de ambos grupos tiende a ser distinta como consecuencia del grado de especialización en materia de informática y telecomunicaciones, existen algunas coincidencias que, entre otras cosas, denotan el comportamiento que se ha dado en la industria, en los medios, en las organizaciones y de boca en boca, por difundir ciertos temas específicos. Entre las principales coincidencias, se mencionan:

- Ambos dan una prioridad similar al respaldo de información, como concepto distintivo de la seguridad en informática.
- Los virus representan la amenaza de mayor riesgo para ambos grupos, seguido de "hackers" y otros agresores externos.
- Los dos grupos perciben el "desconocimiento" como uno de los mayores riesgos contra la seguridad.

A continuación se presentan las diferencias más sobresalientes entre la percepción de los usuarios "informáticos" (directores, gerentes y jefes de sistemas, encargados de la adquisición e instalación de equipos y software de las empresas, etc.) y los "no-informáticos" (ejecutivos de las áreas de administración, producción, ventas, mercadotecnia, operaciones, jurídica, etc.):

Usuarios informáticos.

- Perciben más la integridad y confiabilidad de la información, como un elemento importante de la seguridad informática.
- Este grupo tiene mayor conciencia acerca de los daños que podrían ocasionar los agresores internos.
- Mayor preocupación por herramientas de monitoreo y administración.
- Muestran mayor preocupación por contar con instalaciones físicas adecuadas, así como equipos contra incendio, como medida de protección de las instalaciones donde se encuentran los equipos de cómputo y telecomunicaciones.

Usuarios "No-informáticos".

- Se preocupan más por los conceptos de acceso y confidencialidad de la información, y por los ataques de virus.
- Aunque con una frecuencia baja, sólo este grupo hizo menciones que asocian el uso de software original con el concepto de seguridad.
- Poco conocimiento sobre soluciones tecnológicas específicas y un nivel muy bajo de identificación de marcas relacionadas con productos o servicios de seguridad informática.
- Una mayor proporción de este grupo, recomienda incrementar la capacitación y el uso de contraseñas, como solución ante posibles riesgos.
- Para la protección de instalaciones mencionaron en mayor proporción que los “informáticos" conceptos como el aislamiento del centro de cómputo, así como una supervisión y vigilancia adecuados.

Principales demandas por parte de los usuarios.

Para los usuarios "Informáticos", lo que hace falta por parte de los proveedores de TI, fue, principalmente:

- Información / más difusión.
- Información de soluciones para PyME.
- Capacitación.
- Mejoras en los procesos de actualización de software.
- Políticas razonables de precio.

En cuanto a las necesidades más importantes de capacitación y difusión para este grupo de usuarios, se mencionaron las siguientes:

- Control de acceso de usuarios, hardware y software.
- Monitoreo y administración de redes.
- Seguridad en Internet.
- Más acerca de "hackers".
- Manejo general de información.
- Costo-Beneficio de los diferentes productos y servicios.
- Más acerca de virus.
- Seguridad en telecomunicaciones.

En el grupo de los usuarios "No-informáticos", las principales demandas que manifestaron hacia los proveedores de tecnología, fueron:

- Mayor información.
- Mejoras en los procesos de actualización de software.
- Mayor asesoría / consultoría.
- Políticas razonables de precio.
- Facilidad en el uso de hardware y software.
- Mayor capacitación.

Las inquietudes principales de este grupo por aprender y profundizar en el tema de seguridad, giraron alrededor de conceptos como:

- Control de acceso de usuarios, hardware y software.
- Más acerca de virus.
- Seguridad en Internet.
- Más acerca de "hackers".
- Seguridad en Informática en general.

En este entorno, aún cuando las personas respondan adecuadamente de forma verbal, la realidad es que la mayoría toma a la seguridad de la información como acto de fe. Lo anterior resulta muy arriesgado, ya que existe un sinnúmero de riesgos o fallas que al acumularse, pueden exponer a su organización a riesgos importantes, tales como la interrupción en sus operaciones, pérdidas financieras o daño a su reputación.

Lamentablemente, cada vez es más frecuente observar que aquellos que toman decisiones se inclinan en favor de las iniciativas de bajo costo, resultando en un incentivo negativo para otras entidades dentro de la organización extendida para no invertir en controles apropiados, puesto que es probable que el precio del fracaso recaiga en otros.

Según los resultados de los estudios, en una organización típica se observa lo siguiente:

Gente.

- La falta de conciencia en los usuarios, las limitaciones presupuestales y las dificultades para mostrar el valor de la función de seguridad de la información

fueron señaladas como los principales obstáculos para definir una estrategia de seguridad de la información efectiva.

Paradójicamente, entre los participantes de nuestro país:

- Únicamente el 30% estuvo muy de acuerdo en que una iniciativa importante fuera el elevar la conciencia o el entrenamiento de los empleados.
- Más de la mitad no provee entrenamiento continuo sobre controles y la seguridad de la información.
- Sólo el 28% considera que el tema de seguridad de la información es una prioridad para el CEO.

Proceso.

- Alrededor del 75% no valida regularmente con un tercero independiente el cumplimiento de sus requerimientos de seguridad.
- Más del 40% no entrena a sus empleados sobre el tema de clasificación de datos, por ejemplo: confidencialidad.

Tecnología.

- Casi el 100% implantó tecnología de antivirus para su protección.
- Menos del 60% llevó a cabo pruebas de ataque y penetración de manera regular.
- Más del 50% vería comprometida la continuidad de la operación de su negocio si se presenta una contingencia, ya que no tienen un Plan de Continuidad de Operaciones o si lo tienen, no lo prueban.

2.5 Seguridad Informática, disponibilidad de la información y continuidad de negocios.

La información es una de las partes fundamentales del capital de las organizaciones. Por lo mismo, debe resguardarse de la misma manera que cualquier otro tipo de capital y fluir hacia los interactuantes operativos y estratégicos, previamente definidos, en los momentos en que ésta sea requerida. Esto quiere decir que la Seguridad de la Información, en términos de negocios, no se limita al resguardo y aislamiento de los datos y su infraestructura; su ámbito tiene que ver también con la Disponibilidad de la información y la Continuidad del negocio mismo.

La adopción de componentes aislados, como programas antivirus o firewalls, permite eliminar sólo una fracción de la vulnerabilidad. Hoy sabemos que menos del 15% de las amenazas de este tipo, pueden ser eliminadas con estas herramientas.

Los mecanismos que se adopten, deben reunir una serie de componentes para asegurar la aplicación de un blindaje integral que garantice seguridad, disponibilidad y continuidad en el uso de recursos informáticos. Los más importantes, son:

1. Política de Seguridad de la Información.
2. Capacitación y difusión permanente de políticas y procedimientos.
3. Asignación de responsabilidades de seguridad.
4. Sistema de detección física y reporte de incidentes de seguridad.
5. Sistema de detección y control antivirus.
6. Proceso de planeación de continuidad del negocio e infraestructura de recuperación.
7. Herramientas de monitoreo y control de activos informáticos.
8. Alternativa de tercerización (outsourcing).

Uno de los principales recursos que permiten reducir la vulnerabilidad por acciones negligentes, accidentales o deliberadas, es el diseño de políticas y procedimientos de seguridad de la información, las cuales deben ser comunicadas y establecidas como obligatorias en todos los niveles de la organización. Éstas deben ser consistentes con los riesgos, los límites de vulnerabilidad, las necesidades de disponibilidad y los requerimientos de recuperación para la continuidad de las operaciones.

Más del 85% de las fallas de seguridad en informática se deben a errores, omisiones o actos deliberados del personal interno o de usuarios autorizados. Las herramientas de capacitación y divulgación, en este sentido, son fundamentales para mejorar la seguridad de las organizaciones. Ahora bien, una capacitación programada y una estrategia adecuada de difusión, no son suficientes por sí solas. Cada uno de los miembros de la organización juega un papel relacionado con la seguridad, por lo que resulta indispensable que haya una asignación precisa de funciones y división de responsabilidades, para observar y verificar las prácticas que se realizan en este sentido.

Los sistemas de detección, monitoreo y automatización, deben formar parte de la infraestructura de protección de la información. Por un lado, se encuentran los mecanismos de identificación y restricción de acceso a las instalaciones, como puertas, exclusas, dispositivos sensibles al movimiento, circuitos cerrados de televisión, tarjetas de proximidad, mecanismos de identificación biométrica y fotográfica, con las herramientas de software y hardware necesarias, entre otros. Asimismo, se debe contar con sistemas de detección y control de accesos electrónicos, como los conocidos firewalls y antivirus.

Hasta aquí, se puede constituir una infraestructura básica de Seguridad de la Información, prácticamente accesible, en términos de costos, a cualquier empresa o institución. Son medidas preventivas que, si bien demandan planeación y organización por parte de los responsables del negocio y de todos los recursos humanos, pueden ser implementadas con cierta facilidad.

Ahora bien, en términos del negocio, ¿Qué sucede si surgen eventualidades, como una falla de energía, un incendio o simplemente una descuido? ¿Qué tan importante es que la información sea accesible todo el tiempo? ¿Cuál es el costo de que "se caiga el sistema" y cuánto tiempo está dispuesta la organización, o sus clientes, a permanecer sin acceso? Es aquí donde se trasciende el concepto de "Protección", para dejar paso al de “Disponibilidad" y "Continuidad de la Operación".

La relación Costo-Riesgo es algo que debe realizarse cuidadosamente, ya que la infraestructura necesaria para sostener la operación del negocio en forma permanente, puede requerir desde miles hasta millones de dólares. Habrá negocios para los que una planta de luz de cierta capacidad, pueda ser suficiente. Sin embargo, otras organizaciones con grandes volúmenes de transacciones o una alta responsabilidad frente a sus usuarios, podrían necesitar apoyos tecnológicos de alta precisión y gran envergadura, para mantener sus componentes críticos en actividad durante las 24 horas del día, los 7 días de la semana y los 365 días del año. Hay que contemplar que, cuando la infraestructura tecnológica en su conjunto o alguno de sus componentes críticos falla, es preciso contar con mecanismos alternos de recuperación, cuyo costo asociado dependerá de la criticidad y el nivel de dependencia de la tecnología para continuar con la operación del negocio. Entre estas soluciones, se encuentran dispositivos de monitoreo y control de los activos informáticos, infraestructura fina y completa en los centros de cómputo y telecomunicaciones, recursos humanos especializados, metodologías, procesos y herramientas, etc. Todos estos elementos se definen en un Plan de Continuidad del Negocio (BCS), en conjunto con un Plan de Recuperación en caso de Desastre (DRP).

2.6 Políticas de Seguridad.

Elementos que conforman la seguridad informática.

La seguridad informática debe apoyar la misión de la organización.

El propósito de la seguridad informática es salvaguardar la información y los bienes de una organización, por medio de la selección y la aplicación de medidas apropiadas. En su sentido más amplio, la seguridad en informática ayuda a la organización a proteger sus bienes físicos y financieros, su reputación y todos sus activos y recursos tangibles e intangibles. La seguridad es un medio, no un fin. Los procedimientos que se implementen no son universales ni generalizables, sino que tienen que ver con el desarrollo y la búsqueda de sincronía con la misión y propósitos de la organización.

La seguridad informática es parte integral y fundamental de las directrices de la organización.

Los sistemas de información y de computación son, cada vez más, elementos críticos en la estrategia y funcionamiento de las organizaciones. Su protección es prioritaria para garantizar el buen funcionamiento y el cumplimiento de metas de la organización.

La seguridad en informática tiene que ser costo-efectiva.

La relación costo-beneficio de un sistema de seguridad, debe ser examinada con toda atención, tanto en sus consecuencias monetarias como en términos no monetarios, para asegurar que el costo no exceda los beneficios esperados. Invertir en medidas de seguridad en informática reduce la frecuencia y la severidad de los daños en cualquier ámbito; cuánto invertir y en qué, dependerá precisamente del valor (en tiempo y dinero) de lo que se quiera proteger, en relación con el costo de hacerlo. No puede ser más caro un sistema de seguridad, que el valor de la información que busca proteger, por lo que se requiere la realización de estudios serios de niveles de riesgo antes de implementar una política general de seguridad en informática.

La seguridad informática debe ser multinivel.

El concepto "multinivel" en materia de acceso, es igual al que se hace rutinariamente en un espacio físico. Este criterio se utiliza en las empresas para aislar áreas de información, la cual se clasifica por niveles de confidencialidad. Una vez clasificada la información, se implementan los procedimientos físicos, de equipamiento y de configuración que se requieren para cada nivel. Una correcta clasificación de información y su ubicación en el nivel de seguridad que le corresponde, resulta en un esquema de seguridad eficiente y práctico. Las medidas de seguridad en informática que pretenden cubrir demasiado, entorpecen y encarecen la operación de un organismo y se convierten, paradójicamente, en un riesgo de seguridad, al ampliar la cantidad de personas que requieren conocer claves y procedimientos de acceso.

Por otra parte, la totalidad de los accesos informáticos a los sistemas de una organización debe estar distribuida entre diversas personas. Esto reduce la posibilidad de robo y fraude, al tener que estar involucradas múltiples personas para llevarlos a cabo, y evita que una sola persona pueda ser percibida como blanco de ataque por parte de agresores.

La seguridad informática debe ser evaluada y modificada periódicamente.

Los equipos de cómputo, telecomunicaciones y el ambiente en el que trabajan, son dinámicos. La tecnología, los usuarios, la información, los peligros y riesgos, cambian constantemente, lo que puede ocasionar que los programas de seguridad implementados pierdan vigencia y, por consiguiente, efectividad. Existe la necesidad de elaborar un calendario de evaluación periódica en relación con los sistemas de seguridad.

Los programas de seguridad en informática, no pueden ser estáticos y deben modificarse de manera permanente, ya que a medida que los procedimientos comienzan a ser rutinarios, inicia un natural relajamiento por parte de quienes los vigilan y, al mismo tiempo, posibles agresores podrían haber ya evaluado su funcionamiento y encontrado puntos de vulnerabilidad. Precisamente la búsqueda de los huecos de seguridad debe ser una función continua dentro de una organización. Si ésta no los encuentra, sus agresores seguramente lo harán.

La seguridad informática y los derechos humanos.

Uno de los obstáculos mayores para lograr establecer sistemas de seguridad efectivos, es la cuestión social. ¿Dónde interfiere el sistema de seguridad con los derechos de los trabajadores? ¿Pueden los sistemas de seguridad interferir con el derecho a la privacidad? ¿Qué se debe hacer? El principio básico es que las medidas de seguridad deben ser implementadas tomando en cuenta los derechos e intereses de todos los involucrados. Esto tiene que ver con balancear las necesidades de seguridad con los supuestos sociales. Por otro lado, se debe entender que por definición las relaciones entre seguridad y derechos humanos no son necesariamente antagónicas. De hecho, un sistema de seguridad bien implementado puede incluso aumentar el nivel de privacidad y de respeto de los empleados.

Distribución de responsabilidades en Seguridad Informática.

La asignación de funciones y responsabilidades en seguridad informática, debe ser clara y explícita. Si bien el tamaño de la organización y la importancia de la información determinarán las características específicas del programa de seguridad en informática, en todos los casos deberá quedar establecido y documentado claramente quiénes son los responsables de cada parte y cuáles son sus funciones específicas.

En general, los puestos que tienen que ver con los procesos de seguridad son:

Director general.

La responsabilidad última recae siempre en la dirección general. No se puede implementar ningún sistema de seguridad sin su aprobación y apoyo. La dirección general establece los niveles de seguridad, los propósitos, objetivos y prioridades, lo cual no quiere decir que deba tener claves de acceso informático a todos los sistemas, por la seguridad de la organización y del mismo director general. Es quien, en primer lugar, tiene la responsabilidad de dar un buen ejemplo a los empleados, siguiendo las pautas y reglas establecidas.

Director de sistemas.

Si bien la dirección general es en quien recae la responsabilidad final, es en la dirección de sistemas donde el proceso y metodología se implementan. La dirección de sistemas tiene un reto doble: mantener la eficacia en el manejo y flujo de información para las otras áreas y utilizar un sistema de seguridad confiable, que no entorpezca la operación.

Proveedores de tecnología.

En el mundo globalizado en el que vivimos, donde enormes cantidades de información están al alcance de todos, es más importante que nunca mantener una relación de asociados con los proveedores de tecnología y conocer las medidas que ellos mismos aplican a sus sistemas de seguridad, confiabilidad de sus tecnologías, etcétera. El personal de cómputo de la empresa (programadores, técnicos, personal de "help desk"), debe ser considerado también como proveedor de tecnología, el cual tiene que estar enterado y capacitado respecto de los procedimientos y políticas de seguridad informática en sus lugares de trabajo. Son ellos quienes operan y proveen de una mayor eficiencia a los procesos que se han decidido implementar.

Áreas de apoyo.

Un sistema de seguridad informática es un todo y las áreas que lo conforman deben tener una función y asignación de responsabilidades específicas. Las áreas más comunes de apoyo son:

- Seguridad de la empresa: responsables del acceso y salida tanto de personas como de bienes.
- Auditores: responsables de vigilar la eficiencia y estado de los sistemas de cómputo, así como de los equipos.
- Personal encargado de recuperación en caso de desastre: algunos organismos tienen personal dedicado a identificar y planear qué hacer en casos de desastres naturales. Esta área debe incluir planes de recuperación para los sistemas de información de los organismos, así como planes de continuidad de servicios de negocio.
- Control de calidad: el área de control de calidad tiene la responsabilidad de incluir los sistemas de seguridad en todos los procesos de calidad que se vayan a implementar.

- Personal: el área de personal deberá conocer el sistema de seguridad que se haya implementado en la organización e incluirlo en los manuales y dinámicas de inducción que se realicen para los empleados nuevos, así como en los programas de entrenamiento y capacitación que se tengan planeados para el personal de la organización.
- Usuarios: es con ellos donde, al fin y al cabo, se comprueba si el sistema elegido funciona correctamente. ¿Conocen las reglas y procesos del sistema de información? ¿Los siguen efectivamente? ¿El sistema es sencillo de operar? ¿Han existido más problemas de seguridad desde que el sistema se implementó, se han reducido o han continuado igual?

Diez pasos para una red segura.

Una red segura es el núcleo de una infraestructura segura. Los atributos de una red segura son: viabilidad total; inteligencia de identidad y contextos; políticas distribuidas; control centralizado; interoperabilidad abierta; administración de una sola acción a nivel de sistemas, y protección y respuesta dinámicas. Estos atributos deben desarrollarse en toda la línea de productos de la organización.

Los diez elementos para una estrategia adecuada de seguridad son:

- Desarrollo de una Arquitectura de Red Segura para proteger y controlar todos los sistemas IT.
- Tener múltiples métodos de control de acceso concurrente por puerto.
- Ser capaz de aplicar controles de políticas a cada aplicación por dispositivo conectado.
- Tener capacidades de protección preactiva, tanto basadas en red como en agentes.
- Desplegar una Arquitectura de Respuesta Dinámica para modificar el comportamiento en tiempo real.
- Las políticas de cuarentena únicamente deben controlar lo servicios agresores para ser efectivas.
- Las acciones de cuarentena deben permitir servicios y protocolos de remedio.
- Planear los dispositivos multi-modales en la estrategia de seguridad.
- Utilizar interfaces abiertas siempre que sea posible.
- Utilizar métricas y mediciones para definir el valor y generar un flujo de conciencia en toda la organización.

Seis pasos para el control de vulnerabilidades.

- Crear una política que defina el estado ideal de la configuración de los equipos, la identidad de los usuarios y el acceso a los recursos.
- Identificar las vulnerabilidades básicas de la organización y sus políticas.
- Jerarquizar las actividades, a fin de mitigar los riesgos.
- Escudar el ambiente utilizando herramientas de seguridad.
- Aminorar la vulnerabilidad eliminando su raíz.
- Dar mantenimiento y monitoreo constante al entorno, para identificar nuevas vulnerabilidades e identificar si existen desviaciones en las políticas.

C A P Í T U L O

I I I

AUDITORÍA EN SEGURIDAD DE REDES

CAPÍTULO III

AUDITORÍA EN SEGURIDAD DE REDES

3.1 Qué es una auditoría.

El término *auditoría* se ha empleado con frecuencia incorrectamente ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase "tiene auditoría" como sinónimo de que, en dicha entidad antes de realizarse la auditoría, ya se habían detectado fallas.

El concepto de auditoría es mucho más que esto. *Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.*

La palabra auditoría proviene del latín *auditorius* y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír. Por otra parte, el diccionario Español Sopena lo define como “revisor de cuentas colegiado”. En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y eficacia. Si consultamos el Boletín de Normas de Auditoría del Instituto Mexicano de Contadores nos dice: "la auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable".

De todo esto sacamos como conclusión que la auditoría es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas, estas sugerencias plasmadas en el informe final reciben el nombre de *recomendaciones*.

3.2 La auditoría informática.

Por tanto, se puede decir que auditoría informática es la revisión y evaluación de controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad en la organización, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones.

El campo de acción de la auditoría informática es (según Willmar): [20]

- La evaluación administrativa del área de informática.
- La evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información.
- La evaluación de la eficiencia y eficacia con la que se trabaja.
- La evaluación del proceso de datos, de los sistemas y equipos de cómputo (paquetes y programas, arquitectura de sistemas, bases de datos, comunicaciones, etc.).
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Los principales objetivos de la auditoría informática son:

- Salvaguardar los activos. Se refiere a la protección de la arquitectura de sistemas (equipos), paquetes y programas, así como de los recursos humanos.
- Integridad de datos. Los datos deben mantener consistencia y no duplicarse.
- Efectividad de sistemas. Los sistemas deben cumplir con los objetivos de la organización.
- Eficiencia de los sistemas. Que se cumplan los objetivos con los menores recursos.
- Seguridad y confidencialidad.

Auditoría interna y auditoría externa.

La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. La auditoría interna existe por expresa decisión de la empresa, o sea que puede optar por su disolución en cualquier momento.

Por otro lado, la auditoría externa es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la auditoría interna, debido al mayor distanciamiento entre auditores y auditados.

La auditoría informática interna cuenta con algunas ventajas adicionales muy importantes respecto a la auditoría externa. La auditora interna tiene la ventaja de que puede actuar periódicamente realizando revisiones globales, como parte de su plan anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las auditorías,

[20] Chávez Chávez, Erika V. *Fundamentos de auditoría informática y su aplicación a la seguridad en redes de ordenadores.* México, ENEP Aragón, 2003. pp. 26-28.

especialmente cuando las consecuencias de las recomendaciones habidas benefician su trabajo.

Una empresa o institución que posee auditoría interna puede y debe en ocasiones contratar servicios de auditoría externa. Las razones para hacerlo suelen ser:

- Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.
- Contrastar algún informe interno con el que resulte del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.
- Aunque la auditoría interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto es necesario que se le realicen auditorías externas para tener una visión desde fuera de la empresa.

La auditoría informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz político ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar por iniciativa del propio órgano o a instancias de la dirección o cliente.

Tipos de auditoría informática.

La información de la empresa y para la empresa, siempre importante, se ha convertido en un activo real de la misma. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la *Auditoría de Inversión Informática*.

Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la *Auditoría de Seguridad Informática* en general o la auditoría de Seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se está en el campo de la *Auditoría de Organización Informática.* Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial.

3.2.1 Procedimiento de una auditoría informática (programa). [21]

Realizar una auditoría en informática es un trabajo complejo. Por ello, para lograr los objetivos, el auditor necesita dividir los sistemas en una serie de subsistemas, identificar los componentes que realizan las actividades básicas de cada subsistema, evaluar la confianza de cada componente y la de los subsistemas, y en forma agregada evaluar cada subsistema hasta llegar a una evaluación global sobre la confianza total del sistema. Esto se debe realizar sin olvidar el postulado de Investigación de Operaciones que señala que:

[21] Franco Delgado, Guadalupe. *La auditoría informática.* México, F.I. UNAM, 2005. pp. 96-113.

"la suma de los óptimos parciales de los subsistemas no es igual al óptimo del sistema, pero nos da una buena aproximación".

Para poder analizar y dimensionar la estructura a auditar se debe solicitar:

1. A nivel organizacional total:
   - Objetivos a corto y largo plazo.
   - Manual de la organización.
   - Antecedentes o historia del organismo.
   - Políticas generales.

2. A nivel del área de informática:
   - Objetivos a corto y largo plazo.
   - Manual de organización del área que incluya puestos, funciones y niveles jerárquicos.
   - Manual de políticas, reglamentos internos y lineamientos generales.
   - Número de personas y puestos en el área.

3. Recursos materiales y técnicos:
   - Solicitar documentos sobre los equipos, así como el número de ellos, su localización y sus características (de los equipos instalados, por instalar y programados).
   - Estudios de vulnerabilidad.
   - Fechas de instalación de los equipos y planes de instalación.
   - Contratos vigentes de compra, renta y servicios de mantenimiento.
   - Contratos de seguros.
   - Convenios que se tienen con otras instalaciones.
   - Configuración de los equipos y capacidades actuales y máximas.
   - Configuración de equipos de comunicación (redes internas y externas) y localización de los mismos.
   - Planes de expansión.
   - Ubicación general de los equipos.
   - Políticas de operación.
   - Políticas de uso de los equipos.
   - Políticas de seguridad física y prevención contra contingencias internas y externas.

En el momento de hacer la planeación de la auditoría o bien su realización, se debe evaluar que pueden presentarse cualquiera de las siguientes situaciones:

- Se solicita la información y se ve que:
  - No se tiene y se necesita.
  - No se tiene y no se necesita.
- Se tiene la información, pero:
  - No se usa.
  - Es incompleta

- No está actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de que no se disponga de la información y se considera que no se necesita, se debe evaluar la causa por la que no es necesaria, ya que se puede estar solicitando un tipo de información que debido a las características del organismo no se requiera. En el caso de que no se tenga la información pero que sea necesaria, se debe recomendar que se elabore con las necesidades y con el uso que se le va a dar. Si se tiene la información pero no se utiliza, se debe analizar porqué no se usa.

El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (no se toman en cuenta los rumores, ni la información sin fundamento). Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

Un programa de auditoría es un grupo de procedimientos documentados y diseñados para cumplir con los objetivos planeados de la auditoría. Aunque un programa de auditoría no sigue necesariamente un grupo de pasos, el auditor de informática debe seguir la secuencia de etapas del programa para obtener una comprensión de la entidad bajo auditoría, evaluar la estructura de control y entonces examinar los controles para hacer el dictamen. Un ejemplo de las actividades de la auditoría en seis etapas se muestra y se describe a continuación:

1. Alcance y objetivo de la auditoría.
2. Estudio inicial del entorno auditable.
3. Determinación de los recursos necesarios para realizar la auditoría.
4. Planeación.
5. Actividades de la auditoría.
6. Informe final.

1. Alcance y objetivos de la auditoría.

El alcance de la auditoría expresa los limites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las aplicaciones y las áreas a auditar. El efecto de acotar el trabajo resulta muy benéfico para ambas partes, inclusive se deben establecer las excepciones, es decir, lo que no se va a auditar.

Los objetivos de la auditoría son:

- Proporcionar a la gerencia la garantía de que los controles se satisfacen.
- En donde existan debilidades de los mismos evidenciar los riesgos resultantes.
- Dar consejo sobre acciones correctivas.

Para el establecimiento del alcance de la auditoría se debe investigar y analizar

- Los procesos de negocio involucrados.
- Las plataformas y sistemas de información que sostienen el proceso de negocio, así como su interrelación con otros sistemas y plataformas.
- Roles del área de sistemas.
- Riesgos asociados del proceso.

Para identificar los requerimientos de información asociados al proceso de negocio se deberán seleccionar los riesgos inherentes del área de sistemas para lo cual tenemos que identificar:

- Cambios recientes en el medio ambiente del negocio con alto impacto en los sistemas.
- Cambios recientes dentro del área de sistemas, nuevos desarrollos, equipos e instalaciones.
- Incidentes recientes relacionados con los controles y el medio ambiente del negocio.
- Controles de monitoreo aplicados al área de sistemas por parte de la gerencia.
- Reportes recientes de certificación o auditoría.
- Resultados recientes de auto-evaluaciones.
- El grado de dependencia de la organización hacia los sistemas de información.
- El uso de software sensible.

2. Estudio inicial del entorno auditable.

En esta etapa es cuando se obtiene y se documenta la comprensión de los aspectos relevantes de los sistemas de información del cliente y los controles generales relacionados. Para realizar el estudio inicial del entorno auditable han de examinarse las funciones y actividades generales de la informática de la empresa. Para su realización, el auditor debe conocer la organización del entorno a auditar y esto implica conocer a la brevedad lo siguiente:

El organigrama:
El organigrama expresa la estructura oficial de la organización a auditar.

Departamentos:
Son los órganos que siguen inmediatamente a la dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

Relaciones jerárquicas y funcionales entre órganos:
Las relaciones de jerarquía implican la correspondiente subordinación. Las funcionales indican relaciones no estrictamente de subordinación. El equipo auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama.

Flujos de información:
La estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extra-departamentales.

Número de puestos de trabajo:
El equipo auditor comprobará que los nombres de los puestos de trabajo en la organización corresponden a las funciones reales.

Número de personas por puesto de trabajo:
La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno operacional:
El equipo auditor debe poseer una adecuada referencia del entorno en el que va ha desenvolverse. Ese conocimiento previo se obtiene mediante la revisión de la siguiente información:

Situación geográfica de los sistemas:
Se determinará la ubicación geográfica de los distintos centros de proceso de datos de la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como, el uso de los mismos estándares de trabajo.

Arquitectura y configuración de hardware y software:
Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías. Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

Inventario de hardware y software:
El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a hardware figurarán los servidores locales y remotos, periféricos de todo tipo, impresoras, etc. El inventario de software debe contener todos los productos desde software básico (sistemas operativos y paquetería) hasta las utilerías adquiridas o desarrolladas internamente.

Comunicación y redes:
Los auditores dispondrán del número, situación y características principales de las líneas, de los accesos a la red pública de comunicaciones y de las redes locales de la empresa.

Aplicaciones, bases de datos y archivos:
Considerar los siguientes puntos:

- Volumen, antigüedad y complejidad de las aplicaciones.
- Metodología del diseño y programación.
- Documentación.
- Cantidad y complejidad de bases de datos y archivos.

- Descripción general de los sistemas instalados y de los que están por instalarse, incluyendo su documentación.

3. Determinación de los recursos necesarios para realizar la auditoría.

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría. Los recursos humanos y materiales pueden desglosarse como sigue:

Recursos materiales.

Los recursos materiales del auditor son dos:

- Software.
    - Programas propios de la auditoría: son muy potentes y flexibles; habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.
    - Monitores: se utilizan en función del grado de desarrollo observado en los sistemas auditados y de la calidad y cantidad de los datos ya existentes.
- Hardware. Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en el equipo del auditado para lo cual habrá de convenir tiempo de máquina, espacio de disco, disponibilidad de impresora, etc.

Recursos Humanos.

La cantidad de los recursos humanos y sus características estarán en función del volumen y la materia auditable. Este recurso establecerá el personal que deberá participar y sus características. El personal que intervenga deberá estar capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo. También se debe contar con personas asignadas por los usuarios para el momento en que se solicite información o se efectúe alguna entrevista de comprobación de hipótesis. En el caso de la auditoría informática en muchas ocasiones será necesario contar con expertos en campos muy especializados.

4. Planeación (elaboración del plan y los programas de trabajo).

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo. Un componente básico de una buena planeación es la relación de los recursos de auditoría disponibles con las tareas definidas en el plan de auditoría. El plan se elabora considerando los siguientes criterios:

Revisión por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa; y en el segundo, parcial y más económica.

Volumen. Este determina la cantidad de auditores requeridos, así como, la cantidad de especialistas necesarios.

El plan y los programas de trabajo deben de considerar o tomar como base los objetivos de control para el establecimiento del plan y los programas de trabajo. El plan tiene la siguiente información:

- Asignación de recursos y esfuerzos globales necesarios.
- Establecimiento de prioridades de las áreas por auditar, tomando como base las prioridades del cliente.
- Estructuración de tareas por integrante del grupo.
- Expresar claramente todas las ayudas que el auditor ha de recibir del auditado.

Han sido desarrolladas numerosas técnicas de administración de proyectos que pueden ser utilizadas para administrar proyectos de auditoría. Algunas son automatizadas y otras son manuales. Todas ellas incorporan los siguientes pasos básicos:

- Desarrollar un plan detallado. El plan debe distribuir los pasos de auditoría necesarios a través de una línea de tiempo. Deben hacerse estimaciones realistas de un tiempo requerido para cada tarea de auditoría dando la debida consideración a la disponibilidad de los auditados.
- Reporte de la actividad del proyecto contra lo planeado. Debe existir algún tipo de sistema que reporte el progreso actual de la auditoría comparado contra los pasos planeados.
- Ajustar el plan y tomar acciones correctivas cuando se requieran. Los logros reales deben ser medidos contra el plan establecido sobre una base continua. Cambios a las asignaciones del auditor o a programas planeados deben realizarse cuando se requiera.

5. Desarrollo de la auditoría.

La auditoría informática requiere de las siguientes técnicas para la consecución de sus objetivos:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.

Se recomienda seguir el siguiente procedimiento para la revisión de cada objetivo de control:

- Entendimiento: puede ser a través de entrevistas a personas clave dueñas del proceso, mediante la investigación o búsqueda de documentación apropiada con respecto a políticas y procedimientos útiles en este proceso.
- Evaluación: revisando que las políticas, procedimientos y cualquier documento en general garanticen la observancia del control.
- Calificación del grado de cumplimiento: mediante la realización de un conjunto de pruebas adecuadas al objetivo de control en cuestión.
- Sustentación de riesgos incurridos al no satisfacer el objetivo de control: esto se realiza básicamente con la utilización de pruebas comparativas (benchmarks) de la industria y/o recomendaciones de la misma, además a través de la identificación de inconsistencias, producto de una incorrecta aplicación de las políticas y procedimientos.

Herramientas:

- Cuestionario general inicial.
- Cuestionario o checklist.
- Estándares.
- Monitores.
- Simuladores.
- Paquetes de auditoría.
- Matrices de riesgo.

6. Informe final.

Una auditoría informática no se puede considerar completa hasta que no plasme sus resultados (recomendaciones u observaciones) en un documento llamado informe final. Considerar lo siguiente:

- El informe debe incluir solamente hechos importantes.
- La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- El informe debe consolidar los hechos que se describen en el mismo.

La consolidación de los hechos debe satisfacer al menos los siguientes criterios:

- El hecho debe poder ser sometido a cambios.
- No deben existir alternativas visibles que superen al cambio propuesto.
- La recomendación del auditor sobre el hecho debe mantener las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida, que deberá considerar el siguiente flujo:

1. Hecho encontrado.
    - Ha de ser relevante para el auditor y para el cliente.
    - Ha de ser exacto y además convincente.

   - No deben existir hechos repetidos.
2. Consecuencias del hecho.
   - Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.
3. Repercusión del hecho.
   - Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos de la empresa.
4. Conclusión del hecho.
   - No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa y compleja.
5. Recomendación del auditor informático.
   - Deberá entenderse por sí sola, por simple lectura.
   - Deberá estar suficientemente soportada en el propio texto.
   - Deberá ser concreta y exacta en el tiempo para que pueda ser verificada su implementación.
   - La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

Estructura del informe final:

- El informe comienza con la fecha de comienzo de la auditoría y la de redacción. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo.
- Definición de objetivos y alcance de la auditoría.
- Enumeración de temas considerados. Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.
- Cuerpo expositivo. Para cada tema, se seguirá el siguiente orden:
  a. Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
  b. Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
  c. Puntos débiles y amenazas.
  d. Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
  e. Redacción posterior de la Carta de Introducción o Presentación.
- Carta de Introducción o Presentación del informe final. Tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa o a la persona concreta que contrató la auditoría. Así como pueden existir tantas copias del informe final como solicite el cliente, la auditoría no hará copias de la Carta de Introducción. Poseerá los siguientes atributos:
  - Incluirá fecha, naturaleza, objetivos y alcance.
  - Cuantificará la importancia de las áreas analizadas.
  - Proporcionará una conclusión general, concretando las áreas de gran debilidad.
  - Presentará las debilidades en orden de importancia y gravedad.

- No se escribirán nunca recomendaciones.

3.2.2 Obtención y evaluación de la evidencia.

La selección del tipo de evidencia de auditoría es crucial, por lo que el auditor debe planificar el uso de la mejor evidencia, de tal manera que sea consistente con la importancia del objetivo de la auditoría, y el tiempo y esfuerzo involucrados en obtener tal evidencia.

EVIDENCIA.

Las Normas de Auditoría Generalmente Aceptadas, en la norma 3ª, determinan que "debe obtenerse evidencia suficiente y competente, mediante la realización y evaluación de las pruebas de auditoría que se consideren necesarias, al objeto de obtener una base de juicio razonable sobre los datos contenidos en los sistemas de información que se examinan y poder expresar una opinión respecto de los mismos". La evidencia es uno de los fundamentos de la auditoría, estando constituida por todos aquellos hechos susceptibles de ser probados por el auditor en relación con los sistemas informáticos que examina, que se manifiesta a través de las técnicas de auditoría aplicada y de acuerdo con el juicio profesional.

Evidencia física.

Permite al auditor constatar la existencia real de los activos y la calidad de los mismos, mediante el procedimiento de inspección ocular. Puede incluir observación de actividades, propiedades y funciones de los sistemas de información.

Evidencia documental.

Se obtiene a través de la revisión de documentos considerados importantes por el auditor. Hay dos tipos de evidencias documentales: las creadas dentro de la organización y las creadas fuera. Las evidencias documentales de auditoría pueden ser: los resultados de datos calculados, el registro de transacciones, el control de registro de auditorías previas o documentos como: políticas, procedimientos escritos y diagramas de los sistemas existentes.

Evidencia analítica.

Se obtiene del conjunto de procedimientos que implican la realización de cálculos aritméticos y comprobaciones matemáticas.

Evidencia verbal.

Se obtiene a través del contacto personal con los distintos responsables y empleados de la compañía y con terceras personas independientes; son declaraciones que pueden tener carácter formal e informal.

Evidencia de control interno.

La evidencia de un sistema de control interno eficaz y que además se cumpla, constituye para el auditor una evidencia válida del correcto funcionamiento de la empresa.

CARACTERÍSTICAS DE LA EVIDENCIA.

La ***suficiencia*** está relacionada con la cantidad de evidencia que permite al auditor formar una opinión sobre su trabajo de verificación.

La ***competencia*** de la evidencia es cualitativa, una evidencia es competente cuando es apropiada para el fin que persigue el auditor. Para ser suficiente la evidencia debe ser convincente para justificar los contenidos de los informes.

Validez es la fuerza o credibilidad de la evidencia en dar soporte a las conclusiones concernientes a la naturaleza de la entidad en examen; a mayor grado de confianza de la fuente y forma de la evidencia, más valiosa será.

Relevancia se refiere al grado de relación entre las evidencias y los objetivos del auditor.

TÉCNICAS DE OBTENCIÓN DE LA EVIDENCIA.

El elegir la técnica o método adecuado dependerá del alcance de la auditoría. Los procedimientos utilizados para obtener evidencia de auditoría varían de acuerdo al sistema de información que está siendo auditado. El auditor debe seleccionar el procedimiento más apropiado para el objetivo de la auditoría. Deben considerarse los siguientes procedimientos: consultas, observaciones, inspección, confirmación y reejecución. Los procedimientos anteriores pueden aplicarse por medio del uso de técnicas de auditoría manual, técnicas de auditoría asistida por computadora o ambos.

1. Obtención de evidencia por objetivo de control.

En el caso de la metodología de COBIT los auditores comparan los controles del proceso de TI a auditar contra la lista detallada de objetivos de control para determinar si es posible hacer un mapeo adecuado entre los objetivos de control existentes y los propuestos por COBIT, de esa forma se procede a establecer el cumplimiento adecuado o no. Una vez satisfechos con el nivel de control implantado por la organización, los auditores seleccionan de la lista detallada de objetivos de control los que son más importantes, de acuerdo con el conocimiento que tienen sobre los riesgos y objetivos relacionados del proceso de TI a auditar.

Una vez que se han determinado los objetivos de control que se revisarán durante el proceso de auditoría, el auditor deberá determinar los procedimientos de auditoría que serán utilizados para la obtención de evidencia, incluyendo aquellos de naturaleza especializada.

2. Técnicas de obtención de evidencias en sistemas manuales.

Las entrevistas y cuestionarios han sido ampliamente utilizados como una técnica de obtención de evidencias en sistemas manuales, sin embargo, su importancia no ha disminuido en sistemas computarizados.

Entrevistas.

El auditor puede utilizar las entrevistas para:

1. Los analistas y programadores de sistemas que diseñaron e implementaron el sistema pueden ser entrevistados de tal forma que el auditor puede obtener una mejor comprensión de los controles y funciones del sistema.
2. El personal puede ser entrevistado para determinar qué problemas existen respecto a los datos.
3. Los usuarios del sistema pueden ser entrevistados para determinar el impacto del sistema en la calidad de su vida laboral.
4. Si un fraude es descubierto, el personal puede ser entrevistado para determinar quién perpetró el fraude.
5. Los operadores pueden ser entrevistados para identificar a los sistemas que aparentemente consumen cantidades anormales de recursos.
6. El controlador puede ser entrevistado para identificar sistemas críticos dentro de la organización.

Las entrevistas pueden utilizarse para obtener información tanto cualitativa como cuantitativa. Por último, el objetivo es preguntar abierta, completa y honestamente para obtener respuestas de quienes tienen mayor conocimiento en algún punto que el que pudiera tener el auditor.

Cuestionarios.

Los cuestionarios han sido usados tradicionalmente para evaluar controles en sistemas. Las respuestas a las preguntas indican la presencia o ausencia de un control o la no aplicación de un control determinado. Sin embargo, los cuestionarios tienen otros propósitos como una herramienta de obtención de evidencia pues pueden usarse para evaluar la efectividad de un sistema. También pueden usarse para identificar áreas donde un sistema de información puede tener ineficiencias potenciales.

Diagramas de flujo de control.

Los diagramas de flujo de control muestran qué controles existen en un sistema y donde pueden existir éstos. Tienen tres propósitos de auditoría:

- Comprensión. La construcción de un diagrama de flujo de control resalta aquellas áreas donde el auditor no tiene suficiente conocimiento, ya sea de controles del sistema o del sistema mismo.

- Evaluación. Un auditor experimentado reconoce los patrones de un diagrama de flujo de control que sugiere la presencia ya sea de fortalezas o debilidades de los controles en el sistema.
- Comunicación. El diagrama de flujo de control puede usarse para relacionar la comprensión que tiene el auditor sobre el sistema y los controles asociados a éste.

EVALUACIÓN DE LA EVIDENCIA.

Después de desarrollar un programa de auditoría y de reunir evidencia de la misma, el siguiente paso es evaluar la información reunida para desarrollar una opinión de auditoría. Esto requiere al auditor considerar una serie de fortalezas y debilidades para entonces poder obtener las conclusiones y recomendaciones del proceso de auditoría.

El auditor informático debe evaluar los resultados de la evidencia recopilada de conformidad con los requerimientos y objetivos de control establecidos durante la planeación. Esto exige un considerable juicio profesional ya que frecuentemente los controles no son claros. Se debe enfocar a los objetivos globales de análisis y no en la naturaleza de la evidencia obtenida.

Es poco conocido sobre cómo alguna evidencia debe ser sopesada y combinada para hacer esta evaluación global. Es más, los auditores deben confiar en su intuición y experiencia para determinar el impacto de las fortalezas y debilidades que un sistema tiene en la calidad del sistema mismo.

En algunas ocasiones un control fuerte puede compensar a un control débil en otra área. El auditor debe estar conciente de compensar controles en áreas donde han sido identificados como débiles. Los controles de superposición son similares a los de compensación. Un control de superposición puede realizar otro control adecuado.

3.3 Metodología de la auditoría informática.

A continuación se describirán brevemente algunas de las guías internacionales que se revisaron con el fin de determinar la mejor alternativa para plantear la metodología a seguir para el presente trabajo.

3.3.1 COBIT. [22]

COBIT es ampliamente usado a nivel mundial y reconocido como un estándar por organizaciones mundiales y líderes en el ramo de la auditoría tales como: ISACA, ISACF y el ITGI (IT Governance Institute). COBIT está basado en el establecimiento de objetivos de control a procesos, no a herramientas o a productos.

Los Objetivos de Control para la Información y la Tecnología Relacionada (COBIT, Control Objectives for Information and Related Technology) es un estándar que se puede aplicar a cualquier organización sin importar su plataforma o estructura tecnológica. COBIT es el marco de control y auditoría más utilizado para asegurar el alineamiento de la tecnología de la información de la empresa, ya que cada necesidad del negocio queda relacionada con un objetivo de control que puede ser auditado.

Con el fin de asegurar que los requerimientos de información del negocio se satisfacen, deben definirse, implementarse y monitorearse medidas de control adecuadas para estos recursos, para lo cual se requiere un marco referencial de objetivos de control. COBIT consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación.

Los dominios se identifican con nombres que la gerencia utilizaría en las actividades cotidianas de la organización y son:

- Planificación y Organización (PO).
- Adquisición e Implementación (AI).
- Entrega y Soporte (DS).
- Monitoreo y evaluación (M).

COBIT está integrado por cuatro componentes principales:

1. Un resumen ejecutivo. Está dirigido a los ejecutivos de alto nivel de la organización. Constituye una introducción a los conceptos y principios del marco de trabajo de COBIT.
2. El marco de trabajo. Ayuda a unir los objetivos de control de la TI con los del negocio.
3. Los objetivos de control. En este documento cada uno de los 34 procesos de control considerados en los cuatro dominios lógicos y en el marco de trabajo se asocia con sus respectivos objetivos de control.
4. Lineamientos de auditoría. Establece la metodología a seguir para realizar la verificación del cumplimiento de los controles establecidos a cada uno de los

[22] *Ibíd.*, pp.87-96.

procesos identificados. Considerando el ámbito tan extenso que compete a una auditoría informática, COBIT puede complementarse con estándares específicos, por ejemplo, en el caso de que se quiera auditar el nivel de seguridad de una aplicación se puede recurrir a los estándares de seguridad como los del NIST o el Libro Naranja.

De los 34 procesos que componen el COBIT, agrupados en 4 dominios, hemos considerado para este trabajo 3 controles (o procesos) y sus 34 subcontroles respectivos que pueden ser aplicables a la seguridad en redes. Estos se encuentran desglosados en el Apéndice A.1. Es posible que algunos de estos controles sean similares a los del BS 7799.

3.3.2 BS 7799-1:2000, *Tecnología de la información — Código de práctica para la administración de seguridad de la información.* [23]

La seguridad de la información no es sinónimo de seguridad informática. Incluye aspectos técnicos, pero se extiende al ámbito de la organización y contempla aspectos estrictamente jurídicos. BS 7799-1:2000 está aprobada y corresponde al estándar internacional ISO/IEC 17799:2000. Actualmente se tiene ya desarrollado el estándar ISO/IEC 17799:2005 que hace incompatible su uso conjunto con el BS 7799-2:2002. Se espera que el próximo año salga su versión estandarizada llamada ISO/IEC 27001.

BS ISO/IEC 7799 proporciona un conjunto de controles que comprenden las mejores prácticas de seguridad de información. Pretende servir como un punto de referencia al identificar el rango de controles necesarios para la mayoría de las situaciones donde los sistemas de información son usados en la industria y el comercio. No todos los controles descritos en este documento serán relevantes para cada situación.

Una vez que los requerimientos han sido identificados, los controles deberán ser seleccionados e implementados para asegurar que los riesgos están reducidos a un nivel aceptable. Los controles pueden ser seleccionados de este documento o de otros conjuntos de controles, o diseñados para necesidades específicas. Deben ser seleccionados basándose en el costo de la implementación en relación a los riesgos a reducir y a las pérdidas potenciales si un incumplimiento de seguridad ocurre. Los controles se pueden clasificar como basados en requerimientos legislativos o como las mejores prácticas para seguridad de información.

Habiendo realizado una revisión del BS ISO/IEC 7799, que consta de 10 cláusulas de control, divididas en 36 objetivos de control que comprenden 127 controles (y muchos subcontroles), hemos seleccionado aquéllos que están relacionados con la seguridad en redes. Se han seleccionado explicaciones del BS 7799-2:2002, para sintetizar información sobre los controles, pero la numeración corresponde al documento BS 7799-1:2000.

Como bien se expresó anteriormente, la seguridad de la información comprende más que aspectos técnicos, incluyendo cuestiones administrativas, legales y de concientización. La

[23] BS 7799-1:2005, *Information technology — Code of practice for information security management.*

existencia de un análisis de riesgos y de políticas de seguridad es, por ejemplo, de más importancia que la implementación a ciegas de tecnología de seguridad. De esta forma se podrá observar que se incluyen controles, objetivos y cláusulas que no pertenecen necesariamente a aspectos técnicos o de TI en seguridad de redes, y es necesario aclarar que no se puede distinguir en algunas situaciones entre la seguridad de sistemas y la de redes (de hecho, se considera a la red un sistema). Estos controles se exponen en el Apéndice A.2.

BS 7799-2:2002, *Sistemas de administración de la seguridad de la información — Especificación con guía para su uso.* [24]

La segunda parte del estándar BS 7799 especifica la forma de implementar los controles seleccionados de la norma ISO 17799. Es una especificación sobre cómo construir, operar, mantener y mejorar Sistemas de Administración de Seguridad de la Información (ISMS). Está desarrollada siguiendo el ciclo PDCA (Plan-Do-Check-Act) del modelo Deming, por lo que tiene procesos comunes, presentando una interesante sinergia con la implementación Turnbull de Gestión de Riesgos de Negocio.

3.3.3 Criterios Comunes (CC) para la Evaluación de la Seguridad de la Tecnología de la Información. [25]

Corresponde con el estándar internacional ISO/IEC 15408 (Information Technology – Security Techniques – Evaluation Criteria for IT Security) y pretende ser usado como base para la evaluación de propiedades de seguridad de sistemas y productos de TI. Es un documento más complejo que el BS7799 (aunque no tan específico y no contiene controles sino elementos funcionales de seguridad) al ser aplicable a cualquier TI y está dividido en tres partes.

La primera parte (Introducción y modelo general) presenta definiciones y un modelo general de evaluación. También se presentan constructos para expresar los objetivos de seguridad y para seleccionar y definir los requerimientos de seguridad.

La segunda parte de los CC, Requerimientos funcionales de seguridad, contiene un catálogo de componentes de seguridad. Estos requerimientos describen el comportamiento esperado de un Objetivo de Evaluación (TOE, Target of Evaluation) o de su entorno. Los componentes expresan requerimientos de seguridad pensados para contestar a las amenazas en el ambiente de operación del TOE y/o cubren políticas de seguridad organizacionales.

La tercera parte de los CC (Requerimientos de confianza de seguridad) establece un conjunto de componentes de confianza para los requerimientos del TOE. Cataloga el conjunto de componentes, familias y clases de confianza. Define un criterio de evaluación para los Perfiles de Protección (PPs) y los Objetivos de Seguridad (STs) y presenta una Evaluación de Niveles de Confianza (EALs) que van desde el EAL1 (probado

[24] *BS 7799-2:2002, Information security management systems — Specification with guidance for use*.
[25] *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004.

funcionalmente) hasta el EAL7 (diseño verificado y probado formalmente). Estos niveles se pueden hacer corresponder con algunos de los niveles de seguridad del TCSEC (Orange Book).

El catálogo de los componentes de seguridad se divide en 11 clases, éstas en 67 familias que a su vez se dividen en 136 componentes y éstos en elementos funcionales, todo esto presentado alfabéticamente. Se debe seleccionar un componente apropiado una vez que una familia ha sido identificada como una parte necesaria o útil para sus requerimientos de seguridad; existe jerarquía de algunos componentes de tal forma que pueden satisfacer otro(s). Los elementos funcionales son los miembros de un componente y constituyen el más pequeño requerimiento funcional de seguridad del CC. Generalmente se seleccionan todos los elementos funcionales de un componente. Se hace referencia a cada elemento mencionado por una notación simplificada que tiene la estructura siguiente:

FXX_YYY.M.N (p.e. FDP_IFF.4.2)
donde:

- F – requerimiento funcional
- XX – clase
- YYY – familia
- M – *emésimo* componente
- N – *enésimo* elemento del componente

Los elementos que seleccionamos se muestran en el Apéndice A.3.

3.3.4 Criterio de Evaluación de Sistemas de Cómputo Seguros (TCSEC), US DoD 5200.28-STD o Libro Naranja. [26]

El criterio definido en este documento clasifica a los sistemas en cuatro divisiones jerárquicas de protección de seguridad. Ellas proporcionan una base para la evaluación de la efectividad de controles de seguridad implementados en productos de procesamiento de datos. El Libro Naranja define cuatro extensas divisiones jerárquicas de seguridad para la protección de la información. En orden creciente de confiabilidad se tienen:

D- Protección Mínima. Esta división contiene solamente una clase. Esta reservada para los sistemas que han sido evaluados pero que no pueden cumplir los requisitos para una clase más alta de la evaluación.
C- Protección Discrecional. Las clases en esta división proporcionan una protección discrecional (necesidad de identificación) y, a través de inclusión de capacidades de auditoría, exige la responsabilidad de los usuarios de las acciones que realiza. La protección discrecional se aplica a una Base de Computadoras Confiables (TCB) con protección de objetos optativos (p.e. archivo, directorio, dispositivos, etc.).
B- Protección Obligatoria. La división B especifica que el sistema de protección del TCB debe ser obligatorio, no

[26] *Trusted Computer Systems Evaluation Criteria* (TCSEC), US DoD 5200.28-STD, December 1985.

sólo discrecional. La noción de un TCB que preserve la integridad de etiquetas de sensibilidad de la información y se utilizan para hacer cumplir un conjunto de reglas obligatorias del control de acceso, es un requisito importante en esta división. Los sistemas en esta división deben llevar las etiquetas de sensibilidad en las estructuras de datos importantes del sistema.
A-Protección Verificada. Se caracteriza por el uso de métodos formales para la verificación de seguridad y así garantizar que los controles de seguridad obligatoria y discrecional empleados en el sistema. Se requiere de amplia documentación para demostrar que el TCB resuelve los requisitos de seguridad en todos los aspectos del diseño, desarrollo e implementación. Se deben de cubrir todos los requisitos de B3 más otros criterios adicionales.

Tabla 3. 1 Categorías de seguridad

Cada división consiste en una o más clases numeradas, entre más grande sea el número se indica un mayor grado de seguridad. La división C contiene dos distintas clases C1 y C2. La división B contiene 3 clases B1, B2 y B3. La división A cuenta con solo una clase A1. Cada clase se define con un grupo específico de criterios que un sistema debe cubrir, para ser certificado con la evaluación en alguna clase. Este criterio cae en 4 categorías generales: Políticas de seguridad, Responsabilidad, Confianza y Documentación.

Se tienen seis requisitos fundamentales; cuatro de ellos parten de la necesidad de proporcionar un control de acceso a la información y los dos restantes de cómo puede obtenerse una seguridad demostrable, logrando así un sistema informático confiable.

1 POLÍTICA DE SEGURIDAD - Debe existir una política de seguridad explícita y bien definida reforzada por el sistema.
2 MARCAS - El control de acceso por etiquetas debe de estar asociado a los objetos. Marcar cada objeto con una etiqueta que identifique confiablemente el nivel de la sensibilidad del objeto y/o los modos de obtener acceso y acordar quien puede tener acceso potencial al objeto.
3 IDENTIFICACIÓN - Los eventos individuales deben de ser identificados. Cada acceso a la información debe ser registrado teniendo como base quién está teniendo acceso a la información y qué autorización posee para ocupar cierta clase de información.
4 RESPONSABILIDAD - Las auditorías de la información deben ser selectivamente guardadas y protegidas de las acciones que puedan afectar la seguridad y de esta forma poder rastrear al responsable.
5 ASEGURAMIENTO - El sistema informático debe contener los mecanismos de hardware/software que puedan ser evaluados independientemente para proporcionar una seguridad suficiente que el sistema haga cumplir los requisitos 1 a 4 mencionados anteriormente.
6 PROTECCIÓN CONTINUA - Los mecanismos de seguridad que hacen cumplir estos requisitos básicos, se deben de proteger continuamente contra cambios no autorizados o modificaciones que traten de alterarlos.

Tabla 3. 2 Requisitos de seguridad

Se tienen 27 características o controles en las 6 clases, agrupadas en 4 requisitos. Se han seleccionado aquéllos que más se podrían relacionar con la seguridad en redes, aunque parece que el Libro Naranja está más bien enfocado a la seguridad de sistemas, y sobre todo, a las divisiones o niveles de seguridad. Los controles se muestran en el Apéndice A.4.

3.3.5 FISCAM. [27]

La metodología general para auditoría de este documento consta de 4 fases: planeación, control interno, testeo y reporte.

Planeación.

El auditor obtiene un entendimiento de las operaciones, controles y riesgos relacionados (Usar Apéndices I y II del FISCAM). En vista de esos riesgos, el auditor tentativamente concluye cuáles controles son probablemente efectivos. En este caso y si son relevantes para los objetivos de auditoría, el auditor debe determinar la naturaleza y extensión del trabajo de auditoría necesario para confirmar sus conclusiones tentativas. Si los controles no son probablemente efectivos, el auditor debe obtener un suficiente entendimiento de los riesgos de control relacionados para (1) desarrollar averiguaciones apropiadas y (2) determinar la naturaleza, tiempo y extensión del testeo que será necesitado.

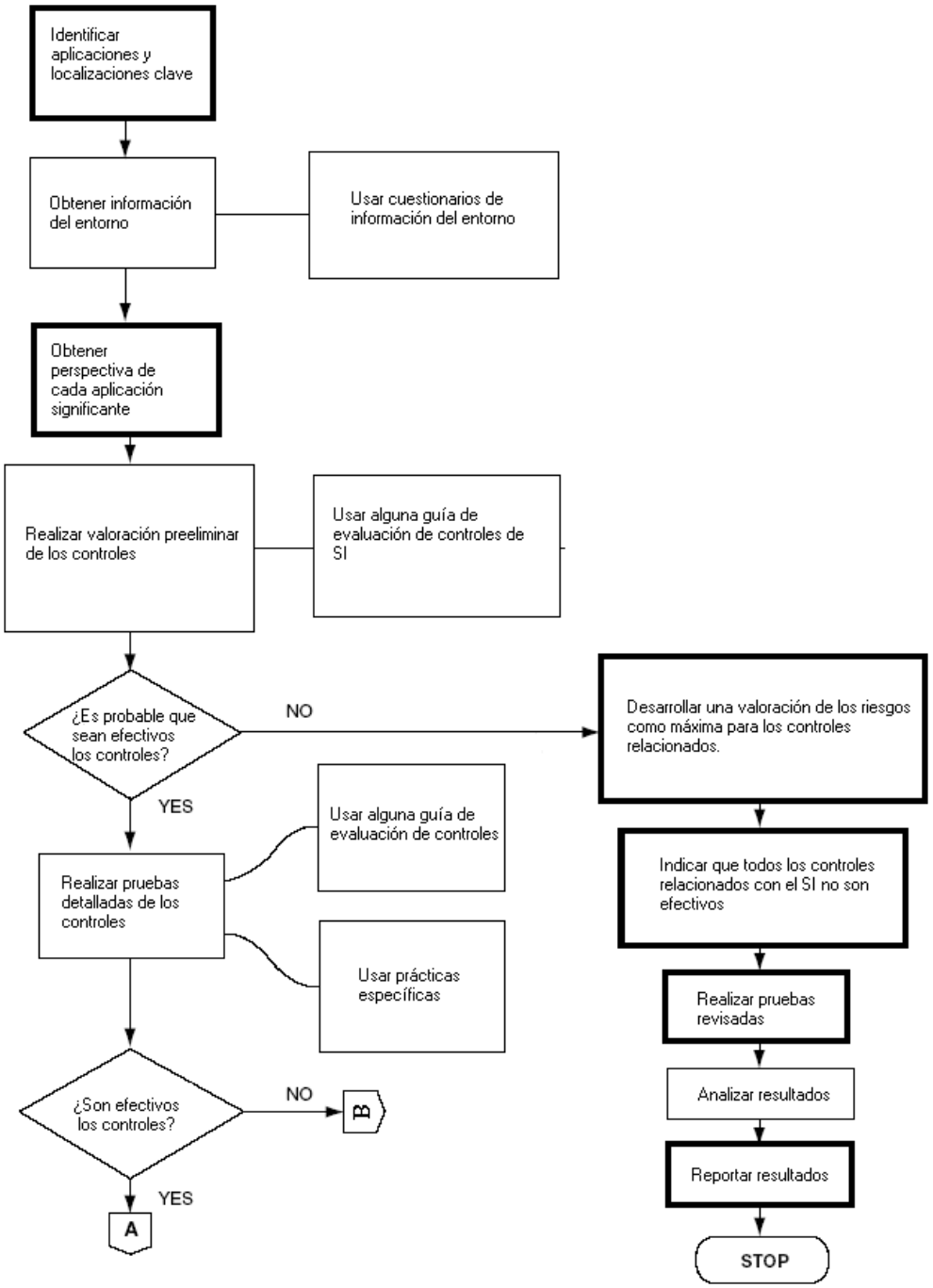
Control interno.

Los auditores obtienen información detallada con las políticas de control, procedimientos y objetivos, y realizan pruebas de actividades de control. Los objetivos de estas pruebas son para determinar si los controles están operando efectivamente. Primero se prueban los controles generales con procedimientos como observación, preguntas e inspección.

Reporte.

El auditor saca conclusiones y reportes. El reporte debe incluir cada debilidad en términos de los criterios relacionados, la condición identificada, la causa de la debilidad y el actual o potencial impacto en la entidad. Consideramos de importancia el siguiente diagrama de flujo del FISCAM, donde se detalla el proceso de una auditoría.

[27] *Federal information system controls audit manual* (GAO/AIMD-12.19.6), United States General Accounting Office, January 1999.


Identificar aplicaciones y localizaciones clave
Obtener información del entorno
Usar cuestionarios de información del entorno
Obtener perspectiva de cada aplicación significante
Realizar valoración preeliminar de los controles
Usar alguna guía de evaluación de controles de SI
¿Es probable que sean efectivos los controles?
NO
YES
Desarrollar una valoración de los riesgos como máxima para los controles relacionados.
Usar alguna guía de evaluación de controles
Realizar pruebas detalladas de los controles
Usar prácticas específicas
Indicar que todos los controles relacionados con el SI no son efectivos
Realizar pruebas revisadas
Analizar resultados
¿Son efectivos los controles?
NO
B
YES
A
Reportar resultados
STOP

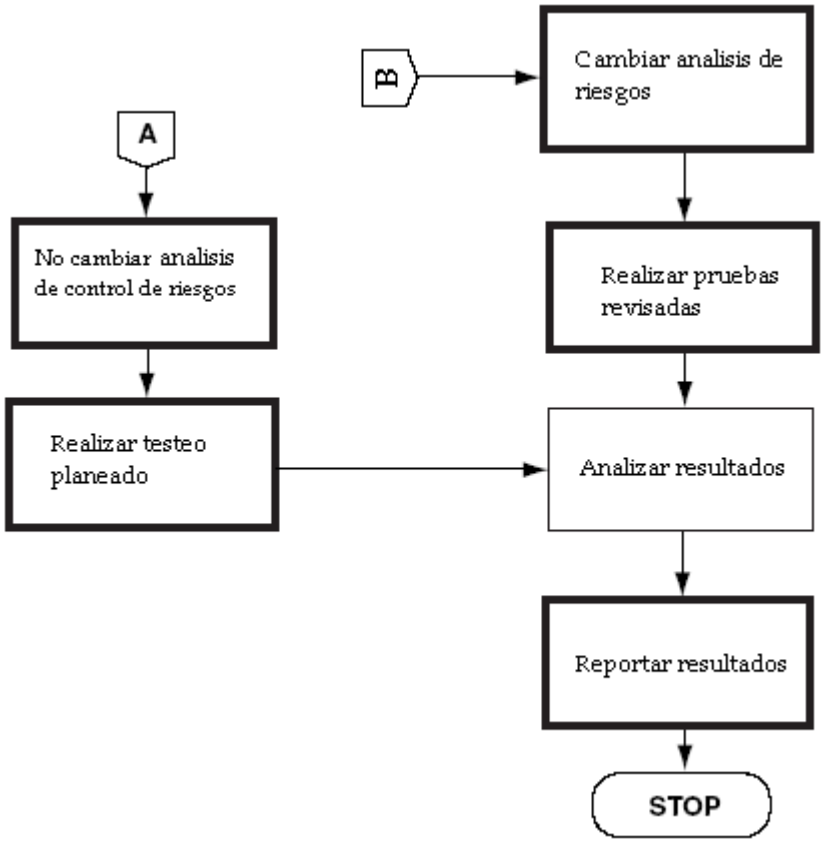


Figura 3. 1 Pasos en el análisis de controles de auditoría

3.3.6 NIST 800-42. [28]

Recomendaciones del NIST:

- Hacer del examen de seguridad de redes una rutina y parte integral del sistema, de las operaciones y la administración de la red.
- Examinar primero los sistemas más importantes: aquellos sistemas que son públicamente accesibles, esto es, routers, firewalls, web servers, e-mail servers y algún sistema que esté abierto al público o de misión crítica.
- Ser precavido al examinar: algunos tipos de exámenes pueden imitar los signos de un ataque. Por eso es imperativo que se haga de manera coordinada con el consentimiento y conocimiento de los funcionarios apropiados.
- Asegurar que las políticas de seguridad reflejan exactamente las necesidades de la organización: las políticas deben ser usadas como una base de comparación con los resultados del examen.
- Integrar el examen de seguridad en el proceso de gestión de riesgos.
- Asegurar que los administradores de red y del sistema están entrenados y son capaces.

[28] NIST, SP 800-42, *Guideline on Network Security Testing*, October 2003.

- Asegurar que los sistemas están actualizados con parches.
- Entender las capacidades y limitaciones del examen de vulnerabilidad.

El testeo (o examen, prueba, etc.) de seguridad es quizá el determinante más concluyente de si un sistema está configurado y continuará configurado para los controles y políticas de seguridad correctas. Las pruebas sugeridas en este documento están dirigidas principalmente a:

- Firewalls, internos y externos.
- Routers y switches.
- Sistemas relacionados con la seguridad perimetral de red, como IDS's.
- Web servers, email servers, y otros servidores de aplicación.
- Otros servidores como DNS o directory servers o file servers (NFS, FTP, etc.).

Estos sistemas deberían ser examinados en primer lugar antes de proceder con el equipo general y sistemas relacionados. Las pruebas descritas en este documento son aplicables mientras los sistemas están corriendo en sus entornos.

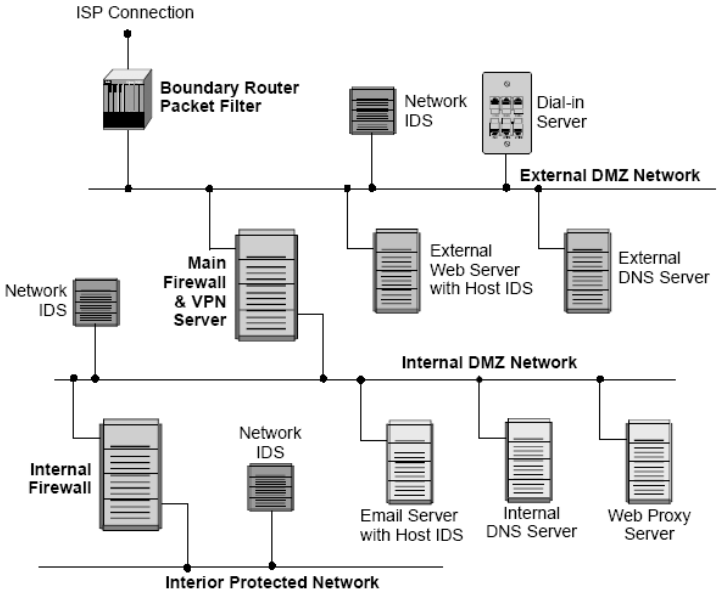


Figura 3. 2 Sistemas de misión crítica para examen inicial

Los resultados de los exámenes de seguridad pueden ser usados de las siguientes formas:

- Como un punto de referencia para una acción correctiva.
- En la definición de actividades de mitigación para hacer frente a vulnerabilidades identificadas.
- Como un punto de referencia para examinar el progreso de una organización en el conocimiento de los requerimientos de seguridad del sistema.
- Para valorar el status de la implementación de los requerimientos de seguridad del sistema.

- Para conducir un análisis de costo/beneficio para mejoras al sistema de seguridad.
- Para mejorar otras actividades del ciclo de vida, como análisis de riesgos, certificación, autorización y realización de mejoras.

TÉCNICAS DE EXAMEN DE SEGURIDAD.

Escaneo de red.

Implica el uso de escaneo de puertos para identificar todos los hosts potencialmente conectados a una red organizacional, los servicios de red operando en aquellos hosts (como el HTTP, FTP, etc.) y las aplicaciones específicas corriendo el servicio identificado. Algunos escáneres proporcionan información adicional con la que se puede identificar el SO objetivo (OS fingerprinting). Sin embargo, los escáneres de puertos no identifican vulnerabilidades. Estas sólo pueden ser identificadas por humanos que interpretan el mapeo y los resultados del escaneo.

Las organizaciones deberían realizar el escaneo de red para:

- Buscar hosts no autorizados conectados a la red organizacional.
- Identificar servicios vulnerables.
- Identificar desviaciones de los servicios permitidos definidos en las políticas de seguridad.
- Prepararse para la prueba de penetración.
- Ayudar en la configuración de IDS's.
- Colectar evidencia forense.

Se necesita un alto nivel de habilidad y experiencia para interpretar los resultados. El escaneo puede también interrumpir las operaciones de red al consumir el ancho de banda y retrasando los tiempos de respuesta de red. Para evitar esto, el software de escaneo debe ser cuidadosamente seleccionado y la operación puede ser realizada después de horas de operación, pero algunos sistemas pueden estar apagados. Los resultados del escaneo de red deben ser documentados y las siguientes acciones correctivas pueden ser recomendadas y/o realizadas:

- Investigar y desconectar los hosts no autorizados.
- Inutilizar o remover servicios no necesarios y vulnerables.
- Modificar los hosts vulnerables para restringir el acceso a los servicios vulnerables a un número limitado de hosts requeridos.
- Modificar los firewalls para restringir el acceso exterior a los servicios vulnerables conocidos.

Escaneo de vulnerabilidad.

Los escáneres de vulnerabilidad proporcionan información sobre las vulnerabilidades asociadas e incluso sobre como mitigarlas. Es un medio rápido y fácil para cuantificar la exposición de la organización a las vulnerabilidades de superficie, sin embargo, no reconoce el peligro de vulnerabilidades combinadas, dando un panorama engañoso. Esto se corrige añadiendo un examen de penetración. Los escáneres de vulnerabilidad también pueden reconocer versiones de software expiradas, parches aplicables o actualizaciones del sistema y validar el cumplimiento con las políticas de seguridad de la organización. Estos escáneres emplean grandes bases de datos de vulnerabilidades. En adición, pueden hacer correcciones y reparar algunas vulnerabilidades descubiertas.

Aunque el proceso es altamente automatizado, en ocasiones reporta vulnerabilidades donde no existen. Esto significa que un individuo con experiencia y habilidad en redes y seguridad en sistemas operativos debe interpretar los resultados. Como estos escáneres necesitan más información para identificar las vulnerabilidades, tienden a generar más tráfico que los escáneres de puertos. Otra limitación es que dependen de la constante actualización de la base de datos para reconocer las últimas vulnerabilidades. Los escáneres de vulnerabilidad tienen las siguientes habilidades:

- Identifican los hosts activos en la red.
- Identifican los servicios activos y vulnerables en los hosts.
- Identifican las aplicaciones.
- Identifican SO’s.
- Identifican vulnerabilidades asociadas con los SO’s y aplicaciones encontradas.
- Identifican configuraciones erróneas.
- Prueba de cumplimiento con políticas de seguridad/uso de los hosts.
- Establece una base para la prueba de penetración.

Las siguientes acciones correctivas pueden ser recomendadas y/o realizadas como resultado del escaneo de vulnerabilidad:

- Actualizar o parchar sistemas vulnerables para mitigar las vulnerabilidades identificadas como sea apropiado.
- Desplegar medidas mitigantes si el sistema no puede ser inmediatamente parchado.
- Mejorar el programa de administración de configuraciones y procedimientos para asegurar que los sistemas son actualizados continuamente.
- Asignar personal para monitorear las alertas de seguridad, examinar su aplicabilidad a la organización e iniciar los cambios apropiados al sistema.
- Modificar las políticas de seguridad de la organización, arquitectura u otra documentación para asegurar que las practicas de seguridad incluyen migraciones y actualizaciones oportunas.

Password cracking.

El password cracking verifica que los usuarios están empleando passwords suficientemente fuertes. Las siguientes acciones correctivas pueden ser recomendadas y/o realizadas como resultado del password cracking:

- Si los passwords crackeados fueron seleccionados de acuerdo a la política, esta debería ser modificada para reducir el porcentaje de passwords crackeados.
- Si los passwords crackeados no fueron seleccionados por medio de una política, los usuarios deben ser educados en los impactos posibles de las selecciones mal realizadas. Si las violaciones por el usuario son persistentes se deben considerar pasos adicionales para obtener el cumplimiento.

Revisiones de logs.

Varios logs del sistema pueden ser usados para identificar desviaciones de las políticas de seguridad, incluyendo firewall logs, IDS logs o server logs. La revisión manual de los logs es extremadamente engorrosa y consume mucho tiempo. Herramientas de auditoría automatizada proporcionan medios para reducir el tiempo de revisión requerido y para generar reportes que resuman el contenido de los logs de un conjunto de actividades específicas. Las siguientes acciones pueden ser recomendadas si el sistema no está configurado de acuerdo a las políticas:

- Remover servicios vulnerables si no son necesitados.
- Reconfigurar el sistema para reducir la oportunidad de comprometerlo.
- Cambiar la política del firewall para limitar el acceso al sistema o servicio vulnerable.
- Cambiar la política del firewall para limitar los accesos desde la subred IP que es el origen del compromiso.

Probadores de integridad de archivos.

Un probador de integridad de archivos computa y almacena un checksum por cada archivo guardado y establece una base de datos de checksums de archivos. Esto proporciona una herramienta para el administrador/auditor para reconocer cambios a archivos, particularmente cambios no autorizados. Los checksums almacenados deberían ser recomputarizados regularmente para probar el valor actual contra el valor almacenado para identificar cualquier modificación. Un probador de integridad de archivos es usualmente incluido con cualquier sistema de detección de intrusiones basado en host. Si se detectan modificaciones de esta forma, la posibilidad de un incidente de seguridad debería ser considerada e investigada de acuerdo a las políticas de respuesta a incidentes y sus procedimientos.

Detectores de virus.

Se deben recomendar los siguientes pasos:

- Los archivos de definición de virus deben ser actualizados al menos semanalmente y cuando un brote de un virus nuevo ocurre.

- El software antivirus debe ser configurado para correr continuamente en segundo plano y si es posible, usar heurística para buscar virus.
- Después que la definición de virus es actualizada, debe ser hecho un escaneo completo del sistema.

Examen de WLAN (War Driving).

Los riesgos adicionales en redes inalámbricas resultan cuando los access points son configurados en el modo de seguridad menor. Una organización necesitará probar periódicamente sus redes de WLAN no autorizadas o mal configuradas y escanear sus sitios de señales entrantes de vecinas WLAN. Creando una o más computadoras portables con tarjetas de red inalámbricas y herramientas de prueba para detectar WLAN, ayudará en este esfuerzo. La frecuencia para probar WLAN dependerá de algunos factores:

- Factores físicos de la localización a ser examinada.
- El nivel de amenaza con que se enfrenta la organización.
- El control organizacional sobre recursos de red.
- El uso de técnicas de seguridad más robustas en la red como WPA (Wi-Fi Protected Access) o RSN (Robust Security Network).
- Sensitividad de los datos en la red.

Se deberá recomendar que cuando existen grandes amenazas se debería realizar ese examen al menos mensualmente. También son recomendadas auditorías aleatorias.

Prueba de penetración.

Es la prueba de seguridad en la que los evaluadores intentan evitar las características de seguridad de un sistema, basados en el entendimiento de su diseño e implementación. Su propósito es identificar los métodos para obtener acceso usando herramientas y técnicas similares a las de los atacantes. La prueba de penetración deberá ser realizada después de una cuidadosa consideración, notificación y planeación. Al menos, puede alentar el tiempo de respuesta de la red debido al escaneo de red y de vulnerabilidad. Es posible que los sistemas puedan ser dañados en el curso de la prueba de penetración y puedan quedar inoperables. Aunque este riesgo es mitigado por el uso de examinadores de penetración experimentados, nunca está completamente eliminado. Como la prueba de penetración es diseñada para simular un ataque y usa herramientas y técnicas que pueden estar restringidas por la ley, regulaciones federales y políticas organizacionales, es imperativo obtener permiso formal para conducir este examen. Este permiso debe incluir:

- Direcciones/rangos IP específicas a ser examinadas.
- Hosts restringidos.
- Una lista de técnicas de prueba aceptables y herramientas.
- Horas en que serán realizadas las pruebas.
- Identificación de un periodo definido para los exámenes.

- Direcciones IP de las máquinas desde las cuáles serán conducidas las pruebas de penetración para que los administradores puedan diferenciar los ataques de prueba de penetración legítimos de los ataques maliciosos.
- Sistemas y redes objetivo.
- Medidas para prevenir cumplimientos legales de estas falsas alarmas.
- Manejo de la información colectada por el equipo de prueba de penetración.

Una prueba de penetración puede ser diseñada para simular un ataque interno o externo. Si ambos son realizados, el exterior deberá ser primero. La simulación externa considera que no se tiene más información que las direcciones/rangos IP objetivos. En la prueba de penetración interna los examinadores poseen algún nivel de acceso a la red y la información que un usuario con ese privilegio les podría proporcionar.

La prueba de penetración consiste en cuatro fases. En la fase de planeación las reglas son identificadas, la aprobación de la administración está finalizada y los objetivos son identificados. En la fase de descubrimiento se escanea la red para identificar objetivos potenciales. La segunda etapa de la fase de descubrimiento es el análisis de vulnerabilidad. La ejecución del ataque es el corazón de la prueba de penetración. Si el ataque es exitoso, la vulnerabilidad es verificada y las garantías son identificadas para mitigar la exposición de seguridad asociada. Frecuentemente, los logros del ataque no conceden el máximo nivel de acceso, por lo que el proceso se repite desde el descubrimiento. La fase de reporte ocurre simultáneamente con las otras tres fases y al final de la prueba se elabora un reporte general para describir las vulnerabilidades identificadas, proporcionar un índice de riesgo y para dar guía en la mitigación de las debilidades descubiertas.

La prueba de penetración es importante para determinar que tan vulnerable es la red de la organización y el nivel de daño que puede ocurrir si la red está comprometida. A causa del alto costo y del impacto potencial, puede ser suficiente realizarla anualmente. Los resultados deberían ser tomados muy seriamente y las vulnerabilidades descubiertas mitigadas. Los resultados deberían ser presentados prontamente a los directivos. Las medidas correctivas recomendadas/realizadas incluyen cerrar las vulnerabilidades descubiertas y explotadas, la modificación de las políticas de seguridad, crear procedimientos para mejorar las prácticas de seguridad y conducir un entrenamiento en concientización de seguridad para asegurar que entienden las implicaciones de pobres prácticas de seguridad y malas configuraciones del sistema. Si se realizan otras pruebas en el sistema (p.e. escaneo de red y de vulnerabilidad) servirán como preparación para el siguiente ejercicio de prueba de penetración y prepararse para un ataque real.

Acciones después de la prueba.

Estos exámenes revelan asuntos que necesitan ser dirigidos rápidamente. La manera como estos asuntos son dirigidos y mitigados, es la parte más importante del proceso de pruebas. Las causas y métodos más comunes para dirigirlos son los siguientes:

- Carencia o pobres políticas de seguridad organizacionales: las políticas son importantes porque aseguran la consistencia.

- Malas configuraciones: ocurre cuando un sistema no es configurado en una manera segura o recomendada. Hay varias acciones para remediar o minimizar las posibilidades de configuración errónea:
  1. Crear un proceso de administración de configuraciones para sistemas críticos y redes. Este proceso controla los cambios realizados a un sistema o red y asegura su cumplimiento con las políticas. No debe entorpecer la aplicación a tiempo de actualizaciones y parches de seguridad.
  2. Crear checklists de configuración (o usar las completamente disponibles). Están disponibles de muchas fuentes incluyendo agencias Federales, vendedores e individuos.
- Software no fiable: para el software desarrollado por la organización, los procedimientos apropiados para desarrollo y prueba de código deberían ser implementados. Para el software de vendedores se deberían regularmente revisar las actualizaciones y parches de los vendedores y aplicarlos de manera oportuna.
- Fallo en la aplicación de parches: muchos administradores no tienen tiempo, recursos o conocimiento para aplicar parches en forma oportuna.

Los resultados del examen podrían mostrar también la necesidad de realizar cambios de gran escala en la red y en la arquitectura de seguridad de la organización. Algunos principios que siempre se deben tener en mente son:

- Simplicidad.
- Fallo seguro.
- Mediación completa.
- Diseño abierto.
- Separación de privilegios.
- Aceptabilidad psicológica.
- Defensa estratificada.
- Grabación de transgresiones.

Estrategias para la prueba de seguridad.

1) Determinar la categoría de seguridad del SI.

Basándose en la publicación del FIPS 199, las categorías están basadas en el impacto potencial cuando ciertos eventos ponen en peligro los SI. Estas categorías de seguridad son usadas en conjunción con información de vulnerabilidades y amenazas en al análisis de riesgos. FIPS Publication 199 define tres niveles de impacto potencial:

- Impacto potencial bajo: con efecto adverso limitado en operaciones, bienes e individuos.
- Impacto potencial moderado: con efecto adverso serio.
- Impacto potencial alto: con efecto adverso severo o catastrófico.

2) Determinar el costo por sistema al realizar cada tipo de prueba.

El costo depende de algunos factores:

- Tamaño del sistema a ser examinado.
- Complejidad del sistema a ser examinado (una red con distintos SO's es más costosa).
- Nivel de interacción humana requerido por cada prueba.
- La factibilidad de seleccionar una muestra para hacer las pruebas y determinar el tamaño de dicha muestra (no tienen sentido en técnicas más sencillas como el escaneo de red pero sí para la prueba de penetración).

3) Identificar los beneficios de cada tipo de prueba por sistema.

Para asegurarse que el costo de las pruebas no excede su valor, los beneficios deben ser identificados y cuantificados como sea posible. Tomar en cuenta el valor del conocimiento de los sistemas y redes, la probabilidad reducida de una intrusión exitosa o de una disrupción.

4) Priorizar los sistemas a examinar.

Con los resultados anteriores se deben priorizar los sistemas para el examen de seguridad. Se debería realizar una lista clasificada por categoría de seguridad, costo y beneficio. Los recursos disponibles deberían ser identificados y comparados con los recursos requeridos. Se considera un examen mínimo para los sistemas con más alto impacto. Después que los recursos son identificados para los sistemas críticos, los sistemas de menor prioridad pueden ser probados con menor frecuencia.

3.3.7 OSSTMM 2.1. [29]

El objetivo de este manual es crear un método aceptado para ejecutar un test de seguridad minucioso. Se presentan una serie de pasos que deben ser vistos durante la realización de un test exhaustivo. Lo más importante en esta metodología es que los diferentes tests son evaluados y ejecutados donde sean aplicables, hasta arribar a los resultados esperados dentro de un período de tiempo determinado. Solo así el testeador habrá ejecutado el test en conformidad con el modelo OSSTMM, y por ello, el informe podrá ser considerado mínimamente exhaustivo.

Esta metodología cubre únicamente el testeo de seguridad externo, es decir, testear la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, para evadir los componentes de seguridad, procesos y alarmas y ganar acceso privilegiado. Está también dentro del alcance de este documento proveer un método estandarizado para realizar un exhaustivo test de seguridad de cada sección con presencia de seguridad (por ejemplo, seguridad física, seguridad inalámbrica, seguridad de comunicaciones, seguridad de la información, seguridad de las tecnologías de Internet y seguridad de procesos) de una organización.

[29] OSSTMM 2.1. *Manual de la Metodología Abierta de Testeo de Seguridad*. ISECOM.

El test de seguridad descrito es un test práctico y eficiente de vulnerabilidades conocidas, filtraciones de información, infracciones de la ley, estándares de la industria y prácticas recomendadas. ISECOM exige que un test de seguridad solamente sea considerado un test OSSTMM si es:

- Cuantificable.
- Consistente y que se pueda repetir.
- Válido mas allá del período de tiempo "actual".
- Basado en el mérito del testeador y analista, y no en marcas comerciales.
- Exhaustivo.
- Concordante con leyes individuales y locales y el derecho humano a la privacidad.

Para mayor claridad, ISECOM aplica los siguientes términos a los diferentes tipos de testeos de seguridad de redes, basados en tiempo y costo:

1. Búsqueda de vulnerabilidades: se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.
2. Escaneo de la seguridad: se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.
3. Test de intrusión: se refiere en general a los proyectos orientados a objetivos en los cuales se incluye ganar acceso privilegiado.
4. Evaluación de riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación de negocios, las justificaciones legales y las justificaciones específicas de la industria.
5. Auditoría de seguridad: hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.
6. Hacking ético: se refiere generalmente a los tests de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.
7. Test de seguridad: es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

SEGURIDAD “PERFECTA”

Inalámbricos:

- El uso de características de seguridad sería una solidez.
- Poner en cuarentena y verificar todos los dispositivos inalámbricos antes de aceptarlos.
- Mantener establecidos los límites de la distancia y la fuerza de la señal inalámbrica.
- Límites confiables (para sistemas y usuarios).

- Encriptar todo el tráfico.
- Permitir únicamente la accesibilidad con responsabilidad.
- Capa de seguridad.
- Tratar a los dispositivos inalámbricos como redes separadas de los ya establecidos.
- Provocar una alarma en los accesos de cuentas fallidas o duplicadas.
- Monitorear y registrar la accesibilidad de todo tráfico de comunicaciones no expresadas.
- No permitir y limitar puenteos no autorizados de inalámbricos a cableados.
- Nodos descentralizados.

Entrada (gateway) y servicios de Internet:

- No desencriptar accesos remotos.
- No desautenticar accesos remotos.
- Negar toda restricción y permitir específicamente.
- Monitorearlo y registrarlo todo.
- Descentralizar.
- Límite de confianza inter-sistemas.
- Poner en cuarentena todas las entradas y validarlas.
- Instalar solo las aplicaciones/demonios necesarios.
- Capa de seguridad.
- Invisible es mejor, no mostrar nada excepto los propios servicios.
- Prevenir errores de configuración.

Aplicaciones:

- El uso de características de seguridad serían una solidez.
- Asegurar las justificaciones de los asuntos de todas las entradas y salidas en la aplicación.
- Poner en cuarentena y validar todas las entradas.
- Limites confiables (para sistemas y usuarios).
- Encriptación de datos.
- Revolver los componentes.
- Todas las acciones ocurren en el lado del servidor.
- Capa de seguridad.
- Invisible es mejor, mostrar los propios servicios.
- Provocarlo para alarma.

Gente:

- Autoridad descentralizada.
- Responsabilidad personal.
- Controles de seguridad y privacidad personal.
- Accesible sólo a través del gateway personal.
- Legalidad y ética entrenada y definida de las políticas de seguridad.

- Limitar la necesidad de conocer el acceso a la información e infraestructura.

De las distintas secciones del OSSTMM, consideramos de importancia la sección (C) que se incluye en el apéndice A.

3.4 Situación de la auditoría informática en México.

El auditor interno. [30]

En promedio, si empresas grandes cuentan con un personal de 150 personas en Reingeniería, de las cuales la mitad (75) son de auditoría, únicamente 1 o 2 son auditores internos en TI.

Inicialmente los auditores en TI eran auditores contadores. Ahora los auditores en TI son ingenieros que no pierden la base de la auditoría financiera tradicional. Un auditor en TI por supuesto da el soporte al área de Auditoría, pero como ésta no es continua, muchas veces realizan el trabajo de Soporte o Sistemas. Estos auditores están (o deben estar) integrados con las demás áreas de la Auditoría en la forma de Auditorías Integrales.

Estos auditores cuentan con el respaldo de muchos organismos, como lo son el Instituto de Auditores Internos e ISACA, y marcos de referencia especializados, como el COSO, COBIT, algunas ISO's, BS, etc.; todo esto constituye demasiada información y hace falta tiempo para poderla comprender y aplicar correctamente.

Ahora bien, ¿cuál es el papel de la auditoría interna de TI en la organización? ¿Qué necesita del auditor la alta Gerencia? En primer lugar, los resultados de la auditoría deben agregar valor, no gastos; esto es, aumentar ingresos. Para ello hay que presentar informes de alto impacto y hay que considerar que las empresas no sólo quieren cumplir con las leyes, sino generar ganancias. Además, la auditoría interna es una excelente oportunidad para obtener una radiografía de la empresa y para tener una idea global del control interno.

Otro aspecto de la auditoría es que debe utilizar un lenguaje de negocios al presentar los hallazgos. Se debe considerar el problema, su cuantificación e impacto en el negocio; estos son factores cruciales para su entendimiento y consideración por la alta Gerencia. Por ejemplo se tiene lo siguiente en un informe:

"Detectamos 20 cuentas de empleados que ya no trabajan en la empresa que podrían ser utilizadas para afectar la integridad de la información".

El lenguaje a usar debe ser no menos técnico pero sí considerar el impacto en el negocio:

"De un total de 100 cuentas identificamos 5 casos que corresponden a empleados que ya no trabajan en la empresa desde hace un año, que cuentan con atributos para modificar información y que en los últimos 3 meses han tenido actividad. Aunque no se identificaron afectaciones existe el riesgo de realizar transacciones no autorizadas".

[30] Información proporcionada en la conferencia *Bajo la lupa: la perspectiva del auditor*, por Aurelio Jaimes Peña, Gerente de Auditoría de Sistemas, TELMEX, en el Business Innovation Forum 2005 de Netmedia.

Un requisito más de la función de auditoría es que debe promover soluciones concretas, citando al responsable y la fecha del compromiso. Además debe promover las soluciones que corrijan el efecto y la causa. Ejemplo:

"Recomendación: Eliminar las cuentas identificadas".

Sustituir por:

"El Ing. Juan Jiménez, Administrador del Sistema de Inventarios, eliminará las cuentas identificadas el 30 de Octubre 2005 y desarrollará e implementará procedimiento para revisar periódicamente la vigencia y atributos de los usuarios".

Por último debe asegurar el cumplimiento de los compromisos, o sea, se debe realizar un seguimiento.

El auditor externo.

Según Diódoro Batalla, Gerente CARe de Mancera Ernst & Young, el auditor externo tiene cuatro papeles importantes en la empresa:

1. Apoyar en la evaluación del control interno (apoyo a al auditoría interna).
2. Implementar ERP's.
3. Examinar controles de TI.
4. Mejorar la eficiencia y efectividad del negocio.

Por su parte Carlos Zamora Sotelo, Presidente de ISACA Capítulo México, menciona tres roles del auditor externo:

1. Identificar, medir y controlar riesgos por el uso de TI (administración de riesgos).
2. Agregar valor al negocio, evaluar si la inversión en TI da fruto (métricas).
3. Cumplimiento con regulaciones, efectividad del control y seguimiento de políticas (procesos del negocio).

Menciona también que los auditores en TI deben tener conocimiento en:

1. Leyes y regulaciones.
2. Procesos del negocio.
3. Riesgos de la organización.
4. Papel de directores, usuarios y sistemas.
5. Cultura y estrategias organizacionales.
6. Administración de proyectos.

En cuanto a la certificación CISA, de ISACA, los conocimientos que lo distinguen son:

1. Procedimientos de auditoría.
2. Leyes locales e internas que afectan a la organización.
3. Redes y telecomunicaciones.

4. Seguridad.
5. Desarrollo e implementación de SI.
6. Planes de contingencia y recuperación de desastres.
7. Administración de procesos, reingeniería y análisis de riesgos.

La metodología. [31]

Los auditores necesitan comprender el alcance de los estándares de la auditoría de IT, su aplicabilidad y cómo utilizarlos en auditorías reales. También necesitan comprender la diferencia entre los estándares técnicos que pueden ayudarlos a brindar recomendaciones de mejora, entender su uso en sus auditorías de IT, revisar cómo se realiza la selección de procesos de la gestión de tecnología de información y plataformas a auditar. Al mismo tiempo, los gerentes y personal IT necesitan conocer los criterios utilizados por los auditores, tanto internos como externos, para ahorrar tiempo en el proceso y presentar la información en la forma en que les serán requeridos.

Estas metodologías ayudan a la identificación de objetivos y prioridades del negocio, que a su vez determinan los controles que toda organización requiere:

Figura 3.3 Procesos del negocio e información

[31] Conferencia *El recurso del Método*, dictada por Lucio Molina Focazzio, Vicepresidente Internacional de ISACA, realizada en el evento anterior.

Como se puede observar, las metodologías usadas, tanto por la función auditora como por la de control interno, cubren aspectos distintos de la información como son los distintos criterios de la información y procesos de la organización:

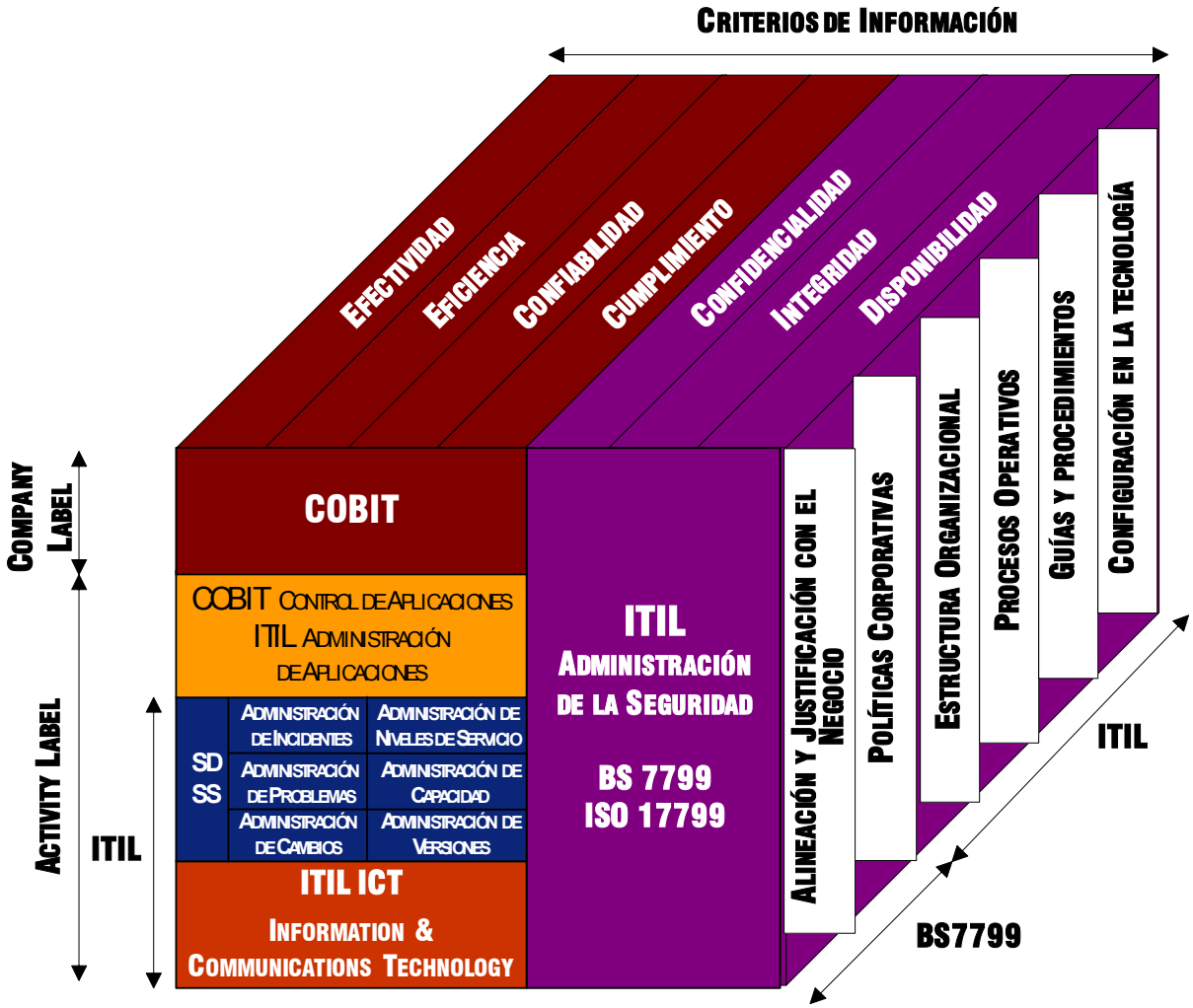


Figura 3.4 Alcance de las metodologías

Así es como algunas de estas metodologías se encuentran más enfocadas a la TI o al negocio. Así tenemos al COSO-SOX (Sarbanes-Oxley) enfocado hacia las reglamentaciones, el COBIT hacia el control y auditoría, y el BS7799 en seguridad. También se pueden categorizar como modelo de medición (COBIT, COSO, SOX) o como criterio de certificación externo (BS7799, CMM). Como se observa no todas abarcan todos los aspectos.

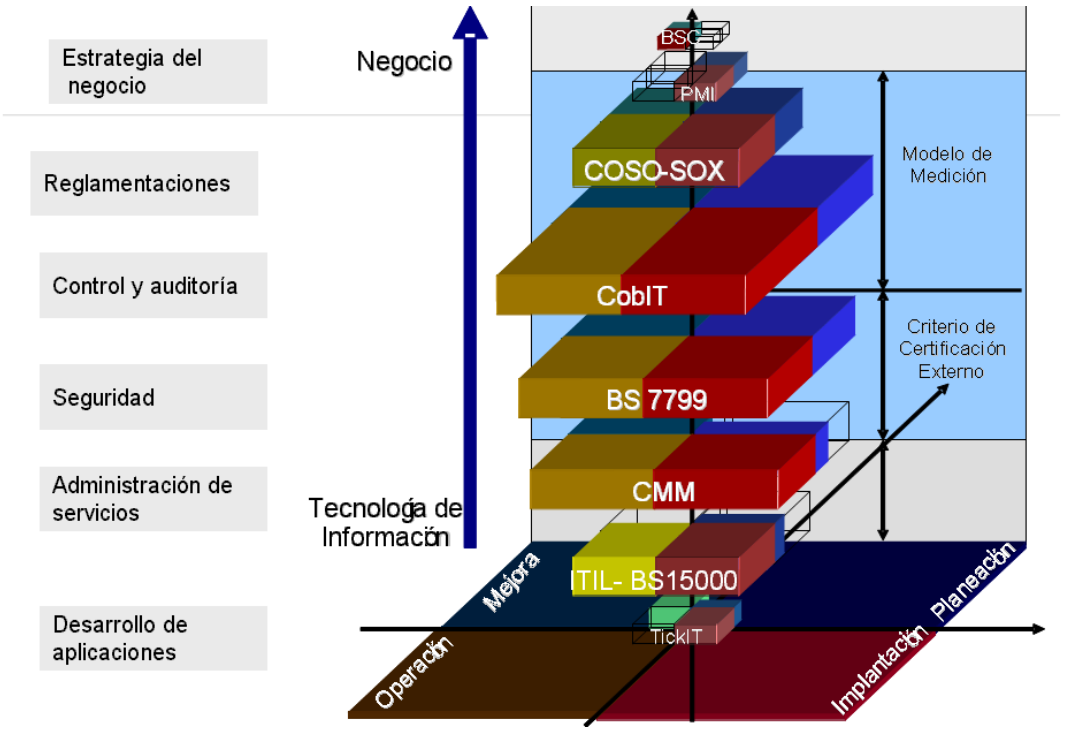


Figura 3.5 Alcance de las metodologías

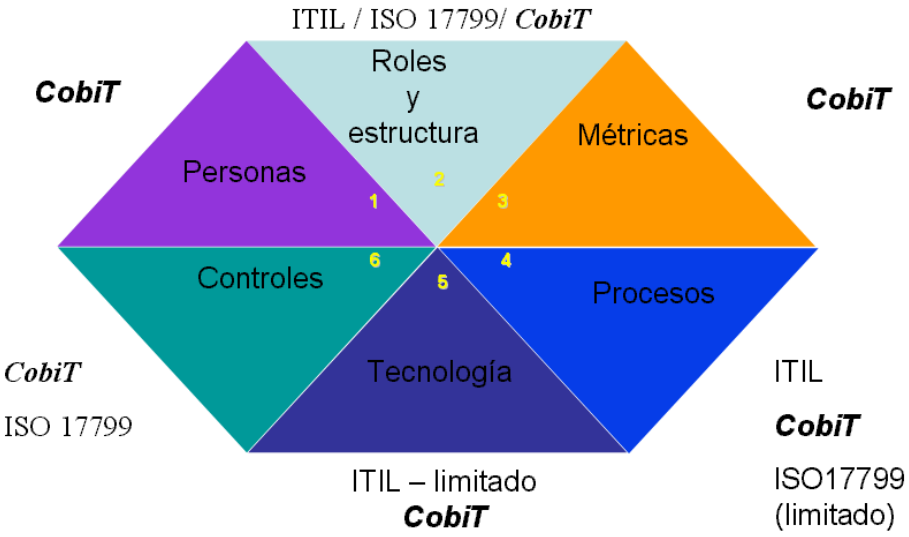


Figura 3.6 Alcance de las metodologías

El marco a elegir depende ya de los objetivos de la auditoría y su alcance, de las características de los SI y TI a auditar, y del conocimiento de los auditores.

C A P Í T U L O

I V

PROPUESTA DE UNA METODOLOGÍA DE AUDITORÍA EN SEGURIDAD INFORMÁTICA PARA LAN

CAPÍTULO IV

PROPUESTA DE UNA METODOLOGÍA DE AUDITORÍA EN SEGURIDAD INFORMÁTICA PARA LAN

4.1 Definición.

La auditoría en seguridad de LAN es un examen crítico que se realiza para evaluar la eficacia y eficiencia de la seguridad de LAN en un organismo, de sus controles, sistemas y procedimientos relacionados. Incluye el análisis, la verificación y la exposición de debilidades y disfunciones.

La metodología OSSTMM v. 2.0 hace una diferencia muy clara entre la auditoría en seguridad y otros tipos de testeo que erróneamente en la práctica se consideran iguales. Entre estos métodos de testeo la auditoría en seguridad de redes es el más costoso y el que involucra más gasto de tiempo. De esta forma, en este contexto se define a la auditoría en seguridad como a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes. En la figura siguiente se muestra la relación mencionada de la auditoría de seguridad.

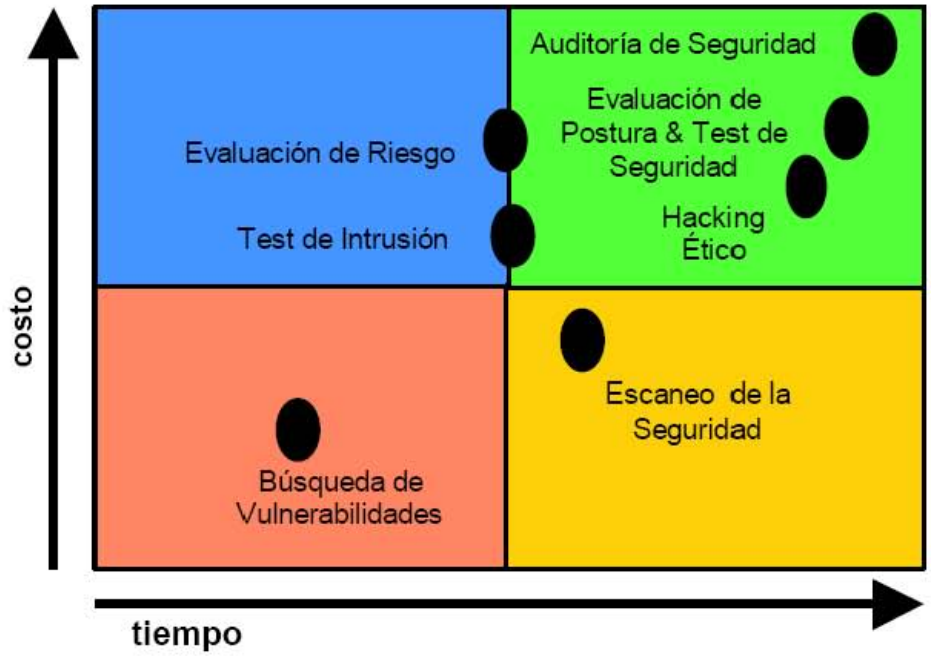


Figura 4. 1 Tipos de exámenes de seguridad

4.2 Metodología.

Aunque varía el número de pasos en las distintas metodologías de auditoría en seguridad (por ejemplo el FISCAM sólo considera cuatro) nosotros consideramos al menos ocho etapas fundamentales en esta auditoría, las cuáles son:

1. Determinación del alcance y objetivo.
2. Estudio inicial del entorno de la LAN.
3. Determinación de la muestra.
4. Determinación de los recursos necesarios.
5. Planeación.
6. Realización de la auditoría.
7. Informe.
8. Seguimiento.

A continuación expondremos en detalle estas etapas.

4.2.1. Determinación del alcance y objetivo.

El alcance debe de estar muy bien definido ya que nos expresa el límite de la misma en cuanto a los sistemas, equipos y áreas físicas y lógicas, quedando acordado entre auditores y clientes (gerencia de TI o managers de sistemas). El área a auditar es llamada sujeto de la auditoría, en este caso un organismo gubernamental. En cambio, el alcance de la auditoría identifica los sistemas específicos o áreas de la organización a ser estudiados.

En esta fase de la auditoría los auditores deben obtener un entendimiento de las operaciones de la entidad y deben identificar las operaciones más importantes que son soportadas y relacionadas con la seguridad y el correcto funcionamiento de la red.

Según la metodología OSSTMM, en la definición del ámbito de la auditoría se considera lo siguiente:

- El ámbito o alcance debe estar claramente definido contractualmente antes de verificar cualquier vulnerabilidad en los servicios de red.
- El ámbito debe explicar claramente los límites del análisis de seguridad.

Para establecer el alcance de la auditoría se debe investigar y analizar:

- Los procesos de la organización relacionados con la seguridad de información.
- Los SI's y TI's que soportan tales procesos.
- Sus riesgos inherentes, tanto de la tecnología como de los procesos mismos.

Estos riesgos se determinan identificando:

- Cambios recientes en la organización (estructura, objetivos, meta, mandos, funciones, gobierno corporativo, etc.).

- Cambios o factores tecnológicos (instalaciones, hardware y software de redes, tamaño, configuraciones, etc.).
- Incidentes recientes sobre la seguridad de la red.
- Controles de monitoreo aplicados a la red por la gerencia.
- Reportes y resultados recientes de evaluaciones internas y auditorías.
- El grado de dependencia de la organización hacia la LAN.
- El uso de software sensible que permita realizar cambios no autorizados.

El alcance tiene que figurar o incluirse expresamente en el informe final, de modo que quede perfectamente determinado no sólo hasta qué puntos se ha llegado, sino cuáles materias o áreas han sido omitidas (excepciones). La indefinición de los alcances de la auditoría compromete el éxito de la misma.

La metodología que hemos desarrollado, adaptada a un entorno gubernamental, considera dentro del área de la auditoría de seguridad en LAN las cláusulas de control siguientes (también llamadas segmentos se seguridad):

- Cláusula 1: Políticas de seguridad.
- Cláusula 2: Gobierno de la seguridad.
- Cláusula 3: Control y clasificación de bienes.
- Cláusula 4: Seguridad de los empleados.
- Cláusula 5: Seguridad física de la LAN y su entorno.
- Cláusula 6: Administración de las comunicaciones.
- Cláusula 7: Control de acceso a la LAN.
- Cláusula 8: Desarrollo de seguridad de una LAN.
- Cláusula 9: Obediencia.

En el desarrollo de la estrategia de auditoría es crucial la consideración de la profundidad de la cobertura necesitada para la administración de riesgos, el análisis de las políticas y los procedimientos. La consideración de la cobertura necesaria tiene que estar basada en las necesidades del negocio u organización, por eso no será necesario auditar cada aspecto de riesgo, política y procedimiento, sino sólo algunos factores serán relevantes para considerar en esta etapa, incluyendo lo siguiente:

- El análisis de riesgos de la organización será revisado sólo en una auditoría anual, para tener certeza que la continuidad es apropiada.
- Dentro del análisis de riesgos, políticas y procedimientos existen algunos sistemas o procesos de alto riesgo que también serán revisados anualmente.
- En la organización deberá tenerse en cuenta que aquellos riesgos identificados como críticos para el logro de sus objetivos deberían de ser completamente auditados.
- Un rango adecuado de riesgos no clave necesitan ser incluidos en la cobertura de la auditoría para dar credibilidad a las sugerencias que realizan.
- Los riesgos o áreas no identificados como clave necesitarán alguna atención y análisis para estar seguros que no tendrán impactos materiales y financieros adversos.

- El conocimiento actual de la organización sobre administración de riesgos, políticas y procedimientos, que informe sobre la probabilidad de deficiencias, implicará una mayor cobertura de la auditoría.

La cobertura de la auditoría más efectiva debe determinarse tratando de cubrir las consideraciones acerca de que tan bien está planeado el proceso de seguridad y que tan bien este proceso opera en la práctica. La extensión de auditar procesos no clave debe ser profundamente estudiada, por razones del costo de la auditoría pero también por la posibilidad de no ser completa.

El alcance se complementa con los objetivos de la auditoría. La auditoría en seguridad para LAN tiene como objetivo fundamental que se cumplan los tres principios básicos de la seguridad en la LAN organizacional: confidencialidad, integridad y disponibilidad. Por lo tanto, proporciona a la gerencia la garantía de que los objetivos de control y las políticas relacionadas se satisfacen. Esto quiere decir que las vulnerabilidades, debilidades y fallas evidentes y potenciales fueron encontradas, analizadas, mitigadas y/o corregidas (estos dos últimos puntos tras aplicar las recomendaciones de la auditoría).

Además, los controles, sistemas y procedimientos deben cumplir con los objetivos de la organización. Es indispensable que los objetivos señalados se cumplan con los menores recursos. Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de tal forma que las metas fijadas puedan ser cumplidas.

Las razones por las cuales el cliente desea realizar la auditoría pueden ser por:

- Reglas internas de la organización.
- Incrementos no previstos en los costos.
- Pérdidas financieras.
- Obligaciones legales.
- Ineficiencia global notoria.
- Pérdida en la continuidad de las comunicaciones.
- Compromiso de la información.

Los cuatro principales objetivos de esta auditoría son:

- Garantizar la continuidad y operatividad de la organización, que depende de manera importante de la seguridad de su red organizacional.
- Proporcionar la garantía de que sus controles se cumplen, desde sus normas generales hasta sus procedimientos y políticas.
- Evidenciar los riesgos actuales y potenciales de las debilidades.
- Proporcionar las recomendaciones más adecuadas para cubrir las debilidades o vulnerabilidades.

Cabe señalar que también se deben especificar los objetivos relacionados a cada uno de los segmentos o cláusulas que abarca la auditoría en seguridad de la LAN.

Los objetivos de la auditoría también deben ser definidos entre auditores y clientes, aunque dentro de la auditoría sólo se pueden realizar observaciones a la directiva sobre la garantía del cumplimiento de los objetivos de control sobre seguridad y evidenciar los riesgos y debilidades que resulten de las evaluaciones; asimismo se debe aconsejar sobre acciones correctivas, siendo labor de la directiva que estas recomendaciones se lleven a cabo.

En nuestro trabajo, esta auditoría contemplará en su metodología la poca disponibilidad de recursos, tanto financieros como humanos, considerando que la entidad a auditar es un organismo gubernamental, manejando con ello los escasos presupuestos asignados resultado de no considerar el área TI como un área productiva dentro de la acción gubernamental.

Las características de una organización gubernamental son importantes en la determinación del alcance y los objetivos de esta auditoría. Dentro de estas características se encuentran las siguientes:

- El presupuesto destinado a las TI's es bastante limitado y en caso de alguna implementación, compra o actualización se debe realizar un proceso engorroso de justificación.
- Este tipo de organizaciones se distinguen por una gran complejidad. Como resultado se observa un elevado número de secciones organizacionales y físicas, por ende un número elevado de personal.
- Las TI's no son homogéneas (distintas arquitecturas, S.O., etc.) y en ocasiones obsoletas.
- Los usuarios cuentan con un bajo o variable conocimiento y conciencia en el uso de las TI's.
- Los usuarios cuentan con distintos privilegios de acceso.
- Un número muy alto de procesos organizacionales no están automatizados o no son eficientes.

Para tener una visión global de las características de las organizaciones gubernamentales se presenta la siguiente gráfica. Se observa que en sus TI's el gobierno tiene (debería tener) una seguridad muy alta, poca eficiencia-efectividad y un cumplimiento mediano de sus controles. Se observa una diferencia con la banca, que también tiene una alta seguridad y un cumplimiento mediano, pero tiene una alta eficiencia-efectividad; en el caso de las PyMES tienen escasa seguridad y nulo cumplimiento de sus controles si es que existen, pero poseen una eficiencia-efectividad considerable.

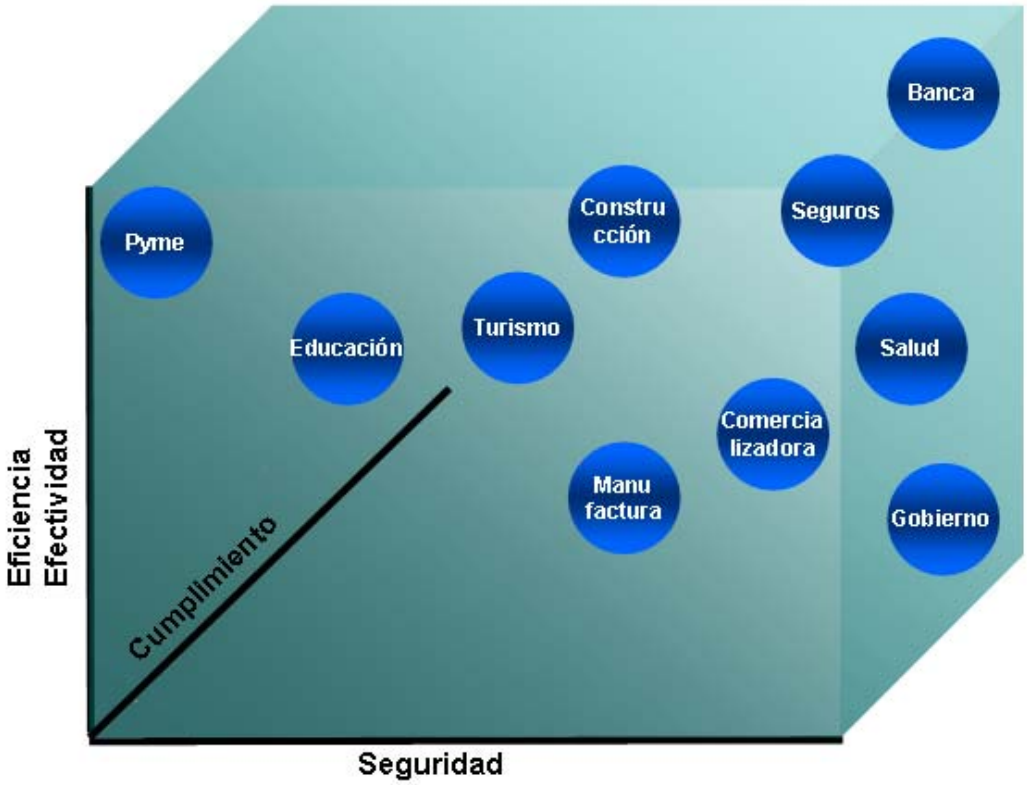


Figura 4. 2 Seguridad en los organismos gubernamentales

4.2.2. Estudio inicial del entorno de la LAN.

El estudio de la LAN nos lleva a un análisis estructural de la organización misma, de su organigrama, dominios lógicos y las topologías de las TI's. Para que los auditores tengan un conocimiento global de la LAN, su entorno y de su administración, deberán saber de manera breve pero completa lo siguiente:

- El organigrama de la organización, que muestra la estructura oficial de esta organización.
- Los departamentos en los que está dividido el organismo, cuyas funciones serán conocidas por los auditores.
- Las relaciones funcionales y jerárquicas entre dichos departamentos, que serán verificadas por el equipo auditor.
- Los flujos de información a través de toda la organización.
- Los puestos de trabajo, especialmente del departamento de informática, mismos que serán revisados para comprobar sus funciones reales y comprobar que no haya puestos con nombres distintos con la misma función (redundancia funcional).
- Número de empleados por cada puesto de trabajo, especialmente del departamento mencionado.

En el estudio inicial conoceremos el entorno operacional de la LAN revisando la siguiente información:

- Planos de la infraestructura de todas las redes, especialmente de la LAN a estudiar.
- Diagrama de la arquitectura de la red, mostrando la interconexión, configuración y distribución de todos los equipos, tanto la asignación de cada dominio lógico como su ubicación geográfica. La configuración del equipo debería estar directamente relacionada con las políticas de seguridad.
- Inventario del hardware, software y su estructuración, relacionado con la LAN, incluyendo servidores locales, remotos y los sistemas de misión crítica.
- Todos los servicios de comunicación de voz y datos, incluyendo VPN's y los accesos de comunicación a la red pública.

Algo muy relevante y necesario será conocer las políticas (tanto a nivel organizacional como a nivel de seguridad informática) y los controles de la dirección con sus respectivos dominios de jurisdicción, y así conocer la administración de la organización y de la red de la información. Todo esto debe tener un documento de registro y si no se tiene se recomendará que se elabore a la brevedad, para conocer la estructura operacional de la empresa.

Los auditores deberán solicitar, si es que existen, estudios de auditorías previas realizadas a la organización sobre la seguridad en redes, como:

- Reportes de auditorías internas.
- Reportes de auditorías externas.
- Reportes recientes de control interno.
- Documentos de análisis de riesgos.
- Estudios de consultorías.
- Estudios de vulnerabilidades.
- La documentación existente sobre la configuración de seguridad de hardware y software.
- Manuales de seguridad elaborados por la organización.

4.2.3. Determinación de la muestra.

Para formar una opinión de auditoría de los SI's, los auditores frecuentemente no examinan toda la información disponible por ser impráctica (los recursos tiempo, dinero y esfuerzo son limitados) y conclusiones válidas pueden ser logradas por medio del muestreo de auditoría.

Según el procedimiento 060.040 "Audit Sampling", del estándar de auditoría de SI's 060 de ISACA, "Performance of Audit Work", el muestreo apropiado y su evaluación reunirá los requerimientos de evidencia suficiente, confiable y relevante, soportados por el análisis apropiado.

Algunos ejemplos del examen de cumplimiento de los controles donde el muestreo puede ser considerado incluyen los derechos de acceso de usuarios, procedimientos de control, documentación de procedimientos, excepciones de seguimiento, revisión de logs, auditoría de licencias de software, etc.

El documento mencionado define al muestreo de auditoría como la aplicación de los procedimientos de auditoría a menos del 100% de la población que permita al auditor evaluar la evidencia de auditoría, de alguna característica seleccionada, para formar una conclusión sobre la población.

En el muestreo estadístico las conclusiones son válidas para la población. En cambio, en el muestreo no estadístico las conclusiones no pueden ser extrapoladas hacia la población al no ser probable que la muestra sea representativa de la población.

En el diseño del tamaño y estructura de una muestra de auditoría los auditores deben considerar los objetivos específicos de la auditoría, la naturaleza de la población y los métodos de selección y muestreo más probables para lograr esos objetivos. La unidad de muestreo depende del propósito de la muestra. Para la prueba del cumplimiento de controles es usado el muestreo por atributos donde la unidad de muestreo es un evento o transacción.

Para un diseño efectivo y eficiente de la muestra puede ser apropiada la estratificación, que es el proceso de dividir la población en subpoblaciones con características similares de tal forma que cada unidad de muestreo pertenezca a una de esas subpoblaciones.

De los dos métodos de muestreo estadístico (aleatorio y sistemático) y los dos métodos de muestreo no estadístico (deliberado y por juicio) se considera ideal en nuestro método una combinación de ambos. Se utiliza el muestreo por juicio, en el que el auditor coloca una parcialidad en la elección de la muestra, en la selección de los sistemas críticos o perimetrales de la LAN o de su seguridad. Para la selección de eventos en un sistema particular (cuentas y passwords, atributos de cuentas, logs, configuraciones, etc.) puede realizarse un muestreo estadístico, aleatorio o sistemático.

Para la determinación de los recursos necesarios se debe dividir el sistema total (la red y su entorno) en una serie de subsistemas, a continuación se deberán determinar las categorías de seguridad para cada uno de los subsistemas críticos catalogándolos en impacto potencial bajo, moderado o alto.

Enseguida se determinará el costo en cada subsistema crítico elegido al realizar la auditoría considerando la factibilidad de realizar un muestreo si el tamaño y complejidad del sistema es muy alto. También se realizará una valoración de los beneficios por cada uno de los costos, y se deberá cumplir que la magnitud de éstos últimos es significativamente menor. Finalmente se categorizará en orden de prioridad cada uno de los subsistemas incluyendo su relación costo/beneficio. El auditor sugerirá inicialmente la auditoría obligatoria para los subsistemas con más alto impacto.

4.2.4. Determinación de los recursos necesarios.

Después del estudio inicial y de la determinación de la muestra se determinan los recursos humanos y materiales que se emplearán en la auditoría, los cuales están en función del tamaño y complejidad de la organización, de su LAN, de las arquitecturas empleadas, de la homogeneidad de la TI y de su administración.

En función de lo anterior se determinará el número de auditores competentes y con alto compromiso y el número requerido de personal de la organización auditada con alto conocimiento y experiencia de los sistemas a examinar. Las características y perfiles del personal seleccionado dependen de la materia auditable. En este caso, al tratarse de seguridad en redes, son necesarios los siguientes perfiles profesionales de los auditores:

- Experto en seguridad informática (auditor CISA, CISSP, BS 7799-2, CSIRT, CCSA, CCSE).
- Experto en redes (LAN y WLAN).
- Experto en legislación de seguridad informática.

En el caso del personal auditado se requerirá la participación de:

- Administrador de la red.
- Responsable de la seguridad de la red.
- Técnicos de sistemas.

Los auditores deberán basar sus acciones en un *código de ética profesional* que comprende:

- Cumplir e implementar los estándares, procedimientos y controles apropiados para los SI's.
- Realizar sus deberes con objetividad, diligencia y cuidado profesional, de acuerdo con sus estándares profesionales y mejores prácticas.
- Mantener la privacidad y confidencialidad obtenida en el curso de sus deberes, a menos que una revelación sea requerida por una autoridad legal. Tal información no debe ser usada para beneficio personal o liberada a partes inapropiadas.
- Servir en el interés de sus clientes en una forma legal y honesta, manteniendo altos estándares de conducta y carácter, y no realizar actos desacreditables a la profesión.
- Mantener una alta competencia en sus campos respectivos.
- Informar a las partes apropiadas de los resultados del trabajo hecho, revelando todos los hechos significantes encontrados.
- Soportar la educación profesional de sus clientes para mejorar su entendimiento en la seguridad y control de los SI's.

En el caso de auditores CISA (por citar un ejemplo), deberán adherirse al código de ética profesional de ISACA en la realización de todos sus actos como establece el Estándar de Auditoría en SI's 030.

Se pueden establecer varios criterios para determinar el número de auditores empleados en esta auditoría:

- El primero es utilizar un equipo de auditores para realizar las entrevistas y cuestionarios a los involucrados con la seguridad de la red y su administración, y otro equipo de auditores para la búsqueda y estudio de la evidencia. La razón de hacerlo así es porque será frecuente que la misma persona a la que se le realiza la entrevista sea la misma de la que se necesite su colaboración para la obtención de la evidencia posterior en los testeos. Por ello no se podrá trabajar paralelamente en ambos asuntos.
- Otro criterio es la consideración de que se tienen básicamente tres tipos de cláusulas de control a revisar (gestión de la seguridad, la seguridad misma y la parte del cumplimiento de lo anterior), por ende consideramos a un tipo de experto por cada tipo de cláusula (tres expertos). Considerando la complejidad de cada una de las cláusulas, consideramos que se necesitarían (al menos) dos auditores expertos en seguridad informática para el primer tipo, gestión de la seguridad; mínimo dos auditores expertos en redes para el segundo grupo, seguridad en redes; y un auditor experto en legislación de seguridad informática para la parte legal.
- El siguiente criterio es el hecho que se tienen nueve cláusulas de control y un tiempo promedio de auditoría de 120 horas. Se consideraría que aproximadamente se realizaría la auditoría de cada cláusula en un día, con el grupo especificado en el punto anterior.

El hardware necesario y las demás herramientas utilizadas generalmente son aportadas por el equipo auditor, como es el software especializado de auditoría en seguridad, software específico de testeo, checklists propios de la empresa auditora, manuales de testeo y configuración de redes, normas internacionales y recomendaciones de la industria. Por supuesto que la evidencia se realizará sobre y con los sistemas del cliente.

4.2.5. Planeación.

Esta fase comprende principalmente la elaboración del plan de trabajo y la programación de actividades. Para realizar esto es imperativo tener ya un conocimiento completo de la red y su entorno, haber priorizado los sistemas a evaluar (de acuerdo con las necesidades del cliente) y saber cuáles serán examinados (de acuerdo con los recursos del cliente, los objetivos de la auditoría y la determinación de la muestra). Se habrán determinado qué sistemas se evaluarán de la LAN organizacional, si se revisará algún dominio lógico o físico, la seguridad perimetral o si se tratará de un examen de seguridad interno o externo.

El estándar de auditoría 050, “Planning”, establece que el auditor de SI debe planear la cobertura de la auditoría para cubrir los objetivos de la misma y cumplir con las leyes aplicables y las normas profesionales de auditoría. Además, el auditor debe desarrollar y documentar un plan de auditoría que detalle los plazos, el alcance y los recursos requeridos. El plan debe incluir cada una de las tareas de la auditoría detalladas cronológicamente, los auditores que las realizarán y la exposición explícita de ayuda por parte del staff de la organización auditada.

En nuestra metodología, de acuerdo a la determinación de los recursos realizada anteriormente, se establecerá un plan de trabajo de 144 horas. Esto significa que se realizará durante los cinco días hábiles de tres semanas más tres días, considerando por cada día un trabajo de 8 horas. En la primera fase se realizará la obtención de la evidencia mediante entrevistas y cuestionarios. En la segunda fase se realizará la obtención y corroboración de la evidencia anterior por medio de testeos manuales (evidencia directa), checklists y la utilización de las demás herramientas de la auditoría que se especificarán en el siguiente apartado. Cada día se realizará un cubrimiento de una cláusula de control (en promedio) de la primera fase y después se auditará cada cláusula de control de la segunda fase (2 x 9 días hábiles = 144 horas/auditoría).

	Tareas	1ª Semana					2ª Semana					3ª Semana					4ª Sem.		
Primera Fase	Cláusula 1																		
	Cláusula 2																		
	Cláusula 3																		
	Cláusula 4																		
	Cláusula 5																		
	Cláusula 6																		
	Cláusula 7																		
	Cláusula 8																		
	Cláusula 9																		
Segunda Fase	Cláusula 1																		
	Cláusula 2																		
	Cláusula 3																		
	Cláusula 4																		
	Cláusula 5																		
	Cláusula 6																		
	Cláusula 7																		
	Cláusula 8																		
	Cláusula 9																		

2 auditores expertos en gestión de controles de seguridad
2 auditores expertos en seguridad de redes
1 auditor experto en legislación

Tabla 4. 1 Programación de las actividades de auditoría

Por otro lado, los auditores deben evaluar constantemente el equilibrio entre los recursos disponibles y las actividades de la auditoría. El plan de auditoría debe ser lo suficientemente realista para considerar la disponibilidad de tiempo de la empresa auditada, y se deberá realizar un reporte donde se establecerán y compararán dinámicamente los avances con lo planeado.

En caso de no concordar deben realizarse ajustes al plan y realizar las acciones correctivas necesarias. El estándar de auditoría mencionado establece que el programa puede requerir ajustes para abordar situaciones no previstas como nuevos riesgos, suposiciones incorrectas, hallazgos en los procedimientos ya realizados, etc.

4.2.6. Realización de la auditoría.

La metodología que hemos seleccionado para esta fase (la auditoría en sí misma) está basada en COBIT y en BS 7799-1:2000, fundamentada en la revisión de los procesos de la red, su entorno, sus controles implementados por la organización y los controles que los auditores han seleccionado de las mejores y más adecuadas metodologías, estándares y marcos de control. De esta forma consideramos los siguientes seis pasos:

1. Selección de los objetivos de control y controles de seguridad de la LAN.
2. Ponderación de los sectores auditados.
3. Entrevistas y cuestionarios.
4. Realización de pruebas.
5. Cruzamiento de información y calificación.
6. Cálculos y resultados de la auditoría.

1. Selección de los objetivos de control y controles de seguridad de la LAN.

El equipo de los auditores seleccionará los objetivos de control y controles más adecuados para cada una de las cláusulas acordadas en la determinación del alcance y objetivo, de acuerdo a las características de la organización y de la red, haciéndolo de las metodologías y marcos que más se adecuen. El documento *IS Standards, Guidelines and Procedures for Auditing and Control Professionals* de ISACA dice que el profesional en seguridad y control debe aplicar su propio juicio profesional en circunstancias específicas presentadas por los sistemas particulares o el entorno de TI. En nuestro caso seleccionamos los mejores controles y criterios relacionados con seguridad de COBIT, BS-7799, CC y del TCSEC, y los adaptamos apropiadamente a la seguridad de LAN, mismos que serán presentados a continuación.

CONTROLES DE SEGURIDAD EN LAN

Cláusula (de control) 1: Políticas de seguridad.

Objetivo (de control) 1.1: Políticas de seguridad de la LAN.
Proporcionar a la dirección la administración y el soporte de las políticas de seguridad de la LAN.

Control 1.1.1: *Documento de políticas de seguridad de la LAN o bien, documento de políticas de seguridad de la información que incluya expresamente las políticas de seguridad de la LAN.*

Este documento debe existir, estar aprobado por la administración, ser publicado y comunicado a todos los empleados. Como mínimo de debe incluir:

- Una definición de seguridad de la LAN, sus objetivos y alcance.
- Metas y principios de la seguridad de la LAN.
- Una breve explicación de las políticas, principios, estándares y obediencia.
- Una definición de responsabilidades generales y específicas para la administración de la seguridad de la LAN.
- Referencias a la documentación que puede soportar a las políticas.

Control 1.1.2: *Revisión y evaluación de las políticas de seguridad de la LAN.*

Las políticas serán revisadas regularmente conforme a un plan establecido y en caso de cambios organizacionales, de los SI's o TI's, serán redefinidas. Las revisiones periódicas deberán incluir lo siguiente:

- Efectividad de las políticas.
- Costo e impacto de los controles en la eficiencia del negocio.
- Efectos y cambios en la tecnología.

Cláusula 2: Gobierno de la seguridad.

Objetivo 2.1: Administración de seguridad de la LAN.
Para dirigir la seguridad de la LAN en la organización.

Control 2.1.1: *Gestión de administración y coordinación de la seguridad de la LAN.*

Para que existan dirección y soporte administrativo claros en la implementación y cumplimiento de los controles de seguridad de la LAN debe haber representantes administrativos de las áreas o procesos clave de la organización. La administración debe considerar lo siguiente:

- Revisión y aprobación de las políticas.
- Monitoreo de cambios significativos de amenazas a la LAN.

- Revisión y monitoreo de incidentes de seguridad en la red.
- Aprobación de iniciativas para mejorar la seguridad de la LAN.
- Definición de roles y responsabilidades para la seguridad de la red.
- Acuerdos de metodologías y procesos específicos para la seguridad de la LAN.
- Garantizar que la seguridad es parte del proceso de planeación de la red.

Control 2.1.2: *Asignación de responsabilidades de seguridad de la LAN.*

Serán definidas claramente las responsabilidades para la protección y cumplimiento de los procesos de seguridad de la LAN. Las políticas de seguridad de la LAN deben proporcionar una guía general en la asignación de estos roles y responsabilidades. Una práctica común es nombrar un propietario para cada activo de la red. Además los niveles de autorización deben ser claramente definidos y documentados.

Control 2.1.3: *Asesoramiento de especialistas en seguridad de LAN.*

Ofrecido por consultores internos o externos a la organización en caso de configuraciones, fallos o situaciones críticas. Este asesoramiento debe ser realizado al mínimo tiempo posible del incidente de seguridad y los consultores deben tener acceso directo a la administración.

Control 2.1.4: *Revisión independiente de la seguridad de la LAN.*

La implementación y cumplimento de los controles se revisará independientemente por auditores externos y/o internos, para asegurar que son efectivos y viables.

Control 2.1.5: *Reacreditación.*

Se realizará periódicamente por un equipo “tigre” para mantener actualizado el nivel de seguridad aprobado por la administración. El equipo “tigre” es un grupo técnico que verifica la seguridad actuando de forma incógnita tratando de violar las medidas de seguridad establecidas e identificando las áreas vulnerables.

Objetivo 2.2: Seguridad en el acceso a la LAN por terceras personas.
Para mantener la seguridad y bienes de la LAN accesados por terceras personas.

Control 2.2.1: *Identificación de riesgos de acceso de terceras personas a la LAN.*

En el análisis de riesgos se contemplará la posibilidad de accesos no autorizados o indebidos de terceras personas a la LAN, así como el impacto de ellos, y se implementarán los debidos controles de seguridad, considerando que su acceso puede ser físico y/o lógico.

Identidad de terceras personas físicas:

- Personal de mantenimiento y soporte.
- Personal de limpieza.
- Personal de seguridad perimetral.
- Personal de servicio social o prácticas profesionales.
- Personal de consultoría.

Identidad de terceras personas lógicas:

- Intrusos, hackers o crackers.
- Proveedores de servicios VPN's y conectividad.

Control 2.2.2: *Especificaciones de seguridad en contratos con terceras personas.*

Los contratos con terceras personas deberán incluir los acuerdos formales de seguridad, respecto a la seguridad de la LAN de la organización y su estructura, para asegurar el cumplimiento con las políticas y estándares de seguridad adoptados.

Consideraciones mínimas de seguridad para un contrato que involucre LAN:

1. La política general de seguridad de la LAN.
2. Procedimientos y controles para la protección de bienes.
3. Descripción de cada servicio que será realizado.
4. Niveles de servicio aceptables e inaceptables.
5. Responsabilidades respectivas de las partes del acuerdo.
6. Responsabilidades legales de ambas partes.
7. Derechos de propiedad intelectual y copyright.
8. Acuerdos de control de acceso.
9. Derecho a monitorear y revocar el uso de la LAN.
10. Responsabilidades de la instalación y mantenimiento de hardware y software.
11. Un proceso claro y específico de administración de cambios.
12. Controles para asegurar la protección contra software malicioso.
13. Acuerdos para el reporte de incidentes de seguridad.

Objetivo 2.3: Análisis de riesgos.
La identificación de riesgos de la LAN y el análisis de su impacto permitirán tomar medidas para mitigarlos.

Control 2.3.1: *Evaluación de riesgos de la LAN.*

Deberá establecerse una evaluación sistemática de riesgos, determinando la forma en que deben ser manejados a un nivel aceptable. La administración debe asegurar que se realicen reevaluaciones sobre los riesgos actualizadas con las auditorías, inspecciones e incidentes identificados.

Control 2.3.2: *Identificación y medición de riesgos.*

Los elementos esenciales de riesgo incluyen activos tangibles e intangibles, valor de los activos, amenazas, vulnerabilidades, protecciones, consecuencias y probabilidad de amenaza. Se debe incluir una clasificación cualitativa y/o cuantitativa de riesgos basada en planeaciones y auditorías. Los especialistas de TI deben dirigir la selección de los controles implementados para las acciones contra los riesgos.

Control 2.3.3: *Plan de acción contra riesgos.*

Se definirá un plan de acción contra riesgos para asegurar que el costo-efectividad de los controles y las medidas de seguridad de la LAN mitiguen los riesgos en forma continua.

Cláusula 3: Control y clasificación de bienes.

Objetivo 3.1: Responsabilidad de los bienes o activos.
Para mantener la protección apropiada de los bienes relacionados con la LAN.

Control 3.1.1: *Inventario de bienes relacionados con la LAN.*

Redactar y actualizar un inventario de bienes asociados con la LAN y su entorno, especialmente de los sistemas críticos, incluyendo su valor relativo y su importancia. Se incluirán los siguientes tipos:

- Bienes de información (incluyendo información lógica y en papel).
- Software.
- Bienes físicos.
- Servicios (incluyendo servicios de comunicación).

Control 3.1.2: *Responsabilidad de los bienes relacionados con la LAN.*

Se definirá al responsable de los activos inventariados, lo cual debe estar documentado, y será actualizado y revisado periódicamente.

Objetivo 3.2: Clasificación de la información.
Asegurar que la información recibe un nivel de protección apropiado, dependiendo de su grado de sensitividad y criticidad.

Control 3.2.1: *Manuales de clasificación de la información.*

Serán elaborados manuales de clasificación de la información con el objetivo de implementar rangos de acceso según las categorías de seguridad de la información.

Control 3.2.2: *Manuales de clasificación de niveles de seguridad en la LAN.*

La gerencia deberá definir, implementar y mantener niveles de seguridad para cada una de las clasificaciones de datos identificadas con un nivel superior al de "no requiere protección". Estos niveles de seguridad deberán representar el conjunto de medidas de seguridad y control apropiados para cada una de las clasificaciones, y deberán ser reevaluados periódicamente y modificados en consecuencia. Por ejemplo, usar los niveles del TCSEC:

- Protección Mínima.
- Protección Discrecional.
- Protección Obligatoria.
- Protección Controlada.

Control 3.2.3: *Manejo y rotulación de la información.*

Serán definidos procedimientos apropiados para el manejo y rotulación de la información de acuerdo a los manuales de clasificación, los cuales incluyen:

- Copia.
- Almacenamiento.
- Transmisión por la red.
- Transmisión por voz.
- Destrucción.

Cláusula 4: Seguridad de los empleados.

Objetivo 4.1: Seguridad en la definición de puestos.
Para reducir el riesgo de error humano, fraude o mal uso de facilidades.

Control 4.1.1: *Incluir la seguridad en las responsabilidades de puestos.*

Serán documentados, definidos y asignados los roles y responsabilidades de seguridad de la LAN en los puestos de trabajo.

Control 4.1.2: *Términos y condiciones de empleo.*

Las responsabilidades de los empleados respecto a la seguridad de la LAN serán establecidas en los términos y condiciones del contrato, incluyendo acuerdos de confidencialidad y responsabilidades legales. Estas responsabilidades deben continuar por un periodo definido después del fin del empleo.

Objetivo 4.2: Entrenamiento del personal.
Asegurar que los usuarios están consientes de la seguridad LAN, sus amenazas y que están preparados para soportar las políticas de seguridad en su trabajo.

Control 4.2.1: *Entrenamiento y culturización en seguridad de la LAN.*

Todos los empleados recibirán el entrenamiento y actualización adecuados a su perfil en seguridad de la red y se promoverá la concientización de la misma, con los medios más adecuados.

Objetivo 4.3: Respuesta a incidentes de seguridad de la LAN.
Para minimizar y monitorear el daño de los incidentes y malos funcionamientos.

Control 4.3.1: *Reporte de incidentes de seguridad de la LAN.*

Los incidentes de seguridad deben ser reportados a través de canales de administración apropiados, lo más rápido posible. Un procedimiento formal de reporte debe ser reestablecido junto con un procedimiento de respuesta a incidentes, definiendo las acciones a ser tomadas en un reporte de incidentes.

Control 4.3.2: *Reporte de debilidades de seguridad de la LAN.*

Los usuarios de la LAN deberán reportar cualquier debilidad observada o anomalía detectada lo más rápidamente posible.

Control 4.3.3: *Reporte de mal funcionamiento del software en la LAN*.

Deben ser establecidos procedimientos para reportar mal funcionamientos del software, las acciones que deben ser consideradas son:

- Cualquier problema y/o mensaje que aparezca debe ser notificado.
- El equipo debe ser aislado lo más pronto posible debiendo ser detenidas sus acciones.

Control 4.3.4: *Aprendizaje de los incidentes.*

Debe establecerse un mecanismo para que los costos de incidentes y malos funcionamientos sean cuantificados. Esta información puede servir para el análisis de riesgos, la mejora continua o la adición de controles.

Control 4.3.5: Disciplina en seguridad de la LAN.

La violación de políticas y procedimientos de seguridad de la red serán manejadas mediante una acción disciplinaria.

Cláusula 5: Seguridad física de la LAN y su entorno.

Objetivo 5.1: Aseguramiento de áreas de la red y su entorno.
Para prevenir accesos no autorizados, daños e interferencia a los procesos críticos e información del negocio. La protección proporcionada debe estar de acuerdo con los riesgos identificados.

Control 5.1.1: *Perímetro de seguridad física.*

Distintos niveles físicos de seguridad serán usados para proteger áreas de la red, su entorno y su cableado. Cada nivel o barrera establece un perímetro de seguridad, incrementando la protección total proporcionada. La posición y fuerza de cada barrera depende de los resultados de un análisis de riesgos. Se deben considerar los siguientes controles:

- El perímetro de seguridad debe estar claramente definido.
- El perímetro debe ser físicamente sólido y los accesos deben estar adecuadamente protegidos.
- Debe haber un área de recepción u otros medios de control de acceso al *site* o a las distintas áreas de la red. El acceso permitirá sólo personal autorizado.
- Las barreras físicas deberían estar extendidas del piso real al techo real, para prevenir acceso no autorizado y contaminación/daño por siniestros.
- Las salidas de emergencia en un perímetro de seguridad deben tener alarmas.

Control 5.1.2: *Controles de entrada física.*

Las áreas sensibles de la red deben estar protegidas por controles de acceso apropiados para asegurar que sólo el personal autorizado tiene acceso. Considerar los controles siguientes:

- Los visitantes a las áreas seguras de la red deben ser supervisados y debe ser registrado su tiempo de acceso y de salida. Además, el acceso sólo será para propósitos específicos y autorizados, y cualquier procedimiento que realicen se regirá por los procedimientos determinados.
- El acceso a los procesos sensibles de la red será controlado y restringido sólo a personal autorizado. Deben ser usados controles de autenticación (por ejemplo smart cards) para autorizar y validar todos los accesos. Debe ser mantenido seguramente un registro del seguimiento de todos los accesos.
- Todo el personal debe usar alguna identificación visible y debe fomentársele el cuestionar a todos los extraños no escoltados y que no vistan la identificación visible.
- Los derechos de acceso a las áreas seguras de la red deben ser regularmente revisados y actualizados.

Control 5.1.3: *Seguridad de las áreas de la LAN.*

Se debe tener en cuenta la posibilidad de desastres naturales o producidos por el hombre mediante la implementación de estándares y reglamentaciones, en torno a la salud y seguridad de estas áreas de la red. Considerar los siguientes controles:

- Establecer medidas de control en los accesos para evitar la entrada de personal ajeno.
- Las instalaciones deben ser discretas y tener una indicación mínima de su propósito con signos no obvios fuera y dentro de las instalaciones que identifiquen la presencia de las áreas sensibles de red.
- Puertas y ventanas deben estar cerradas cuando no hay personal en las instalaciones y una protección externa debe ser considerada para ventanas, especialmente para instalaciones localizadas en la planta baja.
- Un sistema de detección de intrusos debe ser instalado adecuadamente en los accesos de las áreas críticas de red (puertas, ventanas, etc.) y debe ser regularmente examinado. Las áreas desocupadas deben tener alarmas activadas todo el tiempo.
- Las áreas sensibles de la LAN administradas por la organización deben estar físicamente separadas de aquéllas administradas por terceras partes.
- Los directorios y libros telefónicos internos que identifiquen localizaciones de áreas sensibles de la LAN no deben ser fácilmente accesibles para el público.
- Los materiales peligrosos o combustibles deben ser almacenados seguramente a una correcta distancia del área sensible.
- Los medios de respaldo deben estar colocados a una distancia segura para evitar daños ocasionados por un desastre en el *site* principal.
- Las áreas sensibles de la LAN deben ser monitoreadas continuamente (por ejemplo, con circuito cerrado) tanto para personal ajeno e interno, para prevenir oportunidades de actividades maliciosas.

Objetivo 5.2: Seguridad del equipo de la LAN.
Para prevenir pérdida, daño, compromiso o interrupción del sistema.

Control 5.2.1: *Colocación y protección del equipo de la LAN.*

El equipo de la red será colocado y protegido adecuadamente para reducir en lo posible las amenazas ambientales y el acceso no autorizado. Considerar lo siguiente:

- El equipo debe estar colocado de tal forma que se minimice la necesidad de su acceso.
- El equipo crítico de red y el de respaldo debe estar colocado de tal forma que se reduzca su visibilidad.
- Implementar controles para minimizar el riesgo de amenazas como robo, fuego, explosivos, humo, agua, vibración, interferencia eléctrica y electromagnética.

- Considerar políticas para evitar que el personal coma, beba y fume en proximidad de estos equipos.

Control 5.2.2: *Suministro de energía ininterrumpible.*

El equipo de la LAN debe estar protegido constantemente contra fallos de energía eléctrica mediante UPS (*uninterruptible power supply,* suministro de energía ininterrumpible), múltiples suministros de energía y generadores de respaldo. Estos suministros están recomendados para los sistemas críticos de la red.

Control 5.2.3: *Seguridad del cableado de la LAN y su alimentación.*

El cableado de comunicaciones y de energía debe estar protegido contra daño y/o intercepción. Tomar en cuenta lo siguiente:

- Las líneas de energía y de datos deben estar bajo tierra, ocultos o protegidos adecuadamente.
- El cableado de la red debe estar protegido de una intercepción no autorizada o daño.
- Los cables de energía deben estar convenientemente segregados de los cables de datos para prevenir interferencia.
- Para sistemas críticos considerar la instalación de conductos especiales, cuartos de seguridad (IDF's), terminales de las conexiones, uso de rutas o medios de transmisión alternos, uso de fibra óptica y barridos del cableado para localizar conexiones no autorizadas.

Control 5.2.4: *Mantenimiento del equipo de la LAN.*

El equipo de la red recibirá mantenimiento para permitir continuamente su disponibilidad e integridad. Además, este mantenimiento debe realizarse de acuerdo a las recomendaciones del proveedor, por el personal adecuado y autorizado. Se llevará un registro de las operaciones de mantenimiento y se implementarán controles adicionales cuando el equipo es llevado fuera de las instalaciones (para evitar pérdida o robo de datos).

Control 5.2.5: *Seguridad en el desecho y re-uso del equipo de red.*

Todo el equipo de red de desecho que contenga información o configuraciones debe ser físicamente destruido o formateado usando la función de borrado estándar. Los equipos especiales pueden requerir un análisis de riesgos para determinar si serán destruidos, reparados o desechados.

Cláusula 6: Administración de las comunicaciones y las operaciones de la LAN.

Objetivo 6.1: Procedimientos y responsabilidades.
Para asegurar la operación segura y correcta de la LAN. Incluye el desarrollo de instrucciones de operación apropiadas y procedimientos de respuesta a incidentes. Además se implementará la segregación de responsabilidades.

Control 6.1.1: *Documentación de procedimientos de operación de la LAN.*

Estos procedimientos serán documentados y mantenidos como documentos formales, así los cambios serán autorizados por la administración. Los procedimientos deberán especificar las instrucciones para la ejecución detallada de cada tarea incluyendo:

- Proceso y manejo de información.
- Instrucciones para manejo de errores, condiciones excepcionales y restricciones para el uso de utilidades.
- Contactos para el soporte de dificultades técnicas u operacionales.
- Procedimientos para el reinicio y recuperación en caso de falla del sistema.
- Procedimientos para las facilidades de comunicaciones y mantenimiento del equipo.

Control 6.1.2: *Control de cambios operacionales.*

Deben establecerse procedimientos para controlar satisfactoriamente todos los cambios al equipo, software y procedimientos. Considerar los siguientes controles:

- Identificación y documentación de cambios significativos.
- Valoración del impacto potencial de tales cambios.
- Procedimiento de aprobación formal para los cambios propuestos.
- Comunicación de cambios a las personas relevantes.

Control 6.1.3: *Procedimientos para la gestión de incidentes.*

Las responsabilidades y procedimientos para la gestión de incidentes serán establecidos para asegurar una respuesta rápida, efectiva y metódica. Considerar los siguientes controles:

1. Establecer procedimientos para cubrir todos los tipos potenciales de incidentes de seguridad, incluyendo:
   - Fallos en el sistema y pérdida del servicio.
   - DoS (denegación del servicio)
   - Ruptura de la confidencialidad.
2. En adición a los planes normales de contingencia, los procedimientos deben incluir:
   - Análisis e identificación de la causa del incidente.
   - Análisis e implementación de remedios para prevenir la recurrencia.
   - Colección de evidencia.

- Comunicación con los afectados o relacionados con la recuperación del incidente.
- Reporte de las acciones a la autoridad apropiada.

3. Las pistas de auditoría y evidencias similares podrían ser colectadas y aseguradas apropiadamente para:
   - Análisis de problemas internos.
   - Usarse como evidencia en incumplimientos legales.
4. Las acciones para recuperarse de incidentes de seguridad y fallas del sistema deben ser cuidadosa y formalmente controladas. Los procedimientos deben asegurar que:
   - Sólo personal claramente identificado y autorizado tiene acceso permitido a los sistemas y datos.
   - Toda acción de emergencia tomada debe estar documentada en detalle.
   - Las acciones de emergencia deben ser reportadas a la administración y revisadas de manera ordenada.

Control 6.1.4: *Separación de responsabilidades.*

Se separará la administración o ejecución de algunas tareas o responsabilidades para reducir oportunidades de modificaciones no autorizadas o mal funcionamiento de información y servicios. Debe tenerse cuidado que una sola persona pueda perpetrar fraude en áreas de responsabilidad individual; por ello la realización de un evento debe ser separada de su autorización. Se debe asegurar que el personal sólo lleve a cabo las tareas establecidas en la definición de sus puestos. Es importante segregar las siguientes funciones:

- Administración de redes.
- Administración de seguridad.
- Auditoría a la seguridad.

Objetivo 6.2: Protección contra software malicioso.
Para proteger la integridad de la información.

Control 6.2.1: *Controles contra software malicioso.*

Las medidas de prevención, detección y corrección contra software malicioso serán implementadas para el uso correcto de la LAN, basándose en la concientización, apropiados controles de acceso y controles de administración de cambios. Considerar lo siguiente:

- Establecer una política para el cumplimiento con licencias de software y prohibir el uso de software no autorizado.
- Una política formal para la protección contra riesgos asociados con la conexión a redes externas o indicar qué medidas de protección deben ser tomadas.
- Instalación y actualización de antivirus y software de reparación.

- Realizar revisiones regulares de software y datos de los sistemas críticos. La presencia de archivos no autorizados debe ser investigada.
- Revisar todos los correos electrónicos, archivos adjuntos y descargas de software en busca de software malicioso antes de su uso, de preferencia cuando entran a la red de la organización.
- Procedimientos y responsabilidades para tratar con el manejo de protección antivirus, entrenamiento en su uso, reporte y recuperación de ataques de virus.

Objetivo 6.3: Back up.
Para mantener la integridad y disponibilidad de los servicios de comunicación.

Control 6.3.1: *Respaldo de información.*

Para garantizar la disponibilidad continua de los servicios en la LAN se realizarán reproducciones de respaldo de la información, especialmente de los sistemas críticos. Considerar los siguientes controles:

- Un nivel mínimo de la información de respaldo, sus copias y procedimientos deben ser almacenados en una región remota, a suficiente distancia para escapar de cualquier desastre.
- La información de respaldo debe tener la suficiente protección física y ambiental, consistente con los controles aplicados en el *site*.
- Los respaldos deben ser examinados regularmente para asegurar que son efectivos y que están listos para una recuperación.

Control 6.3.2: *Logs de operación.*

El personal debe mantener un registro de sus actividades y debe ser sujeto a revisiones regulares. Los logs deben incluir:

- Tiempos de comienzo y fin.
- Errores del sistema y acciones correctivas tomadas.
- Identificación de la persona que realizó la entrada al sistema.

Objetivo 6.4: Administración de la LAN.
Para asegurar la protección de la información en la red.

Control 6.4.1: *Controles de seguridad de la LAN.*

Serán implementados para obtener y mantener la seguridad de la LAN. Considerar los siguientes controles:

- La responsabilidad de la seguridad de las redes debe estar explícitamente separada de otro tipo de operaciones.

- Las responsabilidades y procedimientos de la administración del equipo remoto deben estar establecidas.
- Deben establecerse controles para la protección de la confidencialidad e integridad de los datos que pasan por redes públicas, así como la disponibilidad de los servicios de red.

Objetivo 6.5: Intercambio de información.
Para prevenir pérdida, modificación o mal uso de la información intercambiada.

Control 6.5.1: *Seguridad de la información en tránsito por la LAN.*

La información en tránsito por la red será protegida en sus tres principios de seguridad. Se recomienda el uso de firmas digitales y encripción para la confidencialidad.

Control 6.5.2: *Seguridad del comercio electrónico.*

Se implementará para evitar fraudes, disputas de contrato y revelación/modificación de la información. Implementar controles para manejar la autenticación, la autorización, procesos de contrato y transacciones.

Control 6.5.3: *Seguridad del correo electrónico.*

Será desarrollada una política para el uso del correo electrónico y se implementarán controles para reducir los riesgos de seguridad relacionados con él. Incluir lo siguiente:

- Ataques al correo electrónico (virus, intercepción, etc.).
- Protección de los mensajes adjuntos.
- Guías sobre el uso del correo.
- Responsabilidad del empleado al comprometer a la compañía.
- Uso de técnicas criptográficas en el correo.
- Retención de mensajes que podrían usarse en una litigación.
- Controles para la autenticación de mensajes.

Control 6.5.4: *Seguridad en sistemas disponibles públicamente.*

Toda la información disponible públicamente debe haber sido formalmente autorizada y será protegida la integridad y confidencialidad de la información mediante mecanismos apropiados (firma digital, criptografía, etc.). Se debe garantizar que la información cumpla las legislaciones pertinentes. El acceso a estos sistemas de publicación no debe permitir el acceso a otra parte de la red.

Cláusula 7: Control de acceso a la LAN.

Objetivo 7.1: Requerimientos para el control de acceso a la LAN.

Para controlar el acceso a la información.

Control 7.1.1: *Política de control de acceso a la LAN.*

La política definirá los requerimientos para el control de acceso a la LAN y deben estar documentados. Las reglas y derechos del control de acceso para cada usuario o grupo de ellos deben estar claramente establecidos en la declaración de la política de acceso. La política debe tomar en cuenta lo siguiente:

- Consistencia entre el control de acceso y las políticas de clasificación de la información de los diferentes sistemas y redes.
- Legislación relevante y cualquier obligación contractual considerando la protección del acceso a datos o servicios.
- Perfiles de acceso de usuarios estándar para categorías comunes de trabajo.
- Administración de derechos de acceso en un entorno distribuido y de red que reconozca todos los tipos de conexiones disponibles.

Objetivo 7.2: Administración de acceso de los usuarios a la LAN.
Para prevenir accesos no autorizados a los sistemas de información.

Control 7.2.1: *Registro del usuario.*

Debe existir un procedimiento de registro y eliminación de usuarios que le concedan acceso a la red y a los servicios de la misma. El proceso formal de registro de usuarios debe incluir:

- El uso único de ID para que los usuarios puedan conectarse y hacerlos responsables de sus acciones.
- Revisar que los usuarios tengan la autorización de la administración para el uso de los servicios y sistemas de información.
- Revisar que el nivel de acceso garantizado es apropiado para el propósito de la organización y es consistente con las políticas de seguridad de la misma.
- Dar a los usuarios una declaración escrita de sus derechos de acceso.
- Pedir a los usuarios que firmen un acuerdo indicando que entienden las condiciones de acceso.
- Asegurar que los proveedores de servicio no proporcionan acceso hasta que los procedimientos de autorización han sido completados.
- Mantener un registro formal de todas las personas registradas para el uso del servicio.
- Remover inmediatamente los derechos de acceso de usuarios que han cambiado de puesto o han dejado la organización.
- Revisar periódicamente y remover ID's redundantes de usuarios.
- Asegurar que ID's redundantes no sean manejadas por otros usuarios.

Control 7.2.2: *Administración de privilegios de cuentas de usuario de red.*

La designación y uso de privilegios serán restringidos y controlados mediante un procedimiento establecido. Para la protección contra accesos no autorizados se debe tener la asignación de privilegios controlados a través de un proceso formal de autorización. Se deben considerar los siguientes pasos:

- Los privilegios asociados a cada sistema deben ser identificados.
- Debe ser mantenido un proceso de autorización y registro de todos los privilegios asignados. Los privilegios no deben ser asignados hasta que el proceso de autorización esté completo.
- El desarrollo y uso de rutinas del sistema deben ser promovidos para evitar la necesidad de proporcionar privilegios del sistema a usuarios.
- Los privilegios deben ser asignados para una identidad de usuario diferente de aquéllos usados para propósito general.

Control 7.2.3: *Administración de passwords de red.*

Mediante un proceso formal de administración será controlada la creación/designación, revisión y eliminación de los passwords.

Control 7.2.4: *Revisión de los privilegios de acceso a la red.*

Se llevará un procedimiento formal para la revisión regular de los privilegios de acceso. Para mantener un control efectivo de los derechos de acceso a la red se debe revisar que:

- Los derechos de acceso de los usuarios son revisados en intervalos regulares y después de cambios.
- La autorización para privilegios especiales de derechos de acceso debe ser revisada en intervalos más frecuentes.

Objetivo 7.3: Responsabilidades del usuario.
Para prevenir acceso de usuarios no autorizados.

Control 7.3.1: *Uso de los passwords de red.*

Los usuarios de la red realizarán buena práctica y uso de sus passwords. Todos los usuarios deben estar advertidos para:

- Mantener la confidencialidad de sus passwords.
- Evitar mantener un documento escrito del password a menos que pueda ser almacenado seguramente.
- Cambiar los passwords donde haya cualquier indicación de compromisos posibles.
- Seleccionar passwords con una longitud mínima de seis caracteres, fácil de recordar, no basado en información personal y combinar caracteres alfanuméricos.

- Cambiar passwords en intervalos regulares o basados en el número de accesos y evitar reutilizar passwords antiguos.
- No compartir passwords individuales.

Control 7.3.2: *Protección del equipo no atendido.*

Es deber del usuario proteger adecuadamente, mediante los procedimientos mínimos de seguridad, el equipo temporalmente no atendido.

Objetivo 7.4: Control de acceso a la LAN.
Para la protección de los servicios de red.

Control 7.4.1: *Política de uso de los servicios de la red.*

Se dará autorización de uso a los servicios sólo a usuarios que tengan accesos específicos y responsabilidad de los mismos. Esta política debe ser formulada incluyendo el uso de redes y sus servicios; ésta debe cubrir:

- Las redes y sus servicios que tienen acceso permitido.
- Procedimientos de autorización para determinar quién tiene permitido acceder a estas redes y sus servicios.
- Controles y procedimientos de administración para proteger el acceso a las conexiones de red y sus servicios.

Control 7.4.2: *Autenticación de cuentas de usuarios externos.*

Todos los usuarios externos deberán tener acceso autentificado. Es importante determinar en un análisis de riesgos el nivel de protección requerido y seleccionar el método de autenticación apropiado.

Control 7.4.3: *Segregación de la LAN.*

Se introducirán controles para seccionar sistemas de información, servicios y usuarios. Un método para controlar la seguridad de redes grandes es dividirla en dominios de red, cada uno protegido por un perímetro de seguridad definido. Tal perímetro puede ser implementado instalando un gateway seguro entre las dos redes a ser interconectadas y para controlar el flujo de información entre los dos dominios (firewall). El criterio para la segregación de redes debe estar basado en la política de control de acceso y los requerimientos de acceso.

Objetivo 7.5: Monitoreo de acceso y uso de la red de actividades no autorizadas.
Estos sistemas deben ser monitoreados y registrados para detectar desviaciones de las políticas de control de acceso y para proporcionar evidencia en caso de incidentes de seguridad.

Control 7.5.1: *Logging de acontecimientos.*

Se llevarán a cabo tiempos de monitoreo producidos y mantenidos durante el control de acceso. El registro de logs de auditoría y de otros eventos relevantes de seguridad debe ser realizado y mantenido por un periodo para futuras investigaciones y monitoreos de accesos. Deben incluir ID's de usuarios, datos y tiempos de inicio y fin de sesión, localización y registros de intentos de acceso exitosos o fallidos.

Objetivo 7.6: Cómputo móvil.
Para asegurar la seguridad de la información cuando se usa la computación móvil.

Control 7.6.1: *Cómputo móvil.*

Las políticas y controles deberán proteger a la LAN contra los riesgos de trabajo de los usuarios externos. Una política formal debe ser adoptada para tomar en cuenta los posibles riesgos del cómputo móvil. Esta política debe incluir los requerimientos para protección física, controles de acceso, técnicas de criptografía, respaldo y protección contra virus. Debe también incluir reglas y recomendaciones para la conexión móvil a la red en lugares públicos.

Cláusula 8: Desarrollo de seguridad de una LAN.

Objetivo 8.1: Controles criptográficos.
Para proteger la confidencialidad, autenticidad e integridad de la información con el uso de estos controles criptográficos.

Control 8.1.1: *Política para el uso de controles criptográficos.*

Sólo serán desarrollados para la protección de la información, tomando una decisión para saber si una solución criptográfica es apropiada; deben ser vistas como parte de un proceso más amplio de una valoración de riesgos y de una selección de controles.

Control 8.1.2: *Encripción.*

Será utilizada para protección de la confidencialidad de la información crítica o sensible, basada en una valoración de riesgos. El nivel requerido de protección debe ser identificado tomando en cuenta: el tipo, la calidad del algoritmo de encripción y la longitud de la clave a ser usada.

Control 8.1.3: *Firma digital.*

Será aplicada para proteger la veracidad y la integridad de información electrónica. Puede ser implementada usando una técnica criptográfica basada únicamente en pares relacionados de claves, donde una clave es usada para crear una firma (clave

privada) y la otra para revisar la firma (clave pública). Considerar la necesidad de establecer el tipo y calidad del algoritmo de firma y la longitud de la clave a ser usados. La clave criptográfica usada para la firma digital debe ser diferente a aquélla usada para la encripción.

Control 8.1.4: *Servicios de no-repudio.*

Serán usados donde pueden ser necesarios para resolver problemas de discordancia de eventos de ocurrencia o no-ocurrencia. Estos servicios están basados en el uso de técnicas de encripción y firma digital.

Control 8.1.5: *Administración de claves criptográficas.*

Se buscará la confidencialidad para el soporte de las técnicas criptográficas. Todas las claves criptográficas deben ser protegidas contra modificación y destrucción. Las claves secretas y privadas necesitan protección contra revelaciones no autorizadas. Las técnicas criptográficas pueden ser usadas para este propósito. La protección física debe ser usada en el equipo utilizado para generar, almacenar y archivar dichas claves.

Un sistema de administración de claves debe estar basado en conjunto de estándares, procedimientos y métodos seguros acordados, para generar claves de diferentes sistemas criptográficos y diferentes aplicaciones; generar y obtener claves certificadas, cambio y actualización de claves, y el archivo o destrucción de claves.

Objetivo 8.2: Seguridad en los procesos de desarrollo y soporte.
Para mantener la seguridad de sistemas de aplicación e información.

Control 8.2.1: *Proceso del control de los cambios.*

Este controlará los procedimientos de implementación de cambios y minimizará la corrupción de los sistemas de información. Un procedimiento formal de control de cambios debe ser aplicado para garantizar que la seguridad y procedimientos de control no sean comprometidos. Este proceso incluirá:

- Mantener un registro de los niveles de autorización acordados.
- Revisar que los controles y procedimientos mantengan la integridad, para asegurar que los cambios no los comprometan.
- Mantener una versión de control para todas las actualizaciones de software.
- Mantener una pista de auditoría de todos los cambios requeridos.

Control 8.2.2: *Revisión técnica de cambio de sistema operativo.*

Cuando ocurra un cambio en los sistemas de aplicación, serán revisados y probados.

Cláusula 9: Obediencia.

Objetivo 9.1: Obediencia con los requerimientos legales.
Para evitar violaciones de cualquier legislación.

Control 9.1.1: *Verificación de la legislación aplicable.*

Estos requerimientos se definirán explícitamente, mediante documentación, para cada sistema de información relacionado con la LAN.

Control 9.1.2: *Derechos de propiedad intelectual.*

Mediante las verificaciones legales se implementarán procedimientos para el uso de material de propiedad intelectual respecto al derecho del producto del software.

Control 9.1.3: *Protección de la privacidad de los usuarios y su información.*

Se realizará de acuerdo a la legislación existente por medio de una estructura y control apropiado de la administración.

Control 9.1.4: *Regulación de controles criptográficos.*

Toda relación con el control de acceso y uso de controles criptográficos será regulada mediante legislaciones relacionadas a su uso.

Control 9.1.5: *Colección de la evidencia.*

La producción de evidencias se efectuará mediante prácticas estándares.

Objetivo 9.2: Revisión de políticas de seguridad y obediencia técnica.
Para asegurar la obediencia de los sistemas de la LAN con políticas y estándares de seguridad organizacional.

Control 9.2.1: *Obediencia con políticas de seguridad.*

La administración debe asegurar que todos los procedimientos de seguridad, dentro de su área de responsabilidad, están implementados correctamente. Además, deben ser consideradas revisiones regulares para asegurar la obediencia con estándares y políticas de seguridad que deben incluir:

- Sistemas de información.
- Proveedores de sistemas.
- Propietarios de bienes.
- Usuarios.
- Administradores.

Control 9.2.2: *Revisión de obediencia técnica.*

La implementación y regulación de los sistemas de la LAN serán logradas mediante estándares de seguridad. Requiere la asistencia técnica de especialistas.

Objetivo 9.3: Consideraciones de auditoría de la LAN.
Para maximizar la efectividad y minimizar la interferencia de los procesos de auditoría de la LAN.

Control 9.3.1: *Monitoreo del control interno.*

La administración deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones por medio de supervisiones, comparaciones y exámenes de los controles de seguridad de la LAN. Las desviaciones deberán generar análisis, acciones correctivas y reportes a la alta gerencia. Los exámenes serán repetidos periódicamente y verificados por auditorías independientes para asegurar el correcto funcionamiento de los controles.

Control 9.3.2: *Estatutos de auditoría.*

Se establecerá un estatuto para la función de auditoría estableciendo la responsabilidad, autoridad y obligaciones de la función auditora. El documento será revisado periódicamente para asegurar que se mantiene la independencia, autoridad y responsabilidad de la función de auditoría.

Control 9.3.3: *Controles de auditoría.*

Las auditorías serán planeadas cuidadosamente para eliminar riesgos de disrupción de los procesos. Se debe observar lo siguiente:

- Los requerimientos de auditoría deben estar de acuerdo con la administración.
- El alcance de las revisiones debe ser acordado y controlado.
- Las revisiones deben ser limitadas a accesos de sólo lectura.
- Los recursos de TI para las revisiones deben estar explícitamente identificados y disponibles.
- Todos los procedimientos, requerimientos y responsabilidades deben ser documentados.
- Se establecerá un plan de auditoría para garantizar un aseguramiento independiente con respecto a la seguridad de la LAN y los procedimientos de control interno.
- La auditoría deberá asegurar el cumplimiento de los códigos aplicables de ética profesional y estándares de auditoría.

Control 9.3.4: *Protección de las herramientas de auditoría.*

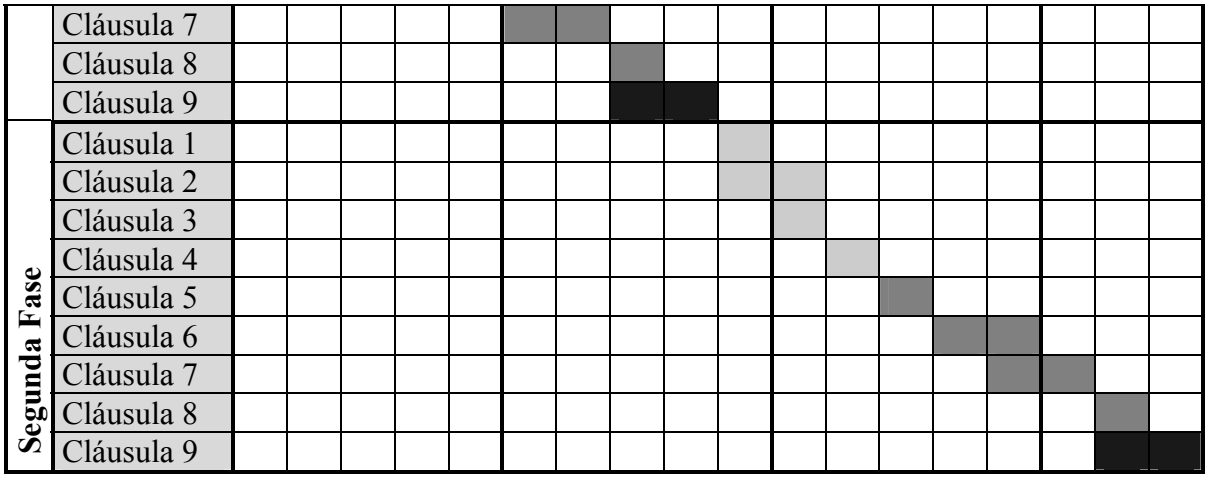
Todas las herramientas de auditoría serán protegidas para prevenir cualquier mal uso o por comprometer el sistema.

Como se puede ver el número de objetivos de control y controles para cada una de las nueve cláusulas no es homogéneo. Por lo tanto no se realizará la auditoría como estaba planeado, difiriendo un poco de la siguiente manera:

Día	Controles a auditar	# de controles
1	C.1.1.1-C.2.2.2	9
2	C.2.3.1-C.3.2.3	8
3	C.4.1.1-C.4.3.5	8
4	C.5.1.1-C.5.2.5	8
5	C.6.1.1-C.6.4.4	8
6	C.6.5.1-C.7.2.3	8
7	C.7.2.4-C.7.6.1	8
8	C.8.1.1-C.9.1.2	9
9	C.9.1.3-C.9.3.4	9
		75

Tabla 4. 2 Controles a auditar por día

Tareas		**1ª Semana**					**2ª Semana**					**3ª Semana**					**4ª Sem.**		
Primera Fase	Cláusula 1																		
	Cláusula 2																		
	Cláusula 3																		
	Cláusula 4																		
	Cláusula 5																		
	Cláusula 6																		



2 auditores expertos en gestión de controles de seguridad
2 auditores expertos en seguridad de redes
1 auditor experto en legislación

Tabla 4. 3 Programación corregida de las actividades de auditoría

El segundo paso de la realización de la auditoría (de esta fase) es el siguiente:

2. Ponderación de los sectores auditados.

Las nueve cláusulas o sectores de la seguridad de la LAN serán ponderadas tanto por los auditores como por los auditados de la siguiente forma.

Primero el equipo auditor asignará los pesos técnicos, esto es, una ponderación de cada una de las cláusulas de control definidas y de todos los objetivos de control que nosotros hemos definido. Posteriormente la organización auditada asignará los pesos políticos, o sea, la misma ponderación anterior pero desde la perspectiva del cliente. A continuación se asignarán los pesos finales de las cláusulas y los objetivos. Estos pesos finales son el promedio del peso técnico y del peso político. Los controles serán evaluados, pero no ponderados.

En este primer paso de la realización de la auditoría se pondera la importancia de la seguridad de la LAN, en los diversos sectores que la conforman. Las asignaciones de pesos a objetivos y cláusulas se realizarán de la siguiente manera:

- Considerando que tenemos nueve cláusulas de control relativas a la seguridad de la LAN, la suma de todos los pesos técnicos de las cláusulas será igual a cien; asimismo la suma de los pesos políticos será cien. Este total de cien puntos es el que se ha asignado a la totalidad del área de la seguridad de la red y se mantiene sin importar el número de cláusulas.

A continuación se mostrarán los pesos técnicos que hemos considerado para cada una de las cláusulas de control y para cada uno de los objetivos; la asignación de los pesos políticos sólo podrá realizarse hasta que se realice la auditoría de forma práctica.

Cláusulas de control	Pesos técnicos (Pt)	Pesos políticos (Pp)	Pesos finales [Pf=(Pt+Pp)/2]
C.1. Políticas de seguridad.	15	-	-
C.2. Gobierno de la seguridad.	13	-	-
C.3. Control y clasificación de bienes.	10	-	-
C.4. Seguridad de los empleados.	9	-	-
C.5. Seguridad física de la LAN y su entorno.	9	-	-
C.6. Administración de las comunicaciones.	11	-	-
C.7. Control de acceso a la LAN.	15	-	-
C.8. Desarrollo de seguridad de una LAN.	9	-	-
C.9. Obediencia.	9	-	-
Total	100	100	100

Tabla 4. 4 Ponderación de cláusulas de control

Cláusula 1: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.1.1. Políticas de seguridad de la LAN.	100	-	-
Total	100	100	100

Tabla 4. 5 Ponderación de los objetivos de la cláusula 1

Cláusula 2: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.2.1. Administración de seguridad de la LAN.	50	-	-
O.2.2. Seguridad en el acceso a la LAN por terceras personas.	20	-	-
O.2.3. Análisis de riesgos.	30	-	-
Total	100	100	100

Tabla 4. 6 Ponderación de los objetivos de la cláusula 2

Cláusula 3: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.3.1. Responsabilidad de los bienes o activos.	50	-	-
O.3.2. Clasificación de la información.	50	-	-
Total	100	100	100

Tabla 4. 7 Ponderación de los objetivos de la cláusula 3

Cláusula 4: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.4.1. Seguridad en la definición de puestos.	25	-	-
O.4.2. Entrenamiento del personal.	50	-	-

O.4.3. Respuesta a incidentes de seguridad de la LAN.	25	-	-
Total	100	100	100

Tabla 4. 8 Ponderación de los objetivos de la cláusula 4

Cláusula 5: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.5.1. Aseguramiento de áreas de la red y su entorno.	50	-	-
O.5.2. Seguridad del equipo de la LAN.	50	-	-
Total	100	100	100

Tabla 4. 9 Ponderación de los objetivos de la cláusula 5

Cláusula 6: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.6.1. Procedimientos y responsabilidades.	30	-	-
O.6.2. Protección contra software malicioso.	15	-	-
O.6.3. Back up.	15	-	-
O.6.4. Administración de la LAN.	25	-	-
O.6.5. Intercambio de información.	15	-	-
Total	100	100	100

Tabla 4. 10 Ponderación de los objetivos de la cláusula 6

Cláusula 7: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.7.1. Requerimientos para el control de acceso a la LAN.	17	-	-
O.7.2. Administración de acceso de los usuarios a la LAN.	17	-	-
O.7.3. Responsabilidades del usuario.	15	-	-
O.7.4. Control de acceso a la LAN.	17	-	-
O.7.5. Monitoreo de acceso y uso de la red de actividades no autorizadas.	17	-	-
O.7.6. Cómputo móvil.	17	-	-
Total	100	100	100

Tabla 4. 11 Ponderación de los objetivos de la cláusula 7

Cláusula 8: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.8.1. Controles criptográficos.	60	-	-
O.8.2. Seguridad en los procesos de desarrollo y soporte.	40	-	-
Total	100	100	100

Tabla 4. 12 Ponderación de los objetivos de la cláusula 8

Cláusula 9: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.9.1. Obediencia con los requerimientos legales.	33	-	-

O.9.2. Revisión de políticas de seguridad y obediencia técnica.	34	-	-
O.9.3. Consideraciones de auditoría de la LAN.	33	-	-
Total	100	100	100

Tabla 4. 13 Ponderación de los objetivos de la cláusula 9

3. Entrevistas y cuestionarios.

Este tercer paso de la realización de la auditoría constituye realmente la primera fase operativa de la obtención de la evidencia, que será realizada fundamentalmente a partir de la realización de entrevistas específicas al personal auditado, señalado en el punto de los recursos de la auditoría.

Las entrevistas deben realizarse con exactitud y su realización adecuada constituye uno de los factores fundamentales del éxito de la auditoría. La adecuación comienza con la completa cooperación del entrevistado; si ésta no se produce, el auditor lo hará saber al cliente.

Las entrevistas son la base de las relaciones personales con el auditado. Se hacen de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
- Mediante entrevistas que no siguen un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
- Mediante entrevistas en las que los auditores siguen un método preestablecido y buscan unas finalidades concretas.

La entrevista es una de las actividades personales más importantes del auditor, en ella se recoge más información y mejor matizada que la proporcionada por medios puramente técnicos o por las respuestas a cuestionarios. La entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas y sencillas. Sin embargo, esta sencillez es sólo aparente; tras ella debe existir una preparación muy elaborada y sistematizada, diferente para cada caso particular.

Deben realizarse varias entrevistas del mismo tema, al menos a dos o tres niveles jerárquicos distintos. En esta auditoría y por su ámbito, será necesario y conveniente entrevistar a la misma persona sobre distintos aspectos de las cláusulas. Después de la realización de las entrevistas se procederá a la aplicación de los cuestionarios, los cuáles serán elaborados a partir de los controles, objetivos y cláusulas que hemos definido.

Salvo excepciones, los cuestionarios deben ser contestados oralmente, ya que superan en riqueza y generalización a cualquier otra forma. Es importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, pero todavía lo es más el modo y el orden de su formulación. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar los cuestionarios de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de los cuestionarios utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios responden fundamentalmente a dos tipos de “filosofía” de calificación o evaluación:

a) De rango, contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. Esta es la forma de calificación que hemos adoptado.
b) Binarios, constituidos por preguntas con respuesta única y excluyente: Sí o No.

Los cuestionarios de rango son adecuados si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que los binarios. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor. Los cuestionarios binarios siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidos, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <sí o no> frente a la mayor riqueza del intervalo.

A continuación mostraremos cuestionarios de extensión variable para cada uno de los controles. Durante la realización de esta fase de la auditoría los auditores calificarán las respuestas del auditado (mismas que serán anotadas), sin estar este último presente, con una escala del uno al cinco, que corresponden a los siguientes significados:

1: Muy deficiente.
2: Deficiente.

3: Mejorable.
4: Aceptable.
5: Correcto.

CUESTIONARIOS DE SEGURIDAD EN LAN

Cláusula 1. Políticas de seguridad.

Objetivo 1.1. Políticas de seguridad de la LAN.

Control 1.1.1. *Documento de políticas de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un documento de políticas de seguridad de la información que incluya la seguridad de la LAN?		
- ¿Este documento está aprobado, publicado y comunicado a todos los empleados?		
- ¿Sabe de qué trata el documento? ¿Comprende el contenido?		
- ¿El documento incluye la definición, objetivos, alcance y responsabilidades de la seguridad de la LAN?		
Total control 1.1.1.		?/20 ?%

Tabla 4. 14 Cuestionario control 1.1.1

Control 1.1.2. *Revisión y evaluación de las políticas de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son revisadas o redefinidas periódicamente las políticas de seguridad de la LAN?		
- ¿Con qué frecuencia se realizan?		
- ¿Qué actividades se realizan en estas revisiones periódicas?		
Total control 1.1.2.		?/15 ?%

Tabla 4. 15 Cuestionario control 1.1.2

Cláusula 2. Gobierno de la seguridad.

Objetivo 2.1. Administración de seguridad de la LAN.

Control 2.1.1. *Gestión de administración y coordinación de la seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen representantes de las áreas clave de la organización en la administración de la seguridad de la LAN? ¿De qué áreas?		
- ¿La coordinación de la seguridad de la LAN revisa y aprueba las políticas de la seguridad de la red?		

- ¿La coordinación de la seguridad de la red considera el monitoreo de las amenazas y de los incidentes de seguridad?		
- ¿La coordinación de la seguridad de la LAN ha definido los roles y responsabilidades para la seguridad de la red?		
- ¿La administración considera a la seguridad dentro de la planeación de la red? ¿De qué forma?		
Total control 2.1.1.		?/25 ?%

Tabla 4. 16 Cuestionario control 2.1.1

Control 2.1.2. *Asignación de responsabilidades de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está definida en las políticas de seguridad una guía para la asignación de roles y responsabilidades de la seguridad de la LAN?		
- ¿Existe un documento en el que estén definidas las responsabilidades de la seguridad de la red?		
- ¿Existe un propietario o responsable para cada activo o proceso de la red?		
Total control 2.1.2.		?/15 ?%

Tabla 4. 17 Cuestionario control 2.1.2

Control 2.1.3. *Asesoramiento de especialistas en seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿En qué eventos/situaciones se recurre al asesoramiento de algún especialista en seguridad de la LAN?		
- ¿En cuánto tiempo es llamado el experto en seguridad desde que ocurre el suceso?		
- ¿Con qué privilegios cuenta el asesor/consultor en los sistemas?		
Total control 2.1.3.		?/15 ?%

Tabla 4. 18 Cuestionario control 2.1.3

Control 2.1.4. *Revisión independiente de la seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿La seguridad de la red es revisada por auditores externos o internos independientes?		
- ¿Qué revisan los auditores en la seguridad de la red? ¿Cuáles son sus objetivos?		
Total control 2.1.4.		?/10 ?%

Tabla 4. 19 Cuestionario control 2.1.4

Control 2.1.5. *Reacreditación.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un grupo especial para mantener actualizado el nivel de seguridad de la red?		
- ¿Qué técnicas utiliza para verificar la seguridad de la red?		
- ¿Es conocido este grupo sólo por la alta directiva (red teaming) o son públicas sus actividades (blue teaming)?		
Total control 2.1.5.		?/15 ?%

Tabla 4. 20 Cuestionario control 2.1.5

Objetivo 2.2. Seguridad en el acceso a la LAN por terceras personas.

Control 2.2.1. *Identificación de riesgos de acceso de terceras personas a la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se contempla al acceso no autorizado de terceras personas en el análisis de riesgos o cualquier otro estudio?		
- ¿Qué controles se han implementado para combatir el riesgo de accesos no autorizados a la red?		
- ¿Se ha definido claramente la identidad de las terceras personas físicas? ¿Cuáles son?		
- ¿Se ha definido expresamente la identidad de las terceras personas lógicas? ¿Cuáles son?		
- ¿Qué controles se han implementado para los accesos del personal de mantenimiento/soporte, limpieza, servicio social, etc.?		
Total control 2.2.1.		?/20 ?%

Tabla 4. 21 Cuestionario control 2.2.1

Control 2.2.2. *Especificaciones de seguridad en contratos con terceras personas.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Incluyen acuerdos formales para la seguridad de la LAN los contratos con terceras personas?		
- ¿Qué consideraciones mínimas de seguridad de la LAN involucra un contrato?		
- ¿En el contrato anterior se incluyen la política de seguridad de la LAN, los acuerdos de control de acceso y el derecho de monitoreo de la LAN?		
Total control 2.2.2.		?/15 ?%

Tabla 4. 22 Cuestionario control 2.2.2

Objetivo 2.3. Análisis de riesgos.

Control 2.3.1. *Evaluación de riesgos de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza una evaluación de riesgos de la seguridad de la LAN?		
- En la evaluación de riesgos, ¿se determina la forma en que deben ser manejados los riesgos de la seguridad de la red?		
- ¿La administración realiza reevaluaciones de riesgos, actualizados con auditorías o estudios anteriores?		
Total control 2.3.1.		?/15 ?%

Tabla 4. 23 Cuestionario control 2.3.1

Control 2.3.2. *Identificación y medición de riesgos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué tipos de riesgos se han identificado en la evaluación de riesgos de la LAN?		
- ¿Se les da a estos riesgos un tipo de clasificación cualitativa y cuantitativa de acuerdo a su impacto?		
- ¿Se han implementado controles para contrarrestar este tipo de riesgos?		
Total control 2.3.2.		?/15 ?%

Tabla 4. 24 Cuestionario control 2.3.2

Control 2.3.3. *Plan de acción contra riesgos.*		
Preguntas	**Respuestas**	**Puntos**
¿Está definido un plan de acción contra riesgos?		
¿Cuáles son sus beneficios y objetivos?		
Total control 2.3.3.		?/10 ?%

Tabla 4. 25 Cuestionario control 2.3.3

Cláusula 3. Control y clasificación de bienes.

Objetivo 3.1. Responsabilidad de los bienes o activos.

Control 3.1.1. *Inventario de bienes relacionados con la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un inventario de bienes relacionados con la LAN?		

- ¿Se realiza una actualización de dicho inventario? ¿Cada cuándo se realiza?		
- ¿Se incluye en el inventario el valor relativo e importancia de cada bien?		
- ¿Qué tipo de bienes incluye este inventario?		
Total control 3.1.1.		?/20 ?%

Tabla 4. 26 Cuestionario control 3.1.1

Control 3.1.2. *Responsabilidad de los bienes relacionados con la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está definido el responsable de los activos inventariados?		
- ¿Está documentado, actualizado y es revisado periódicamente?		
Total control 3.1.2.		?/10 ?%

Tabla 4. 27 Cuestionario control 3.1.2

Objetivo 3.2. Clasificación de la información.

Control 3.2.1. *Manuales de clasificación de la información.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen manuales de clasificación de la información?		
- ¿Cuál es el objetivo de estos manuales?		
Total control 3.2.1.		?/10 ?%

Tabla 4. 28 Cuestionario control 3.2.1

Control 3.2.2. *Manuales de clasificación de niveles de seguridad en la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está definida e implementada la clasificación de los niveles de seguridad en la LAN?		
- ¿Para qué han sido definidos estos niveles de seguridad?		
- ¿Qué niveles de seguridad se han definido?		
Total control 3.2.2.		?/15 ?%

Tabla 4. 29 Cuestionario control 3.2.2

Control 3.2.3. *Manejo y rotulación de la información.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Han sido definidos procedimientos para el manejo y rotulación de la información?		
- ¿Qué incluyen y cuál es el alcance de estos procedimientos?		
Total control 3.2.3.		?/10

	?%

Tabla 4. 30 Cuestionario control 3.2.3

Cláusula 4. Seguridad de los empleados.

Objetivo 4.1. Seguridad en la definición de puestos.

Control 4.1.1. *Incluir la seguridad en las responsabilidades de puestos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se encuentran definidos y documentados los roles y responsabilidades de seguridad de la LAN en los puestos de trabajo?		
- ¿Se han asignado prácticamente a los puestos de trabajo?		
Total control 4.1.1.		?/10 ?%

Tabla 4. 31 Cuestionario control 4.1.1

Control 4.1.2. *Términos y condiciones de empleo.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son establecidas responsabilidades respecto a la seguridad de la LAN en los términos y condiciones del contrato de los empleados?		
- ¿Qué aspectos incluyen?		
- ¿Se consideran acuerdos de confidencialidad y responsabilidades legales?		
- ¿Las responsabilidades definidas continúan después del término del empleo?		
Total control 4.1.2.		?/20 ?%

Tabla 4. 32 Cuestionario control 4.1.2

Objetivo 4.2. Entrenamiento del personal.

Control 4.2.1. *Entrenamiento y culturización en seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Los empleados reciben adecuados entrenamiento/actualización en seguridad de la red? ¿Cuáles empleados?		
- ¿Se promueve un entrenamiento sobre concientización de la seguridad de la red? ¿De qué forma?		
- ¿Con qué frecuencia se realizan estos entrenamientos descritos?		
Total control 4.2.1.		?/15 ?%

Tabla 4. 33 Cuestionario control 4.2.1

Objetivo 4.3. Respuesta a incidentes de seguridad de la LAN.

Control 4.3.1. *Reporte de incidentes de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son reportados los incidentes de seguridad de la red?		
- ¿Existe un procedimiento formal de reporte de estos incidentes?		
- ¿Existe un procedimiento de respuesta a incidentes de seguridad?		
- ¿Qué tan rápido son reportados y atendidos los incidentes de seguridad?		
Total control 4.3.1.		?/20 ?%

Tabla 4. 34 Cuestionario control 4.3.1

Control 4.3.2. *Reporte de debilidades de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son reportadas por los usuarios las debilidades de la LAN?		
- ¿Con qué agilidad son reportadas y atendidas tales debilidades?		
- ¿Existe un procedimiento formal adecuado para su reporte?		
Total control 4.3.2.		?/15 ?%

Tabla 4. 35 Cuestionario control 4.3.2

Control 4.3.3. *Reporte de mal funcionamiento del software en la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son reportados los malos funcionamientos del software?		
- ¿Existe un procedimiento establecido para realizar/atender los reportes de mal funcionamiento de software?		
- ¿Qué acciones son tomadas inicialmente en el reporte/atención del mal funcionamiento de software?		
Total control 4.3.3.		?/15 ?%

Tabla 4. 36 Cuestionario control 4.3.3

Control 4.3.4. *Aprendizaje de los incidentes.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento para cuantificar los costos de los incidentes de seguridad y del mal funcionamiento de software?		
- Los costos/daños de los incidentes anteriores ¿son usados en el análisis de riesgos, en la mejora continua o algún tipo de análisis?		
Total control 4.3.4.		?/10 ?%

Tabla 4. 37 Cuestionario control 4.3.4

Control 4.3.5. Disciplina en seguridad de la LAN.		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué acciones son tomadas cuando se viola alguna política o procedimiento que afecte la seguridad de la red?		
Total control 4.3.5.		?/5 ?%

Tabla 4. 38 Cuestionario control 4.3.5

Cláusula 5. Seguridad física de la LAN y su entorno.

Objetivo 5.1. Aseguramiento de áreas de la red y su entorno.

Control 5.1.1. *Perímetro de seguridad física.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe y está bien definido un perímetro físico de seguridad para proteger las áreas de la red? ¿Está formado por varias capas?		
- ¿Por qué se ha establecido (bajo qué análisis) este perímetro de seguridad?		
- ¿Qué controles de seguridad física se han establecido para el site y otras áreas de la LAN?		
- ¿Poseen alarmas las salidas de emergencia del perímetro de seguridad?		
Total control 5.1.1.		?/20 ?%

Tabla 4. 39 Cuestionario control 5.1.1

Control 5.1.2. *Controles de entrada física.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué controles de acceso existen en las áreas sensibles de la red?		
- ¿Se maneja un procedimiento para el acceso y estancia de visitantes a las áreas seguras de la red? ¿Es registrado su tiempo de acceso y de salida?		
- ¿Qué controles de autenticación son usados para validar los accesos? ¿Se lleva un registro de todos los accesos?		
- ¿Todo el personal porta visiblemente una identificación?		
- ¿Son revisados y actualizados los derechos de acceso a las áreas seguras de la red?		
Total control 5.1.2.		?/25 ?%

Tabla 4. 40 Cuestionario control 5.1.2

Control 5.1.3. *Seguridad de las áreas de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- En el área de la LAN, ¿se consideran controles contra la posibilidad de desastres naturales y humanos?		
- ¿Qué elementos se consideran para mantener la discreción de las instalaciones de la red?		
- ¿Se han instalado sistemas de detección de intrusos, alarmas o circuito cerrado para monitorear el acceso a las áreas críticas de la red?		
- ¿Se mantienen aislados del site los materiales peligrosos?		
- ¿Qué medidas físicas y de construcción se tienen en cuenta para la protección del site?		
Total control 5.1.3.		?/25 ?%

Tabla 4. 41 Cuestionario control 5.1.3

Objetivo 5.2. Seguridad del equipo de la LAN.

Control 5.2.1. *Colocación y protección del equipo de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué consideraciones se han implementado para la colocación y protección del equipo de la red?		
- ¿Se ha colocado el equipo de red de tal forma que se minimice su acceso y visibilidad?		
- ¿Qué controles se han implementado para proteger al equipo de la red contra amenazas naturales e interferencia electromagnética?		
- ¿Se han implementado políticas para evitar que el personal coma y fume cerca del equipo de red?		
Total control 5.2.1.		?/20 ?%

Tabla 4. 42 Cuestionario control 5.2.1

Control 5.2.2. *Suministro de energía ininterrumpible.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué medidas protegen la disponibilidad de la LAN contra fallos de energía?		
- ¿Tienen esta protección los sistemas críticos de la red?		
Total control 5.2.2.		?/10 ?%

Tabla 4. 43 Cuestionario control 5.2.2

Control 5.2.3. *Seguridad del cableado de la LAN y su alimentación.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué protecciones se han establecido en el cableado de comunicaciones y energía?		
- ¿Está protegido el cableado de la red contra la intercepción, daño o interferencia?		
- ¿Existen localizaciones especiales para las conexiones de los sistemas críticos?		
- ¿Se considera el uso de la fibra óptica y de barridos oculares o electrónicos del cableado para localizar pinchamientos?		
Total control 5.2.3.		?/20 ?%

Tabla 4. 44 Cuestionario control 5.2.3

Control 5.2.4. *Mantenimiento del equipo de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Recibe el equipo de la red mantenimiento periódico?		
- ¿Se realiza este mantenimiento con procedimientos y personal adecuados y autorizados?		
- ¿Se tiene un registro de todas las operaciones de mantenimiento?		
- ¿Se consideran controles especiales cuando el equipo es llevado fuera de las instalaciones?		
Total control 5.2.4.		?/20 ?%

Tabla 4. 45 Cuestionario control 5.2.4

Control 5.2.5. *Seguridad en el desecho y re-uso del equipo de red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué procedimiento se realiza con el equipo de desecho de la red que contiene información o configuraciones?		
- ¿Son sometidos los equipos especiales a un análisis de riesgos o a alguna evaluación para determinar su destino?		
Total control 5.2.5.		?/10 ?%

Tabla 4. 46 Cuestionario control 5.2.5

Cláusula 6. Administración de las comunicaciones y las operaciones de la LAN.

Objetivo 6.1. Procedimientos y responsabilidades.

Control 6.1.1. *Documentación de procedimientos de operación de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe la documentación de los procedimientos de operación de la LAN? ¿Son mantenidos como documentos formales?		
- ¿Qué instrucciones detalladas generales se encuentran en estos		

procedimientos?		
Total control 6.1.1.		?/10 ?%

Tabla 4. 47 Cuestionario control 6.1.1

Control 6.1.2. *Control de cambios operacionales.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen procedimientos que controlen los cambios al equipo, software y procedimientos relacionados con la LAN?		
- ¿Qué controles se han establecido en estos procedimientos?		
- ¿Se ha considerado la valoración del impacto potencial de estos cambios, su aprobación formal y su comunicación?		
Total control 6.1.2.		?/15 ?%

Tabla 4. 48 Cuestionario control 6.1.2

Control 6.1.3. *Procedimientos para la gestión de incidentes.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen procedimientos y responsabilidades para la gestión de incidentes de seguridad relacionados con la LAN?		
- ¿Qué tipos de incidentes cubren estos procedimientos?		
- ¿Cuáles son los pasos básicos de estos procedimientos?		
- ¿Se considera la colección apropiada de la evidencia para fines forenses?		
- ¿Qué acciones se consideran para la recuperación de incidentes?		
Total control 6.1.3.		?/25 ?%

Tabla 4. 49 Cuestionario control 6.1.3

Control 6.1.4. *Separación de responsabilidades.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se considera la segregación en las responsabilidades o tareas relacionadas con la seguridad de la red?		
- ¿Se considera que el personal únicamente realice las tareas definidas en su puesto?		
- ¿Se encuentran segregadas la Administración de la red, la Administración de la seguridad y el Área de Auditoría?		
Total control 6.1.4.		?/15 ?%

Tabla 4. 50 Cuestionario control 6.1.4

Objetivo 6.2. Protección contra software malicioso.

Control 6.2.1. *Controles contra software malicioso.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué controles existen contra el software malicioso?		
- ¿Existe una política para el cumplimiento de las licencias en todo el software de la organización?		
- ¿Existen controles de seguridad para la conexión a redes externas?		
- ¿Existen procedimientos y responsabilidades para los eventos y procesos relacionados con antivirus?		
- ¿Se realizan revisiones regulares de software y datos en los sistemas críticos, revisión de correos electrónicos y descargas?		
Total control 6.2.1.		?/25 ?%

Tabla 4. 51 Cuestionario control 6.2.1

Objetivo 6.3. Back up.

Control 6.3.1. *Respaldo de información.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realizan regularmente respaldos de información de los sistemas críticos de la LAN? ¿De qué forma?		
- ¿Qué consideraciones se tienen en los respaldos de la red? ¿Son revisados regularmente? ¿Se considera la destrucción total del site?		
Total control 6.3.1.		?/10 ?%

Tabla 4. 52 Cuestionario control 6.3.1

Control 6.3.2. *Logs de operación.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se mantiene y revisa un registro de los logs, de los sistemas críticos de la red?		
- ¿Qué información contienen los logs de operación?		
Total control 6.3.2.		?/10 ?%

Tabla 4. 53 Cuestionario control 6.3.2

Objetivo 6.4. Administración de la LAN.

Control 6.4.1. *Controles de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen controles explícitos para la seguridad de la LAN? ¿Son revisados, implementados y mantenidos?		
- ¿Está explícitamente separada de otras operaciones la responsabilidad de la seguridad de la red?		

- ¿Han sido establecidas las responsabilidades y procedimientos de la administración del equipo remoto?		
- ¿Qué controles se han establecido para la protección de la confidencialidad e integridad de los datos que transitan por la LAN y la red pública?		
Total control 6.4.1.		?/20 ?%

Tabla 4. 54 Cuestionario control 6.4.1

Objetivo 6.5. Intercambio de información.

Control 6.5.1. *Seguridad de la información en tránsito por la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está protegida la información en tránsito en su confidencialidad, integridad y disponibilidad?		
- ¿Qué técnicas se usan para la confidencialidad de la información en tránsito?		
Total control 6.5.1.		?/10 ?%

Tabla 4. 55 Cuestionario control 6.5.1

Control 6.5.2. *Seguridad del comercio electrónico.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se han considerado controles para la mantener la seguridad del comercio electrónico?		
- ¿Qué tipo de eventos y transacciones son protegidas? ¿Mediante qué mecanismos?		
Total control 6.5.2.		?/10 ?%

Tabla 4. 56 Cuestionario control 6.5.2

Control 6.5.3. *Seguridad del correo electrónico.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen políticas y controles para el uso del correo electrónico?		
- ¿Qué controles y procedimientos se han establecido para la seguridad en su uso?		
- ¿Se responsabiliza a los empleados que comprometan la seguridad? ¿De qué forma?		
Total control 6.5.3.		?/15 ?%

Tabla 4. 57 Cuestionario control 6.5.3

Control 6.5.4. *Seguridad en sistemas disponibles públicamente.*

Preguntas	Respuestas	Puntos
- ¿Está autorizada y protegida la información pública de la organización? ¿De qué forma está protegida?		
- ¿Se ha eliminado la posibilidad de acceso por este medio a la red organizacional?		
Total control 6.5.4.		?/10 ?%

Tabla 4. 58 Cuestionario control 6.5.4

Cláusula 7. Control de acceso a la LAN.

Objetivo 7.1. Requerimientos para el control de acceso a la LAN.

Control 7.1.1. *Política de control de acceso a la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está definida y documentada una política para el control de acceso a la LAN, estableciendo reglas y derechos de acceso a los usuarios?		
- ¿Existe consistencia entre el control de acceso y la clasificación de la información?		
- ¿Están definidas obligaciones contractuales para el acceso a datos y servicios?		
Total control 7.1.1.		?/15 ?%

Tabla 4. 59 Cuestionario control 7.1.1

Objetivo 7.2. Administración de acceso de los usuarios a la LAN.

Control 7.2.1. *Registro del usuario.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento de registro y borrado de cuentas de usuario? ¿Qué incluye?		
- ¿Revisa el procedimiento que el nivel de acceso sea apropiado y consistente con las políticas de seguridad?		
- ¿Los usuarios firman un acuerdo de condiciones de acceso?		
- ¿Las cuentas son revisadas periódicamente y removidas para evitar redundancia o mal manejo?		
Total control 7.2.1.		?/20 ?%

Tabla 4. 60 Cuestionario control 7.2.1

Control 7.2.2. *Administración de privilegios de cuentas de usuario de red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento para designar, autorizar y usar		

privilegios de cuentas de acceso a la red?		
- ¿Qué consideraciones se incluyen en este procedimiento?		
- ¿Son identificados los privilegios asociados a cada sistema?		
Total control 7.2.2.		?/15 ?%

Tabla 4. 61 Cuestionario control 7.2.2

Control 7.2.3. *Administración de passwords de red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento de administración para controlar todos los procesos de los passwords de la red? ¿Qué incluye?		
Total control 7.2.3.		?/5 ?%

Tabla 4. 62 Cuestionario control 7.2.3

Control 7.2.4. *Revisión de los privilegios de acceso a la red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento formal para la revisión regular de los privilegios de acceso a la red? ¿Qué aspectos trata?		
Total control 7.2.4.		?/5 ?%

Tabla 4. 63 Cuestionario control 7.2.4

Objetivo 7.3. Responsabilidades del usuario.

Control 7.3.1. *Uso de los passwords de red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe una práctica para advertir a los usuarios sobre el buen uso de los passwords?		
- ¿Qué prácticas son dadas a conocer a los usuarios?		
Total control 7.3.1.		?/10 ?%

Tabla 4. 64 Cuestionario control 7.3.1

Control 7.3.2. *Protección del equipo no atendido.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué medidas deben realizar los usuarios para proteger el equipo no atendido?		
Total control 7.3.2.		?/5 ?%

Tabla 4. 65 Cuestionario control 7.3.2

Objetivo 7.4. Control de acceso a la LAN.

Control 7.4.1. *Política de uso de los servicios de la red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe una política que defina y autorice el uso de los servicios de red?		
- ¿Qué incluye la política? ¿Se consideran procedimientos de autorización y protección?		
Total control 7.4.1.		?/10 ?%

Tabla 4. 66 Cuestionario control 7.4.1

Control 7.4.2. *Autenticación de cuentas de usuarios externos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Tienen un control de acceso autentificado los usuarios externos a la LAN? ¿Qué método usan?		
Total control 7.4.2.		?/5 ?%

Tabla 4. 67 Cuestionario control 7.4.2

Control 7.4.3. *Segregación de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen controles o implementaciones para segregar la LAN?		
- ¿Es protegido cada segmento con algún sistema de seguridad? ¿Cuál es el uso de los firewalls?		
- ¿Bajo qué criterios se realiza la segregación de la LAN?		
Total control 7.4.3.		?/15 ?%

Tabla 4. 68 Cuestionario control 7.4.3

Objetivo 7.5. Monitoreo de acceso y uso de la red de actividades no autorizadas.

Control 7.5.1. *Logging de acontecimientos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza un monitoreo y registro del acceso/uso de la red?		
- ¿Qué información es registrada durante estos accesos?		
Total control 7.5.1.		?/10 ?%

Tabla 4. 69 Cuestionario control 7.5.1

Objetivo 7.6. Cómputo móvil.

Control 7.6.1. *Cómputo móvil.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Están definidas políticas y controles para cubrir los riesgos del cómputo móvil?		
- ¿Qué consideraciones y controles se incluyen?		
Total control 7.6.1.		?/10 ?%

Tabla 4. 70 Cuestionario control 7.6.1

Cláusula 8. Desarrollo de seguridad de una LAN.

Objetivo 8.1. Controles criptográficos.

Control 8.1.1. *Política para el uso de controles criptográficos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe una política para el uso de controles criptográficos? ¿Cuáles son usados?		
- ¿La criptografía usada se basa en una decisión tomada a partir de un análisis de riesgos?		
Total control 8.1.1.		?/10 ?%

Tabla 4. 71 Cuestionario control 8.1.1

Control 8.1.2. *Encripción.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Es usada la encripción el algún proceso? ¿Para qué es usada?		
- ¿Su uso y características (de la encripción) son basados en un análisis de riesgos?		
Total control 8.1.2.		?/10 ?%

Tabla 4. 72 Cuestionario control 8.1.2

Control 8.1.3. *Firma digital.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Es usada la firma digital? ¿Cuál es el objetivo?		
- ¿Qué algoritmo se usa y bajo qué análisis se determinó?		
Total control 8.1.3.		?/10 ?%

Tabla 4. 73 Cuestionario control 8.1.3

Control 8.1.4. *Servicios de no-repudio.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son usados servicios de no-repudio? ¿Cuáles y para qué son usados		
Total control 8.1.4.		?/10 ?%

Tabla 4. 74 Cuestionario control 8.1.4

Control 8.1.5. *Administración de claves criptográficas.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza un proceso de administración de claves criptográficas?		
- ¿Qué aspectos físicos se consideran para su protección?		
- ¿Qué método/sistema de administración de claves se usa?		
Total control 8.1.5.		?/15 ?%

Tabla 4. 75 Cuestionario control 8.1.5

Objetivo 8.2. Seguridad en los procesos de desarrollo y soporte.

Control 8.2.1. *Proceso del control de los cambios.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento para la implementación de los cambios del sistema de la red?		
- ¿Qué aspectos se incluyen en este procedimiento? ¿Se controla la versión del software usado?		
Total control 8.2.1.		?/10 ?%

Tabla 4. 76 Cuestionario control 8.2.1

Control 8.2.2. *Revisión técnica de cambio de sistema operativo.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza una revisión y aprobación para realizar cambios al sistema operativo? ¿Qué incluye esta revisión técnica?		
Total control 8.2.2.		?/5 ?%

Tabla 4. 77 Cuestionario control 8.2.2

Cláusula 9. Obediencia.

Objetivo 9.1. Obediencia con los requerimientos legales.

Control 9.1.1. *Verificación de la legislación aplicable.*

Preguntas	Respuestas	Puntos
- ¿Son verificados los requerimientos de la legislación aplicable a la seguridad de la red?		
Total control 9.1.1.		?/5 ?%

Tabla 4. 78 Cuestionario control 9.1.1

Control 9.1.2. *Derechos de propiedad intelectual.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son verificados los derechos de propiedad intelectual mediante un procedimiento de revisión?		
Total control 9.1.2.		?/5 ?%

Tabla 4. 79 Cuestionario control 9.1.2

Control 9.1.3. *Protección de la privacidad de los usuarios y su información.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un control y administración para la protección de la privacidad de la información de los empleados?		
Total control 9.1.3.		?/5 ?%

Tabla 4. 80 Cuestionario control 9.1.3

Control 9.1.4. *Regulación de controles criptográficos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está regulado y verificado el uso de controles criptográficos?		
Total control 9.1.4.		?/5 ?%

Tabla 4. 81 Cuestionario control 9.1.4

Control 9.1.5. *Colección de la evidencia.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Las evidencias colectadas siguen algún estándar?		
Total control 9.1.5.		?/5 ?%

Tabla 4. 82 Cuestionario control 9.1.5

Objetivo 9.2. Revisión de políticas de seguridad y obediencia técnica.

Control 9.2.1. *Obediencia con políticas de seguridad.*

Preguntas	Respuestas	Puntos
- ¿Se realiza un análisis y una revisión para asegurar la implementación correcta de los procedimientos de seguridad?		
- ¿Qué aspectos se consideran para esta obediencia?		
Total control 9.2.1.		?/10 ?%

Tabla 4. 83 Cuestionario control 9.2.1

Control 9.2.2. *Revisión de obediencia técnica.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza una revisión especializada para el cumplimiento técnico de los sistemas de la LAN? ¿Usan especialistas?		
Total control 9.2.2.		?/5 ?%

Tabla 4. 84 Cuestionario control 9.2.2

Objetivo 9.3. Consideraciones de auditoría de la LAN.

Control 9.3.1. *Monitoreo del control interno.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se efectúa un monitoreo de la efectividad de los controles internos de seguridad de la red?		
- ¿Las desviaciones de la efectividad son analizadas, reportadas y corregidas?		
- ¿Los controles internos y su efectividad son verificados por auditorías?		
Total control 9.3.1.		?/15 ?%

Tabla 4. 85 Cuestionario control 9.3.1

Control 9.3.2. *Estatutos de auditoría.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se ha definido un estatuto para las funciones de auditoría? ¿Qué contiene?		
Total control 9.3.2.		?/5 ?%

Tabla 4. 86 Cuestionario control 9.3.2

Control 9.3.3. *Controles de auditoría.*		
Preguntas	**Respuestas**	**Puntos**

- ¿Se han establecido controles de auditoría que involucren la seguridad de la red?		
- ¿Qué controles se consideran en su planeación (de la auditoría)?		
Total control 9.3.3.		?/10 ?%

Tabla 4. 87 Cuestionario control 9.3.3

Control 9.3.4. *Protección de las herramientas de auditoría.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué medidas se han establecido para proteger las herramientas de auditoría?		
Total control 9.3.4.		?/5 ?%

Tabla 4. 88 Cuestionario control 9.3.4

4. Realización de pruebas.

Posteriormente a las entrevistas, según nuestro plan, se procederá a la realización de las pruebas para verificar los datos solicitados y facilitados por el cliente, constituye la segunda fase operativa de la realización de la auditoría. Inicialmente se obtendrá la documentación de los controles implementados por la organización auditada, respecto a cada uno de los procesos identificados en las cláusulas, los objetivos y los controles.

Para la evaluación se revisará que las políticas, procedimientos y cualquier documento en general garanticen la observancia del control. Después se calificará el grado de cumplimiento al realizar un conjunto de pruebas apropiadas a los objetivos de control.

DOCUMENTACIÓN.

En este punto la evidencia a buscar será del tipo documental, revisando todos los documentos sobre políticas y procedimientos. Esta evidencia es la siguiente:

Control 1.1.1
- Documento de políticas de seguridad de la LAN, o un documento que las contenga.

Control 1.1.2
- Documento de la última revisión y/o evaluación periódica de la seguridad de la LAN.

Control 2.1.1
- Existencia de un departamento o función que administre y coordine la seguridad de la LAN.
- Documento que defina la función y objetivo de este departamento y su organigrama.

Control 2.1.2

- Documento que defina claramente la asignación de las responsabilidades de la seguridad de la LAN.
- Guía general para la asignación de roles y responsabilidades.

Control 2.1.3

- Documento de políticas de seguridad de la LAN que contenga la idea de este control y contemple la necesidad del asesoramiento de especialistas en seguridad.
- Documentos recientes sobre la descripción del trabajo realizado por estos especialistas o asesores.

Control 2.1.4

- Documento de políticas de seguridad que contemple la revisión de la seguridad independiente por auditores.
- Informe de revisión de seguridad realizado por auditores internos y/o externos.

Control 2.1.5

- Documento de políticas de seguridad que contemple la verificación de la seguridad de la LAN por un grupo técnico incógnito.
- Informes recientes de esta verificación de la seguridad.
- Procedimientos de verificación de la seguridad de la LAN utilizados por este grupo.

Control 2.2.1

- Políticas de seguridad sobre la identificación de riesgos de acceso de terceras personas.
- Documento de análisis de riesgos de accesos no autorizados.

Control 2.2.2

- Política sobre especificaciones de seguridad en contratos con terceras personas relacionados con la LAN.
- Contratos recientes con terceras personas relacionados con la LAN.

Control 3.1.1

- Documento de políticas que incluya un control sobre el inventario de bienes.
- Inventario actualizado de bienes informáticos o de la red.

Control 3.1.2

- Documento de políticas que incluya la responsabilidad de los bienes de la LAN.
- Documento actualizado de responsabilidades de activos de la red.

Control 3.2.1

- Documento de políticas que incluya la elaboración de manuales de la clasificación de la información.
- Manual de clasificación de la información.

Control 3.2.2

- Documento de políticas que incluya la elaboración de manuales de clasificación de niveles de seguridad de la LAN.
- Manual de clasificación de niveles de seguridad de la LAN.
- Manual de clasificación de la información.

Control 3.2.3

- Documento de políticas que incluya el manejo y rotulación de la información.
- Procedimientos del manejo y rotulación de la información.
- Manual de clasificación de la información.

Control 4.1.1

- Documento de políticas que incluya la definición y asignación de los roles y responsabilidades de la seguridad de la LAN en todos los puestos de trabajo.
- Documento de definición de responsabilidades de puestos.

Control 4.1.2

- Documento de política de términos y condiciones de empleo.
- Documento de términos y condiciones de contrato, acuerdos o cláusulas de responsabilidades legales.

Control 4.2.1

- Documento de políticas donde se incluya el entrenamiento y culturización en la seguridad.
- Programa de actividades de entrenamiento y cursos de seguridad.

Control 4.3.1

- Documento de políticas para reportes de incidentes de seguridad de la LAN.
- Procedimiento del reporte para incidentes de seguridad.
- Un registro de incidentes recientes y las acciones tomadas en los mismos.

Control 4.3.2

- Política del reporte de debilidades de seguridad de la LAN.
- Procedimientos para el reporte de incidentes que contenga las debilidades reportadas.
- Registro que incluya las debilidades reportadas y su seguimiento.

Control 4.3.3

- Política del reporte de mal funcionamiento del software en la LAN.
- Procedimientos para el reporte y atención del mal funcionamiento del software.
- Registro de los reportes y de sus soluciones al mal funcionamiento del software.

Control 4.3.4

- Política donde se incluya el aprendizaje de los incidentes.
- Documento de análisis de riesgos recientes.

Control 4.3.5
- Política de disciplina de seguridad.

Control 5.1.1
- Política donde se incluya la definición del perímetro de seguridad física.
- Documento de análisis de riesgos.

Control 5.1.2
- Políticas donde se incluyan los controles de entrada física a las áreas sensibles.
- Registros actualizados de accesos físicos.
- Documento de derechos de acceso.

Control 5.1.3
- Documento de políticas para la seguridad de las áreas de la LAN.
- Reglamento para la salud y seguridad física de las áreas de la LAN.

Control 5.2.1
- Documento de políticas de seguridad que trate de la debida colocación y protección del equipo de la LAN.
- Reglamento de controles internos para la protección del equipo de la LAN.

Control 5.2.2
- Políticas de seguridad para el suministro de energía ininterrumpible para los sistemas críticos de la red.

Control 5.2.3
- Documento de políticas de seguridad para la seguridad del cableado de la LAN y su alimentación.
- Planos de diseño del cableado estructurado actualizado de toda la organización.

Control 5.2.4
- Documento de políticas de seguridad que contemple el mantenimiento del equipo de la LAN.
- Documento de recomendaciones del los proveedores para el mantenimiento de los mismos.
- Registro actualizado de las operaciones de mantenimiento de los proveedores a sus respectivos equipos.

Control 5.2.5
- Política que contemple la seguridad en el desecho y re-uso del equipo de red.
- Documento de análisis de riesgos.
- Registro actualizado de los equipos desechados y/o re-usados.

Control 6.1.1
- Documento de política para la operación de la LAN.

- Procedimientos de operación de la LAN.

Control 6.1.2
- Documento de políticas para los cambios operacionales.
- Procedimientos para el control de cambios operacionales.

Control 6.1.3
- Documento de políticas para la gestión de incidentes.
- Procedimientos para la administración de incidentes.
- Documento de definición de responsabilidades de puestos.

Control 6.1.4
- Políticas para la separación de responsabilidades.
- Guía general para la asignación de roles y responsabilidades.
- Documento de definición de responsabilidades de puestos.

Control 6.2.1
- Políticas de seguridad para protección contra software malicioso.
- Política de licencias autorizadas de software.
- Registros regulares de instalación y actualizaciones de antivirus y/o parches.
- Registros de pasados ataques de virus, sus consecuencias y las acciones tomadas.
- Procedimientos para la detección de software malicioso que entra a la red.
- Documento de definición de responsabilidades de puestos.

Control 6.3.1
- Políticas de seguridad para el respaldo de la información.
- Procedimientos para el respaldo de la información, su protección y almacenaje.

Control 6.3.2
- Documento de políticas que contemple los logs de operación.
- Registros y revisiones regulares de las actividades con logs.

Control 6.4.1
- Política que defina la administración de la LAN.
- Documento que contenga los controles de la administración de la seguridad de la LAN.
- Documento que defina claramente la asignación de las responsabilidades de la seguridad de la LAN.

Control 6.5.1
- Política que contemple la seguridad de la información en tránsito por la red.
- Procedimientos para la firma digital y la encripción de la información.

Control 6.5.2
- Política que defina la seguridad del comercio electrónico.

- Procedimientos para el comercio electrónico.

Control 6.5.3
- Documento de política que defina la seguridad de correo electrónico.
- Documento de definición de responsabilidades de puestos.
- Procedimientos y/o controles para la seguridad de correo electrónico.

Control 6.5.4
- Política que defina la seguridad en los sistemas disponibles públicamente.
- Procedimientos y mecanismos para la seguridad en los sistemas disponibles públicamente.

Control 7.1.1
- Documento de políticas de control de acceso a la LAN.
- Documento de políticas de clasificación de la información.
- Legislación de obligaciones contractuales.

Control 7.2.1
- Políticas para el registro de usuarios de la red.
- Procedimiento de registro y eliminación de usuarios para el acceso a la red y a sus servicios.

Control 7.2.2
- Políticas para la administración de los privilegios de las cuentas de los usuarios de la LAN.
- Procedimiento para la designación, restricción y control de los privilegios de la red.
- Registro actualizado de todos los privilegios autorizados y asignados.

Control 7.2.3
- Políticas para la administración de passwords de acceso a la red.
- Procedimiento de administración para el control de la creación, designación, revisión y eliminación de los passwords.
- Registro actualizado de todos los passwords.

Control 7.2.4
- Documento de políticas para la revisión de los privilegios de acceso a la red.
- Procedimientos para este control.
- Documento de las últimas revisiones de estos privilegios.

Control 7.3.1
- Políticas para el usuario en el uso de los passwords.
- Documento de definición de responsabilidades de puestos.
- Reglamento para la buena práctica y uso de los passwords.

Control 7.3.2

- Políticas para la seguridad del equipo no atendido.
- Documento de definición de responsabilidades de puestos.
- Procedimientos para la protección del equipo no atendido.

Control 7.4.1
- Documento de políticas de uso de los servicios de la LAN.
- Procedimientos de autorización para determinar el acceso a la red y sus servicios.

Control 7.4.2
- Políticas para la autenticación de cuentas para usuarios externos de la red.
- Procedimiento del método para la autenticación de usuarios.

Control 7.4.3
- Políticas para la segregación de la LAN.
- Procedimientos, controles y/o métodos para este control.

Control 7.5.1
- Políticas para el monitoreo de accesos y uso de la red.
- Procesos para el monitoreo de la seguridad de la LAN.
- Registros regulares y actualizados de logs sobre acontecimientos relevantes de seguridad en la red.

Control 7.6.1
- Políticas de seguridad para la LAN en el uso de cómputo móvil.
- Procedimientos para la protección de la red en el uso de cómputo móvil.
- Reglamentos y recomendaciones para la conexión móvil a la LAN.

Control 8.1.1
- Política para el uso de criptografía.
- Procedimientos para el uso de criptografía.
- Documento de análisis de riesgos para el uso de criptografía.
- Manual de clasificación de niveles de seguridad de la LAN.

Control 8.1.2
- Políticas para el uso de encripción.
- Procedimientos para el uso de encripción.
- Documento de análisis de riesgos para el uso de encripción.
- Manual de clasificación de niveles de seguridad de la LAN.

Control 8.1.3
- Políticas en el uso de firma digital.
- Procedimientos para el uso de firma digital.
- Manual de clasificación de niveles de seguridad de la LAN.

Control 8.1.4

- Documento de políticas para los servicios de no-repudio.
- Procedimientos para el uso de este tipo de servicios.

Control 8.1.5
- Políticas para la administración de claves criptográficas.
- Procedimientos para la protección, creación, modificación, destrucción, almacenaje y archivo de las claves criptográficas.
- Estándares, procedimientos y/o métodos para la administración de claves criptográficas.

Control 8.2.1
- Políticas para la seguridad en el control de los cambios en los procesos de desarrollo y soporte.
- Procedimientos para la implementación de cambios de los sistemas de información.
- Procedimientos para el control de cambios.
- Documento de los registros de las ultimas versiones y de los actuales cambios.

Control 8.2.2
- Políticas de seguridad en los cambios de sistema operativo.
- Procedimientos para los cambios de sistema operativo.
- Procedimientos para la revisión y pruebas en los cambios de sistema operativo.

Control 9.1.1
- Documento de legislación actualizada para cada sistema de información relacionado con la LAN.

Control 9.1.2
- Política que contemple los derechos de propiedad intelectual.
- Documento de contratos de derechos de propiedad intelectual.
- Procedimientos para el uso y manejo del material con derecho de propiedad intelectual.

Control 9.1.3
- Política para la protección de la privacidad del usuario y su información.
- Documento legislativo que contemple este control.

Control 9.1.4
- Política que trate la regulación de controles criptográficos.
- Documento legislativo que regule el uso de estos controles.

Control 9.1.5
- Políticas que contemple la colección de la evidencia.
- Estándares para la producción de evidencias.
- Procedimientos para la producción de éstas.

Control 9.2.1

- Informes de revisiones regulares y recientes a los procedimientos de seguridad para asegurar que la administración está implementándolos correctamente y que además asegure la obediencia de las políticas de seguridad.
- Programa de estas revisiones.

Control 9.2.2
- Informes de revisiones regulares de obediencia técnica por parte de una asistencia técnica especializada.

Control 9.3.1
- Políticas para el monitoreo del control interno de la red.
- Registros periódicos del monitoreo de control interno.
- Procedimientos de este monitoreo.
- Documento de análisis, acciones reportadas y correctivas, proporcionado por los auditores internos, o auditores independientes si es el caso.

Control 9.3.2
- Política que trate los estatutos de auditoría.
- Revisiones periódicas y actualizadas para asegurar la independencia y responsabilidad de la función de auditoría.

Control 9.3.3
- Política que trate los controles de la auditoría.
- Documento de la planeación de la auditoría.
- Documento de los procedimientos, requerimientos y responsabilidades de la auditoría.
- Documento de código de ética profesional y estándares de auditoría.

Control 9.3.4
- Política para la protección de las herramientas de auditoría.

PRUEBAS.

No es parte del alcance de este trabajo el cubrir las pruebas, exámenes y procedimientos de seguridad que se realizan en las auditorías, debido a su complejidad, el dominio técnico y la experiencia de un auditor que las lleva a cabo para verificar que los controles documentados se han implementado. Casi a manera de ejemplo mostraremos algunos procedimientos de auditoría de SI, tomados de los procedimientos de ISACA y del NIST:

a. Procedimientos para la firma digital y la administración de claves.

- Determinar si la Autoridad de Certificación (AC) tiene o no una estructura de organización efectiva capaz de facilitar la efectiva administración de la información y de sistemas.
- Determinar si la AC ha recibido acreditación apropiada por organizaciones de estándares internacionales para asegurar comunicaciones.

- Identificar que servicios ofrecen las AC, como registro de usuarios, distribución, actualización, respaldo, recuperación, revocación, redistribución, deshabilitación y rehabilitación de claves. Determinar si los servicios de administración y operación de las AC, y los servicios externos son adecuados.
- Determinar si existe y si es efectivo un programa de entrenamiento y si es un proceso continuo. Una de las más grandes amenazas de seguridad es la falta de conocimiento.
- Determinar si las AC específicamente cumplen con BS 7799 (ISO 17799) u otro estándar aplicable para la estructura de la seguridad organizacional.
- Determinar si una evaluación de seguridad formal ha sido realizada y obtenida una certificación.
- Determinar si la certificación de calidad ISO 9000 ha sido obtenida.
- Determinar si las AC tienen un manual de operación pública para cumplir con los requerimientos de legislación para la acreditación de AC's. Solicitar la acreditación, las AC publican el manual de operación que detalla las responsabilidades y operaciones de las AC y sus controles, el suministro y uso de los servicios.
- Determinar si la seguridad de la recuperación y respaldo de claves es mantenido. En el caso de que la información de clave de un usuario es accidentalmente borrada o el usuario olvida su password, debe ser siempre posible recuperar la clave, si la seguridad no es comprometida.
- Determinar si las AC tienen un adecuado plan de recuperación de desastres. La recuperación de desastres junto con un efectivo procedimiento de respaldo proporciona la seguridad razonable de la continuidad de operaciones en el caso de que las AC experimenten una disrupción para esta primera operación.
- Determinar si hay soporte centralizado para administrar la encripción de claves. La administración de claves requiere varias funciones: actualización, respaldo, recuperación, revocación, redistribución, inhabilitación y rehabilitación. Estas funciones deben ser tratadas centralmente y la administración central de claves ayuda a mantener la integridad del sistema.
- Determinar si las AC proporcionan una política y procedimientos completos y detallados. La tecnología sola no es suficiente para proporcionar seguridad razonable. Los controles organizacionales (documentación de políticas, procedimientos, estándares y guías; educación técnica; conciencia de seguridad; y una administración aprobada) también son extremadamente importantes.
- Determinar si la actualización de claves es obligatoria (conforme a la política organizacional), segura y transparentemente.
- Determinar si las AC mantienen registros de eventos relevantes de seguridad. Una pista de auditoría segura reduce el riesgo de compromiso y también ayuda a contener cualquier daño que pudiera suceder hacia la violación de la seguridad.

b. Procedimientos para la detección de intrusos.

Determinar si:

- Una tercera parte proporciona información y asistencia en respuesta a incidentes.
- El sistema comunica firewalls y/o routers y si esta comunicación es segura, o si es una red y/o canal separado requerido para comunicaciones seguras.

- El IDS incluye una herramienta para generación de reportes escritos que resuma los eventos diarios.
- Existe la disponibilidad de mecanismos de respuesta automatizada.

Proporcionar seguridad razonable de que:

- Las firmas son actualizadas a menudo.
- Las actualizaciones son distribuidas vía un método seguro (como encripción o sellado digital).
- Los IDS pueden detectar varios diferentes tipos de ataques.
- Existe información de que el último ataque es usado para mantener actualizado el IDS.
- El IDS tiene la capacidad de analizar los protocolos de aplicación de nivel superior con suficiente detalle.
- Los IDS no requieren software para ser instalado en el host.
- Las comunicaciones entre el censor y el administrador central son lo suficientemente robustos.
- La alarma de captura es confiable. Si un alto volumen de alarmas es generado todas ellas deben ser capturadas y puestas en una base de datos.
- Los datos obtenidos de los IDS son apropiada y eficientemente administrados.
- Un detallado procedimiento en el lugar, explicando las acciones a ser tomadas cuando el IDS detecte problemas.
- El mecanismo de operación de los IDS es conocido por el personal.
- El IDS puede ser usado para realizar otra actividad de administración de red adjunta como la administración de dispositivos de red.
- El IDS es apropiado para el despliegue sobre el perímetro de la red así como dentro de la red.
- El IDS detecta abusos generados internamente por usuarios no autorizados por un largo periodo de tiempo.
- La lista de gente teniendo acceso al IDS es pequeña y controlada.
- El IDS saca provecho de los logs producidos por otros sistemas.
- El IDS está integrado con otros productos de evaluación de vulnerabilidad.
- El método para alertar a la administración de la seguridad y operación del IDS es eficiente y efectivo.

c. Procedimientos para virus y lógica maliciosa.

- Examinar evaluaciones y análisis administrativos de los recursos críticos y los tipos de protección a implementar. La política organizacional antivirus debe estar basada en una evaluación de riesgos y vulnerabilidades para la mejor protección de los sistemas de información de la organización.
- Identificar todos los posibles tipos de entradas a los sistemas computacionales.
    - Medios físicos (diskettes, CD-ROMs y medios removibles).
    - Periféricos para PC (módems, dispositivos conectados vía serial, USB o puertos infrarrojos).

  - Conexiones remotas de laptops operando fuera de la organización.
- Examinar las políticas antivirus para usuarios finales, porque diferentes tipos de usuarios pueden tener diferentes comportamientos, recursos y métodos disponibles para perpetuar el virus. El resultado de este análisis serán útiles en la revisión de las políticas de la organización para determinar si éste es apropiado y si direcciona todos los riesgos asociados con los usuarios de los sistemas de la organización.
- Examinar las medidas de las políticas antivirus propuestas para evitar la infección de virus. Éste consiste principalmente de los procedimientos organizacionales y de la comunicación dentro de la organización.
- Revisión de las políticas organizacionales sobre software no autorizado para determinar qué restricciones existen en torno a esta situación y cómo estas restricciones son impuestas. La organización debe tener métodos para detectar y evaluar el riesgo de software no autorizado siendo instalado y empleado.
- Examinar las políticas para mitigar el riesgo de infección de virus (acciones preventivas para evitar la infección).
  - Los tipos de documentos o archivos que pueden resultar perjudiciales.
  - El riesgo asociado con e-mails.
  - Reportar comportamientos sospechosos de los sistemas en uso.
  - Los usuarios toman una parte importante de la prevención tentativa contra virus. Uno de sus roles es identificar potenciales fuentes de infección.
- Determinar si la política de software antivirus está claramente definida y aplicada.
- Examinar los procedimientos de la organización para el reporte de ocurrencias de virus. Ésta debe incluir a quién en la organización se le debe reportar la identificación de un virus (helpdesk, taskforce antivirus), procedimientos de respuesta a incidentes y reporte del evento. También deben incluir especificaciones de qué procedimientos deben ser seguidos, límites de quién puede deshabilitar o alterar la configuración de software antivirus instalado en Workstations de usuarios, escalación y reporte de procedimientos.
- Revisión de procedimientos existentes diseñados para detener el brote de un virus y para el correcto recurso infectado en caso de que un virus no sea detectado y erradicado por el software antivirus.
- Proporcionar seguridad razonable para que la política antivirus esté absolutamente documentada y con procedimientos escritos para implementarla como un nivel más detallado. Cualquier procedimiento sin una adecuada documentación es inefectivo.
- Proporcionar seguridad razonable de que los usuarios estén entrenados en el procedimiento para una política de seguridad antivirus, incluyendo el testeo de material aprendido.

d. Procedimiento para revisar firewalls.

Reunir información preeliminar:

- Obtener la política de seguridad del firewall.
- Identificar los servicios que el firewall debe proteger.
- Revisar un análisis de la red existente, la identificación de los puntos de entrada, los tipos de tráfico manejados por los firewalls, las alarmas y el esquema de notificación.

- Revisar el plan para manejar las pruebas de penetración.
- Identificar las reglas de filtrado. Verificar que todo firewall restringe todo acceso, a excepción de lo especificado por las reglas.

Filtrado de paquetes:

- Cuando el router es usado como el firewall perimetral y existe otro firewall detrás, documentar cómo afecta esto a los controles proporcionados por el otro firewall.
- Obtener información de cómo está siendo usado el filtrado de paquetes.
- Valorar el efecto en los controles e identificar las áreas clave de riesgos creados por el filtrado de paquetes. Confirmar que:
    - Sólo se permite acceso a aquellas direcciones que tratan de ser accedidas del exterior.
    - No se permite el uso de servicios no autorizados, como FTP y Telnet.
    - No se permite el acceso a ciertos puertos.
    - Sólo se permiten paquetes que provienen de sitios autorizados del exterior de la red.
- Confirmar que existen reglas para evitar falsificación de la IP (IP spoofing).
- Evaluar reglas de control de acceso u otras medidas para excluir paquetes que representen comunicaciones no deseables como DoS o ataques.

Firewalls híbridos:

- Documentar cómo el uso del firewall híbrido afecta a los controles de la red.
- Investigar cómo los tres tipos de firewalls están siendo usados (filtrado de paquetes, inspección de estado y proxy servers). Determinar qué lógica se usa para el paso del tráfico en cada tipo.
- Valorar el efecto en los controles e identificar las áreas clave de riesgos creados por una aproximación híbrida.

Proxy firewalls:

- Investigar el uso del proxy (qué tráfico es mandado por él y qué dispositivos reciben la salida).

Configuración general:

- Verificar que el firewall es invisible desde el exterior.
- Confirmar que cada regla en el firewall es consistente con la política de seguridad.
- DNS, e-mail o cualquier software o servicios no relacionados con las funciones del firewall no deben estar instalados o procesados por el firewall.
- Deben estar configurados para ocultar información DNS de redes externas.
- Un router usado como firewall no proporciona una solución firewall. Verificar qué más se implementa en este caso.
- Ocultar información de la red de fuentes externas.
- Configurar los firewalls para denegar todos los servicios menos los explícitamente permitidos.
- Traducir direcciones de nodos internos de la red que tienen comunicación con redes externas.
- Escanear, filtrar o bloquear Java, JavaScript y Activex.

- Aplicar fuertes medidas de seguridad al host donde reside el firewall.
- Aplicar los debidos parches de seguridad a los componentes del sistema firewall.
- Determinar qué procedimientos existen para verificar políticas (prueba de penetración, etc.).
- Verificar las herramientas de integridad para los archivos sensibles del sistema donde está el firewall.
- Monitorear las alertas del firewall en una base regular.
- Registrar con logs toda actividad del firewall.

e. Procedimiento para evaluar el control sobre metodologías de encripción.

- Verificar que el proceso usado para seleccionar un algoritmo de encripción es el más efectivo y eficiente. Para determinar el mejor algoritmo se debe considerar el ambiente donde opera.
- Revisar la documentación que asegura que el algoritmo escogido asegura toda la protección al nivel deseado, es efectivo en costo y conveniente.
- Verificar la integración con la arquitectura del sistema. El sistema de encripción no debe interferir con la operación normal del sistema.
- Verificar que la clave del sistema criptográfico asegura todas las propiedades requeridas, incluyendo longitud, composición y administración de la clave.
- Averiguar si la clave del sistema criptográfico es fácil de generar y modificar.
- Averiguar si la clave para acceder al sistema criptográfico no es fácilmente adivinable.

5. Cruzamiento de información y calificación.

En esta parte de la realización de la auditoría, los auditores calificarán las dos partes de la evidencia obtenidas anteriormente (pasos 3 y 4). Primero se realizará una revisión y evaluación de las entrevistas y cuestionarios. Hay que ser cuidadosos en dos cuestiones: es posible que algunos de los controles no apliquen para el tipo de organización que estamos auditando, debido a las características particulares del organismo y de los sistemas de información implementados. Por otro lado, dada la estructuración de los cuestionarios para los controles, varias de las preguntas están seriadas, esto es, si la primera pregunta resulta ser negativa las siguientes también lo serán. De esta manera se tendrá un especial cuidado al enfrentarse con la calificación de estos dos casos.

Después se evaluará la documentación obtenida: los auditores analizarán si la documentación recavada es suficiente, concisa, actualizada, adecuada y completa, que garantice la observancia de un control y de las respuestas proporcionadas en las entrevistas/cuestionarios. Como parte de esta misma evaluación, aunque con un grado de dominio técnico y experiencia muy grande, se encuentra la evaluación de los checklists y exámenes de seguridad. Como sea, la finalidad de ambas partes es comprobar que lo que se dice se hace y está documentado. Si las pruebas realizadas por el equipo auditor no fueran consistentes con la información facilitada por el auditado, se deberá recabar nueva información y reverificar los resultados de las pruebas auditoras. La evaluación de los checklists, las pruebas realizadas, la información facilitada por el cliente y el análisis de

todos los datos disponibles, configuran todos los elementos necesarios para calcular y establecer los resultados de la auditoría, que se materializarán en el informe final.

La forma como afectará la evidencia obtenida en el paso 4 es la siguiente. Se usará una calificación binaria, 1 y 0. La calificación 1 se asignará a la evidencia que sea congruente con los cuestionarios/entrevistas y se multiplicará por cada total de cada control (queda igual). La calificación 0 se dará a la evidencia que sea contradictoria y se multiplicará por cada total de cada control (la calificación es cero).

Como se puede observar, el afirmar en los cuestionarios un control que en la práctica no existe y no está documentado, anula la calificación de dicho control. De forma contraria, desconocer un control o política que en la práctica si existe y está documentado, igualmente anula la calificación de dicho control. De ahí la importancia que el personal auditado y entrevistado debe ser clave en los procesos de seguridad de la LAN.

6. Cálculos y resultados de la auditoría.

Falta calcular el porcentaje de bondad de cada área; éste se obtiene calculando el promedio de las respuestas obtenidas, recordando que deben afectarse por sus pesos correspondientes. Una vez realizados los cálculos, se ordenarán y clasificarán los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

Para lograr esto, ya que se tiene el total de cada uno de los 75 controles (su %), se obtendrá el promedio de cada uno de los 27 objetivos de control:

$$\overline{\text{O.n.m}} = \frac{\sum_{i=1}^{j} \text{Total control n.m.i}}{j}$$

Después se realiza el cálculo matemático de las 9 cláusulas, sabiendo que cada uno de los objetivos que las componen tiene un peso relacionado (el peso final):

$$\overline{\text{C.n}} = \frac{\sum_{m=1}^{j} \overline{\text{O.n.m}} * \text{Pf}_{\text{O.n.m}}}{100}$$

Cláusula 1: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.1.1. Políticas de seguridad de la LAN.		
Evaluación Cláusula 1		

Tabla 4. 89 Evaluación de la cláusula 1

Cláusula 2: Objetivos de control	P_f	Evaluación (O.n.m)
O.2.1. Administración de seguridad de la LAN.		
O.2.2. Seguridad en el acceso a la LAN por terceras personas.		
O.2.3. Análisis de riesgos.		
Evaluación Cláusula 2		

Tabla 4. 90 Evaluación de la cláusula 2

Cláusula 3: Objetivos de control	P_f	Evaluación (O.n.m)
O.3.1. Responsabilidad de los bienes o activos.		
O.3.2. Clasificación de la información.		
Evaluación Cláusula 3		

Tabla 4. 91 Evaluación de la cláusula 3

Cláusula 4: Objetivos de control	P_f	Evaluación (O.n.m)
O.4.1. Seguridad en la definición de puestos.		
O.4.2. Entrenamiento del personal.		
O.4.3. Respuesta a incidentes de seguridad de la LAN.		
Evaluación Cláusula 4		

Tabla 4. 92 Evaluación de la cláusula 4

Cláusula 5: Objetivos de control	P_f	Evaluación (O.n.m)
O.5.1. Aseguramiento de áreas de la red y su entorno.		
O.5.2. Seguridad del equipo de la LAN.		
Evaluación Cláusula 5		

Tabla 4. 93 Evaluación de la cláusula 5

Cláusula 6: Objetivos de control	P_f	Evaluación (O.n.m)
O.6.1. Procedimientos y responsabilidades.		
O.6.2. Protección contra software malicioso.		
O.6.3. Back up.		
O.6.4. Administración de la LAN.		
O.6.5. Intercambio de información.		
Evaluación Cláusula 6		

Tabla 4. 94 Evaluación de la cláusula 6

Cláusula 7: Objetivos de control	P_f	Evaluación (O.n.m)
O.7.1. Requerimientos para el control de acceso a la LAN.		

O.7.2. Administración de acceso de los usuarios a la LAN.		
O.7.3. Responsabilidades del usuario.		
O.7.4. Control de acceso a la LAN.		
O.7.5. Monitoreo de acceso y uso de la red de actividades no autorizadas.		
O.7.6. Cómputo móvil.		
Evaluación Cláusula 7		

Tabla 4. 95 Evaluación de la cláusula 7

Cláusula 8: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.8.1. Controles criptográficos.		
O.8.2. Seguridad en los procesos de desarrollo y soporte.		
Evaluación Cláusula 8		

Tabla 4. 96 Evaluación de la cláusula 8

Cláusula 9: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.9.1. Obediencia con los requerimientos legales.		
O.9.2. Revisión de políticas de seguridad y obediencia técnica.		
O.9.3. Consideraciones de auditoría de la LAN.		
Evaluación Cláusula 9		

Tabla 4. 97 Evaluación de la cláusula 9

Finalmente se obtendrá el cálculo matemático de la auditoría. Se multiplica la evaluación de cada una de las cláusulas por sus pesos finales correspondientes y se divide esto entre 100:

$$\text{Seguridad LAN} = \frac{\sum_{n=1}^{j} \overline{C.n} * Pf_{C.n}}{100}$$

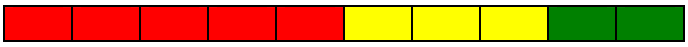
Cláusulas de control	**P_f**	**Evaluación (C.n)**
C.1. Políticas de seguridad.		
C.2. Gobierno de la seguridad.		
C.3. Control y clasificación de bienes.		
C.4. Seguridad de los empleados.		
C.5. Seguridad física de la LAN y su entorno.		
C.6. Administración de las comunicaciones.		
C.7. Control de acceso a la LAN.		
C.8. Desarrollo de seguridad de una LAN.		
C.9. Obediencia.		

Promedio total de la seguridad de la LAN	

Tabla 4. 98 Evaluación total de la seguridad de la LAN

Por último, se procede a mostrar las áreas auditadas con gráficos de barras, exponiéndose primero las cláusulas y luego los objetivos de cada cláusula. Si es necesario se mostrarán gráficas de los controles de un objetivo. En todos los casos se referenciarán respecto a tres zonas: roja, amarilla y verde.

La zona roja corresponde a una situación de debilidad que requiere acciones a corto plazo. Serán las más prioritarias, tanto en la exposición del informe como en la toma de medidas para la corrección. La zona amarilla corresponde a una situación discreta que requiere acciones a medio plazo, figurando a continuación de las contenidas en la zona roja. La zona verde requiere solamente alguna acción de mantenimiento a largo plazo.



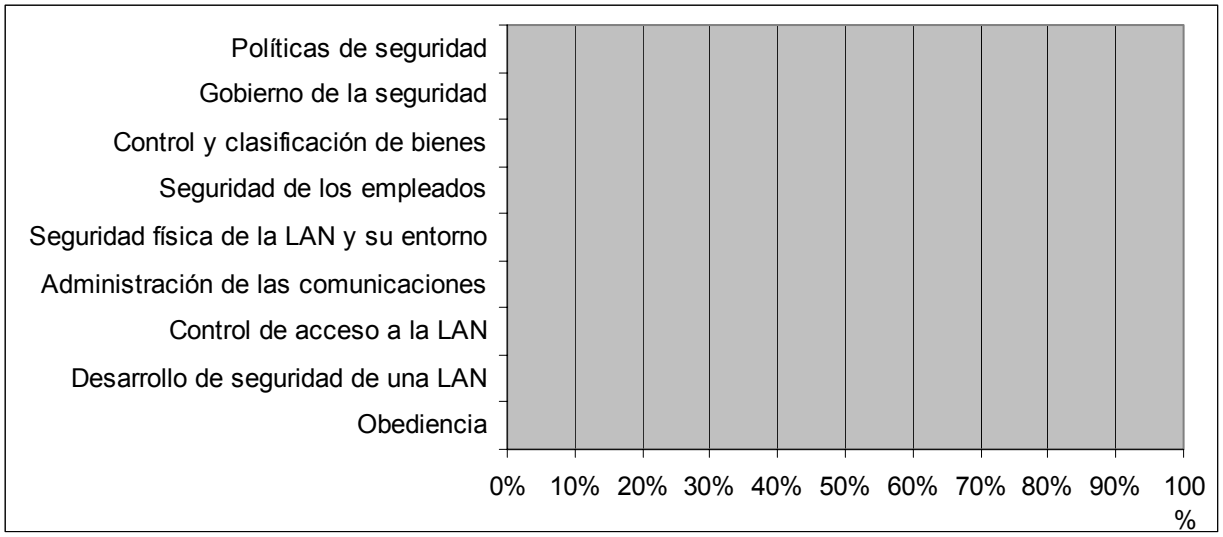


Figura 4. 3 Ejemplo de gráfica de evaluación

4.2.7. Informe.

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad. Es primordial la realización de esta fase para la completa culminación de los trabajos de auditoría, ya que incluyen los resultados importantes obtenidos, las recomendaciones y observaciones por cada uno de ellos.

En primer lugar se preparará el borrador del informe y su discusión con el cliente. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor. Es de destacar que si hubiese desacuerdo, es posible que el auditado redacte un contrainforme del punto cuestionado. Esta acta se incorporará al Informe Final.

De esta manera la aparición de un hecho implicará la existencia de una debilidad que deberá ser tomada y tratada por la organización para su pronta corrección. Es importante que las recomendaciones realizadas en el informe final sean compatibles con las políticas y normas existentes en la organización. Además, los hechos encontrados deben poder ser verificables si es necesario. Esto significa que deben ser verificados objetivamente, documentados, probados y soportados.

La estructura del informe presenta la siguiente información:

- Datos de la organización, fechas de la auditoría (inicio y término) y del informe, nombres del equipo auditor y de todas las personas involucradas en la auditoría, incluyendo su departamento, responsabilidad y puesto de trabajo en la organización.
- Definición de objetivos y alcance de la auditoría.
- Enumeración de áreas consideradas en la auditoría (cláusulas de control).
- Para cada una de las áreas o cláusulas de control se expondrá lo siguiente:

- Situación actual de la seguridad de la LAN.
- Tendencias.
- Vulnerabilidades y amenazas, las cuales deberán ser relevantes, exactas y convincentes. Además se deberán considerar sus consecuencias en la organización y en los planes de la misma.
- Y el aspecto importante y fundamental del informe que son las recomendaciones y planes de acción. Deben de estar suficientemente soportadas y ser concretas; irán dirigidas a los responsables de su implementación.

Las recomendaciones del informe son de tres tipos:

- Recomendaciones correspondientes a la zona roja. Serán muy detalladas e irán en primer lugar, con la máxima prioridad. La redacción de las recomendaciones se hará de modo que sea simple verificar el cumplimiento de la misma por parte del cliente.
- Recomendaciones correspondientes a la zona amarilla. Son las que deben observarse a medio plazo, e igualmente irán priorizadas.
- Recomendaciones correspondientes a la zona verde. Suelen referirse a medidas de mantenimiento. Pueden ser omitidas. Puede detallarse alguna de este tipo cuando una acción sencilla y económica pueda originar beneficios importantes.

Y por último, los auditores deberán elaborar un documento llamado C*arta de Introducción,* el cual sólo expone una síntesis de la situación actual de seguridad obtenida por medio de la auditoría, por lo tanto su extensión deberá ser breve (máximo cuatro páginas). Es importante señalar que en ella no se incluirán recomendaciones, a diferencia del Informe Final. Además, es dirigida al representante máximo de la organización o cliente de la auditoría. La Carta de Introducción tendrá la estructura siguiente:

- Fecha, objetivos y alcance.
- Cuantificación de la importancia de las áreas evaluadas.
- Señalamiento de las áreas de mayor debilidad e importancia en orden decreciente, y su impacto en la economía y misión de la empresa.

4.2.8. Seguimiento.

Según el estándar de auditoría 080 “Follow-Up Activities”, después de informar/reportar sobre los hallazgos y las recomendaciones, el auditor de SI debe solicitar y evaluar la información relevante para concluir si la gerencia tomó las acciones apropiadas de manera oportuna.

La función de auditoría interna de SI debe establecer un proceso de seguimiento para monitorear y asegurar que las acciones de la gerencia efectivamente han sido implementadas o que la gerencia superior ha aceptado el riesgo de no haber tomado la acción pertinente. La responsabilidad por estas actividades de seguimiento puede definirse en el estatuto de auditoría.

La naturaleza, los plazos y la extensión de las actividades de seguimiento deben tener en cuenta la importancia de los hallazgos reportados y el impacto, en caso de no haberse tomado las acciones correctivas. Los plazos de las actividades de seguimiento de una auditoría de SI en relación con el informe original deben basarse en el juicio profesional y depender de una serie de consideraciones tales como la naturaleza o magnitud de los riesgos y costos asociados a la entidad.

Dependiendo del alcance y de los términos del contrato, los auditores externos de SI pueden recurrir a la función de auditoría interna de SI para realizar el seguimiento de sus recomendaciones aceptadas. Como parte de las actividades de seguimiento, el auditor de SI deberá evaluar si los hallazgos no implementados siguen siendo importantes.

4.3 Consideraciones en la metodología para WLAN.

Las redes WLAN son un subconjunto o tipo de LAN, por lo tanto una metodología de auditoría de su seguridad cubre las mismas ocho etapas desarrolladas para LAN. Pero las WLAN tienen algunas características en su topología, medio de transmisión y protocolos que las vuelven más vulnerables.

Por lo tanto en la etapa seis (realización de la auditoría) consideraremos puntos adicionales a los realizados y se añadirá una cláusula más (la 10); estos puntos están materializados en los siguientes controles, planeación, ponderaciones, cuestionarios, pruebas y cálculos, y son adiciones a los pasos 1, 2, 3, 4 y 6 de esta sexta etapa. Cabe aclarar que al aplicar en esta metodología (para WLAN) las etapas desarrolladas, se tomará la palabra LAN como WLAN.

1. Selección de los objetivos de control y controles de seguridad de la WLAN.

Cláusula 10: Consideraciones para WLAN.

Objetivo 10.1: Políticas de seguridad para WLAN.
Proporcionar a la dirección la administración y el gobierno de la seguridad de la WLAN.

Control 10.1.1: *Políticas de seguridad para WLAN.*

> La organización debe tener una política de seguridad adecuada para el uso de la tecnología inalámbrica, incluyendo los estándares adoptados. Se deberá considerar el entrenamiento del personal, los peligros nuevos que implica esta tecnología, su monitoreo y un análisis de riesgos que la considere. Será importante contemplar un plan que tome en cuenta el robo de dispositivos inalámbricos.

Control 10.1.2: *Política para direccionar la REM.*

> Debe existir una política de seguridad para direccionar la REM (Radiación Electromagnética). Considerar la capacitación de cierto personal en este aspecto y los perímetros físicos de seguridad adecuados que eviten la intercepción. Además, se deberán considerar factores de salud y la protección de hardware y

comunicaciones sensibles a la radiación. Las comunicaciones más importantes deben ser de fibra.

Objetivo 10.2: Seguridad de access points.
Para la protección del acceso a la WLAN, los servicios de red y la información.

Control 10.2.1: *Instalación de los access points.*

La instalación de los access points obedecerá a una planeación adecuada. Considerar los siguientes controles:

- Controles de acceso físicos para access points.
- Cobertura adecuada.
- Verificar que no exista interferencia con otras comunicaciones.
- Colocación apropiada de los access points (lejos de muros exteriores y ventanas).

Control 10.2.2: *Configuración de los access points.*

La configuración estará basada en un análisis previo para evitar comprometer la seguridad. Considerar lo siguientes aspectos:

- Horario de operación.
- Configuraciones máximas de seguridad, incluyendo la criptografía, autenticación, privacidad y el tamaño máximo de la clave de encripción.
- Estado de configuración remota deshabilitada.
- Deshabilitación de protocolos inseguros.
- Almacenamiento seguro y fuerte administración de passwords.
- Administración del tráfico para access points sobre una subred alambrada dedicada.

Objetivo 10.3: Implementación de seguridad en la WLAN.
Para asegurar la protección de la información y el control de acceso a la WLAN.

Control 10.3.1: *Extensión del perímetro de seguridad física.*

Se deben determinar las áreas y la distancia por las que se extiende la WLAN más allá de los límites físicos de la organización e implementar los controles adecuados para extender el perímetro de seguridad. Determinar qué tan lejos se puede obtener acceso a la WLAN con una antena con ganancia.

Control 10.3.2: *Servicios de seguridad.*

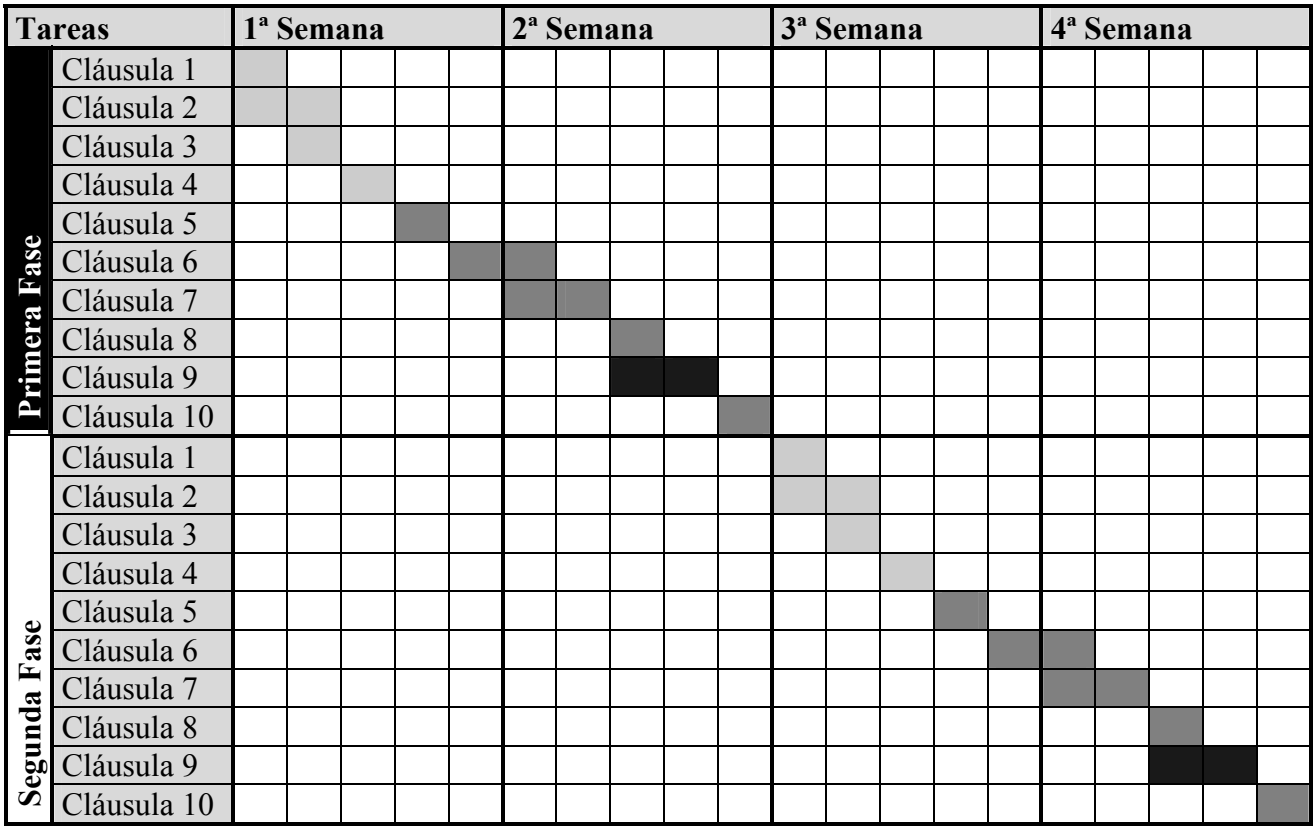
Se deberá usar el esquema de encripción más adecuado, basado en un análisis de riesgos ya que algunos son muy débiles y es fácil romperlos. Considerar los siguientes controles:

- Se debe usar un IDS sobre la WLAN.
- Considerar la instalación de un firewall entre la infraestructura cableada y la red inalámbrica.
- Las partes sensibles de la red cableada no deben tener acceso por la red inalámbrica.
- La autenticación se debe realizar con nombre de usuario y password.
- Usar los más adecuados algoritmos y protocolos de autenticación y, donde sea necesario, en capas.
- Todo cliente WLAN debe tener antivirus, firewall, configuración de máxima seguridad, deshabilitado el modo ad-hoc y usar VPN con una fuerte encripción para el acceso a recursos en situaciones de seguridad máxima.

Control 10.3.3: *Monitoreo de la WLAN.*

Se deberá probar y monitorear periódicamente la WLAN para evitar malas configuraciones y accesos no autorizados. Considerar el uso de exámenes móviles como el War Driving y probar la eficacia del IDS. La frecuencia de estos monitoreos y pruebas dependen de la sensibilidad de la información y servicios accesibles por la red, los protocolos de seguridad usados y los factores físicos. El análisis de riesgos debe determinar esta frecuencia.

Esta cláusula añade tres objetivos y siete controles a los anteriores. Por lo tanto se considerará un día adicional para la revisión de estos siete controles (10.1.1-10.3.3) para cada una de las dos fases. De esta manera, cada una de las fases se realizará en dos semanas. Además los auditores serán expertos en redes inalámbricas y su seguridad.



2 auditores expertos en gestión de controles de seguridad
2 auditores expertos en seguridad de redes inalámbricas
1 auditor experto en legislación

Tabla 4. 99 Programación corregida de las actividades de auditoría para WLAN

2. Ponderación de los sectores auditados.

En la ponderación se añadirá una cláusula de tal forma que la suma de los pesos ya no será de 100 como se muestra a continuación:

Cláusulas de control	Pesos técnicos (Pt)	Pesos políticos (Pp)	Pesos finales [Pf=(Pt+Pp)/2]
C.1. Políticas de seguridad.	15	-	-
C.2. Gobierno de la seguridad.	13	-	-
C.3. Control y clasificación de bienes.	10	-	-
C.4. Seguridad de los empleados.	9	-	-
C.5. Seguridad física de la WLAN y su entorno.	9	-	-
C.6. Administración de las comunicaciones.	11	-	-
C.7. Control de acceso a la WLAN.	15	-	-
C.8. Desarrollo de seguridad de una WLAN.	9	-	-
C.9. Obediencia.	9	-	-
C.10. Consideraciones para WLAN.	15	-	-
Total	115	115	115

Tabla 4. 100 Ponderación de cláusulas de control para WLAN

Cláusula 10: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.10.1. Políticas de seguridad para WLAN.	30	-	-
O.10.2. Seguridad de access points.	35	-	-
O.10.3. Implementación de seguridad en la WLAN.	35	-	-
Total	100	100	100

Tabla 4. 101 Ponderación de los objetivos de la cláusula 10

3. Entrevistas y cuestionarios.

CUESTIONARIOS ADICIONALES PARA WLAN

Cláusula 10. Consideraciones para WLAN.

Control 10.1.1. *Políticas de seguridad para WLAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se tiene una política adecuada para dirigir el uso de tecnología inalámbrica?		
- ¿Se consideran en esta política los peligros que implica esta tecnología?		
- ¿El análisis de riesgos actual considera esta tecnología y sus vulnerabilidades?		
- ¿Se tiene en cuenta el peligro para la red que ocasiona el robo de un dispositivo inalámbrico? ¿Qué controles se han contemplado?		
Total control 10.1.1.		?/20 ?%

Tabla 4. 102 Cuestionario control 10.1.1

Control 10.1.2. *Política para direccionar la REM.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe una política de seguridad para la REM?		
- ¿Qué controles físicos se consideran en la política para la propagación de la REM?		
- ¿Qué medidas existen para proteger al hardware, las comunicaciones y personal de la REM?		
Total control 10.1.2.		?/15 ?%

Tabla 4. 103 Cuestionario control 10.1.2

Objetivo 10.2. Seguridad de access points.

Control 10.2.1. *Instalación de los access points.*

Preguntas	Respuestas	Puntos
- ¿Existe un registro de todos los access points y de su ubicación? ¿Esta ubicación fue determinada mediante un análisis?		
- ¿Qué cobertura tienen los access points? ¿Qué capacidad de acceso tienen? ¿Qué porcentaje de este acceso es usado?		
- ¿Se ha verificado que no provoquen interferencia con otras comunicaciones?		
Total control 10.2.1.		?/15 ?%

Tabla 4. 104 Cuestionario control 10.2.1

Control 10.2.2. *Configuración de los access points.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Los access points están apagados cuando no están en uso?		
- ¿Qué configuraciones de seguridad tienen los access points?		
- ¿Qué subred soporta el tráfico de los access points?		
Total control 10.2.2.		?/15 ?%

Tabla 4. 105 Cuestionario control 10.2.2

Objetivo 10.3. Implementación de seguridad en la WLAN.

Control 10.3.1. *Extensión del perímetro de seguridad física.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué medidas de seguridad física existen en los lugares donde las comunicaciones inalámbricas exceden los límites físicos?		
- ¿Se sabe hasta dónde se puede acceder a la red inalámbrica?		
Total control 10.3.1.		?/10 ?%

Tabla 4. 106 Cuestionario control 10.3.1

Control 10.3.2. *Servicios de seguridad.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un IDS en la WLAN?		
- ¿Está instalado un firewall entre la LAN y la WLAN?		
- ¿Qué algoritmo de encripción es usado? ¿Su uso obedece al análisis de riesgos?		
- ¿Qué autenticación se realiza?		
- ¿Qué medidas de seguridad y configuraciones poseen los clientes WLAN?		
Total control 10.3.2.		?/25 ?%

Tabla 4. 107 Cuestionario control 10.3.2

Control 10.3.3. *Monitoreo de la WLAN.*		
Preguntas	**Respuestas**	**Puntos**

- ¿Se realiza un monitoreo de la WLAN para evitar accesos no autorizados? ¿Se realizan pruebas sobre el IDS?		
- ¿Con qué frecuencia se realiza el monitoreo?		
Total control 10.3.3.		?/10 ?%

Tabla 4. 108 Cuestionario control 10.3.3

4. ***Realización de pruebas.***

DOCUMENTACIÓN.

Los siguientes documentos serán revisados para garantizar la observancia de los controles:

Control 10.1.1
- Políticas de seguridad de la WLAN.

Control 10.1.2
- Política para direccionar la REM.

Control 10.2.1
- Documento de políticas sobre la instalación de access points.
- Procedimiento de verificaciones en la instalación de access points.
- Registro de los access points instalados y diagramas de red inalámbrica.

Control 10.2.2
- Política para la configuración de los access points.
- Manual de configuraciones de seguridad de los access points.
- Registro de los access points instalados y diagramas de red inalámbrica.

Control 10.3.1
- Política del perímetro de seguridad física para la WLAN.
- Análisis de riesgos que considere la red inalámbrica.

Control 10.3.2
- Documento de políticas de servicios de seguridad en la WLAN.
- Documento de análisis de riesgos que incluya la WLAN.
- Diagramas de LAN y WLAN.
- Documentos recientes de pruebas de penetración.
- Políticas de servicios de seguridad en clientes WLAN.

Control 10.3.3
- Política de monitoreo de la red inalámbrica.

- Documentos recientes o informes sobre monitoreo de la WLAN, hallazgos encontrados y soluciones manejadas.
- Procedimientos de auditoría interna que contemplen la seguridad de la red inalámbrica.
- Procedimientos de monitoreo y control interno para WLAN.
- Documento de análisis de riesgos.

PRUEBAS.

Se recomienda el siguiente examen (o testeo) para la Wireless LAN, basado en Wireless OSSTMM, que puede emplearse como un checklist:

a. Examen de REM (Radiación Electromagnética).

Evaluar las prácticas, políticas y zonas de áreas sensibles:

- Verificar que la organización tiene una adecuada política de seguridad en el lugar para direccionar las REM.
- Verificar que todo el personal relacionado con las áreas sensibles está entrenado en la reducción de fuga de REM y está familiarizado con las políticas de seguridad.
- Verificar que perímetro físico de seguridad está en lugar, para asegurar que ese acceso a las áreas sensibles no sea fácil de obtener por partes no autorizadas.

Evaluar hardware y colocación:

- Verificar que todos los dispositivos de TI que deben estar protegidos están localizados en áreas apropiadas.
- Verificar la colocación estratégica para crear la mayor protección contra emisiones de REM.

Evaluar el cableado y emisiones:

- Verificar que todas las alimentaciones cableadas dentro y fuera del cuarto protegido estén hechas de fibra, donde sea posible.
- Verificar que todas las alimentaciones cableadas, especialmente esas que no están hechas de fibra, estén protegidas y filtradas para eliminar la REM llevada fuera del cuarto protegido.
- Verificar la distancia para que cualquier fuga sea detectable.
- Determinar la necesidad para la generación de ruido blanco para enmascarar las emisiones REM.

b. Examen de redes inalámbricas 802.11

Evaluar las prácticas y políticas:

- Verificar que la organización tiene una adecuada política de seguridad que dirija el uso de tecnología inalámbrica, incluyendo el uso del 802.11.
- Verificar que todos los usuarios estén entrenados en el uso apropiado y los peligros de la tecnología de red inalámbrica.

- Realizar una evaluación de riesgos de seguridad para determinar el valor de los activos que en la organización están expuestos por la WLAN.
- Verificar que hay en curso auditorías aleatorias de seguridad para monitorear y rastrear dispositivos.
- Verificar que exista un plan para tratar con el robo de dispositivos inalámbricos, en donde los passwords y claves sean rápidamente cambiados.

Evaluar hardware y actualizaciones:

- Verificar que todos los últimos parches y mejoras estén aplicados a todos los dispositivos inalámbricos.
- Verificar que no haya dispositivos en la red que comprometan la seguridad a través de limitaciones en hardware o diseño de software.
- Verificar que todos los dispositivos son parte de la implementación planeada y fueron propiamente configurados y que no hay dispositivos no autorizados en la red que pudieran arriesgar la seguridad por ser conectados o simplemente por ser incorrectamente configurados.
- Revisar los accesos registrados y verificar que ningún dispositivo no autorizado está obteniendo acceso a la red inalámbrica.

Evaluar el control de acceso, el perímetro de seguridad y la capacidad de interceptar o interferir la comunicación:

- Determinar el nivel de controles de acceso físico para access points y dispositivos de control.
- Realizar una revisión del lugar para medir y establecer la cobertura de los access points de la organización.
- Verificar que los dispositivos de la red inalámbrica no interfieren con otros dispositivos electrónicos con frecuencias similares.
- Determinar los controles de acceso físico que hay en el lugar para controlar el acceso a las partes seguras de la organización, incluyendo las áreas por la cual la red inalámbrica se extiende.
- Determinar las zonas donde las comunicaciones inalámbricas se extienden más allá de los límites físicos de la organización y la distancia a la cual se extiende.
- Determinar qué tan lejos el acceso puede ser obtenido para la WLAN, usando antenas comunes de alta ganancia.
- Determinar las medidas de seguridad que existen donde las comunicaciones inalámbricas exceden los límites físicos.
- Si la intención es restringir el acceso a la WLAN a zonas dentro del edificio y no a áreas externas, verificar que los access point estén colocados en las áreas interiores del edificio y no cerca del muro exterior y ventanas.
- Determinar qué tipo de IDS está en uso sobre la WLAN y las áreas que son accesibles a ésta.
- Probar la efectividad del sistema IDS.

Evaluar accesos administrativos a dispositivos inalámbricos:

- Determinar si los access point están apagados durante el tiempo del día cuando ellos no estarán en uso.
- Verificar que la función de reinicializar los access point está siendo realizada sólo por personal autorizado y sólo cuando sea necesario.
- Verificar que los access point estén reestablecidos para el último ajuste de seguridad después de que es usada una reinicialización.
- Verificar que la administración de interfaces para los access point tiene autenticación de usuarios.
- Verificar que los access point tengan una fuerte administración de passwords.
- Verificar que toda administrativa de passwords tenga cambios regularmente y se almacenen con seguridad.
- Si los routers inalámbricos o access point permiten configuración remota, verificar que esté deshabilitada.
- Para máxima seguridad, verificar que la configuración de los access point y routers inalámbricos puede solamente ser realizada por acceso a través del puerto serial.
- Verificar que la administración de tráfico para los access point es sobre una subred dedicada alambrada.

Evaluar configuración, autenticación y encripción de redes wireless:

- Verificar que la clave WEP no sea almacenada en texto-simple en un registro de claves en el cliente con permisos débiles, el cual permite a usuarios locales desencriptar el tráfico de la red.
- Verificar que todos los protocolos de administración inseguros e innecesarios de los access point han sido deshabilitados.
- Verificar que todos los parámetros predeterminados han sido cambiados para los access point.
- Verificar que todas las características de seguridad de los productos WLAN han sido habilitadas, incluyendo las características de criptografía, autenticación y privacidad WEP.
- Verificar que el tamaño de la clave de encripción sea por lo menos de 128 bits o lo más larga posible.
- Verificar que las claves predeterminadas repartidas sean periódicamente sustituidas por más claves seguras únicas.
- Asegurarse que un firewall configurado apropiadamente ha sido instalado entre la infraestructura cableada y la red inalámbrica.
- Si la instalación requiere máxima seguridad, verificar qué partes sensibles de la red cableada están sin ruta accesible para la red inalámbrica y qué dispositivos en la red inalámbrica están siempre en las porciones sensibles de la red cableada.
- Verificar que toda la tecnología en la WLAN tiene todo de las últimas mejoras y parches de seguridad.
- Verificar que los usuarios están autenticados con nombre de usuario y password en las WLAN y qué tipo de autenticación es usado.
- Verificar qué autenticación de red no es susceptible para playback de previas autenticaciones para obtener acceso a recursos de red.
- Verificar que IPSec es usado en vez del WEP predeterminado como el protocolo de seguridad.

- Verificar que un protocolo de autenticación, como el 802.1x, es usado encima del WEP.
- Si la instalación requiere máxima seguridad, verificar que un algoritmo de encripción más seguro que el algoritmo predeterminado RC4 está en uso (como el 3DES o el AES).
- Si la instalación requiere máxima seguridad, verificar que autenticación de usuarios para las WLAN es obtenida a través de métodos más seguros.
- Verificar que el acceso es otorgado a las maquinas clientes con direcciones MAC registradas.
- Verificar que toda característica de seguridad posible es proporcionada por la arquitectura en uso.

Evaluar clientes wireless:

- Verificar que todo cliente wireless tiene software antivirus instalado.
- Verificar que todo cliente wireless tiene un firewall instalado.
- Verificar que todo cliente wireless está al día en parches y está configurado para máxima seguridad.
- Si la instalación requiere máxima seguridad, verificar que todos los clientes inalámbricos usan una VPN para obtener acceso a algunos recursos, incluyendo el Internet, sobre la WLAN.
- Verificar que las VPN's tienen fuerte encripción, al menos 3DES o mejor.
- Verificar que modo ad-hoc ha sido deshabilitado, a no ser que el entorno es tal que el riesgo es tolerable.

6. Cálculos y resultados de la auditoría.

Los tres objetivos de control de la cláusula 10 se calificarán de la manera definida. Después se evaluará esta cláusula de la misma forma que las otras:

Cláusula 10: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.10.1. Políticas de seguridad para WLAN.		
O.10.2. Seguridad de access points.		
O.10.3. Implementación de seguridad en la WLAN.		
Evaluación Cláusula 10		

Tabla 4. 109 Evaluación de la cláusula 10

Finalmente se obtendrá el cálculo matemático de la auditoría como muestra el método anterior, sólo que en este caso se divide entre 115:

$$\text{Seguridad WLAN} = \frac{\sum_{n=1}^{j} \overline{C.n} * Pf_{C.n}}{115}$$

Cláusulas de control	**P_f**	**Evaluación (C.n)**
C.1. Políticas de seguridad.		

C.2. Gobierno de la seguridad.		
C.3. Control y clasificación de bienes.		
C.4. Seguridad de los empleados.		
C.5. Seguridad física de la WLAN y su entorno.		
C.6. Administración de las comunicaciones.		
C.7. Control de acceso a la WLAN.		
C.8. Desarrollo de seguridad de una WLAN.		
C.9. Obediencia.		
C.10. Consideraciones para WLAN.		
Promedio total de la seguridad de la WLAN		

Tabla 4. 110 Evaluación total de la seguridad de la WLAN

4.4 Consideraciones para organizaciones no gubernamentales.

La metodología de auditoría que se ha presentado a lo largo de este capítulo puede aplicarse a otro tipo de organizaciones con otras características a las consideradas. Sobre todo, el principal aspecto que varía es la determinación del alcance y objetivo, y se incluirían, por supuesto, las cláusulas de control más adecuadas a su entorno (para LAN o WLAN).

Es relevante que otras organizaciones (como las PyMEs) posiblemente destinen menos recursos a sus auditorías o que no existan; pero hay otras, como la banca, que manejan información sumamente sensible y se tendría un fuerte impacto económico en el negocio al producirse violaciones a los tres servicios básicos de seguridad. Además, es probable que sus redes locales no sean tan grandes como lo son en los sectores gubernamentales. Por ello, sería conveniente realizar un análisis costo/beneficio para poder destinar más recursos en los exámenes no documentales del paso de la realización de pruebas, en la fase de la realización de la auditoría, en forma de pruebas de penetración bien planeadas, ya que engloban otros tipos de exámenes de seguridad que proveen mucha información acerca del estado actual y real de la seguridad de la red.

Otro factor importante radica en el hecho de que la auditoría interna pueda operar de una manera más continua en algunas de estas organizaciones. De esta forma, se tendría una evaluación de la seguridad de la red organizacional más constante, apoyada en la experiencia de auditorías previas y en cada ocasión con informes más pequeños (menos problemas de seguridad).

CONCLUSIONES

En México existe una carencia y deficiencia en la difusión, capacitación y fomento de la seguridad informática, desde la organización completa hasta el individuo. Esto tiene como consecuencia estar en desventaja frente a las vulnerabilidades más comunes, centrar la preocupación en los virus y hackers dejando en segundo término (u olvidado) la planeación de la seguridad, las políticas, el seguimiento y las auditorías, la capacitación y educación, la disponibilidad de los sistemas, el control de acceso, y el buen servicio a usuarios y clientes, por ejemplo.

Habiendo establecido un panorama de la problemática de la seguridad en redes hemos realizado una revisión de las guías internacionales de más uso: COBIT, BS7799, CC, TCSEC, FISCAM, NIST 800-42, OSSTMM.

De todas ellas hemos extraído y analizado los elementos más útiles referentes a la seguridad/auditoría de redes de comunicaciones, observando que algunas de estas guías enfatizan más en el aspecto técnico (OSSTMM, por ejemplo), mientras que otras más en la parte de gestión (COBIT, por ejemplo) y algunas con un equilibrio entre ambos aspectos (BS7799).

Finalmente desarrollamos una propuesta de una metodología de auditoría en seguridad informática para LAN, definiéndola como una metodología de un examen crítico realizado para evaluar la eficacia-eficiencia de la seguridad de la LAN en un organismo, de sus controles, sistemas y procedimientos.

Nuestra metodología considera ocho etapas fundamentales:

9. Determinación del alcance y objetivo.
10. Estudio inicial del entorno de la LAN.
11. Determinación de la muestra.
12. Determinación de los recursos necesarios.
13. Planeación.
14. Realización de la auditoría.
15. Informe.
16. Seguimiento.

La etapa de la realización de la auditoría (6) comprende los pasos siguientes:

7. Selección de los objetivos de control y controles de seguridad de la LAN.
8. Ponderación de los sectores auditados.
9. Entrevistas y cuestionarios.
10. Realización de pruebas.
11. Cruzamiento de información y calificación.
12. Cálculos y resultados de la auditoría.

Para lo cual desarrollamos 75 controles de seguridad agrupados en las cláusulas siguientes:

Cláusula 1: Políticas de seguridad.
Cláusula 2: Gobierno de la seguridad.
Cláusula 3: Control y clasificación de bienes.
Cláusula 4: Seguridad de los empleados.
Cláusula 5: Seguridad física de la LAN y su entorno.
Cláusula 6: Administración de las comunicaciones.
Cláusula 7: Control de acceso a la LAN.
Cláusula 8: Desarrollo de seguridad de una LAN.
Cláusula 9: Obediencia.

También desarrollamos los cuestionarios del paso 3 agrupados por cláusulas, objetivos y controles de seguridad.

Es importante cuantificar una auditoría y lo hemos realizado por control, por objetivo, por cláusula y, finalmente, de la seguridad de la LAN completa.

Adicionalmente, hemos desarrollado esta misma metodología de auditoría para WLAN, un caso de la LAN con características muy particulares.

En lo posible hemos aterrizado y probado nuestra metodología aplicándola en un organismo gubernamental en los casos de LAN y WLAN, mostrando todos los detalles en el Apéndice C. Las conclusiones corresponden totalmente con lo investigado en la situación actual de la seguridad informática en México y son abrumadoras:

La seguridad informática de la LAN es apenas suficiente, esto es, no se garantiza que confiabilidad, integridad y disponibilidad de la información se mantengan o lo puedan hacer en un futuro ante la administración de la seguridad y sus controles implementados como lo están ahora. Esto ocasionaría repercusiones considerables en los SI de la entidad y en sus objetivos mismos de funcionalidad.

Se observa una falta de políticas para WLAN, de manera explícita y detallada. Tampoco existe una política de seguridad para la REM ni sus controles físicos de seguridad.

No existen medidas de seguridad física en los lugares donde las comunicaciones inalámbricas exceden los límites físicos, los servicios de seguridad son suficientes pero no completos; lo mismo ocurre con el monitoreo de la WLAN y su control de acceso.

No obstante, he aquí la importancia de esta metodología que desarrollamos: ya que hemos detectado las vulnerabilidades y deficiencias en la seguridad de la LAN y han sido plasmadas en el *informe*, ahora sabemos qué parte de la gestión de la seguridad necesita atención urgente y en qué, además de localizar los puntos de atención a mediano y largo plazo. Se ha encontrado la causa de la enfermedad y se realiza una recomendación para su cura.

APÉNDICE A

ELEMENTOS Y CRITERIOS EN SEGURIDAD DE TI

APÉNDICE A

ELEMENTOS Y CRITERIOS EN SEGURIDAD DE TI

A.1 Objetivos de control de COBIT v.3.0. [32]

Tabla A. 1 Control DS5: Garantizar la seguridad de los sistemas

DS5.1 Gestión de medidas de seguridad.
La seguridad en TI deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos del negocio. Esto incluye: • Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI. • Implementar el plan de seguridad de TI. • Actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI. • Monitorear la implementación del plan de seguridad de TI.
DS5.2 Identificación, autentificación y acceso.
El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso.
DS5.3 Seguridad de acceso a los datos en línea.
Se deberán implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.
DS5.4 Administración de cuentas de usuario.
Se deberán establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.
DS5.5 Gestión de la revisión de cuentas de usuario.
Se deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso. Se debe llevar a cabo la comparación periódica entre los recursos y los registros de las cuentas para reducir el riesgo de errores, fraudes, alteración no autorizada o accidental.
DS5.6 Control de los usuarios sobre sus cuentas.
Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta(s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre

[32] COBIT, *Objetivos de Control*. 4ª edición. IT Governance Institute.

actividades inusuales.
DS5.7 Vigilancia de seguridad.
La actividad de seguridad debe ser registrada y que cualquier indicación sobre una inminente violación de seguridad ser notificada inmediatamente a todos aquellos que puedan verse afectados y se debe actuar de una manera oportuna.
DS5.8 Clasificación de los datos.
Se implementarán procedimientos para asegurar que todos los datos son clasificados en términos de sensitividad de acuerdo con el esquema de clasificación de datos. Los dueños deben determinar la ubicación o disposición de sus datos y determinar quiénes pueden compartir los datos.
DS5.9 Gestión de identificación y derecho de acceso centralizado.
Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada.
DS5.10 Reporte de actividades de seguridad y violaciones.
Las violaciones y la actividad de seguridad deben ser registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas.
DS5.11 Manejo de incidentes.
Se deberá implementar la capacidad de manejar incidentes de seguridad, dar atención a dichos incidentes. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna.
DS5.12 Reacreditación.
Se deberá llevar a cabo periódicamente una reacreditación de seguridad con el fin de mantener actualizado el nivel de seguridad aprobado formalmente y la aceptación del riesgo residual.
DS5.13 Confianza en las contrapartes.
Se implementarán prácticas de control para verificar la autenticidad de las contrapartes que proporcionan instrucciones o transacciones electrónicas. Esto puede lograrse mediante el intercambio confiable de passwords, tokens o llaves criptográficas.
DS5.14 Autorización de las transacciones.
Se implementarán controles para proporcionar autenticidad a las transacciones y establecer la validez de la identificación solicitada por el usuario ante el sistema. Esto requiere el empleo de técnicas criptográficas para “firmar” y verificar transacciones.
DS5.15 No repudio.

Se deberá asegurar que las transacciones no puedan ser negadas por ninguna de las partes participantes y que se implementen controles para que no se pueda negar el origen o destino de la transacción y que se pueda probar que se envió y recibió la transacción.
DS5.16 Rutas de confianza.
Se deberá asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros.
DS5.17 Protección de funciones de seguridad.
Todo el hardware y software relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas.
DS5.18 Administración de claves criptográficas.
Se deberán definir e implementar procedimientos y protocolos a ser utilizados en la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas contra modificaciones y divulgación no autorizada.
DS5.19 Prevención, detección y corrección de software malicioso.
Se deberán establecer adecuadas medidas de control preventivas, detectivas y correctivas y responder y reportar su presencia.
DS5.20 Arquitectura de cortafuegos y conexiones con redes públicas.
La organización deberá contar con *firewall* adecuados para proteger contra negación de servicios y cualquier acceso no autorizado a los recursos internos si existe conexión con Internet u otras redes públicas; se deberá controlar en ambos sentidos cualquier aplicación y el flujo de administración de infraestructura y se deberá proteger contra ataques de negación del servicio.

Tabla A. 2 Control DS12: Administración de las instalaciones

DS12.1 Seguridad física.
Deberán establecerse medidas apropiadas de seguridad física y medidas de control de acceso para las instalaciones de TI en conformidad con la política general de seguridad. Deben abarcar también las ubicaciones del cableado, servicios de soporte (como la energía eléctrica), medios de respaldo y demás elementos requeridos para la operación del sistema. El acceso deberá restringirse a las personas que hayan sido autorizadas.
DS12.2 Perfil del sitio.
Se deberá asegurar que se mantenga un bajo perfil sobre la identificación física de las instalaciones relacionadas con sus operaciones de TI. La información sobre la ubicación del sitio debe ser limitada y mantenerse con la adecuada reserva.
DS12.5 Protección contra factores ambientales.

Se asegurará que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales. Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.
DS12.6 Fuente de energía ininterrumpible.
Se deberá evaluar la necesidad de contar con generadores y baterías de suministro ininterrumpido de energía para las aplicaciones críticas de tecnología de información, con el fin de protegerse contra fallas y fluctuaciones de energía.

Tabla A. 3 Control M4: Proporcionar auditoría independiente

M4.1 Estatutos de auditoría.
Se deberá establecer el estatuto para la función de auditoría. Este documento deberá establecer la responsabilidad, autoridad y obligaciones de la función de auditoría.
M4.2 Independencia.
El auditor deberá ser independiente del auditado tanto en actitud como en apariencia. Los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado, y en la medida de lo posible, deberá también ser independiente de la propia empresa.
M4.4 Competencia.
Los auditores responsables de las revisiones de las actividades de la función de SI de la organización, deben ser técnicamente competentes y contar en forma general con las habilidades y conocimientos necesarios para desempeñar dichas revisiones en forma efectiva, eficiente y económica.
M4.5 Planeación.
Se deberá establecer un plan de auditoría para garantizar que se obtenga un aseguramiento regular e independiente con respecto a la efectividad, eficiencia y economía de la seguridad y de los procedimientos de control interno. Se deberán determinar las prioridades relacionadas con la obtención de aseguramiento independiente.
M4.6 Ejecución del trabajo de auditoría.
Las auditorías deberán ser supervisadas apropiadamente para proporcionar certeza de que los objetivos de auditoría están siendo alcanzados y que los estándares profesionales de auditoría que sean aplicables están siendo considerados. Los auditores deberán asegurarse de obtener evidencia suficiente, confiable, relevante y útil para alcanzar los objetivos de auditoría de forma efectiva. Los hallazgos y conclusiones de auditoría deben estar soportados por un análisis apropiado y una correcta interpretación de esta evidencia.
M4.7 Reportes.

La función de auditoría de la organización deberá entregar un reporte, en un formato adecuado, a todo el personal interesado una vez concluida su revisión. El reporte de auditoría deberá mostrar los objetivos de la auditoría, el período de cobertura y la naturaleza y extensión de trabajo de auditoría realizado. El reporte deberá identificar la Organización, los destinatarios del informe y cualquier restricción en su circulación. El reporte de auditoría deberá también mostrar los hallazgos, conclusiones y recomendaciones.
M4.8 Seguimiento.
La resolución y atención de los comentarios sobre la auditoría depende de la Gerencia. Los auditores deberán solicitar y evaluar la relacionada con los hallazgos, conclusiones y recomendaciones de auditorías anteriores para determinar si las acciones apropiadas han sido implementadas de manera oportuna.

A.2 Controles del BS 7799-1:2000.

(Cláusula) 3 Políticas de seguridad

(Objetivo) 3.1 *Políticas de seguridad de la información* Para proporcionar dirección y soporte en la administración de la seguridad de la información.	
Controles	
3.1.1 *Documento de políticas de seguridad de la información*	Un documento de políticas debe estar aprobado por la administración, publicado y comunicado, como sea apropiado, a todos los empleados.
3.1.2 *Revisión y evaluación*	Las políticas serán revisadas regularmente, y en caso de cambios influenciables, asegurar que permanecen apropiadamente.

4 Seguridad organizacional

4.1 *Infraestructura de seguridad de la información* Para administrar seguridad de la información en la organización.	
Controles	
4.1.1 *Foro de administración de la seguridad de la información*	Para asegurar que hay una dirección clara y un soporte administrativo visible para que las iniciativas de seguridad estén en lugar.
4.1.2 *Coordinación de la seguridad de la información*	Un foro de funciones cruzadas de representantes administrativos de diferentes partes de la organización coordinará la implementación de controles de seguridad de la información.
4.1.3 A*signación de responsabilidades de seguridad de la información*	Responsabilidades para la protección de bienes individuales y para cumplir procesos de seguridad específicos serán claramente definidas.
4.1.4 *Proceso de autorización para facilidades de procesamiento de la información*	Un proceso administrativo de autorización para nuevas facilidades de procesamiento de la información serán establecidas.
4.1.5 *Consejo de especialistas de seguridad de la información*	Será buscado de consultores internos o externos y coordinado por la organización.
4.1.7 *Revisión independiente de la seguridad de la información*	La implementación de las políticas será revisada independientemente por una auditoría interna o externa.
4.2 *Seguridad en el acceso de terceras personas* Para mantener la seguridad de facilidades del procesamiento de información organizacional y bienes de información accesados por terceras personas.	
Controles	
4.2.1 *Identificación de riesgos de acceso de terceras personas*	Serán calculados los riesgos e implementados controles de seguridad.

4.2.2 *Requerimientos de seguridad en contratos de terceras personas.*	Acuerdos de acceso a la información organizacional por terceras personas serán basados en un contrato formal que contenga los requerimientos de seguridad necesarios.

5 Control y clasificación de bienes

5.1 *Responsabilidad de bienes* Para mantener la protección apropiada de bienes organizacionales.	
Controles	
5.1.1 *Inventario de bienes*	Un inventario de bienes importantes asociados con cada SI será redactado y mantenido.
5.2 *Clasificación de la información* Para asegurar que los bienes de información reciben un nivel de seguridad apropiado.	
Controles	
5.2.1 *Guías de clasificación*	Las clasificaciones serán consideradas por las necesidades de compartir o restringir información.
5.2.2 *Manejo y etiquetado de información*	Un conjunto de procedimientos serán definidos para el manejo y etiquetado de la información de acuerdo con el esquema de clasificación.

6 Seguridad del personal

6.1 *Seguridad en la definición de puestos y recursos* Para reducir los riesgos de error humano, robo, fraude o mal uso de facilidades.	
Controles	
6.1.1 *Incluir la seguridad en las responsabilidades de puestos*	Los roles y responsabilidades de seguridad serán documentados en las definiciones de puestos.
6.1.4 *Términos y condiciones de empleo*	Los términos y condiciones de empleo establecerán la responsabilidad de los empleados en la seguridad de la información.
6.2 *Entrenamiento del usuario* Para asegurar que los usuarios están conscientes de la amenazas en la seguridad de la información.	
Controles	
6.2.1 *Educación y entrenamiento en seguridad de la información*	Todos los empleados (y terceras personas si es necesario) recibirán este entrenamiento y actualizaciones.
6.3 *Responder a incidentes y malfunciones de seguridad* Para minimizar el daño de los incidentes y malfunciones de seguridad, y controlar y aprender de tales incidentes.	
Controles	
6.3.3 *Reportar malfunciones de software.*	Serán establecidos procedimientos para reportar malfunciones de software.
6.3.5 *Proceso disciplinario*	La violación de políticas y procedimientos de seguridad tratada con un proceso disciplinario.

7 Seguridad física y del entorno

7.1 *Áreas seguras* Para prevenir acceso no autorizado, daño e interferencia a las premisas de negocios e información.	
Controles	
7.1.1 *Perímetro de seguridad física*	Se usarán para proteger áreas que contienen facilidades de procesamiento de información.
7.1.2 *Controles de entrada física*	Para asegurar que sólo personal autorizado tiene permitido el acceso.
7.1.3 *Seguridad en oficinas, cuartos y facilidades*	Serán usados controles adicionales y guías para trabajar en áreas seguras para mejorar su seguridad.
7.2 *Seguridad del equipo* Para prevenir pérdida, daño o compromiso de bienes y la interrupción de actividades.	
Controles	
7.2.1 *Colocación y protección del equipo*	El equipo será colocado y protegido para reducir riesgos de amenazas ambientales y peligros, y oportunidades de acceso no autorizado.
7.2.2 *Suministros de energía*	El equipo será protegido contra fallos de energía y otras anomalías eléctricas.
7.2.3 *Seguridad del cableado*	El cableado de comunicaciones, energía o información será protegido de intercepción o daño.
7.2.4 *Mantenimiento del equipo*	El equipo recibirá mantenimiento para permitir su continua disponibilidad e integridad.

8 Administración de las comunicaciones y operaciones

8.3 *Protección contra software malicioso* Para proteger la integridad del software e información de daños por software malicioso.	
Controles	
8.3.1 *Controles contra software malicioso*	Serán implementados controles de detección y prevención para proteger contra software malicioso y procedimientos de de concientización.
8.4 *Housekeeping* Mantener la integridad y disponibilidad del procesamiento de la información y de servicios de comunicación.	
Controles	
8.4.1 *Respaldo de información*	Copias de respaldo de información y software serán tomadas y revisadas regularmente.
8.5 *Administración de red* Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.	
Controles	
8.5.1 *Controles de red*	Serán implementados para lograr y mantener la seguridad en redes.

8.7 *Intercambios de información y software* Para prevenir pérdida, modificación o mal uso de la información intercambiada entre organizaciones.	
Controles	
8.7.2 *Seguridad de medios en tránsito*	Medios en tránsito serán protegidos de acceso no autorizado, mal uso o corrupción.
8.7.3 *Seguridad en comercio electrónico*	Será protegido contra actividad fraudulenta, disputa de contrato y revelación o modificación de la información.
8.7.4 *Seguridad de e-mail*	Será desarrollada una política para el uso de e-mail y serán puestos controles para reducir los riesgos de seguridad inherentes a él.
8.7.6 S*istemas disponibles públicamente*	Habrá un proceso formal de autorización antes que la información está disponible públicamente y su integridad será protegida de modificación no autorizada.

9 Control de acceso

9.1 R*equerimientos para control de acceso* Para controlar el acceso a la información.	
Controles	
9.1.1 *Política de control de acceso*	Requerimientos para control de acceso serán definidos y documentados en la política.
9.2 *Administración de acceso del usuario* Para asegurar que los derechos de acceso están apropiadamente autorizados, asignados y mantenidos.	
Controles	
9.2.1 *Registro del usuario*	Habrá un procedimiento de registro y de de-registro para conceder acceso a sistemas y servicios de información multiusuario.
9.2.2 *Administración de privilegios*	La designación y uso de privilegios será restringida y controlada.
9.2.3 *Administración de passwords*	La designación de passwords será controlada por un proceso de administración formal.
9.2.4 *Revisión de derechos de acceso del usuario*	Se realizará un proceso formal para revisar regularmente derechos de acceso.
9.3 *Responsabilidades del usuario* Para prevenir acceso no autorizado.	
Controles	
9.3.1 *Uso de password*	Usuarios realizarán buenas prácticas de selección y uso de passwords.
9.3.2 *Equipo no atendido*	Usuarios se asegurarán que el equipo no protegido está protegido apropiadamente.
9.4 *Control de acceso a la red* Para proteger servicios de red.	
Controles	
9.4.1 *Política de uso de servicios de red*	Usuarios tendrán sólo acceso directo a los servicios a los que tienen uso autorizado específicamente.

9.4.3 *Autenticación de usuarios de conexiones externas.*	Acceso por usuarios remotos será autenticado.
9.4.6 *Segregación en redes*	Serán introducidos controles para segregar grupos de servicios de información, usuarios y sistemas de información.
9.7 *Monitoreo de uso y acceso al sistema* Para detectar actividades no autorizadas.	
Controles	
9.7.1 *Logging de eventos*	Excepciones de eventos de auditoría serán producidos y mantenidos por un periodo acordado para asistir al monitoreo de control de acceso.
9.8 *Cómputo móvil* Para asegurar la seguridad de la información en el uso de cómputo móvil.	
Controles	
9.8.1 *Cómputo móvil*	Una política y controles serán adoptados par proteger contra los riesgos de trabajar con cómputo móvil.

10 Desarrollo y mantenimiento del sistema

10.3 *Controles criptográficos* Para proteger la confidencialidad, autenticidad o integridad de la información.	
Controles	
10.3.1 *Política para el uso de controles criptográficos*	Será desarrollada para la protección de la información.
10.3.2 *Encriptación*	Será aplicada para proteger la confidencialidad de información sensitiva.
10.3.3 *Firma digital*	Será aplicada para proteger autenticidad e integridad de información electrónica.
10.3.4 *Servicios de no repudio*	Serán usados para resolver disputas sobre la ocurrencia o no ocurrencia de eventos.
10.3.5 *Administración de claves*	Será usada para soportar el uso de técnicas criptográficas.
10.5 *Seguridad en procesos de desarrollo y soporte* Para mantener la seguridad del software de aplicaciones e información.	
Controles	
10.5.1 *Procedimientos de control de cambios*	La implementación de cambios será estrictamente controlada por estos procedimientos.
10.5.2 *Revisión técnica de cambios al sistema operativo*	Los sistemas de aplicación serán revisados y probados cuando ocurran los cambios.

12 Obediencia

12.1 *Obediencia con requerimientos legales* Para evitar violaciones de obligaciones legales, regulatorias o contractuales y de requerimientos de seguridad.

Controles	
12.1.1 *Identificación de legislación aplicable*	Estos requerimientos serán definidos explícitamente y documentados para cada sistema de información.
12.1.2 *Derechos de propiedad intelectual*	Serán implementados procedimientos para asegurar obediencia con restricciones legales en el uso de material al respecto de derechos de propiedad intelectual y el uso de productos de software.
12.1.4 *Protección y privacidad de información personal*	Para protegerla de acuerdo a la legislación.
12.1.6 *Regulación de controles criptográficos*	Para obedecer regulaciones y legislaciones relacionadas con el control de acceso y uso de controles criptográficos.
12.1.7 *Colección de la evidencia*	Obediencia con estándares o prácticas para la producción de evidencia admisible.
12.2 *Revisiones de políticas de seguridad y obediencia técnica* Para asegurar la obediencia de sistemas con las políticas y estándares.	
Controles	
12.2.2 *Revisión de obediencia técnica*	Los sistemas de información serán probados regularmente para la obediencia de la implementación de estándares de seguridad.
12.3 *Consideraciones de auditoría de sistemas* Para maximizar la efectividad y para minimizar la interferencia de procesos de auditoría.	
Controles	
12.3.1 *Controles de auditoría*	Las auditorías serán planeadas cuidadosamente para minimizar riesgo de disrupciones en los procesos.
12.3.2 *Protección de sistemas de auditoría*	El acceso a herramientas de auditoría será protegido para prevenir cualquier posible mal uso o compromiso.

A.3 Elementos de los Criterios Comunes.

Para la seguridad en redes consideramos tomar en cuenta los elementos siguientes del CC v.2.2, donde describimos las clases seleccionadas y las familias de interés. No consideramos necesario llegar al nivel de detalle de los componentes.

Necesitamos definir algunos de las abreviaturas usadas en el catálogo:

TOE: Target of Evaluation (Objetivo de Evaluación); producto o sistema de TI a evaluar que contiene recursos, como medios de almacenamiento electrónicos, dispositivos periféricos y capacidad de cómputo, que puede ser usado para procesar y almacenar información

TSF: TOE Security Functions (Funciones de Seguridad del TOE); conjunto de hardware, software o firmware del TOE en los que se confía para la correcta aplicación de la Política de Seguridad del TOE (TSP).

TSP: TOE Security Policy (Política de Seguridad del TOE); conjunto de reglas que regulan la administración, protección y distribución de los bienes en un TOE.

SFP: Security Function Policy (Política de Función de Seguridad); política de seguridad hecha cumplir por una Función de Seguridad (SF).

CLASE FAU: Auditoría de seguridad Abarca reconocer, grabar, almacenar y analizar información relacionada con actividades relevantes de seguridad. Los registros de auditoría resultantes pueden ser examinados para determinar que actividades relevantes de seguridad ocurrieron y quién es responsable de ellas.
FAU_ARP: Respuesta automática de auditoría de seguridad Define la respuesta tomada en caso de eventos indicativos de una violación potencial de seguridad.
FAU_GEN: Generación de datos de auditoría de seguridad Define los requerimientos para grabar la ocurrencia de eventos de seguridad. Identifica el nivel de auditoría, enumera tipos de eventos que serán auditables por las TSF e identifica el conjunto mínimo de información de los registros de auditoría.
FAU_SAA: Análisis de auditoría de seguridad Define requerimientos para medios automáticos que analizan la actividad del sistema y datos auditables, buscando violaciones de seguridad posible o real. Este análisis puede trabajar en soporte de detección de intrusos o en la respuesta automática a una violación de seguridad inminente. Las acciones a ser tomadas basadas en la detección pueden ser especificadas usando la familia FAU_ARP.
FAU_SAR: Revisión de auditoría de seguridad

Define los requerimientos para herramientas de auditoría que deberían estar disponibles para usuarios autorizados para asistir en la revisión de los datos auditables.
FAU_SEL: Selección de eventos de auditoría de seguridad Define los requerimientos para seleccionar los eventos a ser auditados durante la operación del TOE. Define requerimientos para incluir o excluir eventos del conjunto de eventos auditables.
FAU_STG: Almacenamiento de eventos de auditoría de seguridad Define los requerimientos para las TSF para poder crear y mantener un seguimiento de auditoría de seguridad.

Clase FCO: Comunicación Tiene dos familias concernientes con asegurar la identidad de una parte participante en intercambio de datos, asegurando la identidad del generador de la información transmitida (prueba de origen) y asegurando la del destinatario (prueba de recepción).
FCO_NRO: No repudio de origen Asegura que el originador de la información no puede negar haber enviado información. Esta familia requiere que las TSF proporcionen un método para asegurar que un sujeto que recibe información está provisto de la evidencia del origen de la información.
FCO_NRR: No repudio de recepción Asegura que el destinatario de la información no puede negar recibir información. Esta familia requiere que las TSF proporcionen un método para asegurar que un sujeto que transmite información está provisto de la evidencia de la recepción de la información.

Clase FCS: Soporte criptográfico El TSF puede emplear la funcionalidad criptográfica para ayudar a satisfacer algunos objetivos de seguridad de alto nivel.
FCS_CKM: Administración de claves criptográficas Esta familia soporta el ciclo de vida de las claves criptográficas y define requerimientos para: generación de claves criptográficas, distribución de claves criptográficas, acceso a claves criptográficas y distribución de claves criptográficas.
FCS_COP: Operación criptográfica Esta familia debe ser incluida donde existan requerimientos para realizar operaciones criptográficas, que incluyen: encriptación, desencriptación, generación y/o verificación de firma digital, generación de ckecksums criptográficos, hash seguro (compendio de mensajes), encriptación y/o desencriptación de claves criptográficas y acuerdo de claves criptográficas.

Clase FDP: Protección de datos del usuario Se divide en cuatro grupos de familias que tratan los datos del usuario en un TOE, durante la importación, exportación y almacenamiento, también los atributos de seguridad directamente relacionados con los datos del usuario.
a) Políticas de seguridad para la protección de datos del usuario
FDP_ACC: Política de control de acceso Identifica las SFPs de control de acceso y define el alcance de control de las políticas que forman la parte de control de acceso identificado de la TSP.
FDP_IFC: Política de control de flujo de información Identifica las SFPs de control de flujo de información y define el alcance de control de las políticas que forman la parte de control de acceso identificado de la TSP.
b) Formas de protección de datos del usuario
FDP_ACF: Funciones de control de acceso Describe las reglas para las funciones que pueden implementar una política de control de acceso nombrada en FDP_ACC.
FDP_IFF: Funciones de control de flujo de información Describe las reglas para las funciones que pueden implementar las SFPs de control de flujo de información nombradas en FDP_IFC.
FDP_ITT: Transferencia interna Proporciona los requerimientos que dirigen la protección de los datos del usuario cuando son transmitidos entre las partes de un TOE por un canal interno.
c) Almacenamiento fuera de línea, importación y exportación
FDP_DAU: Autenticación de datos Proporciona un método de garantía de la validez de una unidad de datos específicos que puede ser usada para verificar que el contenido de la información no ha sido modificado o falsificado.
FDP_ETC: Exportación hacia fuera del control de las TSF Define funciones para exportar datos de usuario del TOE tal que sus atributos de seguridad y protección pueden ser preservados o ignorados una vez que han sido exportados.
FDP_ITC: Importación de fuera del control de las TSF Define los mecanismos para la introducción de los datos de usuario en el TOE tal que tiene los atributos de seguridad apropiados y está debidamente protegido. También toma en cuenta las limitaciones de la importación.
d) Comunicación dentro de las TSF

FDP_UCT: Protección de la confidencialidad por la transferencia de datos del usuario dentro del TSF. Define los requerimientos para asegurar la confidencialidad de los datos del usuario cuando son transferidos usando un canal externo entre distintos TOEs.
FDP_UIT: Protección de la integridad por la transferencia de datos del usuario dentro de las TSF. Define los requerimientos para proporcionar integridad de los datos de usuario en tránsito entre las TSF y otro producto confiable de TI, y la recuperación de errores detectables y podría contemplar su corrección.

Clase FIA: Identificación y autenticación Contempla los requerimientos de las funciones para establecer y verificar una identidad de usuario sostenida.
FIA_AFL: Fallos de autenticación Contiene requerimientos para definir valores para algunos números de intentos de autenticación fallidos y las acciones de las TSF en estos casos.
FIA_ATD: Definición de atributos del usuario Define los requerimientos para asociar los atributos de seguridad del usuario con los usuarios.
FIA_UAU: Autenticación del usuario Define los tipos de mecanismos de autenticación del usuario soportados por las TSF.
FIA_UID: Identificación del usuario Define las condiciones bajo las que los usuarios se identificarán antes de hacer cualquier otra acción.

Clase FMT: Administración de seguridad Especifica la administración de algunos aspectos de las TSF.
FMT_MOF: Administración de funciones en las TSF Permite a usuarios autorizados controlar las funciones de seguridad en las TSF.
FMT_MSA: Administración de atributos de seguridad Permite a usuarios autorizados controlar la administración de los atributos de seguridad.
FMT_MTD: Administración de los datos de las TSF Permite a los usuarios autorizados controlar la administración de los datos de las TSF.
FMT_SAE: Expiración de atributos de seguridad Maneja la capacidad de establecer límites de tiempo para la validez de los atributos de

seguridad.
FMT_SMF: Especificación de funciones de administración Permite la especificación de las funciones de administración para ser proporcionadas con el TOE.
FMT_SMR: Roles de administración de seguridad Controla la asignación de diferentes roles a los usuarios.

A.4 Elementos del TCSEC.

Políticas de seguridad:

Control de Acceso Discrecional El Control de Acceso Discrecional (DAC) es un método de restringir el acceso a los archivos basándose en la identidad de los usuarios y/o los grupos a los que pertenecen.
Etiquetas Al iniciar en el nivel B1, el libro naranja propone que cada sujeto (p.e. usuario, proceso) y un objeto almacenado (p.e. archivos, directorios, ventanas, socket) tengan una etiqueta sensitiva asociada a él. Una etiqueta sensitiva de usuario especifica el grado, o nivel de confianza, asociado con ese usuario. Una etiqueta sensitiva de archivo especifica el nivel de confianza que un usuario puede ser capaz de tener al accesar ese archivo.
Integridad de Etiquetas La integridad de etiquetas asegura que las etiquetas sensitivas asociadas con eventos y objetos tienen una representación exacta de los niveles de seguridad de estos eventos y objetos.
Dispositivo Multinivel Un dispositivo multinivel o un canal de comunicaciones multinivel es uno con la capacidad de escribir información con un número diferente de niveles de seguridad. Cuando se escribe información en un dispositivo multinivel, se requiere que el sistema tenga alguna forma de asociar un nivel de seguridad a él.
Dispositivo de Nivel Único Un dispositivo de nivel único o un canal de comunicaciones de nivel único es uno capaz de escribir información con sólo un nivel particular de seguridad. El nivel que se especifica para un dispositivo depende usualmente de su localización física o de la seguridad inherente del tipo de dispositivo.
Control de Acceso Obligatorio Pone el control de todos los accesos como decisiones bajo el control del sistema.

Responsabilidad:

Identificación y Autentificación La identificación y la autentificación es un requerimiento de un sistema de seguridad en todos los niveles. El libro naranja requiere que la identificación del usuario antes de ejecutar cualquier tarea que requiera interacción con el TCB. En la mayoría de los sistemas multiusuario, la identificación en el sistema se hace a través de algún tipo de nombre identificador (login), seguido de un password.
Rutas Seguras Una ruta segura proporciona un medio libre de errores, por el cual un usuario (típicamente una terminal o un a estación de trabajo) puede comunicarse directamente

con un TCB sin interactuar con el sistema a través de aplicaciones inseguras y capas del sistema operativo.
Auditoría La auditoría es el registro, examen y revisión de las actividades relacionadas con la seguridad en un sistema confiable. Una actividad relacionada con la seguridad es cualquier acción relacionada con el acceso de usuarios, o acceso a objetos.

Confianza:

Arquitectura del Sistema El requerimiento de arquitectura del sistema tiene el objeto de diseñar un sistema para hacerlo lo más seguro posible, - sino invulnerable.
Administración de Seguridad Está relacionado el concepto de administración con la separación de obligaciones y que ningún usuario tenga el control total de los mecanismos de seguridad del sistema, para que de ninguna forma un usuario pueda comprometer completamente al sistema.
Recuperación Confiable La recuperación confiable asegura que la seguridad no ha sido violada cuando se cae un sistema o cuando cualquier otra falla del sistema ocurre. Se debe recuperar el sistema de acuerdo con ciertos procedimientos para asegurar la continuidad de la seguridad en el sistema.
Pruebas de Seguridad Estos son los dos tipos básicos de pruebas de seguridad: Prueba de mecanismos y Prueba de interfaz. La prueba de mecanismos significa probar los mecanismos de seguridad, estos mecanismos incluye control de acceso discrecional, etiquetado, control de acceso obligatorio, Identificación y autentificación, prueba de rutas, y auditoría. La prueba de interfaz significa el probar todas las rutinas del usuario que involucren funciones de seguridad.

Documentación:

Guía del Usuario de Características de Seguridad Es un apunte ordinario, sin privilegios para todos los usuarios del sistema. En el se encuentran cosas que es necesario saber acerca de las características del sistema de seguridad y de cómo es que están reforzadas.
Facilidades del Manual de Seguridad Este documento es un apunte de administrador del sistema y/o administradores de seguridad.

A.5 SECCIÓN C - SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET (OSSTMM).

2. Sondeo de Red.

Examinar pistas de la organización a analizar.

1. Inspeccionar los logs del servidor web y los logs de intrusión en busca de eventos de los sistemas.
2. Inspeccionar mensajes de grupos de noticias y listas de distribución en busca de eventos de los sistemas.

Filtración de información.

3. Examinar las cabeceras de los correos electrónicos, los mensajes devueltos y los destinatarios de las alertas y eventos del sistema de los servidores.
4. Buscar información sobre la organización a analizar en los grupos de noticias.
5. Buscar en bases de datos de empleos y en periódicos ofertas de puestos de trabajo en TI dentro de la organización a analizar, referencias a hardware y software.
6. Buscar en servicios P2P conexiones dentro de la red objetivo y datos referentes a la organización.

3. Identificación de los servicios.

Verificación de respuestas para varios protocolos.

1. Verificar y examinar el uso de tráfico y protocolos de enrutamiento.
2. Verificar y examinar el uso de protocolos no estándar.
3. Verificar y examinar el uso de protocolos cifrados.
4. Verificar y examinar el uso de TCP e ICMP sobre IPV6.

Identificación de servicios.

5. Relacionar cada puerto abierto con un servicio y protocolo.
6. Identificar el nivel de parcheado del sistema a partir de su up-time.
7. Identificar la aplicación tras el servicio y su nivel de parcheado.
8. Verificar la aplicación y su versión en el sistema.

Identificación de sistemas.

9. Examinar las respuestas de los sistemas para determinar el tipo de sistema operativo y su nivel de parcheado.
10. Examinar las respuestas de las aplicaciones para determinar su sistema operativo y su nivel de parcheado.
11. Buscar ofertas de trabajo para obtener información sobre los servidores y aplicaciones del objetivo.
12. Buscar en boletines técnicos y grupos de noticias información sobre los servidores y las aplicaciones del objetivo.
13. Relacionar la información recopilada con las respuestas de los sistemas para ajustar los resultados.

4. Búsqueda de información competitiva.

Información del negocio.

1. Realizar un mapa y medir la estructura de directorio de los servidores web.
2. Realizar un mapa y medir la estructura de directorio de los servidores de FTP.
3. Determinar el costo de la infraestructura en SI a partir de sus sistemas operativos, aplicaciones y hardware.
4. Determinar el costo de mantenimiento de la infraestructura a partir del salario de la zona para profesionales de TI, ofertas de trabajo, cantidad de personal, currículums publicados y cargos.
5. Medir el entusiasmo (respuesta) de la organización basándose en grupos de noticias, tableros web y los sitios de respuesta de la industria.
6. Registrar el número de productos que se venden electrónicamente.
7. Registrar el número de productos encontrados en fuentes P2P, sitios de software pirata, cracks disponibles para versiones específicas y documentación tanto interna como de terceras partes sobre los productos.
8. Identificar socios del negocio.
9. Verificar que todos contratos realizados a través de Internet desde la firma digital a la pulsación del botón que implica la aceptación de las cláusulas por parte del cliente final pueden ser repudiadas inmediatamente y durante un período de 7 días.

5. Revisión de Privacidad.

Política.

1. Identificar la política de privacidad pública.
2. Identificar los formularios web.
3. Identificar el tipo y la localización de la base de datos donde se almacenan los datos recolectados.
4. Identificar los datos recolectados por la organización.
5. Identificar la localización de los datos almacenados.
6. Identificar los tipos de cookies.
7. Identificar el tiempo de expiración de las cookies.
8. Identificar la información guardada en las cookies.
9. Verificar los métodos de cifrado de las cookies.
10. Identificar los gifs de publicidad en los servicios web y en los correos electrónicos.
11. Identificar la localización de los gifs de publicidad.

Difamación y falsa divulgación.

12. Identificar las personas, organizaciones e instituciones reales a las que corresponden realmente las ficticias.
13. Identificar personas u organizaciones retratadas de forma negativa.

Apropiación.

14. Identificar personas, organizaciones o materiales que por ellos mismos o por similitud son utilizados comercialmente en sitios web o anuncios publicitarios.
15. Revelación de datos privados.
16. Identificar información de empleados, organizaciones o materiales que contienen información privada.

6. Obtención de documentos.

1. Investigar personas clave vía páginas personales, resúmenes publicados, afiliaciones organizacionales, información de directorios, datos de compañías y el registro electoral.
2. Recopilar direcciones de e-mail corporativas y personales de las personas clave.
3. Buscar en bases de datos de trabajo conjuntos de perfiles tecnológicos requeridos por la organización objetivo.
4. Buscar en grupos de noticias referencias y mensajes enviados desde dentro de la organización y por personas clave de la organización.
5. Buscar documentos que contengan códigos ocultos o datos de revisión.
6. Examinar redes P2P con referencias o envíos desde dentro de la organización y por personas claves de la organización.

7. Búsqueda y verificación de vulnerabilidades.

1. Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.
2. Medir la organización objetivo utilizando herramientas de escaneo.
3. Intentar determinar vulnerabilidades por tipo de aplicación y sistema.
4. Intentar ajustar vulnerabilidades a servicios.
5. Intentar determinar el tipo de aplicación y servicio por vulnerabilidad.
6. Realizar pruebas redundantes al menos con 2 escáneres automáticos de vulnerabilidades.
7. Identificar todas las vulnerabilidades relativas a las aplicaciones.
8. Identificar todas las vulnerabilidades relativas a los sistemas operativos.
9. Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar al sistema objetivo.
10. Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos.
11. Verificar todos los positivos.

8. Testeo de aplicaciones de Internet.

Autenticación.

1. Buscar las posibles combinaciones de contraseñas por fuerza bruta en las aplicaciones.
2. Saltarse el sistema de autenticación con una validación cambiada.
3. Saltarse el sistema de autenticación reproduciendo información de la autenticación.
4. Determinar la lógica de la aplicación para mantener las sesiones de autenticación – número (consecutivo) de intentos fallidos, intentos fuera de tiempo, etc.
5. Determinar las limitaciones de control de acceso en las aplicaciones - permisos de acceso, duración de las sesiones, tiempo inactivo.

Administración de sesiones.

6. Adivinar la secuencia y formato de la ID de sesión.

7. Determinar si la ID de sesión esta formada con información de direcciones IP; ver si la misma información de sesión puede ser recuperada y reutilizada en otra máquina.
8. Determinar las limitaciones de mantenimiento de sesión - uso del ancho de banda, limitaciones de bajadas/subidas de archivos, limitaciones en transacciones, etc.
9. Reproducir la información reunida para engañar a las aplicaciones.

9. Enrutamiento.

El router y sus características.

1. Verificar el tipo de router.
2. Verificar si el router está dando servicio de traducción de direcciones de red (NAT).

Verificar la configuración de las ACL's del router

3. Testear la ACL del router en contra de las políticas de seguridad y en contra de la regla "Deny All".
4. Verificar si el router está filtrando el tráfico de la red local hacia afuera.
5. Verificar que el router esté haciendo detección de direcciones falsas.
6. Verificar las intrusiones desde un escaneo inverso en el módulo de escaneo de puertos.
7. Testear las capacidades externas del router desde el interior.
8. Cuantificar la habilidad que tiene el router para manejar fragmentos de paquetes muy pequeños.
9. Cuantificar la habilidad del router para manejar paquetes grandes.

11. Testeo de control de acceso.

El firewall y sus características.

1. Verificar el tipo de firewall.
2. Verificar si el firewall está dando servicio de NAT.

Verificación de la configuración de las ACL.

3. Testear la ACL del firewall en contra de las políticas de seguridad y en contra de la regla "Denegar Todo".
4. Verificar si el firewall está filtrando el tráfico de la red local hacia afuera.
5. Verificar que el firewall esté haciendo detección de direcciones origen falsas.
6. Verificar las intrusiones desde un escaneo inverso en el módulo de escaneo de puertos.
7. Testear las capacidades externas del firewall desde el interior.
8. Determinar el éxito de los métodos de identificación de firewall a través de los distintos paquetes de respuesta.

Revisión de registros del firewall.

9. Testear el proceso de registro del firewall.
10. Verificar escaneos de vulnerabilidades automatizados.
11. Verificar deficiencias de registros de servicios.

12. Testeo de IDS.

El IDS y sus características.

1. Verificar el tipo de IDS.
2. Determinar la esfera de protección o influencia.
3. Testear los estados de alarma del IDS.

Testeo de configuración del IDS.

4. Testear la configuración del IDS para reacciones múltiples, ataques variados (inundación).
5. Testear la configuración del IDS para reacciones como URL's manipuladas y rutinas de explotación.
6. Testear la configuración del IDS para reacciones ante cambios de velocidad al enviar paquetes.
7. Testear la configuración del IDS para reacciones ante cambios aleatorios de velocidad durante un ataque.
8. Testear la configuración del IDS para reacciones ante cambios aleatorios de protocolos durante un ataque.
9. Testear la configuración del IDS para reacciones ante cambios aleatorios de origen durante un ataque.
10. Testear la configuración del IDS para reacciones ante cambios de puerto de origen.
11. Testear en el IDS la habilidad de manejar paquetes fragmentados.
12. Testear en el IDS la habilidad de manejar métodos de ataques de sistemas específicos.
13. Testear los efectos y reacciones del IDS ante una dirección IP contra varias direcciones.
14. Encontrar alertas de IDS sobre escaneos de vulnerabilidades.
15. Encontrar alertas de IDS sobre descifrado de contraseñas.
16. Encontrar alertas de IDS de testeos de sistemas confiados.

13. Testeo de medidas de contingencia.

1. Medir el mínimo de recursos necesarios que se necesitan en el subsistema para realizar las tareas.
2. Verificar los recursos disponibles en este subsistema que necesiten realizar estas tareas, y qué recursos están protegidos desde este subsistema.
3. Verificar la detección de medidas presentes para la detección de intentos de acceso a los recursos protegidos.
4. Verificar recursos innecesarios.
5. Verificar las propiedades del sistema de contingencia.
6. Verificar la detección de medidas presentes para la detección de accesos no comunes a los recursos necesarios.
7. Medidas de configuración del sistema.

14. Descifrado de contraseñas.

1. Obtener el fichero de contraseñas desde el sistema que guarda nombres de usuario y contraseña.
2. Realizar un ataque automatizado de diccionario al fichero de contraseñas.
3. Realizar un ataque de fuerza bruta al fichero de contraseñas.
4. Usar contraseñas obtenidas o sus variaciones para acceder a sistemas o aplicaciones adicionales.
5. Realizar programas automatizados de descifrado en ficheros cifrados que haya encontrado como intento de recopilar más datos y subrayar la necesidad de un cifrado del sistema o de documentos más fuerte.
6. Verificar la edad de las contraseñas.

15. Testeo de DoS.

1. Verificar que las cuentas administrativas, archivos y recursos de los sistemas están asegurados apropiadamente y todos los accesos están concedidos con “mínimo privilegio”.
2. Comprobar las restricciones de sistemas expuestas a redes sin confianza.
3. Verificar que los puntos de referencia están establecidos a partir de una actividad normal del sistema.
4. Verificar que los procedimientos están en un lugar que responde a una actividad irregular.
5. Verificar la respuesta a una información negativa simulada (ataques propaganda).
6. Testear cargas de red y de servidor excesivas.

16. Evaluación de políticas de seguridad.

1. Comparar la política de seguridad contra el estado actual de la presencia en Internet.
2. Aprobación de la Gerencia. Buscar cualquier signo que revele que la política está aprobada por la gerencia.
3. Cerciorarse de que la documentación está adecuadamente almacenada, ya sea electrónicamente o en otros medios, y que la política ha sido leída y aceptada por el personal incluso antes de que ellos obtengan acceso a los sistemas informáticos.
4. Identificar los procedimientos de manejo de incidentes, para asegurarse de que las brechas de seguridad son manejadas por las personas adecuadas y que son reportadas de manera apropiada.
5. Conexiones entrantes. Verificar los riesgos mencionados que tienen relación directa con las conexiones entrantes de Internet y las medidas que son necesarias implementar para reducir o eliminar dichos riesgos.
6. Conexiones salientes. Buscar cualquier regla de conexiones salientes que no corresponda con la implementación.
7. Medidas de seguridad. Las reglas que exigen la implementación de medidas de seguridad, deben ser cumplidas.
8. Comprobar la política de seguridad contra el estado actual de las conexiones no relacionadas a Internet.
9. Verifique que la política de seguridad establezca las medidas de contención y los tests de ingeniería social basados en el uso indebido de Internet por parte de los

empleados, de acuerdo con la justificación de negocios y las mejores prácticas de seguridad.

APÉNDICE B

FORMATOS DE AUDITORÍA INFORMÁTICA

APÉNDICE B

FORMATOS DE AUDITORÍA INFORMÁTICA

B.1 Formatos varios de auditoría. [33]

Una vez que se ha hecho la planeación, se puede utilizar el formato de la Tabla B.1, el cuál servirá para resumir el plan de trabajo de la auditoría. El control del avance de la auditoría se puede llevar mediante el formato de la Tabla B.2. Como muestra de presentación de las conclusiones está la Tabla B.3 y para el seguimiento de auditoría informática obsérvese la Tabla B.4.

Programa de auditoría informática						
ORGANISMO_____ HOJA NUM._____ DE_____ FECHA DE FORMULACIÓN_____						
FASE	DESCRIPCIÓN	ACTIVIDAD	NUM. PERSONAL PARTICIPANTE	INICIO ESTIMADO	TÉRMINO ESTIMADO	DÍAS HAB. EST.

Tabla B.1 Programa de auditoría informática

[33] Chávez Chávez, Erika V. *Fundamentos de auditoría informática y su aplicación a la seguridad en redes de ordenadores.* México, ENEP Aragón, 2003. pp. 48-58, 170, 171.

Avance del cumplimiento del programa de auditoría informática

ORGANISMO_____ HOJA NUM._____ DE_____

PERIODO QUE REPORTA_____

FASE	SITUACIÓN DE LA AUDITORÍA			PERIODO REAL DE LA AUDITORÍA		DÍAS REALES USADOS	GRADO DE AVANCE	DÍAS HOMBRE EST.	EXPLICACIÓN DE LAS VARIACIONES EN RELACIÓN CON LO PROGRAMADO
	NO INICIADA	EN PROCESO	TERMINADA	INICIADA	TERMINADA				

Tabla B.2 Avance del cumplimiento del programa de auditoría informática

Conclusiones de la auditoría informática

DIRECCIÓN _____ HOJA NUM. _____ DE _____

AUDITORÍA A _____ FECHA DE TÉRMINO DE LA AUDITORÍA _____

NUM.	PROBLEMÁTICA	CAUSAS	REPERCUSIONES	ALTERNATIVAS DE SOLUCIÓN	OBSERVACIONES	FECHA PROGRAMADA IMPLANTACIÓN	RESPONSABLE RECOMENDACIÓN

Tabla B.3 Conclusiones de la auditoría informática

Seguimiento de las recomendaciones de la auditoría informática

PERIODO QUE SE REPORTA _____

DIRECCIÓN _____ HOJA NUM. _____ DE _____

AUDITORÍA A _____ FECHA DE TÉRMINO DE LA AUDITORÍA _____

NUM. OBS.	RECOMENDACIÓN	FECHA ESTIMADA RESOLUCIÓN	FECHA REAL RESOLUCIÓN	MOTIVO POR EL QUE NO SE HA RESUELTO	REPLANTEAMIENTO DE LA SOLUCIÓN	OBSERVACIÓN	FECHA PROBABLE IMPLANTACIÓN	RESPONSABLE RECOMENDACIÓN

Tabla B.4 Seguimiento de las recomendaciones de la auditoría informática

APÉNDICE C

APLICACIÓN DE LA AUDITORÍA

APÉNDICE C

APLICACIÓN DE LA AUDITORÍA

Es necesario expresar algunas limitantes con las que nos enfrentamos al tratar de aplicar la metodología que hemos desarrollado para la auditoría en seguridad para redes:

- Al no ser auditores no contamos con los recursos humanos y materiales para su realización.
- Las empresas no disponen su información a externos y no auditores.
- La poca información que se puede recopilar no es muy específica y es difícil obtener/ver documentación.
- El acceso a los sistemas es prácticamente nulo.
- El poco tiempo que nos pueden destinar informalmente para la realización de este trabajo.
- No se tiene la experiencia en el correcto uso de herramientas de auditoría.

No obstante estos impedimentos, pudimos aplicar de manera directa algunas entrevistas y todos los cuestionarios que hemos realizado al personal encargado de la Seguridad Informática en una entidad de Gobierno. Asimismo nos fue posible revisar someramente una parte de la documentación de las políticas de seguridad y comprobar de manera directa muchas de las respuestas del “auditado”.

Por petición expresa de éste y de acuerdo al código de ética de auditoría, no mencionaremos los nombres ni del auditado ni de la entidad gubernamental analizada. Sólo podemos decir que se trata de un organismo con una red considerablemente grande y que si se maneja información sensible. Pero romperemos la regla de auditoría al hacer públicos en este documento los resultados y análisis que sólo deberían ser entregados a la administración de la entidad. Esto lo hacemos con el objeto de mostrar una pequeña visión práctica (aunque incompleta) de la metodología desarrollada y esperando que este análisis sirva a quien nos ha facilitado la información.

C.1 LAN.

El sujeto de la auditoría en por supuesto un organismo gubernamental y el alcance abarca la LAN completa de la organización y más específicamente el site. Se considerarán las nueve cláusulas de control definidas en el capítulo anterior. En cuanto al objetivo de la auditoría se encuentra fundamentalmente el cumplir con los principios de seguridad de la LAN y garantizar que los controles y políticas se satisfacen mutuamente.

En cuanto a la realización, se han tomado todos los controles de seguridad definidos en el capítulo anterior.

La ponderación final de los sectores auditados es la siguiente:

Cláusulas de control	Pesos técnicos (Pt)	Pesos políticos (Pp)	Pesos finales [Pf=(Pt+Pp)/2]
C.1. Políticas de seguridad.	15	9	12.0
C.2. Gobierno de la seguridad.	13	10	11.5
C.3. Control y clasificación de bienes.	10	8	9.0
C.4. Seguridad de los empleados.	9	10	9.5
C.5. Seguridad física de la LAN y su entorno.	9	15	12.0
C.6. Administración de las comunicaciones.	11	15	13.0
C.7. Control de acceso a la LAN.	15	15	15.0
C.8. Desarrollo de seguridad de una LAN.	9	10	9.5
C.9. Obediencia.	9	8	8.5
Total	100	100	100

Tabla C. 111 Ponderación de cláusulas de control

Cláusula 1: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.1.1. Políticas de seguridad de la LAN.	100	100	100
Total	100	100	100

Tabla C. 112 Ponderación de los objetivos de la cláusula 1

Cláusula 2: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.2.1. Administración de seguridad de la LAN.	50	30	40.0
O.2.2. Seguridad en el acceso a la LAN por terceras personas.	20	40	30.0
O.2.3. Análisis de riesgos.	30	30	30.0
Total	100	100	100

Tabla C. 113 Ponderación de los objetivos de la cláusula 2

Cláusula 3: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.3.1. Responsabilidad de los bienes o activos.	50	60	55.0
O.3.2. Clasificación de la información.	50	40	45.0
Total	100	100	100

Tabla C. 114 Ponderación de los objetivos de la cláusula 3

Cláusula 4: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.4.1. Seguridad en la definición de puestos.	25	20	22.5
O.4.2. Entrenamiento del personal.	50	20	35.0
O.4.3. Respuesta a incidentes de seguridad de la LAN.	25	60	42.5
Total	100	100	100

Tabla C. 115 Ponderación de los objetivos de la cláusula 4

Cláusula 5: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.5.1. Aseguramiento de áreas de la red y su entorno.	50	40	45.0
O.5.2. Seguridad del equipo de la LAN.	50	60	55.0
Total	100	100	100

Tabla C. 116 Ponderación de los objetivos de la cláusula 5

Cláusula 6: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.6.1. Procedimientos y responsabilidades.	30	10	20.0
O.6.2. Protección contra software malicioso.	15	30	22.5
O.6.3. Back up.	15	30	22.5
O.6.4. Administración de la LAN.	25	20	22.5
O.6.5. Intercambio de información.	15	10	12.5
Total	100	100	100

Tabla C. 117 Ponderación de los objetivos de la cláusula 6

Cláusula 7: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.7.1. Requerimientos para el control de acceso a la LAN.	17	10	13.5
O.7.2. Administración de acceso de los usuarios a la LAN.	17	15	16.0
O.7.3. Responsabilidades del usuario.	15	15	15.0
O.7.4. Control de acceso a la LAN.	17	20	18.5
O.7.5. Monitoreo de acceso y uso de la red de actividades no autorizadas.	17	20	18.5
O.7.6. Cómputo móvil.	17	20	18.5
Total	100	100	100

Tabla C. 118 Ponderación de los objetivos de la cláusula 7

Cláusula 8: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.8.1. Controles criptográficos.	60	50	55.0
O.8.2. Seguridad en los procesos de desarrollo y soporte.	40	50	45.0
Total	100	100	100

Tabla C. 119 Ponderación de los objetivos de la cláusula 8

Cláusula 9: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.9.1. Obediencia con los requerimientos legales.	33	30	31.5
O.9.2. Revisión de políticas de seguridad y obediencia técnica.	34	40	37.0
O.9.3. Consideraciones de auditoría de la LAN.	33	30	31.5
Total	100	100	100

Tabla C. 120 Ponderación de los objetivos de la cláusula 9

Las respuestas y calificaciones de los cuestionarios se muestran a continuación:

RESPUESTAS A LOS CUESTIONARIOS DE SEGURIDAD EN LAN

Cláusula 1. Políticas de seguridad.

Objetivo 1.1. Políticas de seguridad de la LAN.

Control 1.1.1. *Documento de políticas de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un documento de políticas de seguridad de la información que incluya la seguridad de la LAN?	Sí existen las políticas.	5
- ¿Este documento está aprobado, publicado y comunicado a todos los empleados?	Sólo a una parte de los empleados, generalmente de sistemas y/o de puestos gerenciales.	2
- ¿Sabe de qué trata el documento? ¿Comprende el contenido?	Sí, yo lo realicé.	2
- ¿El documento incluye la definición, objetivos, alcance y responsabilidades de la seguridad de la LAN?	Sí, aunque algunos de esos puntos no son muy específicos.	2
Total control 1.1.1.		11/20 55%

Tabla C. 121 Cuestionario control 1.1.1

Control 1.1.2. *Revisión y evaluación de las políticas de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son revisadas o redefinidas periódicamente las políticas de seguridad de la LAN?	Son revisadas periódicamente, aunque no han sido redefinidas.	3
- ¿Con qué frecuencia se realizan?	Semestral.	3
- ¿Qué actividades se realizan en estas revisiones periódicas?	Revisión de la factibilidad de las políticas según el entorno.	2
Total control 1.1.2.		8/15 53.33%

Tabla C. 122 Cuestionario control 1.1.2

Cláusula 2. Gobierno de la seguridad.

Objetivo 2.1. Administración de seguridad de la LAN.

Control 2.1.1. *Gestión de administración y coordinación de la seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen representantes de las áreas clave de la organización en la administración de la seguridad de la LAN? ¿De qué áreas?	No de todas, únicamente Telecomunicaciones y Coordinación de Planeación. Es global y por cada área.	3
- ¿La coordinación de la seguridad de la LAN revisa y aprueba las políticas de la seguridad de la red?	La Dirección General es quien las implanta a nivel general y toma la decisión.	3
- ¿La coordinación de la seguridad de la red considera el monitoreo de las amenazas y de los incidentes de seguridad?	Sí son tomados en cuenta estos puntos.	3
- ¿La coordinación de la seguridad de la LAN ha definido los roles y responsabilidades para la seguridad de la red?	Sí.	5
- ¿La administración considera a la seguridad dentro de la planeación de la red? ¿De qué forma?	Sí, aplicando las políticas existentes o creando adiciones según se requiera, aunque en general se realiza empíricamente y en la práctica.	2
Total control 2.1.1.		16/25 64%

Tabla C. 123 Cuestionario control 2.1.1

Control 2.1.2. *Asignación de responsabilidades de seguridad LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está definida en las políticas de seguridad una guía para la asignación de roles y responsabilidades de la seguridad de la LAN?	No está definida.	1
- ¿Existe un documento en el que estén definidas las responsabilidades de la seguridad de la red?	Sí existe el documento.	5
- ¿Existe un propietario o responsable para cada activo o proceso de la red?	Sí, cada activo tiene un responsable.	5
Total control 2.1.2.		11/15 73.33%

Tabla C. 124 Cuestionario control 2.1.2

Control 2.1.3. *Asesoramiento de especialistas en seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿En qué eventos/situaciones se recurre al asesoramiento de algún especialista en seguridad de la LAN?	Cuando se compra software o equipo.	2
- ¿En cuánto tiempo es llamado el experto en seguridad desde que ocurre el suceso?	Si el equipo cuenta con asesoría por un año, se le llama alrededor de una semana del suceso.	2
- ¿Con qué privilegios cuenta el asesor/consultor en los sistemas?	Las mínimas necesarias, esto es, para supervisión.	4
Total control 2.1.3.		8/15 53.33%

Tabla C. 125 Cuestionario control 2.1.3

Control 2.1.4. *Revisión independiente de la seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿La seguridad de la red es revisada por auditores externos o internos independientes?	Por auditores internos, aunque no muy independientes y no es muy frecuente.	2
- ¿Qué revisan los auditores en la seguridad de la red? ¿Cuáles son sus objetivos?	Verifican la topología, los respaldos y aplican pruebas de vulnerabilidad con SW especial.	2
Total control 2.1.4.		4/10 40%

Tabla C. 126 Cuestionario control 2.1.4

Control 2.1.5. *Reacreditación.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un grupo especial para mantener actualizado el nivel de seguridad de la red?	No bien definido, pero se realiza algo al respecto.	1
- ¿Qué técnicas utiliza para verificar la seguridad de la red?	En base a la experiencia (juicio experto). No son realmente técnicas.	1
- ¿Es conocido este grupo sólo por la alta directiva (red teaming) o son públicas sus actividades (blue teaming)?	Sólo por la alta directiva.	1
Total control 2.1.5.		3/15 20%

Tabla C. 127 Cuestionario control 2.1.5

Objetivo 2.2. Seguridad en el acceso a la LAN por terceras personas.

Control 2.2.1. *Identificación de riesgos de acceso de terceras personas a la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se contempla al acceso no autorizado de terceras personas en el análisis de	Sólo en el caso de auditoría.	2

riesgos o cualquier otro estudio?		
- ¿Qué controles se han implementado para combatir el riesgo de accesos no autorizados a la red?	Físico: registro de la persona. Lógico: políticas para acceso (cambio periódico de contraseñas difíciles mayor a 8 caracteres).	2
- ¿Se ha definido claramente la identidad de las terceras personas físicas? ¿Cuáles son?	Sí, limpieza, proveedores, eléctricos, técnicos de aire acondicionado, pintura y equipo de seguridad.	3
- ¿Se ha definido expresamente la identidad de las terceras personas lógicas? ¿Cuáles son?	Intrusos.	2
- ¿Qué controles se han implementado para los accesos del personal de mantenimiento/soporte, limpieza, servicio social, etc.?	Contratos, supervisión directa y con cámaras.	2
Total control 2.2.1.		11/25 44%

Tabla C. 128 Cuestionario control 2.2.1

Control 2.2.2. *Especificaciones de seguridad en contratos con terceras personas.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Incluyen acuerdos formales para la seguridad de la LAN los contratos con terceras personas?	Contratos de confidencialidad.	2
- ¿Qué consideraciones mínimas de seguridad de la LAN involucra un contrato?	Que la información no va a ser divulgada.	1
- ¿En el contrato anterior se incluyen la política de seguridad de la LAN, los acuerdos de control de acceso y el derecho de monitoreo de la LAN?	Sí, son incluidos.	3
Total control 2.2.2.		6/15 40%

Tabla C. 129 Cuestionario control 2.2.2

Objetivo 2.3. Análisis de riesgos.

Control 2.3.1. *Evaluación de riesgos de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza una evaluación de riesgos de la seguridad de la LAN?	Sí es realizada.	3
- En la evaluación de riesgos, ¿se determina la forma en que deben ser manejados los riesgos de la seguridad de la red?	Sí.	3

- ¿La administración realiza reevaluaciones de riesgos, actualizados con auditorías o estudios anteriores?	Sí, aunque en forma mínima.	1
Total control 2.3.1.		7/15 46.66%

Tabla C. 130 Cuestionario control 2.3.1

Control 2.3.2. *Identificación y medición de riesgos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué tipos de riesgos se han identificado en la evaluación de riesgos de la LAN?	Falla de equipos o intrusiones.	2
- ¿Se les da a estos riesgos un tipo de clasificación cualitativa y cuantitativa de acuerdo a su impacto?	Sí, son clasificados por su daño potencial.	2
- ¿Se han implementado controles para contrarrestar este tipo de riesgos?	Sí.	3
Total control 2.3.2.		7/15 46.66%

Tabla C. 131 Cuestionario control 2.3.2

Control 2.3.3. *Plan de acción contra riesgos.*		
Preguntas	**Respuestas**	**Puntos**
¿Está definido un plan de acción contra riesgos?	Sí está definido.	4
¿Cuáles son sus beneficios y objetivos?	Mantener la disponibilidad e integridad de la información.	4
Total control 2.3.3.		8/10 80%

Tabla C. 132 Cuestionario control 2.3.3

Cláusula 3. Control y clasificación de bienes.

Objetivo 3.1. Responsabilidad de los bienes o activos.

Control 3.1.1. *Inventario de bienes relacionados con la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un inventario de bienes relacionados con la LAN?	Sí existe tal inventario.	4
- ¿Se realiza una actualización de dicho inventario? ¿Cada cuándo se realiza?	Es actualizado el inventario cada vez que ocurren cambios.	4
- ¿Se incluye en el inventario el valor relativo e importancia de cada bien?	Sí.	3
- ¿Qué tipo de bienes incluye este inventario?	Equipo de comunicación y servidores.	3

Total control 3.1.1.	14/20 70%

Tabla C. 133 Cuestionario control 3.1.1

Control 3.1.2. *Responsabilidad de los bienes relacionados con la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está definido el responsable de los activos inventariados?	Sí.	4
- ¿Está documentado, actualizado y es revisado periódicamente?	Sí.	5
Total control 3.1.2.		9/10 90%

Tabla C. 134 Cuestionario control 3.1.2

Objetivo 3.2. Clasificación de la información.

Control 3.2.1. *Manuales de clasificación de la información.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen manuales de clasificación de la información?	No está definida la clasificación.	1
- ¿Cuál es el objetivo de estos manuales?	-	1
Total control 3.2.1.		2/10 20%

Tabla C. 135 Cuestionario control 3.2.1

Control 3.2.2. *Manuales de clasificación de niveles de seguridad en la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está definida e implementada la clasificación de los niveles de seguridad en la LAN?	No, aunque se planea hacerse próximamente.	1
- ¿Para qué han sido definidos estos niveles de seguridad?	-	1
- ¿Qué niveles de seguridad se han definido?	-	1
Total control 3.2.2.		3/15 20%

Tabla C. 136 Cuestionario control 3.2.2

Control 3.2.3. *Manejo y rotulación de la información.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Han sido definidos procedimientos para el manejo y rotulación de la información?	No, se piensa realizar próximamente.	1
- ¿Qué incluyen y cuál es el alcance de estos procedimientos?	-	1

Total control 3.2.3.	2/10 20%

Tabla C. 137 Cuestionario control 3.2.3

Cláusula 4. Seguridad de los empleados.

Objetivo 4.1. Seguridad en la definición de puestos.

Control 4.1.1. *Incluir la seguridad en las responsabilidades de puestos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se encuentran definidos y documentados los roles y responsabilidades de seguridad de la LAN en los puestos de trabajo?	Sí están definidos y documentados.	4
- ¿Se han asignado prácticamente a los puestos de trabajo?	Sí, en lo posible.	3
Total control 4.1.1.		7/10 70%

Tabla C. 138 Cuestionario control 4.1.1

Control 4.1.2. *Términos y condiciones de empleo.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son establecidas responsabilidades respecto a la seguridad de la LAN en los términos y condiciones del contrato de los empleados?	No en el contrato pero sí en el área interna.	1
- ¿Qué aspectos incluyen?	-	1
- ¿Se consideran acuerdos de confidencialidad y responsabilidades legales?	-	1
- ¿Las responsabilidades definidas continúan después del término del empleo?	-	1
Total control 4.1.2.		4/20 20%

Tabla C. 139 Cuestionario control 4.1.2

Objetivo 4.2. Entrenamiento del personal.

Control 4.2.1. *Entrenamiento y culturización en seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Los empleados reciben adecuados entrenamiento/actualización en seguridad de la red? ¿Cuáles empleados?	Sí, de acuerdo al perfil de las responsabilidades.	1
- ¿Se promueve un entrenamiento sobre concientización de la seguridad de la	Sí, políticas y recomendaciones publicadas en Web.	1

red? ¿De qué forma?		
- ¿Con qué frecuencia se realizan estos entrenamientos descritos?	Anual.	1
Total control 4.2.1.		3/15 20%

Tabla C. 140 Cuestionario control 4.2.1

Objetivo 4.3. Respuesta a incidentes de seguridad de la LAN.

Control 4.3.1. *Reporte de incidentes de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son reportados los incidentes de seguridad de la red?	Sí.	4
- ¿Existe un procedimiento formal de reporte de estos incidentes?	Sí.	4
- ¿Existe un procedimiento de respuesta a incidentes de seguridad?	Sí.	3
- ¿Qué tan rápido son reportados y atendidos los incidentes de seguridad?	Se les da prioridad sobre otras actividades.	4
Total control 4.3.1.		15/20 75%

Tabla C. 141 Cuestionario control 4.3.1

Control 4.3.2. *Reporte de debilidades de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son reportadas por los usuarios las debilidades de la LAN?	No, carecen de cultura informática.	1
- ¿Con qué agilidad son reportadas y atendidas tales debilidades?	-	1
- ¿Existe un procedimiento formal adecuado para su reporte?	Sí.	2
Total control 4.3.2.		4/15 26.66%

Tabla C. 142 Cuestionario control 4.3.2

Control 4.3.3. *Reporte de mal funcionamiento del software en la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son reportados los malos funcionamientos del software?	Sí.	5
- ¿Existe un procedimiento establecido para realizar/atender los reportes de mal funcionamiento de software?	Sí.	3
- ¿Qué acciones son tomadas inicialmente en el reporte/atención del mal funcionamiento de software?	Basándose en el modelo OSI se verifica funcionamiento físico y causa de problemas de red.	2

Total control 4.3.3.	10/15 66.66%

Tabla C. 143 Cuestionario control 4.3.3

Control 4.3.4. *Aprendizaje de los incidentes.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento para cuantificar los costos de los incidentes de seguridad y del mal funcionamiento de software?	No se toman en cuenta costos económicos, sólo en tiempo.	1
- Los costos/daños de los incidentes anteriores ¿son usados en el análisis de riesgos, en la mejora continua o algún tipo de análisis?	Sí. Puede implicar la compra de otro equipo, su sustitución o redundancia.	1
Total control 4.3.4.		2/10 20%

Tabla C. 144 Cuestionario control 4.3.4

Control 4.3.5. Disciplina en seguridad de la LAN.		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué acciones son tomadas cuando se viola alguna política o procedimiento que afecte la seguridad de la red?	Se analiza la gravedad y puede haber sanciones fuertes (despidos). El Jefe directo es quién lo determina.	3
Total control 4.3.5.		3/5 60%

Tabla C. 145 Cuestionario control 4.3.5

Cláusula 5. Seguridad física de la LAN y su entorno.

Objetivo 5.1. Aseguramiento de áreas de la red y su entorno.

Control 5.1.1. *Perímetro de seguridad física.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe y está bien definido un perímetro físico de seguridad para proteger las áreas de la red? ¿Está formado por varias capas?	Sí existe y hay varias capas o filtros (2).	2
- ¿Por qué se ha establecido (bajo qué análisis) este perímetro de seguridad?	En base a el análisis de la sensibilidad de la información relevante y los servicios.	2
- ¿Qué controles de seguridad física se han establecido para el site y otras áreas de la LAN?	Registro, cámaras y site alterno.	2
- ¿Poseen alarmas las salidas de emergencia del perímetro de seguridad?	No, únicamente en la entrada/salida principal.	1

Total control 5.1.1.	7/20 35%

Tabla C. 146 Cuestionario control 5.1.1

Control 5.1.2. *Controles de entrada física.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué controles de acceso existen en las áreas sensibles de la red?	Bitácoras de acceso y entrada con llave.	2
- ¿Se maneja un procedimiento para el acceso y estancia de visitantes a las áreas seguras de la red? ¿Es registrado su tiempo de acceso y de salida?	Sí.	2
- ¿Qué controles de autenticación son usados para validar los accesos? ¿Se lleva un registro de todos los accesos?	Bitácoras o logs propios de los sistemas.	2
- ¿Todo el personal porta visiblemente una identificación?	Sí.	2
- ¿Son revisados y actualizados los derechos de acceso a las áreas seguras de la red?	Sí.	3
Total control 5.1.2.		11/25 44%

Tabla C. 147 Cuestionario control 5.1.2

Control 5.1.3. *Seguridad de las áreas de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- En el área de la LAN, ¿se consideran controles contra la posibilidad de desastres naturales y humanos?	Sí. Por ejemplo, un site alterno.	3
- ¿Qué elementos se consideran para mantener la discreción de las instalaciones de la red?	Cuartos cerrados.	2
- ¿Se han instalado sistemas de detección de intrusos, alarmas o circuito cerrado para monitorear el acceso a las áreas críticas de la red?	Cámaras de video.	2
- ¿Se mantienen aislados del site los materiales peligrosos?	Sí.	4
- ¿Qué medidas físicas y de construcción se tienen en cuenta para la protección del site?	Muros sólidos, aire acondicionado, extinguidotes y ubicación del site (nivel alto).	2
Total control 5.1.3.		13/25 52%

Tabla C. 148 Cuestionario control 5.1.3

Objetivo 5.2. Seguridad del equipo de la LAN.

Control 5.2.1. *Colocación y protección del equipo de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué consideraciones se han implementado para la colocación y protección del equipo de la red?	Cuartos cerrados bajo llave (incluyendo IDFs).	3
- ¿Se ha colocado el equipo de red de tal forma que se minimice su acceso y visibilidad?	Sí.	3
- ¿Qué controles se han implementado para proteger al equipo de la red contra amenazas naturales e interferencia electromagnética?	Ubicación fuera de interferencias e inundaciones.	3
- ¿Se han implementado políticas para evitar que el personal coma y fume cerca del equipo de red?	Sí.	3
Total control 5.2.1.		12/20 60%

Tabla C. 149 Cuestionario control 5.2.1

Control 5.2.2. *Suministro de energía ininterrumpible.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué medidas protegen la disponibilidad de la LAN contra fallos de energía?	Planta eléctrica (UPS).	5
- ¿Tienen esta protección los sistemas críticos de la red?	Sí.	5
Total control 5.2.2.		10/10 100%

Tabla C. 150 Cuestionario control 5.2.2

Control 5.2.3. *Seguridad del cableado de la LAN y su alimentación.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué protecciones se han establecido en el cableado de comunicaciones y energía?	Se aterrizan las canalizaciones y se ubican fuera de interferencia. Se aplican normas y estándares.	3
- ¿Está protegido el cableado de la red contra la intercepción, daño o interferencia?	Sí.	3
- ¿Existen localizaciones especiales para las conexiones de los sistemas críticos?	Sí.	4
- ¿Se considera el uso de la fibra óptica y de barridos oculares o electrónicos del cableado para localizar pinchamientos?	Sí.	3

Total control 5.2.3.	13/20 65%

Tabla C. 151 Cuestionario control 5.2.3

Control 5.2.4. *Mantenimiento del equipo de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Recibe el equipo de la red mantenimiento periódico?	Sí.	5
- ¿Se realiza este mantenimiento con procedimientos y personal adecuados y autorizados?	Sí.	5
- ¿Se tiene un registro de todas las operaciones de mantenimiento?	No.	1
- ¿Se consideran controles especiales cuando el equipo es llevado fuera de las instalaciones?	Sí, se les proporcionan derechos de acceso mínimos.	3
Total control 5.2.4.		14/20 70%

Tabla C. 152 Cuestionario control 5.2.4

Control 5.2.5. *Seguridad en el desecho y re-uso del equipo de red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué procedimiento se realiza con el equipo de desecho de la red que contiene información o configuraciones?	Se respalda y se borra la información.	3
- ¿Son sometidos los equipos especiales a un análisis de riesgos o a alguna evaluación para determinar su destino?	De manera informal.	1
Total control 5.2.5.		4/10 40%

Tabla C. 153 Cuestionario control 5.2.5

Cláusula 6. Administración de las comunicaciones y las operaciones de la LAN.

Objetivo 6.1. Procedimientos y responsabilidades.

Control 6.1.1. *Documentación de procedimientos de operación de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe la documentación de los procedimientos de operación de la LAN? ¿Son mantenidos como documentos formales?	Sí.	4
- ¿Qué instrucciones detalladas generales se encuentran en estos procedimientos?	Las instrucciones mínimas indispensables para la operación.	2

Total control 6.1.1.	6/10 60%

Tabla C. 154 Cuestionario control 6.1.1

Control 6.1.2. *Control de cambios operacionales.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen procedimientos que controlen los cambios al equipo, software y procedimientos relacionados con la LAN?	Sí, de manera informal.	1
- ¿Qué controles se han establecido en estos procedimientos?	El uso de bitácoras.	1
- ¿Se ha considerado la valoración del impacto potencial de estos cambios, su aprobación formal y su comunicación?	Sí.	4
Total control 6.1.2.		6/15 40%

Tabla C. 155 Cuestionario control 6.1.2

Control 6.1.3. *Procedimientos para la gestión de incidentes.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen procedimientos y responsabilidades para la gestión de incidentes de seguridad relacionados con la LAN?	Sí, de manera informal.	1
- ¿Qué tipos de incidentes cubren estos procedimientos?	Ataques y virus.	2
- ¿Cuáles son los pasos básicos de estos procedimientos?	El uso de herramientas para análisis forense y el registro de las acciones.	2
- ¿Se considera la colección apropiada de la evidencia para fines forenses?	Sí.	3
- ¿Qué acciones se consideran para la recuperación de incidentes?	Aislamiento y detectores de intrusos.	1
Total control 6.1.3.		9/25 36%

Tabla C. 156 Cuestionario control 6.1.3

Control 6.1.4. *Separación de responsabilidades.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se considera la segregación en las responsabilidades o tareas relacionadas con la seguridad de la red?	Sí.	3
- ¿Se considera que el personal únicamente realice las tareas definidas en su puesto?	No.	1

- ¿Se encuentran segregadas la Administración de la red, la Administración de la seguridad y el Área de Auditoría?	No.	1
Total control 6.1.4.		5/15 33.33%

Tabla C. 157 Cuestionario control 6.1.4

Objetivo 6.2. Protección contra software malicioso.

Control 6.2.1. *Controles contra software malicioso.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué controles existen contra el software malicioso?	Uso de dispositivos de seguridad, políticas publicadas en Internet y uso de antivirus.	2
- ¿Existe una política para el cumplimiento de las licencias en todo el software de la organización?	Sí.	2
- ¿Existen controles de seguridad para la conexión a redes externas?	Sí, mediante filtrado Web.	2
- ¿Existen procedimientos y responsabilidades para los eventos y procesos relacionados con antivirus?	Sí, de manera informal.	1
- ¿Se realizan revisiones regulares de software y datos en los sistemas críticos, revisión de correos electrónicos y descargas?	Sí.	1
Total control 6.2.1.		8/25 32%

Tabla C. 158 Cuestionario control 6.2.1

Objetivo 6.3. Back up.

Control 6.3.1. *Respaldo de información.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realizan regularmente respaldos de información de los sistemas críticos de la LAN? ¿De qué forma?	Sí, en medio magnético (disco duro).	2
- ¿Qué consideraciones se tienen en los respaldos de la red? ¿Son revisados regularmente? ¿Se considera la destrucción total del site?	Se respalda cuando hay cambios o de forma anual. También existe un site alterno.	2
Total control 6.3.1.		4/10 40%

Tabla C. 159 Cuestionario control 6.3.1

Control 6.3.2. *Logs de operación.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se mantiene y revisa un registro de los logs, de los sistemas críticos de la red?	Sí.	5
- ¿Qué información contienen los logs de operación?	Sesiones de usuarios, fallas de equipo y advertencias.	3
Total control 6.3.2.		8/10 80%

Tabla C. 160 Cuestionario control 6.3.2

Objetivo 6.4. Administración de la LAN.

Control 6.4.1. *Controles de seguridad de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen controles explícitos para la seguridad de la LAN? ¿Son revisados, implementados y mantenidos?	No formalmente.	1
- ¿Está explícitamente separada de otras operaciones la responsabilidad de la seguridad de la red?	Sí.	4
- ¿Han sido establecidas las responsabilidades y procedimientos de la administración del equipo remoto?	Sí.	4
- ¿Qué controles se han establecido para la protección de la confidencialidad e integridad de los datos que transitan por la LAN y la red pública?	Encripción, uso de certificados y VPN's.	5
Total control 6.4.1.		14/20 70%

Tabla C. 161 Cuestionario control 6.4.1

Objetivo 6.5. Intercambio de información.

Control 6.5.1. *Seguridad de la información en tránsito por la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está protegida la información en tránsito en su confidencialidad, integridad y disponibilidad?	Sí.	5
- ¿Qué técnicas se usan para la confidencialidad de la información en tránsito?	Encripción, uso de certificados y VPN's.	5
Total control 6.5.1.		10/10 100%

Tabla C. 162 Cuestionario control 6.5.1

Control 6.5.2. *Seguridad del comercio electrónico.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se han considerado controles para la mantener la seguridad del comercio electrónico?	No aplica.	
- ¿Qué tipo de eventos y transacciones son protegidas? ¿Mediante qué mecanismos?	No aplica.	
Total control 6.5.2.		

Tabla C. 163 Cuestionario control 6.5.2

Control 6.5.3. *Seguridad del correo electrónico.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen políticas y controles para el uso del correo electrónico?	Sí existen.	5
- ¿Qué controles y procedimientos se han establecido para la seguridad en su uso?	Las políticas de informática, uso de contraseñas, equipo de seguridad perimetral, antivirus.	2
- ¿Se responsabiliza a los empleados que comprometan la seguridad? ¿De qué forma?	Sí, se reporta a su jefe inmediato cuando la falta es menor. Cuando es grave se retira el servicio.	2
Total control 6.5.3.		9/15 60%

Tabla C. 164 Cuestionario control 6.5.3

Control 6.5.4. *Seguridad en sistemas disponibles públicamente.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está autorizada y protegida la información pública de la organización? ¿De qué forma está protegida?	Sí, con el uso de equipo de seguridad.	2
- ¿Se ha eliminado la posibilidad de acceso por este medio a la red organizacional?	Sí.	4
Total control 6.5.4.		6/10 60%

Tabla C. 165 Cuestionario control 6.5.4

Cláusula 7. Control de acceso a la LAN.

Objetivo 7.1. Requerimientos para el control de acceso a la LAN.

Control 7.1.1. *Política de control de acceso a la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está definida y documentada una política para el control de acceso a la LAN, estableciendo reglas y derechos de	Sí.	3

acceso a los usuarios?		
- ¿Existe consistencia entre el control de acceso y la clasificación de la información?	Sí, de manera informal.	1
- ¿Están definidas obligaciones contractuales para el acceso a datos y servicios?	No.	1
Total control 7.1.1.		5/15 33.33%

Tabla C. 166 Cuestionario control 7.1.1

Objetivo 7.2. Administración de acceso de los usuarios a la LAN.

Control 7.2.1. *Registro del usuario.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento de registro y borrado de cuentas de usuario? ¿Qué incluye?	Sí, incluye nombre y adscripción.	3
- ¿Revisa el procedimiento que el nivel de acceso sea apropiado y consistente con las políticas de seguridad?	Sí.	3
- ¿Los usuarios firman un acuerdo de condiciones de acceso?	Sí, de manera informal.	1
- ¿Las cuentas son revisadas periódicamente y removidas para evitar redundancia o mal manejo?	Sí, pero existe un rezago.	2
Total control 7.2.1.		9/20 45%

Tabla C. 167 Cuestionario control 7.2.1

Control 7.2.2. *Administración de privilegios de cuentas de usuario de red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento para designar, autorizar y usar privilegios de cuentas de acceso a la red?	Sí, de manera informal (no está escrito).	1
- ¿Qué consideraciones se incluyen en este procedimiento?	Se consideran privilegios básicos.	2
- ¿Son identificados los privilegios asociados a cada sistema?	Sí.	4
Total control 7.2.2.		7/15 46.66%

Tabla C. 168 Cuestionario control 7.2.2

Control 7.2.3. *Administración de passwords de red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento de	Sí. Incluye sus características de	1

administración para controlar todos los procesos de los passwords de la red? ¿Qué incluye?	asignación.	
Total control 7.2.3.		1/5 20%

Tabla C. 169 Cuestionario control 7.2.3

Control 7.2.4. *Revisión de los privilegios de acceso a la red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento formal para la revisión regular de los privilegios de acceso a la red? ¿Qué aspectos trata?	Sí, informal. Incluye la revisión de permisos o privilegios que tiene cada cuenta.	1
Total control 7.2.4.		1/5 20%

Tabla C. 170 Cuestionario control 7.2.4

Objetivo 7.3. Responsabilidades del usuario.

Control 7.3.1. *Uso de los passwords de red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe una práctica para advertir a los usuarios sobre el buen uso de los passwords?	Sí.	3
- ¿Qué prácticas son dadas a conocer a los usuarios?	El uso personal y cambio de contraseña periódica.	3
Total control 7.3.1.		6/10 60%

Tabla C. 171 Cuestionario control 7.3.1

Control 7.3.2. *Protección del equipo no atendido.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué medidas deben realizar los usuarios para proteger el equipo no atendido?	-	1
Total control 7.3.2.		1/5 20%

Tabla C. 172 Cuestionario control 7.3.2

Objetivo 7.4. Control de acceso a la LAN.

Control 7.4.1. *Política de uso de los servicios de la red.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe una política que defina y autorice el uso de los servicios de red?	Sí.	5
- ¿Qué incluye la política? ¿Se consideran procedimientos de	Cuentas sin compartir, cambio de contraseñas, uso de antivirus, no	2

autorización y protección?	conectar equipo no autorizado.	
Total control 7.4.1.		7/10 70%

Tabla C. 173 Cuestionario control 7.4.1

Control 7.4.2. *Autenticación de cuentas de usuarios externos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Tienen un control de acceso autentificado los usuarios externos a la LAN? ¿Qué método usan?	Sí, basado en la experiencia.	1
Total control 7.4.2.		1/5 20%

Tabla C. 174 Cuestionario control 7.4.2

Control 7.4.3. *Segregación de la LAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existen controles o implementaciones para segregar la LAN?	Sí.	5
- ¿Es protegido cada segmento con algún sistema de seguridad? ¿Cuál es el uso de los firewalls?	Sí, pero no todos, sólo en la WAN. Los firewalls son de frontera.	4
- ¿Bajo qué criterios se realiza la segregación de la LAN?	En base a la criticidad de las aplicaciones.	3
Total control 7.4.3.		12/15 80%

Tabla C. 175 Cuestionario control 7.4.3

Objetivo 7.5. Monitoreo de acceso y uso de la red de actividades no autorizadas.

Control 7.5.1. *Logging de acontecimientos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza un monitoreo y registro del acceso/uso de la red?	Sí.	5
- ¿Qué información es registrada durante estos accesos?	Fecha (hora, día) y uso.	3
Total control 7.5.1.		8/10 80%

Tabla C. 176 Cuestionario control 7.5.1

Objetivo 7.6. Cómputo móvil.

Control 7.6.1. *Cómputo móvil.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Están definidas políticas y controles para cubrir los riesgos del cómputo móvil?	Sí.	5

- ¿Qué consideraciones y controles se incluyen?	Uso de encripción y password.	2
Total control 7.6.1.		7/10 70%

Tabla C. 177 Cuestionario control 7.6.1

Cláusula 8. Desarrollo de seguridad de una LAN.

Objetivo 8.1. Controles criptográficos.

Control 8.1.1. *Política para el uso de controles criptográficos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe una política para el uso de controles criptográficos? ¿Cuáles son usados?	Sí, aunque informal. Se basa en el número de bits y el protocolo.	1
- ¿La criptografía usada se basa en una decisión tomada a partir de un análisis de riesgos?	De manera informal.	1
Total control 8.1.1.		2/10 20%

Tabla C. 178 Cuestionario control 8.1.1

Control 8.1.2. *Encripción.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Es usada la encripción el algún proceso? ¿Para qué es usada?	Sí es usada en Wireless, e-mail y transferencia WAN.	4
- ¿Su uso y características (de la encripción) son basados en un análisis de riesgos?	Informalmente.	1
Total control 8.1.2.		5/10 50%

Tabla C. 179 Cuestionario control 8.1.2

Control 8.1.3. *Firma digital.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Es usada la forma digital? ¿Cuál es el objetivo?	Sí es usada para asegurar la autenticación.	5
- ¿Qué algoritmo se usa y bajo que análisis se determinó?	Se emplean los usados por Microsoft (PKI, Hash, RSA) por su uso comercial y economía.	3
Total control 8.1.3.		8/10 80%

Tabla C. 180 Cuestionario control 8.1.3

Control 8.1.4. *Servicios de no-repudio.*

Preguntas	Respuestas	Puntos
- ¿Son usados servicios de no-repudio? ¿Cuáles y para qué son usados	No son usados.	1
Total control 8.1.4.		1/5 20%

Tabla C. 181 Cuestionario control 8.1.4

Control 8.1.5. *Administración de claves criptográficas.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza un proceso de administración de claves criptográficas?	Sí.	4
- ¿Qué aspectos físicos se consideran para su protección?	Son administradas en el servidor dentro del site.	4
- ¿Qué método/sistema de administración de claves se usa?	Los usados por Microsoft.	3
Total control 8.1.5.		11/15 73.33%

Tabla C. 182 Cuestionario control 8.1.5

Objetivo 8.2. Seguridad en los procesos de desarrollo y soporte.

Control 8.2.1. *Proceso del control de los cambios.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un procedimiento para la implementación de los cambios del sistema de la red?	Sí, pero informal.	1
- ¿Qué aspectos se incluyen en este procedimiento? ¿Se controla la versión del software usado?	Las versiones y el tipo de cambio.	3
Total control 8.2.1.		4/10 40%

Tabla C. 183 Cuestionario control 8.2.1

Control 8.2.2. *Revisión técnica de cambio de sistema operativo.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza una revisión y aprobación para realizar cambios al sistema operativo? ¿Qué incluye esta revisión técnica?	Sí es revisada/aprobada. Se considera el tipo de cambio y la versión.	4
Total control 8.2.2.		4/5 80%

Tabla C. 184 Cuestionario control 8.2.2

Cláusula 9. Obediencia.

Objetivo 9.1. Obediencia con los requerimientos legales.

Control 9.1.1. *Verificación de la legislación aplicable.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son verificados los requerimientos de la legislación aplicable a la seguridad de la red?	Sí.	5
Total control 9.1.1.		5/5 100%

Tabla C. 185 Cuestionario control 9.1.1

Control 9.1.2. *Derechos de propiedad intelectual.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Son verificados los derechos de propiedad intelectual mediante un procedimiento de revisión?	Sí, pero no mediante un procedimiento.	1
Total control 9.1.2.		1/5 20%

Tabla C. 186 Cuestionario control 9.1.2

Control 9.1.3. *Protección de la privacidad de los usuarios y su información.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un control y administración para la protección de la privacidad de la información de los empleados?	Sí.	4
Total control 9.1.3.		4/5 80%

Tabla C. 187 Cuestionario control 9.1.3

Control 9.1.4. *Regulación de controles criptográficos.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Está regulado y verificado el uso de controles criptográficos?	Sí.	4
Total control 9.1.4.		4/5 80%

Tabla C. 188 Cuestionario control 9.1.4

Control 9.1.5. *Colección de la evidencia.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Las evidencias colectadas siguen algún estándar?	No.	1
Total control 9.1.5.		1/5 20%

Tabla C. 189 Cuestionario control 9.1.5

Objetivo 9.2. Revisión de políticas de seguridad y obediencia técnica.

Control 9.2.1. *Obediencia con políticas de seguridad.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza un análisis y una revisión para asegurar la implementación correcta de los procedimientos de seguridad?	Sí.	4
- ¿Qué aspectos se consideran para esta obediencia?	La divulgación y aceptación del personal ejecutivo.	1
Total control 9.2.1.		5/10 50%

Tabla C. 190 Cuestionario control 9.2.1

Control 9.2.2. *Revisión de obediencia técnica.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza una revisión especializada para el cumplimiento técnico de los sistemas de la LAN? ¿Usan especialistas?	Sí y cuando se requiere son llamados especialistas.	3
Total control 9.2.2.		3/5 60%

Tabla C. 191 Cuestionario control 9.2.2

Objetivo 9.3. Consideraciones de auditoría de la LAN.

Control 9.3.1. *Monitoreo del control interno.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se efectúa un monitoreo de la efectividad de los controles internos de seguridad de la red?	Informalmente.	1
- ¿Las desviaciones de la efectividad son analizadas, reportadas y corregidas?	Informalmente y de acuerdo al presupuesto.	1
- ¿Los controles internos y su efectividad son verificados por auditorías?	Sí.	2
Total control 9.3.1.		4/15 26.66%

Tabla C. 192 Cuestionario control 9.3.1

Control 9.3.2. *Estatutos de auditoría.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se ha definido un estatuto para las funciones de auditoría? ¿Qué contiene?	En las auditorías externas es lo que especifiquen los auditores.	2
Total control 9.3.2.		2/5 40%

Tabla C. 193 Cuestionario control 9.3.2

Control 9.3.3. *Controles de auditoría.*		
Preguntas	**Respuestas**	**Puntos**

- ¿Se han establecido controles de auditoría que involucren la seguridad de la red?	No.	1
- ¿Qué controles se consideran en su planeación (de la auditoría)?	-	1
Total control 9.3.3.		2/10 20%

Tabla C. 194 Cuestionario control 9.3.3

Control 9.3.4. *Protección de las herramientas de auditoría.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué medidas se han establecido para proteger las herramientas de auditoría?	No se cuenta con herramientas de auditoría, son proporcionadas por auditores externos.	1
Total control 9.3.4.		1/5 20%

Tabla C. 195 Cuestionario control 9.3.4

Los cálculos y resultados son los siguientes. Para la evaluación de los objetivos se tiene:

$\overline{O.1.1} =$ (55+53.33)/2 = 54.16
$\overline{O.2.1} =$ (64+73.33+53.33+40+20)/5 = 50.13
$\overline{O.2.2} =$ (44+40)/2 = 42.00
$\overline{O.2.3} =$ (46.66+46.66+80)/3 = 57.77
$\overline{O.3.1} =$ (70+90)/2 = 80.00
$\overline{O.3.2} =$ (20+20+20)/3 = 20.00
$\overline{O.4.1} =$ (70+20)/2 = 45.00
$\overline{O.4.2} =$ (20)/1 = 20.00
$\overline{O.4.3} =$ (75+26.66+66.66+20+60)/5 = 49.66
$\overline{O.5.1} =$ (35+44+52)/3 = 43.66
$\overline{O.5.2} =$ (60+100+65+70+40)/5 = 67.00
$\overline{O.6.1} =$ (60+40+36+33.33)/4 = 42.33
$\overline{O.6.2} =$ (32)/1 = 32.00
$\overline{O.6.3} =$ (40+80)/2 = 60.00
$\overline{O.6.4} =$ (70)/1 = 70.00
$\overline{O.6.5} =$ (100+60+60)/3 = 73.33
$\overline{O.7.1} =$ (33.33)/1 = 33.33
$\overline{O.7.2} =$ (45+46.66+20+20)/4 = 32.91
$\overline{O.7.3} =$ (60+20)/2 = 40.00
$\overline{O.7.4} =$ (70+20+80)/3 = 56.66
$\overline{O.7.5} =$ (80)/1 = 80.00
$\overline{O.7.6} =$ (70)/1 = 70.00

$\overline{O.8.1}$ = (20+50+80+20+73.33)/5 = 48.66
$\overline{O.8.2}$ = (40+80)/2 = 60.00
$\overline{O.9.1}$ = (100+20+80+80+20)/5 = 60.00
$\overline{O.9.2}$ = (50+60)/2 = 55.00
$\overline{O.9.3}$ = (26.66+40+20+20)/4 = 26.66

La evaluación de las cláusulas es la siguiente:

Cláusula 1: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.1.1. Políticas de seguridad de la LAN.	100	54.16
Evaluación Cláusula 1	54.16	

Tabla C. 196 Evaluación de la cláusula 1

Cláusula 2: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.2.1. Administración de seguridad de la LAN.	40.0	50.13
O.2.2. Seguridad en el acceso a la LAN por terceras personas.	30.0	42.00
O.2.3. Análisis de riesgos.	30.0	57.77
Evaluación Cláusula 2	49.98	

Tabla C. 197 Evaluación de la cláusula 2

Cláusula 3: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.3.1. Responsabilidad de los bienes o activos.	55.0	80.00
O.3.2. Clasificación de la información.	45.0	20.00
Evaluación Cláusula 3	53.00	

Tabla C. 198 Evaluación de la cláusula 3

Cláusula 4: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.4.1. Seguridad en la definición de puestos.	22.5	45.00
O.4.2. Entrenamiento del personal.	35.0	20.00
O.4.3. Respuesta a incidentes de seguridad de la LAN.	42.5	49.66
Evaluación Cláusula 4	38.23	

Tabla C. 199 Evaluación de la cláusula 4

Cláusula 5: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.5.1. Aseguramiento de áreas de la red y su entorno.	45.0	43.66
O.5.2. Seguridad del equipo de la LAN.	55.0	67.00
Evaluación Cláusula 5	56.49	

Tabla C. 200 Evaluación de la cláusula 5

Cláusula 6: Objetivos de control	**P_f**	**Evaluación (O.n.m)**

O.6.1. Procedimientos y responsabilidades.	20.0	42.33
O.6.2. Protección contra software malicioso.	22.5	32.00
O.6.3. Back up.	22.5	60.00
O.6.4. Administración de la LAN.	22.5	70.00
O.6.5. Intercambio de información.	12.5	73.33
Evaluación Cláusula 6	54.08	

Tabla C. 201 Evaluación de la cláusula 6

Cláusula 7: Objetivos de control	P_f	Evaluación (O.n.m)
O.7.1. Requerimientos para el control de acceso a la LAN.	13.5	33.33
O.7.2. Administración de acceso de los usuarios a la LAN.	16.0	32.91
O.7.3. Responsabilidades del usuario.	15.0	40.00
O.7.4. Control de acceso a la LAN.	18.5	56.66
O.7.5. Monitoreo de acceso y uso de la red de actividades no autorizadas.	18.5	80.00
O.7.6. Cómputo móvil.	18.5	70.00
Evaluación Cláusula 7	53.99	

Tabla C. 202 Evaluación de la cláusula 7

Cláusula 8: Objetivos de control	P_f	Evaluación (O.n.m)
O.8.1. Controles criptográficos.	55.0	48.66
O.8.2. Seguridad en los procesos de desarrollo y soporte.	45.0	60.00
Evaluación Cláusula 8	53.76	

Tabla C. 203 Evaluación de la cláusula 8

Cláusula 9: Objetivos de control	P_f	Evaluación (O.n.m)
O.9.1. Obediencia con los requerimientos legales.	31.5	60.00
O.9.2. Revisión de políticas de seguridad y obediencia técnica.	37.0	55.00
O.9.3. Consideraciones de auditoría de la LAN.	31.5	26.66
Evaluación Cláusula 9	47.64	

Tabla C. 204 Evaluación de la cláusula 9

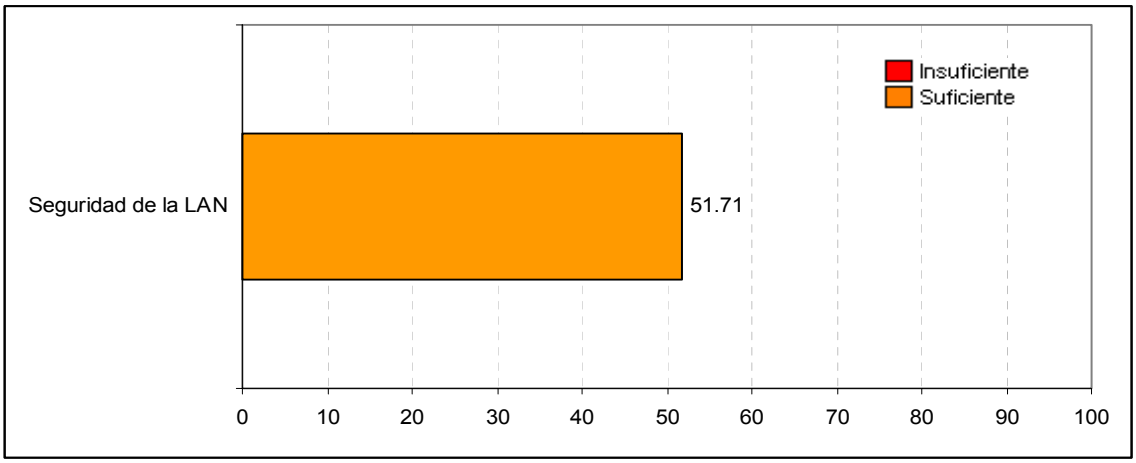
Finalmente, el resultado completo de la auditoría en seguridad:

Cláusulas de control	P_f	Evaluación (C.n)
C.1. Políticas de seguridad.	12.0	54.16
C.2. Gobierno de la seguridad.	11.5	49.98
C.3. Control y clasificación de bienes.	9.0	53.00
C.4. Seguridad de los empleados.	9.5	38.23
C.5. Seguridad física de la LAN y su entorno.	12.0	56.49
C.6. Administración de las comunicaciones.	13.0	54.08
C.7. Control de acceso a la LAN.	15.0	53.99
C.8. Desarrollo de seguridad de una LAN.	9.5	53.76

C.9. Obediencia.	8.5	47.64
Promedio total de la seguridad de la LAN	51.71	

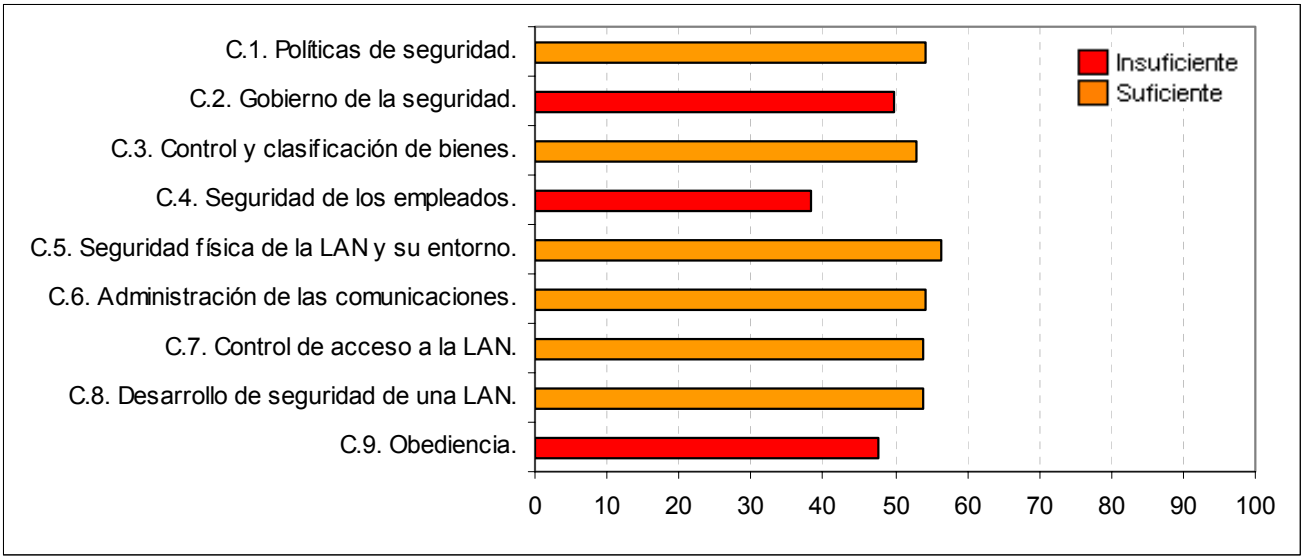
Tabla C. 205 Evaluación total de la seguridad de la LAN

En las siguientes gráficas se muestran los resultados condensados de la auditoría en seguridad:



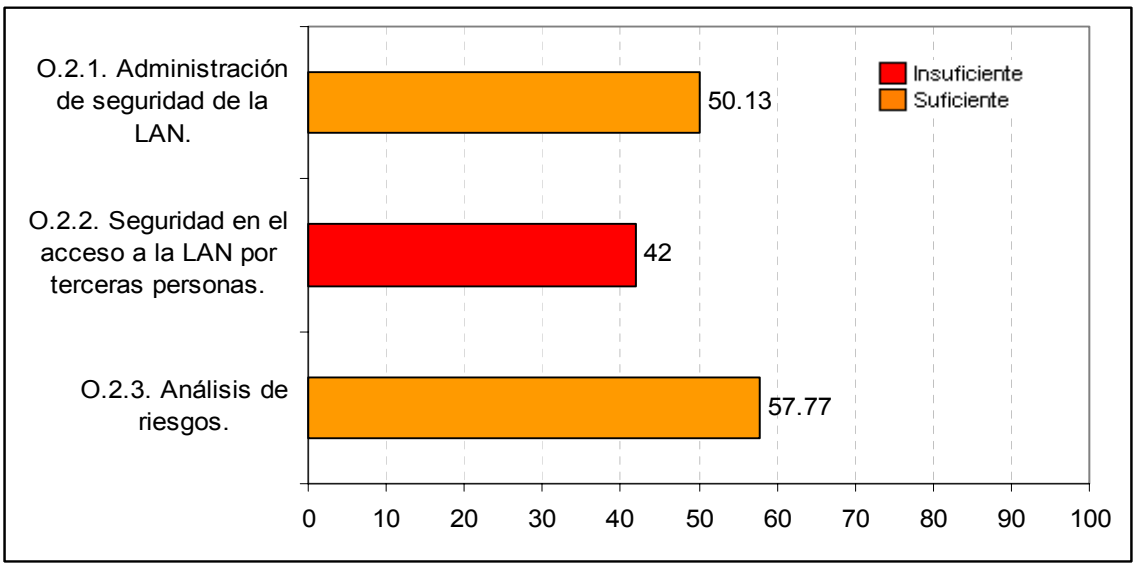
Gráfica C. 1 Evaluación de la seguridad de la LAN

Como se muestra en esta gráfica, la seguridad de la LAN no es insuficiente pero tampoco es adecuada y una puntuación apenas por encima del 50% se considera baja.



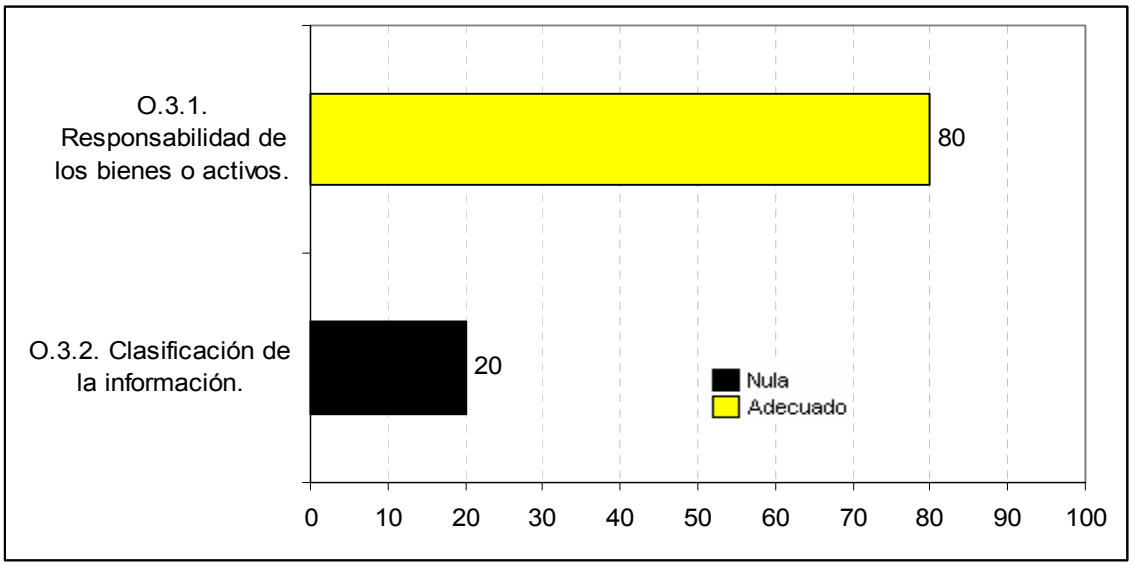
Gráfica C. 2 Evaluación de las cláusulas de control

En esta gráfica se observan tres cláusulas de control que corresponden a situaciones de debilidad en la seguridad: el Gobierno de la seguridad, la seguridad de los empleados y la Obediencia. Las restantes cláusulas apenas están en el nivel de suficiencia.



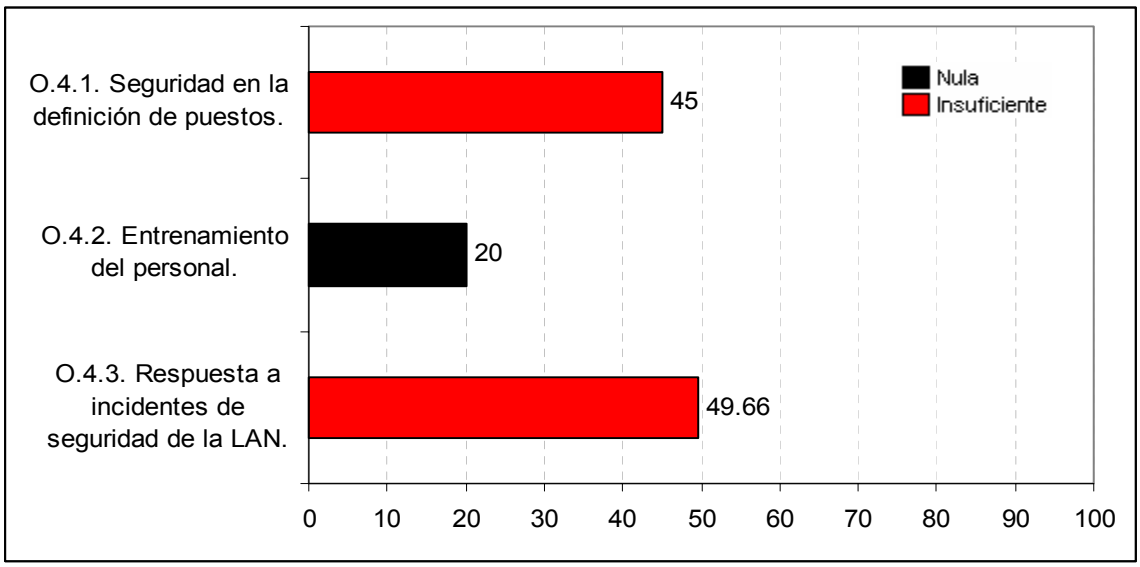
Gráfica C. 3 Evaluación de C.2: Gobierno de la seguridad

La gráfica C.3 muestra una debilidad fuerte en cuanto a la seguridad en el acceso por terceras personas a la LAN. Su administración y el análisis de riesgos sólo son suficientes.



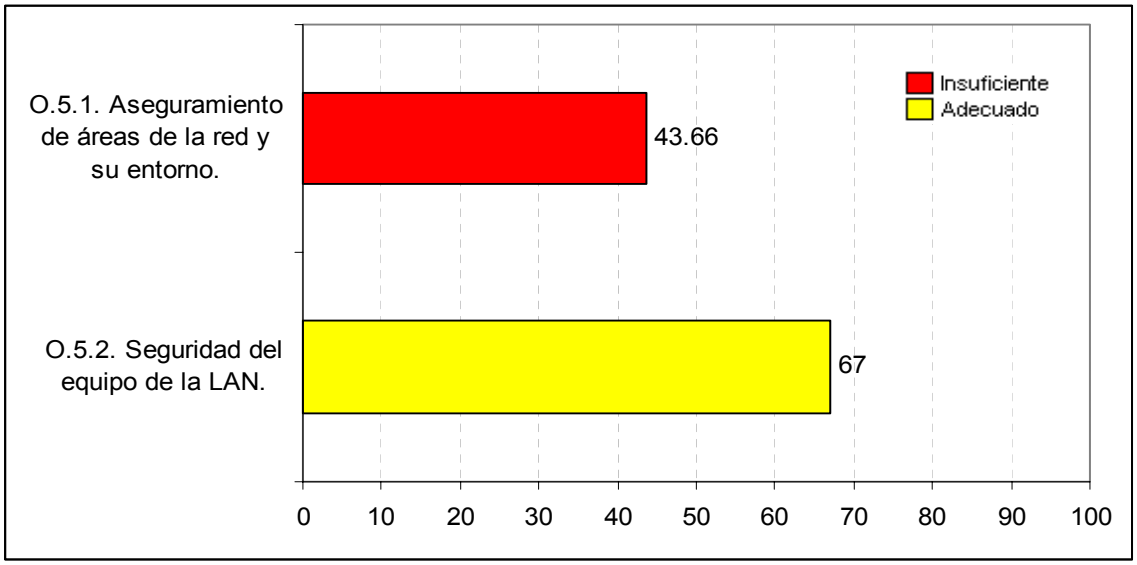
Gráfica C. 4 Evaluación de C.3: Control y clasificación de bienes

En cuanto al control y clasificación de bienes encontramos dos extremos: por un lado la responsabilidad de los activos relacionados con la LAN se considera adecuada, pero la clasificación de la información es prácticamente nula.



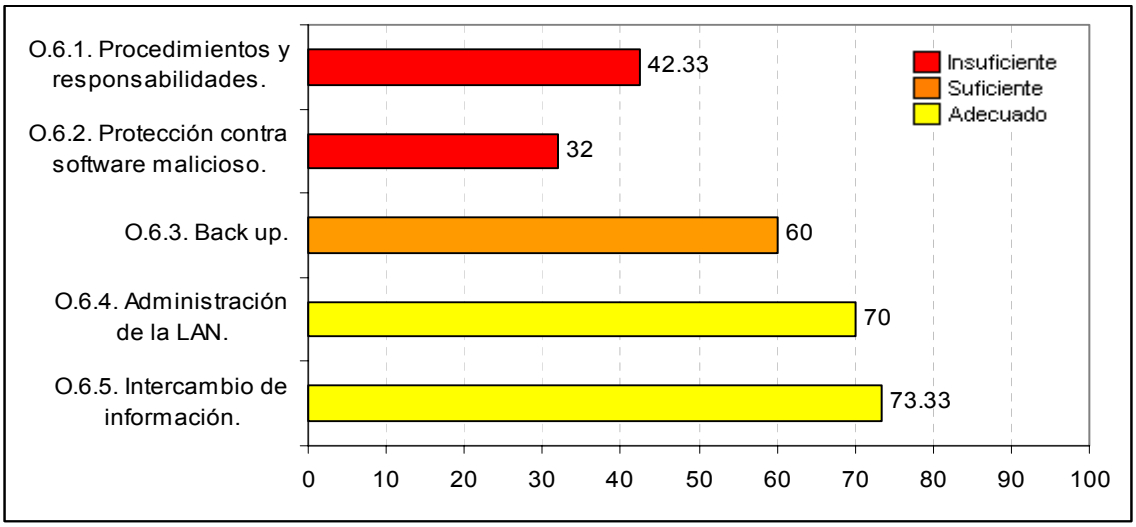
Gráfica C. 5 Evaluación de C.4: Seguridad de los empleados

En la gráfica C.5 se puede advertir que la cláusula 4 representa verdaderamente una brecha en la seguridad muy importante en la LAN, especialmente en cuanto al entrenamiento del personal en cuestiones de seguridad.



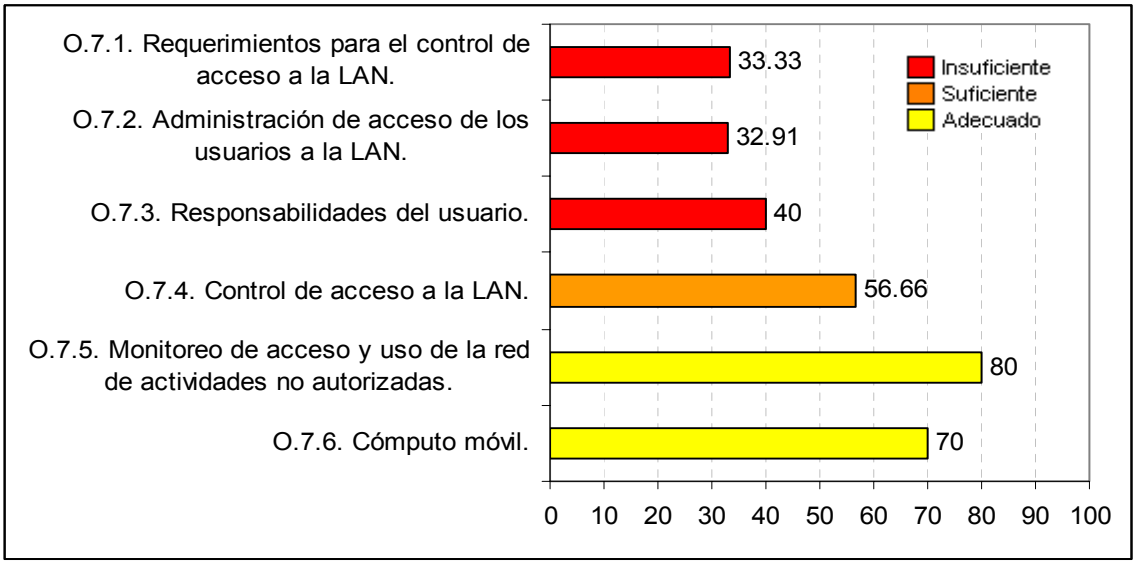
Gráfica C. 6 Evaluación de C.5: Seguridad física de la LAN y su entorno

Los objetivos de la cláusula 5 muestran que el aseguramiento de las áreas de la red es insuficiente, aunque la seguridad del equipo se encuentra de una forma adecuada.



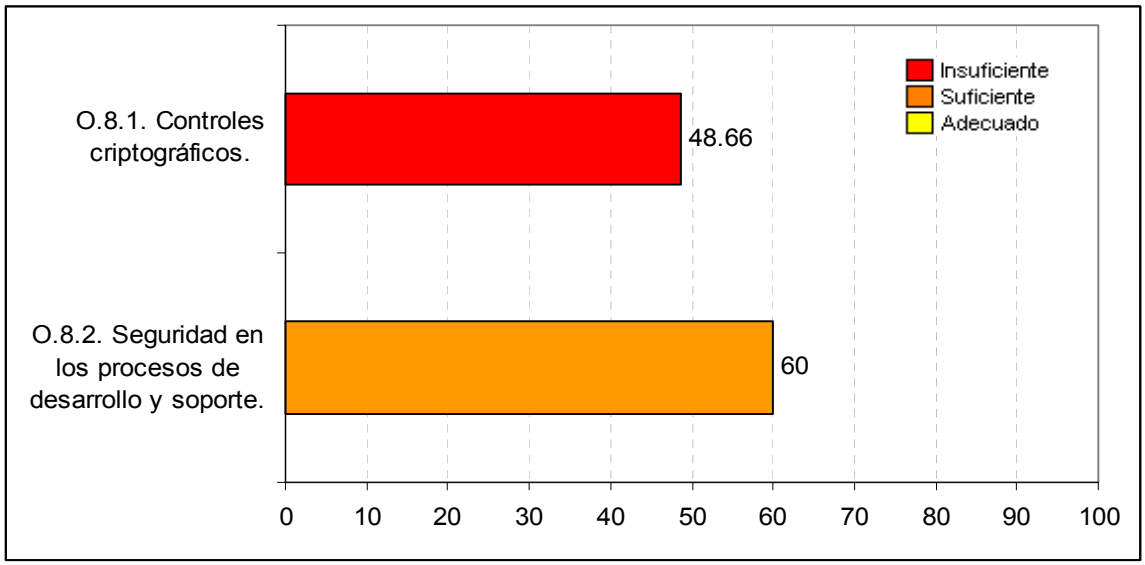
Gráfica C. 7 Evaluación de C.6: Administración de las comunicaciones

En la gráfica C.7 se observa que la administración de las comunicaciones es contrastante ya que aunque existen controles adecuados en la administración de la LAN y el intercambio de información, la definición de procedimientos-responsabilidades y la protección contra el malware es insuficiente. Además, el respaldo no es adecuado.



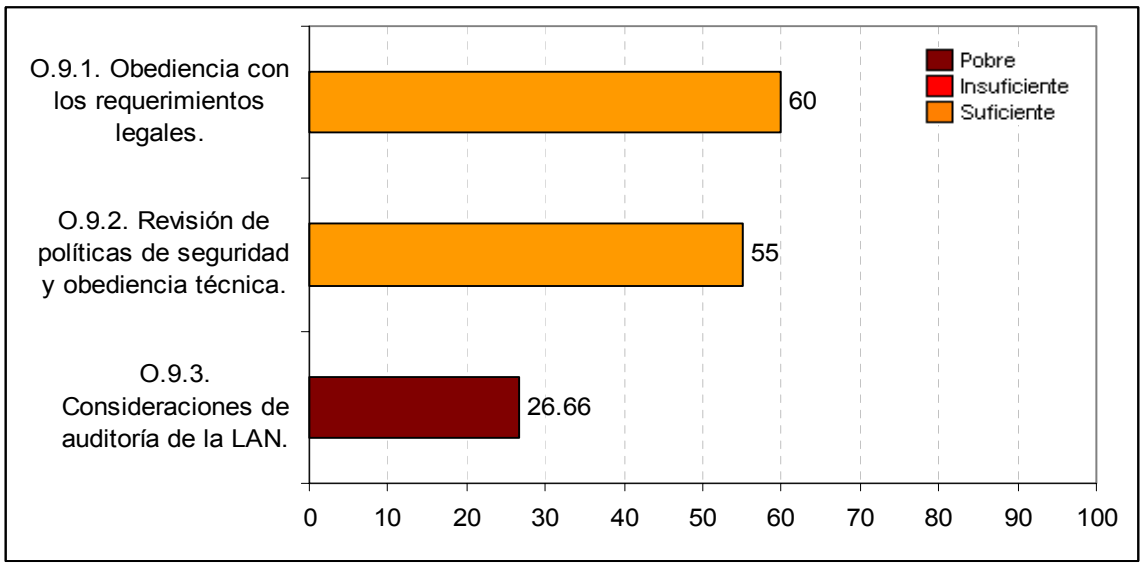
Gráfica C. 8 Evaluación de C.7: Control de acceso a la LAN

En relación al control de acceso, la gráfica C.8 permite ver que sólo se puede considerar adecuado el monitoreo de la red, aunque no la definición de requerimientos y administración del mismo.



Gráfica C. 9 Evaluación de C.8: Desarrollo de seguridad de una LAN

En cuanto a los controles criptográficos, sus políticas y controles observamos una debilidad. Y aunque los procesos de desarrollo y soporte son suficientes, no son los adecuados.



Gráfica C. 10 Evaluación de C.9: Obediencia

La cláusula de obediencia, que corresponde a un problema de seguridad, manifiesta que posee una debilidad fuerte en cuanto a las consideraciones de auditoría. Los dos puntos restantes de obediencia no dejan de ser solamente suficientes.

Situación actual.

La exposición de la situación actual de la seguridad de la LAN en esta entidad de gobierno es entonces la siguiente:

La seguridad informática de la LAN es apenas suficiente, esto es, no se garantiza que confiabilidad, integridad y disponibilidad de la información se mantengan o lo puedan hacer en un futuro ante la administración de la seguridad y sus controles implementados como lo están ahora. Esto ocasionaría repercusiones considerables en los SI de la entidad y en sus objetivos mismos de funcionalidad.

Las cláusulas que presentan debilidades de seguridad y que consideramos como prioridad son las siguientes:

C.4. Seguridad de los empleados.

La seguridad en este aspecto es insuficiente. Detallamos los aspectos críticos:

- El aspecto de mayor gravedad es la falta de entrenamiento, actualización y culturización de los empleados en cuestiones de seguridad y su relación con ellos mismos y la entidad. Sólo se considera cierto entrenamiento para usuarios de sistemas o directivos y en periodos bastante tardíos.

- A continuación figura una brecha en la inclusión de la seguridad en la definición de puestos. No se establecen las cláusulas contractuales de la seguridad, responsabilidades o acuerdos. Aunque los roles y responsabilidades relativas a la seguridad se encuentren definidos, no se observa que se implementen prácticamente de forma adecuada.
- Finalmente la respuesta a los incidentes de seguridad es insuficiente. A pesar de que existen los procedimientos formales para el reporte de incidentes y mal funciones, los usuarios no los realizan; esta es la consecuencia directa del primer aspecto antes mencionado. Tampoco se considera buena la retroalimentación formal que debe realizarse de los incidentes, tanto en su impacto económico como en sus aspectos técnicos, parece que no es un aspecto atendido en la seguridad organizacional. Y aunque se realizan acciones para disciplinar acciones contra violaciones de seguridad interna, la falta de un control central en la imposición de sanciones ocasiona que estas acciones pierdan fuerza y queden como meras sugerencias.

Se recomiendan las siguientes medidas a corto plazo, en orden de prioridad:

- Se debe impartir entrenamiento, actualización y concientización en seguridad a todos los empleados y usuarios de acuerdo con su perfil, de manera periódica y aceptable. Esto incluye la forma de detectar y reportar incidentes, debilidades y mal funciones de la seguridad.
- Las cláusulas contractuales deben contener las responsabilidades de los empleados respecto a la seguridad de la red.
- Los roles y responsabilidades deben ser asignados de acuerdo a su definición y documentación.
- Las responsabilidades de los empleados en cuanto a la seguridad deben ser aplicadas cuando se realice una violación de las políticas y procedimientos. De ser posible, estas decisiones deben estar centralizadas.
- Cuantificar los costos de los incidentes de seguridad y emplearlos en procesos de mejora continua.

C.9. Obediencia.

- No se han establecido controles de auditoría relativos a la seguridad de la red, la organización no cuenta con herramientas de auditoría, no existe un control interno formal ni es analizada su efectividad y no se han definido estatutos para las funciones de la auditoría (incluyendo las externas).
- La seguridad de la LAN no está completa ni correctamente adecuada a los estándares de seguridad internacionales.
- Falta un procedimiento adecuado de revisión de los derechos intelectuales, de control de licencias y colección de evidencia.

Recomendaciones a corto plazo:

- Deben establecerse los estatutos de auditoría incluyendo la responsabilidad, autoridad y obligaciones de la función auditora y del auditado, basándose en códigos y estándares de auditoría.

- Se debe establecer un monitoreo de los controles internos de la seguridad de la LAN, de forma periódica y en cooperación con la auditoría.
- Realizar verificaciones legales para el derecho de uso de software.

Recomendaciones a mediano plazo:

- Asegurar que los procedimientos de seguridad obedezcan a estándares de seguridad empleando asesoría de especialistas.
- Realizar la colección de evidencia de acuerdo a prácticas estándares.

C.2. Gobierno de la seguridad.

- Los controles para el posible acceso de terceras personas a la LAN son insuficientes y no han sido detectados sus riesgos en algún análisis de riesgos. Además, los contratos con terceras personas incluyen pocas consideraciones/acuerdos respecto a la seguridad de la red.
- En la planeación de la red no se ha incluido la seguridad de manera formal, falta la definición de una guía para la asignación de roles/responsabilidades de seguridad de la red, no se recurre realmente a la consultoría de especialistas en seguridad (sólo la asesoría que cubre alguna compra o servicio de equipo, posiblemente por razones de presupuesto) y la revisión de la seguridad por parte de algún grupo de consultores internos, externos o un equipo especial no es ni muy profunda ni muy frecuente, además no se garantiza la completa independencia de estos grupos.
- Observamos una falta de profundidad en el análisis de riesgos, sobre todo en el aprendizaje y aplicación de resultados de estudios o auditorías de seguridad y en la identificación, clasificación y medición de los riesgos de la red.

Recomendaciones a corto plazo:

- Se debe establecer una política que contemple la posibilidad del acceso no autorizado de terceras personas a la LAN, el análisis de su impacto en algún análisis de riesgos y se deben establecer controles más completos y estrictos en base a estos análisis. Es necesario considerar de manera más precisa la identidad de estos elementos.
- Los contratos con terceras personas deben contemplar de manera más específica las responsabilidades legales, los acuerdos de control de acceso, de acuerdo a las políticas y estándares de seguridad adoptados.
- En cuanto a la gestión de la administración de la seguridad de la LAN deben acordarse las metodologías específicas para la seguridad y se debe incluir a la seguridad en el proceso de planeación de la red. Debe establecerse una guía general, por medio de políticas, para la asignación de los roles y responsabilidades de seguridad.
- Debe considerarse seriamente la factibilidad de la consultoría de especialistas en seguridad y la revisión continua en forma independiente por parte de auditores externos o internos, garantizando que dichos resultados serán implementados en controles internos y verificados sus resultados.

Recomendaciones a mediano plazo:

- Establecer una tarea específica, si es que un análisis de riesgos y de factibilidad económica muestra su necesidad, que pruebe y mantenga el nivel de seguridad de la LAN aprobado por la administración, ya sea en forma explícita o incógnita.

A continuación detallaremos las cláusulas que sólo son suficientes y que requieren acciones a mediano plazo:

C3. Control y clasificación de bienes.

- Se observa una nula clasificación de la información, no existen sus manuales ni la clasificación de los niveles de seguridad de la LAN, tampoco existen procedimientos para el manejo y rotulación de la información.

Recomendaciones:

- El objetivo de los bienes o activos se encuentra adecuadamente establecido y es este el que nos da una visión engañosa en la evaluación de esta cláusula. Por lo tanto, consideramos que sea de *prioridad* y de realización a ***corto plazo*** la realización de la clasificación de la información, de sus manuales de clasificación y la definición de los procedimientos para el manejo de la información en todos sus procesos, de acuerdo a la clasificación antes realizada. Con esto se asegura que la información recibe un nivel de protección de acuerdo con su sensibilidad.

C.8. Desarrollo de seguridad de una LAN.

- No existe una política establecida para el uso de controles criptográficos, aunque estos son usados informalmente y su uso tampoco obedece a una evaluación del análisis de riesgos. Los distintos algoritmos usados para criptografía y firma digital caen dentro de este último aspecto mencionado.
- No son usados los servicios de no-repudio y tal vez no se tiene mucho control sobre la administración de las claves criptográficas aunque su uso es adecuado.
- No está definido un procedimiento para la implementación de los cambios del sistema de la red.

Recomendaciones:

- Definir una política para el uso de controles criptográficos basada en una valoración de riesgos y selección de controles, para identificar las soluciones criptográficas más apropiadas. Esta política debe incluir la administración de las claves criptográficas, su administración, distribución y almacenamiento.
- Establecer un proceso para el control de cambios de los sistemas de la LAN de manera formal, documentada y autorizada.

C.7. Control de acceso a la LAN.

- Aunque está definida y documentada una política para el control de acceso a la LAN, estableciendo reglas y derechos de acceso a los usuarios, no existe consistencia con la clasificación de la información (puesto que no se tiene). Tampoco están definidas las obligaciones contractuales para el acceso a datos y servicios y los usuarios no firman un acuerdo de condiciones de acceso. Y aunque las cuentas son revisadas periódicamente no es eficiente el procedimiento. Por la misma razón no existe un procedimiento formal para designar, autorizar y usar privilegios de cuentas de acceso a la red y su revisión.
- No consideramos suficiente la práctica para advertir a los usuarios sobre el buen uso de los passwords y del equipo, especialmente del equipo no atendido.
- Aunque existe una política que defina y autorice el uso de los servicios de red, los aspectos que incluye son pobres. La autenticación del control de acceso de los usuarios externos a la LAN no está bien definida y se realiza informalmente.
- Finalmente, aunque se considera adecuado el monitoreo de la LAN, los datos podrían ser insuficientes en caso de incidentes de seguridad. Los controles definidos para el cómputo móvil también resultan insuficientes.

Recomendaciones:

- La política para el control de acceso debe definirse de acuerdo con la clasificación y uso de la información y debe incluir la legislación y obligaciones para la protección del acceso. Se recomienda su realización a ***corto plazo***.
- La clasificación y designación de privilegios debe establecerse con un procedimiento formal. La revisión de estos privilegios y sus cuentas relacionadas debe ser realizada de forma más efectiva y por medio de un procedimiento establecido. Se recomienda su realización a ***corto plazo***.
- Debe establecerse algún control para informar, concientizar y sancionar a los usuarios con relación al uso de sus passwords y del equipo no atendido. Se recomienda su realización a ***corto plazo***.
- Al política de uso de los servicios de red debe mejorarse cubriendo aspectos específicos como la red a la que se tiene acceso y las responsabilidades del acceso y la autorización formal.
- Es necesario establecer por medio de un análisis de riesgos el método de autenticación para los usuarios externos.
- Considerar una extensión mayor de los logs de acceso y su observancia, así como la implementación de mejores controles, en base al análisis de riesgos, del cómputo móvil.

C.6. Administración de las comunicaciones.

- Se considera pobre en práctica real la aplicación de los controles contra el software malicioso, porque la forma como accede principalmente éste es por el usuario final. Esta es otra repercusión del pobre entrenamiento, concientización y sanciones mencionados anteriormente. Consideramos pobre el monitoreo de las actividades de los usuarios y del cumplimiento con las licencias de software.
- No se encuentran segregadas las funciones de Administración de la red, la Administración de la seguridad y el Área de Auditoría. Además el personal no realiza

únicamente las tareas definidas en su puesto. No existen procedimientos formales y responsabilidades para la gestión de incidentes de seguridad relacionados con la LAN y los incidentes tomados en cuenta en la práctica son pocos. Las acciones para su recuperación por tanto, no obedecen a un procedimiento. No existen procedimientos definidos que controlen los cambios al equipo, software y procedimientos relacionados con la LAN. La documentación de los procedimientos de operación de la LAN es poco detallada.
- Se considera que la periodicidad del respaldo de la información relacionada con la red es muy grande y con medios que podrían ocasionar problemas.

Recomendaciones:

- Reforzar medidas de prevención, detección y corrección contra software malicioso basándose en la concientización, entrenamiento correcto, responsabilidades, controles de acceso apropiados y controles de administración. Verificar el cumplimiento con las licencias de software, prohibir el uso de software no autorizado, realizar revisiones regulares de software y de correos electrónicos y descargas. Se recomienda su realización a ***corto plazo***.
- Debe separarse la administración y ejecución de tareas y responsabilidades relacionadas con la seguridad de la LAN y asegurarse que el personal sólo lleve a cabo las tareas establecidas en la definición de puestos. Se recomienda su realización a ***corto plazo***.
- Mejorar formalmente los procedimientos que cubran todos los tipos potenciales de incidentes de seguridad. Considerar la documentación detallada de todas las acciones realizadas. Se recomienda su realización a ***corto plazo***.
- Establecer procedimientos para mejorar los cambios a los sistemas de red, incluyendo su análisis, aprobación y comunicación. Asimismo los procedimientos de operación de la LAN deben ser mejorados siendo más específicos en todos los procesos y procedimientos. Se recomienda su realización a ***corto plazo***.
- Los respaldos deberán realizarse con medios más apropiados, en base al análisis de riesgos y en periodos más cortos, esto incluye la revisión de estos respaldos.
- Deben establecerse controles explícitos para la seguridad de la red, no sólo cubrir de manera general la seguridad informática.
- Mejorar los controles respecto a la seguridad del correo electrónico incluyendo guías, responsabilidades y la autenticación de mensajes. También la información disponible públicamente debe ser formalmente autorizada y verificada por un análisis para comprobar que no contiene información que comprometa a la organización y sus sistemas.

C.1. Políticas de seguridad.

- Las políticas no son publicadas y comunicadas a todos los empleados, sólo a una parte de los empleados, generalmente de sistemas y/o de puestos gerenciales, además, no son muy específicos aspectos como definiciones, objetivos, alcance, principios de seguridad, documentación explicativa, definición de responsabilidades y referencias a la documentación soportada. La evaluación y redefinición de las políticas no obedece formalmente a la efectividad de las mismas, su costo e impacto.

Recomendaciones:

- Mejorar las políticas de seguridad de la LAN considerando su comunicación a un sector más amplio de usuarios, la inclusión de definiciones, documentación, objetivos, estándares adoptados, legislación cubierta y definición de responsabilidades.
- Perfeccionar la revisión y evaluación periódica de las políticas en base a análisis costo-beneficio y efectividad de las políticas, considerando controles internos y resultados de auditorías.

C.5. Seguridad física de la LAN y su entorno.

- Aunque existe un perímetro de seguridad física, no se ha determinado exactamente en base a un análisis de riesgos y los controles de seguridad física que se han establecido para el site y otras áreas de la LAN se consideran insuficientes.
- Aunque se ha implementado una adecuada protección del equipo de red, no son lo suficientemente seguros. Aunque la seguridad del cableado es también adecuada, no se ha eliminado la posibilidad de su mal uso. Finalmente, no se consideran muchas restricciones de seguridad en cuanto al mantenimiento del equipo de red y el desecho o re-uso del equipo.

Recomendaciones:

- Mejorar la determinación del perímetro de seguridad y de los controles de entrada en base a un análisis de riesgos y reforzar los controles de acceso. Considerar una buena autenticación, supervisión constante, uso de cámaras y alarmas en todas las áreas sensibles y la revisión de los derechos de acceso de manera regular y metódica. Las acciones realizadas durante los accesos deben obedecer a procedimientos preestablecidos. Se recomienda su realización a ***corto plazo***.
- Considerar la mejora de los controles establecidos para la protección del equipo de red y su cableado, así como su monitoreo. Reforzar el cableado existente con fibra en lugares críticos y asegurarse que el usuario no tenga acceso a él.
- Elaborar el registro de las operaciones de mantenimiento al equipo de red.
- Establecer procedimientos más seguros para el re-uso o desecho de equipos.

C.2 WLAN.

En cuanto a la evaluación de las WLAN se considerará en este apartado únicamente la evaluación de la cláusula adicional, la diez, en base a la ponderación siguiente:

Cláusula 10: Objetivos de control	Pesos técnicos	Pesos políticos	Pesos finales
O.10.1. Políticas de seguridad para WLAN.	30	30	30
O.10.2. Seguridad de access points.	35	30	32.5
O.10.3. Implementación de seguridad en la WLAN.	35	40	37.5
Total	100	100	100

Tabla C. 206 Ponderación de los objetivos de la cláusula 10

Las respuestas y calificaciones de los cuestionarios se muestran a continuación:

RESPUESTAS A LOS CUESTIONARIOS ADICIONALES PARA WLAN

Cláusula 10. Consideraciones para WLAN.

Objetivo 10.1. Políticas de seguridad para WLAN.

Control 10.1.1. *Políticas de seguridad para WLAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se tiene una política adecuada para dirigir el uso de tecnología inalámbrica?	Informal.	1
- ¿Se consideran en esta política los peligros que implica esta tecnología?	Informalmente.	1
- ¿El análisis de riesgos actual considera esta tecnología y sus vulnerabilidades?	Informalmente.	1
- ¿Se tiene en cuenta el peligro para la red que ocasiona el robo de un dispositivo inalámbrico? ¿Qué controles se han contemplado?	Sí, informalmente.	1
Total control 10.1.1.		4/20 20%

Tabla C. 207 Cuestionario control 10.1.1

Control 10.1.2. *Política para direccionar la REM.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe una política de seguridad para la REM?	No.	1
- ¿Qué controles físicos se consideran en la política para la propagación de la REM?	-	1
- ¿Qué medidas existen para proteger al	-	1

hardware, las comunicaciones y personal de la REM?		
Total control 10.1.2.		3/15 20%

Tabla C. 208 Cuestionario control 10.1.2

Objetivo 10.2. Seguridad de access points.

Control 10.2.1. *Instalación de los access points.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un registro de todos los access points y de su ubicación? ¿Esta ubicación fue determinada mediante un análisis?	Sí existe el registro y la ubicación determinada con un análisis.	5
- ¿Qué cobertura tienen los access points? ¿Qué capacidad de acceso tienen? ¿Qué porcentaje de este acceso es usado?	Cobertura de 5 Km. sin obstáculos. Tienen capacidad de acceso de 11 Mbps (contra 100 Mbps en LAN). Tiene un acceso del 100%.	5
- ¿Se ha verificado que no provoquen interferencia con otras comunicaciones?	Sí.	5
Total control 10.2.1.		15/15 100%

Tabla C. 209 Cuestionario control 10.2.1

Control 10.2.2. *Configuración de los access points.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Los access points están apagados cuando no están en uso?	Sí.	5
- ¿Qué configuraciones de seguridad tienen los access points?	Para la conexión se usa contraseñas o llaves.	2
- ¿Qué subred soporta el tráfico de los access points?	Redes temporales o nodos de difícil acceso mediante cable.	4
Total control 10.2.2.		11/15 73.33%

Tabla C. 210 Cuestionario control 10.2.2

Objetivo 10.3. Implementación de seguridad en la WLAN.

Control 10.3.1. *Extensión del perímetro de seguridad física.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Qué medidas de seguridad física existen en los lugares donde las comunicaciones inalámbricas exceden los límites físicos?	No.	1
- ¿Se sabe hasta dónde se puede acceder a la red inalámbrica?	Sí se conocen los límites.	5

Total control 10.3.1.	6/10 60%

Tabla C. 211 Cuestionario control 10.3.1

Control 10.3.2. *Servicios de seguridad.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Existe un IDS en la WLAN?	Sí.	5
- ¿Está instalado un firewall entre la LAN y la WLAN?	En algunos sitios.	2
- ¿Qué algoritmo de encripción es usado? ¿Su uso obedece al análisis de riesgos?	Algoritmos comerciales.	2
- ¿Qué autenticación se realiza?	Los estándares.	3
- ¿Qué medidas de seguridad y configuraciones poseen los clientes WLAN?	Encripción y contraseñas.	2
Total control 10.3.2.		14/25 56%

Tabla C. 212 Cuestionario control 10.3.2

Control 10.3.3. *Monitoreo de la WLAN.*		
Preguntas	**Respuestas**	**Puntos**
- ¿Se realiza un monitoreo de la WLAN para evitar accesos no autorizados? ¿Se realizan pruebas sobre el IDS?	Se monitorea y se prueba el IDS.	3
- ¿Con qué frecuencia se realiza el monitoreo?	A vez a la semana.	3
Total control 10.3.3.		6/10 60%

Tabla C. 213 Cuestionario control 10.3.3

Los cálculos y resultados son los siguientes:

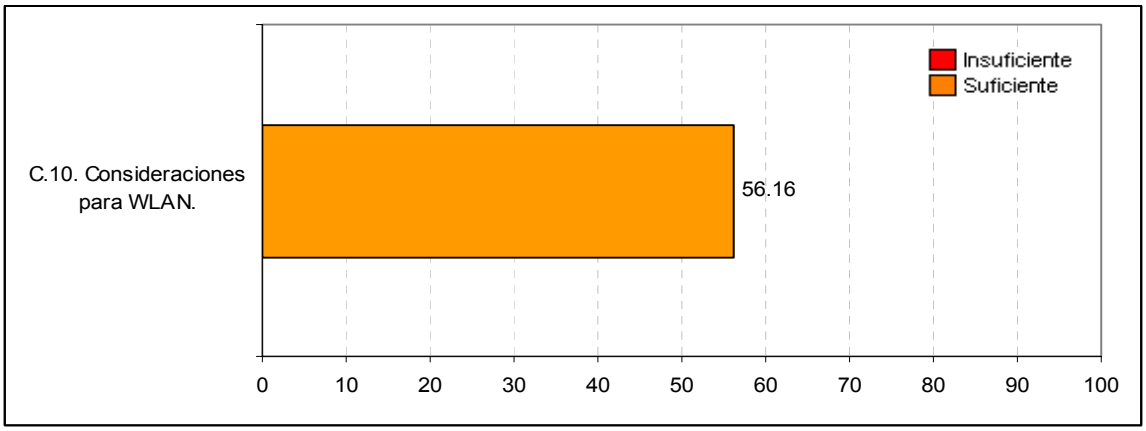
$\overline{O.10.1} =$ (20+20)/2 = 20.00
$\overline{O.10.2} =$ (100+73.33)/2 = 86.66
$\overline{O.10.3} =$ (60+56+60)/3 = 58.66

La evaluación de la cláusula es:

Cláusula 10: Objetivos de control	**P_f**	**Evaluación (O.n.m)**
O.10.1. Políticas de seguridad para WLAN.	30.0	20.00
O.10.2. Seguridad de access points.	32.5	86.66
O.10.3. Implementación de seguridad en la WLAN.	37.5	58.66
Evaluación Cláusula 10	56.16	

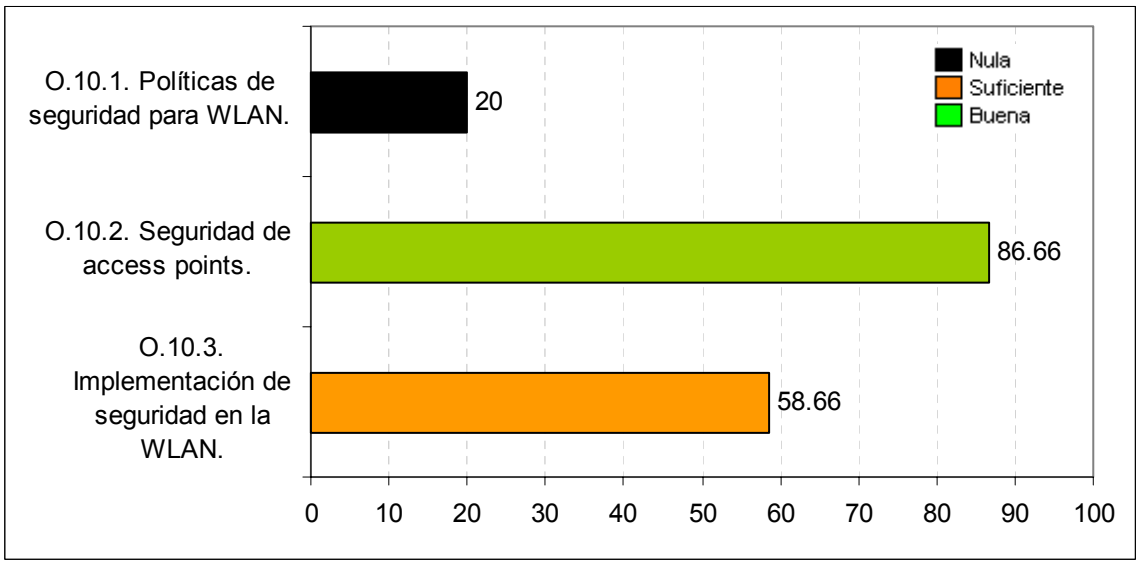
Tabla C. 214 Evaluación de la cláusula 10

En las siguientes gráficas se muestran los resultados:



Gráfica C. 11 Evaluación de la cláusula de control

Se observa en esta gráfica que la situación de la seguridad en la WLAN sólo es suficiente.



Gráfica C. 12 Evaluación de C.10: Consideraciones para WLAN

Sin embargo, al nivel de los objetivos de control observamos que la situación de las políticas de seguridad es mala, al no estar definidas formalmente. La implementación de la seguridad es suficiente, pero no adecuada. Observamos que la seguridad de los access points ha sido implementada correctamente.

Situación actual.

C.10. Consideraciones para WLAN.

- Se observa una falta de políticas para WLAN, de manera explícita y detallada. Tampoco existe una política de seguridad para la REM ni sus controles físicos de seguridad.
- No existen medidas de seguridad física en los lugares donde las comunicaciones inalámbricas exceden los límites físicos, los servicios de seguridad son suficientes pero no completos; lo mismo ocurre con el monitoreo de la WLAN y su control de acceso.

Recomendaciones:

- Establecer las políticas de seguridad formales para la WLAN, incluyendo los estándares apropiados. Considerar el entrenamiento del personal y los riesgos de esta tecnología. Establecer una política para direccional la REM, capacitación del personal y la seguridad adecuada. Se recomienda una acción a ***corto plazo***.
- Implementar controles adecuados para extender el perímetro de seguridad física donde se extienda la WLAN. En base a un análisis de riesgos utilizar el esquema de encripción y el método de autenticación más adecuado.
- Considerar el monitoreo móvil y probar la eficacia del IDS. Determinar la frecuencia con el análisis de riesgos.

BIBLIOGRAFÍA

- Chávez Chávez, Erika V. *Fundamentos de auditoría informática y su aplicación a la seguridad en redes de ordenadores.* México, ENEP Aragón, 2003.
- Franco Delgado, Guadalupe. *La auditoría informática.* México, F.I. UNAM, 2005.
- Gupta, Uma G. *Information Systems. Success in the 21st Century.* New Jersey, Prentice Hall, 2000.
- Laudon C., Kenneth. *Sistemas de información gerencial.* México, Pearson Education, 2002.
- Olguín Romo, Heriberto. *Dirección, organización y administración de centros de tecnología de información.* México, UNAM, Facultad de Ingeniería, 2005.
- Pfleeger. *Security in Computing.* USA, Prentice Hall, 2000.
- Russell y Gangemi. *Computer Security Basics.* USA, O'Reilly & Associates, 1999.
- Teichroew, D. *Information Systems. Encyclopedie of Computer science.* 1976.
- Ventura, Teodoro. *Sistema de información para el seguimiento de proyectos de agua*. Tesis Licenciatura. Universidad de las Américas-Puebla. 1999.

e-Sources

- Álvarez Marañón, Gonzalo. *Amenazas deliberadas a la seguridad de la información.* CSIC. 1997-2000. http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html
- Álvarez Marañón, Gonzalo. *Mecanismos de seguridad.* CSIC. 1997-2000. http://www.iec.csic.es/criptonomicon/seguridad/mecanism.html
- *Encuesta global de la Seguridad de la Información 2004.* Mancera Ernst & Young.
- *Encuesta Mundial de Seguridad IT 2004.* Information Week.
- *Estudio de percepción, Seguridad en Informática México 2004.* Joint Future Systems.
- Heineken, Team. *Introducción a la problemática de la Seguridad Informática.* 2001. http://www.softdownload.com.ar
- Velázquez, Andrés. *Seguridad Informática: Más que una Moda.* DoDoMex - Internet Security Portal. 2005. http://www.dodomex.com/noticias2.php?id=44

Conferencias

- *Bajo la lupa: la perspectiva del auditor*, por Aurelio Jaimes Peña, Gerente de Auditoría de Sistemas, TELMEX, en el Business Innovation Forum 2005 de Netmedia.
- *El recurso del Método*, dictada por Lucio Molina Focazzio, Vicepresidente Internacional de ISACA, realizada en el Business Innovation Forum 2005 de Netmedia.

Guías y estándares

- *COBIT 4.0, Objetivos de Control*. 4ª edición. IT Governance Institute.
- *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004.
- *Federal information system controls audit manual* (GAO/AIMD-12.19.6), United States General Accounting Office, January 1999.
- *ISO/IEC 17799:2005 INFORMATION SECURITY STANDARD.*
- *NIST, SP 800-42, Guideline on Network Security Testing*, October 2003.
- *OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad*. ISECOM.
- *Trusted Computer Systems Evaluation Criteria* (TCSEC), US DoD 5200.28-STD, December 1985.