UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"METODOLOGÍA PARA ESTABLECER UN PLAN DE SEGURIDAD DE LA INFORMACIÓN"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

YURI ADRIÁN GONZÁLEZ ROBLES

CÉSAR ANTONIO MARTÍNEZ OLIVARES

Directora de Tesis: M.I. ELBA KAREN SAÉNZ GARCÍA

México 2008

Dedico este trabajo a la querida memoria de mis abuelas Marina Navarro y Coleta Cedillo; todo mi amor y admiración por siempre.

A Linda: Gracias por compartir mis noches en vela, mis alegrías y mis malos ratos. La luz de tu amor y de tu empeño brilla en mi corazón todos los días.

A Simón: Gracias por todos los sacrificios que hiciste y que día a día construyeron un lugar estable y seguro al que aprendí a llamar “hogar”. Trato de seguir tu ejemplo todos los días.

A Kazumi: Gracias por estar conmigo al final de este ciclo. Tu amorosa labor me ha enseñado la belleza que existe en una vida de orden y disciplina.

A Misato y Minami: Gracias por ser el remanso de felicidad al final de cada jornada. Ustedes hacen que todo valga la pena.

A Jair e Iván: Gracias por ser apoyo y compañeros incondicionales siempre.

Gracias a César Sanabria, Enrique González, Abdell Ruíz y César Martínez por sus invaluables contribuciones y comentarios.

Muy especial agradecimiento a Káren Saenz, Oscar Valdés y Cintia Quezada. Su guía y acertadas observaciones permitieron consolidar un trabajo del que me siento orgulloso.

Gracias a la Universidad Nacional Autónoma de México y la Facultad de Ingeniería, forjadores de profesionales completos.

- Yuri González -

A mis padres, por todo su amor y comprensión, desde siempre, éste trabajo es de ustedes.

Para mis hermanos, Jorge, Adriana, Rocío y Verónica, por su cariño y alentarme a ser mejor persona cada día, los quiero.

Araceli, sabes que sos mi ángel, todo mi cariño por su comprensión y apoyo en mis decisiones y convicciones.

A mi tía Lucia, por ser ejemplo de tenacidad.

A la Universidad Nacional Autónoma de México, y en especial a la Facultad de Ingeniería por permitirme la oportunidad de estudiar en sus aulas y ver una mayor perspectiva del mundo.

A mis entrañables amigos de la Facultad de Ingeniería, saben que sin ustedes mi paso por las aulas de la Facultad no hubiera sido lo mismo.

A quienes permitieron y apoyaron para que éste trabajo fluyera con libertad de pensamiento y acción.

A los profesores de la Facultad de Ingeniería que con su trabajo diario y honesto forjan y pulen el orgullo de ser universitario.

A Karen y Oscar, por confiar en nosotros para la realización de éste trabajo.

A Yuri, por sus enseñanzas como practicante de la seguridad de la información.

César

Introducción.

En la década pasada, los mecanismos criptográficos hicieron su entrada a la escena de Internet.

El recibimiento de estas nuevas herramientas tuvo reacciones en ambos sentidos. Mientras que algunas personas visualizaron en las técnicas criptográficas un elemento que permitiera al ciudadano común resguardar su privacidad de las grandes corporaciones gubernamentales, otras más vaticinaron su uso como la herramienta perfecta para la transferencia de información ilícita procedente de traficantes de droga y traficantes de pornografía infantil. Tampoco faltó quien mencionara que la criptografía sería el catalizador para impulsar de manera definitiva el comercio *en línea*, posibilitando un genuino intercambio global en este nuevo "*y seguro*" mundo cibernético.

Nada de esto ha pasado.

Hoy, tanto como hace 10 años, Internet sigue reflejando las fronteras físicas entre los países, los criminales siguen siendo perseguidos y su captura tiene que ver más con políticas y recursos humanos que con avanzadas técnicas matemáticas para leer contenido cifrado. Podemos decir, incluso, que la criptografía ha hecho poco más que brindar un falso sentido de seguridad a los usuarios de Internet, y eso solamente es bueno para los criminales.[1]

El origen de esta situación no tiene que ver con la criptografía como ciencia matemática. Claro, se han realizado hallazgos que permiten atacar ciertos protocolos dadas las condiciones requeridas, pero todavía son materia de los estudiosos de la teoría de números. Los sólidos fundamentos teóricos que dieron origen a la criptografía apenas han sido tocados.

La problemática de la situación que estamos viviendo (viviendo *en línea*, para precisar) tiene que ver más con la criptografía como una disciplina de la ingeniería. Porque matemáticamente se ha cumplido con la promesa de integrar criptosistemas seguros y resistentes por largos, larguísimos períodos de tiempo. Sin embargo, hemos fallado al tratar de convertir dichos sistemas en una realidad palpable de seguridad de la información para el ciudadano (o ciber ciudadano) común.

Como disciplina, la ingeniería de la seguridad tiene que ver con la construcción de sistemas (no necesariamente informáticos) de los cuales podamos depender aún cuando enfrenten actos de malicia, dolosos o accidentales. La ingeniería de la seguridad requiere de conocimiento multidisciplinario: desde criptógrafos e ingenieros para diseño de procesadores y firmware seguro hasta expertos en levantamiento de requerimientos no funcionales y analistas de procesos de negocios.

No es casual que sean los ingenieros las personas más capacitadas para integrar elementos tan dispares y encontrar la convergencia en la divergencia: la disciplina con la que han sido formados, los califica para aplicar una visión paso a paso, estructurada, medible, repetible y basada en las buenas prácticas existentes.

El presente trabajo pretende documentar un marco de trabajo que permita establecer e implementar un esquema de gobierno de la Seguridad de la Información enmarcado en los estándares y mejores prácticas en materia de seguridad de la información y basado en el análisis de riesgos de los activos de información críticos para la operación de una organización.

El *Capítulo I* presenta una perspectiva histórica de la seguridad de la información. Nos hemos asegurado de tomar algunos de los *peores escenarios* a lo largo de la historia para ejemplificar el por qué la seguridad de la información es importante y repercute mucho más allá de las amenazas y tecnologías del momento. Así mismo, revisamos cómo las modernas tecnologías de información, combinadas con los últimos paradigmas de guerra, dan pie a nuevos conflictos en los que el propósito es inutilizar la infraestructura de comunicación del contrincante.

Siendo la seguridad de la información una disciplina tan *joven* (consideremos que a mediados de los años 60 todavía no era posible distinguir seguridad del cómputo de seguridad de la información) siempre estaremos tentados a integrar estrategias innovadoras que presenten al mundo un nuevo punto de vista del problema. Sin

1 Cfr. Schneier, Bruce. Practical Cryptography. Pág. XVII.

embargo, en el *Capítulo II* se detallan algunas de las mejores prácticas existentes, y se revisa la conveniencia de apegarse a ese cúmulo de conocimientos y experiencia que ha ido madurando gracias a lo errores cometidos por *otros*.

El *Capítulo III* integra una visión sistémica del problema de seguridad. Para este efecto se hace un breve análisis de la base de una estrategia efectiva de protección: los riesgos; qué representan desde el punto de vista de ingeniería y cómo se perciben por el cerebro humano. Posteriormente se hace la presentación de una metodología para llevar a cabo un análisis de esta naturaleza.

El *Capítulo IV* establece la metodología de manera práctica, mediante el uso de ejemplos sobre un sistema ficticio de información, documentando algunas de las actividades de seguridad que se llevaron a cabo como parte de la estrategia de protección de una entidad médica ficticia.

Las conclusiones se dan en dos rubros: al final de cada capítulo se hace una recopilación en donde también se señala lo que consideramos los aspectos más relevantes, y las conclusiones generales incluyen los resultados del trabajo en su totalidad, así como algunos señalamientos en relación con las carencias que hemos percibido durante los años de experiencia que llevamos practicando la seguridad de la información.

CAPÍTULO I

INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

Capítulo I. Introducción a la Seguridad de la Información.

"Donde se queman libros, se acaban quemando hombres."

Heine, 1820.

Hoy día es muy común escuchar que algún sitio Web de cierta corporación fue penetrado por un *hacker* anónimo. Es también común recibir avisos vía correo electrónico que alertan acerca de un nuevo *virus informático* que potencialmente puede borrar toda la información almacenada en la computadora. Así mismo, los grandes fabricantes de software emiten boletines de manera regular que corrigen ciertas partes de sus programas que de otra manera posibilitarían el acceso no autorizado a un atacante que probablemente está sentando del otro lado del mundo.

Inmersos en esta vorágine de términos nuevos que aparecen a la par de tecnologías que prometen ser la panacea en términos de seguridad, es difícil encontrar un punto de referencia que permita atacar la problemática de manera estructurada, utilizando las metodologías y técnicas que permitan resultados que se puedan medir y sean repetibles.

En este sentido, creemos indispensable que el practicante de seguridad de la información comience por establecer una visión histórica del problema que le permita trascender la tecnología de moda o los riesgos del momento.

Estamos convencidos de que al consolidar una perspectiva de esta índole, se tiene una ventaja práctica: porque a partir de las experiencias y *lecciones aprendidas* en el pasado se puede consolidar una postura que permita tomar decisiones que deriven en acciones que realmente contribuyan a mejorar la seguridad de un sistema de información.

Que quede claro de una vez: seguridad de la información va mucho más allá que seguridad informática.

La primera abarca todo el ciclo de vida de la información (generación, procesamiento, transmisión y almacenamiento) en sus diferentes instancias: información escrita, representada en diagramas, proyectada en imágenes o incluso transmitida oralmente en una conversación vía telefonía IP. En éste sentido los principales objetivos que se pretenden con la seguridad de la información es brindar mecanismos de seguridad, los cuales se describen brevemente:

- Confidencialidad: Consiste en garantizar que la información sólo pueda ser accedida por las partes autorizadas para ello, por nadie más.[2]
- Autenticación: Esto consiste en garantizar que las partes o entidades participantes en una comunicación sean las que dicen ser. Es decir, consiste en el proceso de identificación de una parte ante las demás, de una manera no controversial y demostrable.
- Verificación de la integridad: Consiste en proteger los activos del sistema contra modificaciones, alteraciones, borrado, inserción y, en general, contra todo tipo de acción que atente contra la integridad de los activos.
- Disponibilidad: Se refiere a que los recursos de información puedan ser consultados o recuperados en todo momento.

Por otro lado, la seguridad informática tiene que ver solamente con los mecanismos y tecnologías que sustentan los servicios de seguridad de la propia información.

2 Daltabuit, Enrique (2007). La seguridad de la información, págs. 101-103

1.1 Guerra y destrucción de los acervos de información

El desarrollo y florecimiento de las civilizaciones a lo largo de la historia está relacionado íntimamente con la generación y consolidación del conocimiento: científico, tecnológico y cultural. Así mismo, la integración del conocimiento generado en determinado punto del tiempo, históricamente se ha concentrado en acervos de información: desde las pinturas rupestres, pasando por los papiros egipcios y tablillas babilónicas, hasta las relativamente modernas bibliotecas y hemerotecas. (Ver ilustración 1).

A través de los acervos de información es posible transmitir el conocimiento en el tiempo; de tal suerte que la siguiente generación no requiera buscar soluciones a problemas y situaciones que ya se han presentado.

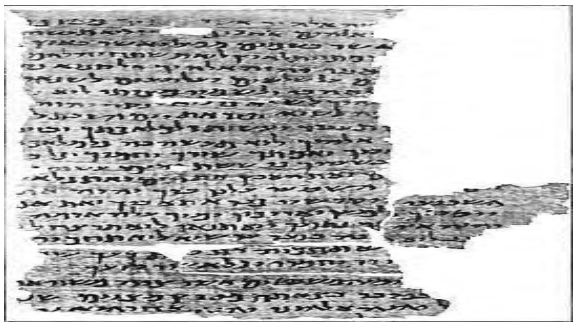


Ilustración 1: Fragmento de la Biblia de los Setenta, traducida del hebreo en Alejandría

Así, por la importancia que revisten, los acervos de información se han consolidado como activos primordiales para el desarrollo de una sociedad cualquiera. No sería aventurado decir que dichos acervos forman parte del patrimonio de una nación. Por ende, éstos se convierten también en objetivos importantes en caso de suscitarse un conflicto bélico entre dos grupos antagonistas, ya sea como botines de guerra o simplemente por quedar expuestos a la destrucción.

En este sentido, tenemos numerosos casos documentados: el 10 de Mayo de 1933, los nazis alemanes quemaron miles de libros que consideraban poco acordes con la filosofía Hitleriana. (Ver ilustración 2). Hacia el año 213 a.C., el emperador Shih-Huang Ti hizo destruir todo cuanto pudiera servir para restituir la memoria del pasado. En 1453, los turcos tomaron Constantinopla y arrasaron con sus prestigiosos manuscritos. En 1813, los soldados norteamericanos tomaron Canadá y York, y quemaron el Parlamento y la biblioteca legislativa. La noche del 9 de Marzo de 1943, un ataque aéreo sobre la Biblioteca de Babiera destruyó medio millón de libros. En 1993 fueron destruidas decenas de bibliotecas por parte de las milicias nacionalistas croatas.[3]

Ilustración 2: Libros de Freud, Einstein, Thomas Mann, Jack London, H.G. Wells y muchos otros arden ante el saludo Nazi.

3 Báez, Fernando (2003). Fuego y pillaje en la biblioteca de Bagdad. **La Nación,** Suplemento Cultura.

La magnitud real de la destrucción de los acervos de información puede ser catastrófica. Este hecho queda plasmado con toda crudeza si se analizan las consecuencias que la destrucción de la biblioteca de Alejandría tuvo para la civilización occidental.

Fundada hace dos mil trescientos años por Tolomeo I, en los estantes de la biblioteca de Alejandría se lograron recopilar y transcribir casi un millón de volúmenes en rollos de papiro.[4] Alrededor de la biblioteca, florecieron grupos científicos, literarios y filosóficos. Ahí estuvo el primer mapamundi, al igual que los primeros tratados de geometría y de álgebra.

En al año 48 a.C., como parte de la guerra entre Julio César y la flota Egipcia el edificio principal de la biblioteca de Alejandría es destruida en un "accidente militar". Posteriormente, en el año 391 d.C., Teodosio ordena la destrucción de los edificios restantes de la biblioteca.[5]

A nivel cultural, este hecho representa una catástrofe para toda la civilización occidental. La información acumulada a lo largo de muchos siglos, se pierde de manera irremediable. La producción cultural y científica de la civilización occidental no sólo se paraliza, sino que entra en una etapa de retroceso en todos sus aspectos: ha comenzado la Edad Media.

Mientras que en la misma época en el mundo islámico florecía la medicina, por ejemplificar, en Europa se perdió la mayor parte del conocimiento de anatomía y cirugía. Abundaba la confianza en la oración y las curaciones milagrosas. Desaparecieron los médicos seculares. Se usaban ampliamente cánticos, pociones, horóscopos y amuletos. Se restringieron o ilegalizaron las disecciones de cadáveres, lo que impedía que los practicantes de medicina adquirieran conocimiento de primera mano del cuerpo humano. La práctica médica se vio tan mermada que no logró salvar a muchos ni siquiera después de bien finalizada la Edad Media. La reina Ana fue la última Estuardo de Gran Bretaña. En los últimos diecisiete años del siglo XVII se quedó embarazada dieciocho veces. Sólo cinco niños nacieron vivos, uno sobrevivió a la infancia y murió antes de llegar a la edad adulta, antes de la coronación de la reina en 1702.[6] (Ver ilustración 3).

Ilustración 3: Un sacerdote bendice a víctimas de La Peste Negra.

La devastadora destrucción de la biblioteca de Alejandría no acabó con la civilización mediterránea gracias a que *de hecho* existió un respaldo del acervo. Afortunadamente, los estudiosos árabes habían realizado una amplia colección de traducciones de los trabajos albergados en Alejandría, misma que llevaron de vuelta a sus ciudades de origen previo a la destrucción de la biblioteca. De esta manera, se preservó parte de los

4 Cfr. Daltabuit, Enrique (2005). La información y su seguridad. Nexos, No. 334.
5 Cfr. Daltabuit, Enrique. Op. Cit.
6 Sagan, Carl. El mundo y sus demonios, págs. 25-26

conocimientos generados a lo largo de los casi mil años de vida de la biblioteca.[7]

Así, de manera paradójica, mientras que la civilización occidental sufría el peor período de su historia, en el mundo árabe se dieron avances en todas las ramas del conocimiento: artes, filosofía, ciencia y tecnología.

No podemos concluir este tema sin mencionar la más reciente tragedia en materia de destrucción de acervos de información.

En Abril de 2003, el gobierno y ejército iraquí colapsan a tan solo tres semanas de comenzada la invasión de ese país por parte del ejército de los Estados Unidos de América. El entonces presidente Sadamm Hussein, abandona el poder y trata de ocultarse para escapar de las fuerzas invasoras.

El 14 de Abril, cuando se corrió la voz de que el dictador había huido, un grupo de saqueadores se encamina a la Biblioteca Nacional de Irak. Este primer grupo de saqueadores (hubo más actos de esta índole posteriormente) sabía dónde estaban los manuscritos más importantes, se apresuró a tomarlos y sin mediar palabra, alentado por la pasividad de los militares estadounidenses, roció con gasolina los anaqueles y le prendió fuego a todo. Horas después, una columna de humo podía verse a más de cuatro kilómetros y en ese incendio voraz desaparecieron miles de obras.[8] (Ver ilustración 4).

Ilustración 4: Biblioteca Nacional de Bagdad.

Las tablillas de arcilla de los sumerios, los primeros libros de la humanidad, de unos 5,300 años de antigüedad quedaron en ruinas. Textos de Súmer, Acadia, Babilonia, Asiria y Caldea, Persia y varias dinastías árabes fueron destruidos. Aquí se incluyen las tablillas del código de Hammurabí, donde aparecía el primer registro de leyes en el mundo. Así mismo, desaparecieron cientos de tablillas de arcilla aún sin descifrar, algunas de las cuales contenían datos sobre el origen de la escritura. Tablillas con el *Poema de Gilgamesh* fueron sustraídas.[9]

Tras este breve repaso de la accidentada historia de los acervos de la información, podemos destacar un par de puntos que posteriormente serán piedras angulares en la concepción y desarrollo del moderno Sistema de Gestión de Seguridad de la Información:

1) Es muy importante contar con un sistema de *ponderación* que permita identificar y dar el justo valor a los activos de información críticos.

2) Es muy importante desarrollar los criterios que permitan dimensionar correctamente el impacto en caso de destrucción (total o parcial) de los activos de información críticos.

7 Cfr. Daltabuit, Enrique. Op. Cit.
8 Cfr. Baéz, Fernando. Op. Cit.
9 Ibid.

Obsérvese que aunque es evidente que se requiere contar con las técnicas y mecanismos que posibiliten la implantación de una estrategia de protección sobre los activos de información críticos, si contamos de antemano con un esquema que nos permita establecer prioridades, estaremos focalizando los esfuerzos y por tanto haciendo más eficiente el plan de protección.

Así, el practicante de la seguridad de la información puede dejar en segundo término las tecnologías y mecanismos para concentrarse realmente en acciones que acarreen beneficios palpables para los activos de información.

Hemos comentado ya dos dimensiones básicas para la integración de un Sistema de Gestión de Seguridad de la Información: los activos de información y las consecuencias de que dichos activos se vean comprometidos.

Ahora requerimos redondear esta introducción con la presentación de una tercera variable: las amenazas.

El ataque de Estados Unidos a Irak que dio pie a la catástrofe de la Biblioteca Nacional de Bagdad, no fue casual, sino que fue una respuesta a ataques que previamente se suscitaron del otro lado del mundo: en la ciudad de Nueva York.

1.2 Guerra asimétrica: un nuevo paradigma de ataque

La construcción del complejo del Centro Internacional de Comercio (WTC, por sus siglas en inglés) en la ciudad de Nueva York dio inicio en 1966, y comenzó a dar alojamiento a sus inquilinos a partir de 1970. Las Torres Gemelas de este complejo se constituyeron rápidamente como un símbolo de la cultura norteamericana.

Distribuido en 64,749 metros cuadrados, el complejo del WTC estaba compuesto por siete edificios, incluyendo un hotel. Los edificios estaban interconectados por un centro comercial subterráneo. Las Torres Gemelas (1 WTC, o la torre norte, y 2 WTC, o la torre sur) eran las construcciones insignia del complejo, conteniendo cerca de un millón de metros cuadrados en espacios para oficina.

Ambas torres tenían 110 locales comerciales, midiendo más de 400 metros. En un día de trabajo común, eran ocupadas hasta por 50,000 trabajadores, y alrededor de 40,000 visitantes pasaban por el complejo.[10](Ver ilustración 5).

Ilustración 5: Complejo WTC.

De acuerdo con la Comisión Nacional sobre Ataques Terroristas en Estados Unidos en su reporte sobre lo acontecido el 11 de Septiembre, conocidos como ataques del 9/11, describe lo siguiente: Es el martes 11 de Septiembre de 2001. El clima es templado y casi sin nubes en la costa este de los Estados Unidos de América.

10 9/11 Commission, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, pág. 278

Millones de hombres y mujeres se alistan para asistir a su trabajo. Algunos se dirigen hacia las Torres Gemelas en la ciudad de Nueva York. Otros se dirigen a las instalaciones del Pentágono en Virginia.

Para aquellas personas que se dirigen a un aeropuerto, las condiciones climáticas no podían ser más favorecedoras para un viaje seguro y placentero. Entre los pasajeros se encontraban Mohamed Atta, Abdul Aziz al Omari, Satam al Suqami, Wail al Shehri, y Waleed al Shehri, que abordaron el vuelo número 11 de American Airlines en el aeropuerto internacional de Boston.

Al mismo tiempo en otra sala del aeropuerto, Marwan Al Shehhi, junto con Fayez Banihammad, Mohand al Shehri, Ahmed al Ghamdi y Hamza al Ghamdi, abordaron el vuelo número 175 de United Airlines.

A las 08:46:40, el vuelo número 11 de American Airlines se estrelló en la torre norte del WTC en Nueva York. Todas las personas abordo, junto con un número indeterminado de personas en la torre murieron de manera instantánea.

A las 09:03:11, el vuelo número 175 de United Airlines impactó la torre sur del WTC. Todas las personas abordo, junto con un número indeterminado de personas en la torre murieron de manera instantánea.[11]

Los ataques terroristas del 11 de Septiembre constituyen ante todo un evento de desproporción incomparable: fueron ejecutados por un minúsculo grupo de personas; medido a escala gubernamental, los recursos utilizados fueron triviales. El grupo mismo fue despachado por una organización con base en uno de los países más pobres, más remotos y menos industrializados en la tierra.[12](Ver ilustración 6)

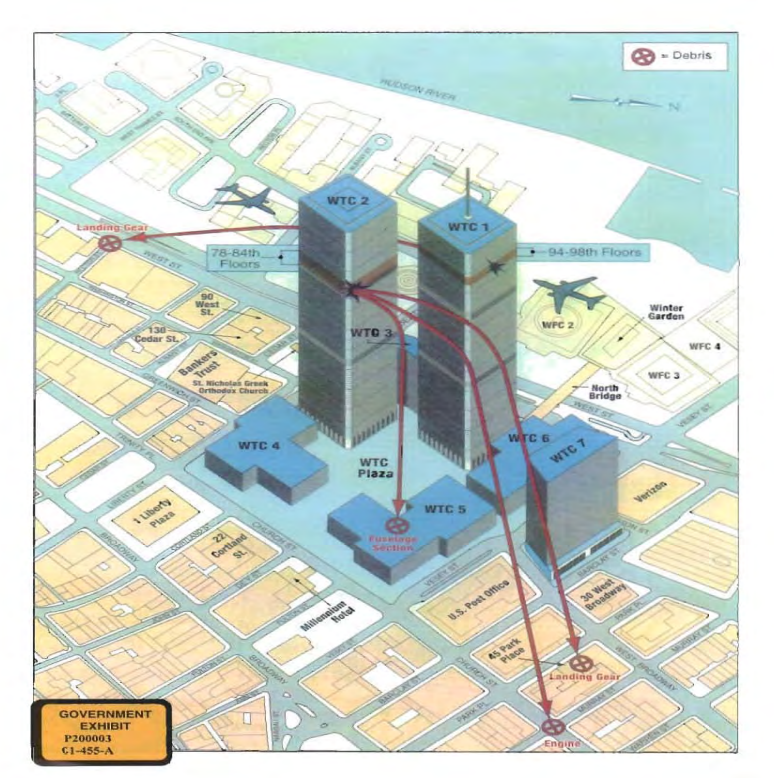


Ilustración 6: Impactos sobre las Torres Gemelas.

11 Ibid., págs. 1-8
12 Ibid., pág. 339

El terrorismo es una forma de *guerra asimétrica*, dada la desproporción de recursos destinados de quienes poseen y desean proteger información y aquéllos que pretenden acceder a ella de forma ilícita, lo cual plantea una nueva problemática a la comunidad de seguridad a nivel mundial en todas sus vertientes, ya que en una guerra asimétrica una de las partes beligerantes puede causar grandes daños a su rival a un muy bajo costo.

Al finalizar la guerra fría entre la desaparecida Unión Soviética y los Estados Unidos de América, las posibilidades de una confrontación *directa* entre dos súper potencias disminuyeron considerablemente. Ya nadie espera ver, por ejemplo, un ejército de tanques invadiendo a la Europa moderna. Lo que es más frecuente encontrar en las últimas décadas son casos de autos bomba, conflictos con el narcotráfico, combate urbano, operaciones para rescate de rehenes y para preservar la paz (*sic.*).[13]

Esta nueva forma de hacer la guerra es pues, característica de la era moderna en que vivimos. Más aún, al mezclar las nuevas tecnologías de información con este nuevo paradigma de guerra, quedan dadas las condiciones para el nacimiento de lo que podemos denominar como *guerra cibernética*.

1.3 Guerra Cibernética

La asimetría característica de los conflictos modernos, es especialmente cierta en su equivalente cibernético. En los casos más extremos, individuos con poco más que un equipo personal de cómputo y acceso a Internet, son capaces de producir daños sustanciales a grandes grupos sociales o entes corporativos.[14]

A guisa de ejemplo, considérese que a mediados de 1999 se popularizó la publicación de *Trin00*, una herramienta que permite lanzar ataques por medio del envío de grandes volúmenes de tráfico en contra de un objetivo. La finalidad de la herramienta es saturar los recursos de determinado servicio e impedir así que las peticiones de clientes legítimos sean atendidas.

Descargar e instalar *Trin00* no requiere más que contar con un equipo personal de cómputo y una conexión a Internet. Para ejecutar el ataque basta solamente con seleccionar el objetivo y hacer clic sobre un botón. No se requiere que el atacante tenga conocimientos o preparación adicional alguna.

En Febrero de 2000, los portales de Amazon, Buy.com, CNN, eBay y Yahoo! fueron afectados por este tipo de ataque. Como consecuencia, los servicios prestados se vieron interrumpidos en períodos desde 3 hasta 10 horas. Las pérdidas reportadas se presentan a continuación.[15](Ver Tabla 1)

Sitio	*Horas fuera de servicio*	*Pérdidas (dólares)*
www.yahoo.com	3 horas	$500,000
www.amazon.com	10 horas	$600,000

Tabla 1: Pérdidas derivadas de ataques de negación de servicio

Cabe señalar, que la guerra cibernética va mucho mas allá de dejar fuera de servicio por algunas horas el sitio web que un grupo de adolescentes accede de manera frecuente. Para dimensionar los impactos de un ataque con estas características, debemos considerar que actualmente los componentes críticos de la infraestructura de todos los países (plantas de generación de energía eléctrica, sistemas de transporte, servicios de telecomunicaciones, etc.) son controlados por sistemas de cómputo.

Las condiciones actuales hacen tan patente la posibilidad de una guerra cibernética que países como China, Taiwán, Corea del Norte, Corea del Sur y Singapur han declarado poseer unidades e instalaciones bélicas

13 Cfr. Staten, Clark. Asymmetric Warfare, the Evolution and Devolution of Terrorism.
14 Amoroso, Edward. Cyber Security. Cap. 1, Sec. “Low Cost, High Return”
15 Cfr. Kessler, Gary. Computer Security Handbook, Cap. 4.

especializadas en este tipo de conflictos.[16]

1.4 Conclusiones

El desarrollo de las civilizaciones a lo largo de la historia está ligado fuertemente a la consolidación de acervos de información que posibilitan el florecimiento de ciencia, tecnología y cultura. Tal es la importancia de éstos que permitir su destrucción, pone en riesgo la existencia de la sociedad misma.

Al constituirse como un *activo* de tal criticidad, los acervos de información se han convertido en objetivos de enemigos tanto internos como externos, y las consecuencias de la destrucción de los mismos tiene alcances que van desde la inhabilitación de un ente corporativo hasta dañar el desarrollo de toda una nación.

Las amenazas también han evolucionado, y las tradicionales formas de hacer la guerra han cambiado en las últimas décadas. No se cuenta ya con la ventaja de tener una declaración formal antes de iniciar un conflicto, y en muchas ocasiones no se tiene tampoco definido bien a bien quién es el enemigo. Mas aún, el análisis costo-beneficio de involucrarse en una guerra (cibernética o no) debe considerarse bajo los nuevos paradigmas de ataque y contra ataque,

Así, se va vislumbrando que el marco de trabajo que permita al practicante establecer un esquema de protección, debe posibilitar:

- La oportuna identificación de los *activos* de información
- El pronto reconocimiento de las principales *amenazas* que los asechan
- El *impacto* en caso de ocurrir algún evento indeseable.

Este marco de trabajo deberá ser además sistemático, estructurado, repetible, eficiente y adaptable a los cambios que se produzcan en el entorno, considerando tanto el factor humano como el tecnológico.

16 Amoroso, Edward. Cyber Security. Cap. I., Sec. “Information Warfare”

CAPÍTULO II

MARCOS DE REFERENCIA PARA EL ESTABLECIMIENTO DE UNA ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

Capítulo II. Marcos de referencia para el establecimiento de una estrategia de Seguridad de la Información

"Si he logrado ver más lejos, ha sido porque he subido a hombros de gigantes"

Newton, 1675.

Entre las dificultades comunes para el practicante que por vez primera se enfrenta con el reto de establecer una estrategia para la protección de la información, destaca la de establecer una *aproximación* al problema que permita aplicar una visión estructurada del mismo. Esto es, una propuesta de solución que posibilite la comprensión global del problema, que facilite la obtención de los indicadores necesarios para medir la efectividad de la propuesta y así posibilite justificar la inversión realizada en materia de seguridad y permita implementar un ciclo de mejora continua de la solución.

Hoy día, sin embargo, el común de las estrategias de protección están basadas casi exclusivamente en *mecanismos* de seguridad de tecnología de información; de tal manera que se montan complejas y costosas soluciones técnicas que mezclan controles de filtrado de paquetes de red y detección de intrusos, agregados de Infraestructura de Clave Pública, soluciones anti-virus y esquemas de autorización tipo *Single Sign On.* Aunque técnicamente atractivo, todo este esquema se viene abajo cuando los empleados copian su contraseña de acceso a los sistemas financieros de la organización en un pedazo de papel que después pegan junto al monitor de su equipo personal de cómputo, por mencionar un ejemplo.

Podemos decir entonces, que **un sistema de seguridad es tan fuerte como su eslabón más débil.** Atacar de manera parcial el problema del establecimiento de un esquema de protección, es el equivalente a poner media cerca al rededor de una casa, y dar un falso sentido de seguridad solamente facilita el trabajo de un posible atacante.

El problema *real* que establece esta máxima de la seguridad, sin embargo, es que muchas veces es difícil darse cuenta de que solamente se está atacando el problema de manera parcial.

De acuerdo con Summers, existen tres aproximaciones básicas al plantear una estrategia de seguridad[17]:

1. Aproximación costo-beneficio: La seguridad de la información siempre establece un compromiso. Siempre hay un costo asociado a la implementación de la seguridad: dicho costo puede ser económico, pero también puede verse reflejado en libertad de uso, privacidad o funcionalidades.[18]

   La aproximación costo-beneficio, nos habla de establecer un sistema de ponderación que nos permita decidir cuáles son los controles requeridos para mitigar las principales amenazas. Así, la aproximación costo-beneficio se traduce en gestión de riesgos: estimar las pérdidas potenciales y comparar con el costo de las salvaguardas necesarias para mitigar dichas pérdidas.

   Esta aproximación se tocará a detalle en el Capítulo 3 de este trabajo.

2. Aproximación de línea base. Sin importar el costo asociado a los controles de seguridad, un nivel mínimo de seguridad debe ser acordado y establecido. Este nivel mínimo de seguridad es conocido como *línea base (baseline,* en inglés).

   La aproximación de línea base, por lo general queda reflejada en documentos que estandarizan la configuración de los dispositivos de tecnología de información. Organizaciones gubernamentales y grupos especializados en seguridad, publican de manera regular documentos para configurar de manera segura dichos dispositivos. Históricamente el Libro Naranja publicado por el Departamento de

17 Cfr. Summers, Rita C. Secure Computing. Threats and Safeguards. Págs. 6-9.
18 Cfr. Schneier Bruce. Beyond Fear, Cap. 1.

Defensa de los Estados Unidos es un ejemplo de un documento de estandarización de línea base.[19](Ver ilustración 7)

En nuestra experiencia la aproximación de línea base ha resultado un excelente punto de partida, porque permite integrar soluciones a corto plazo que atacan los problemas de seguridad de la información que son más patentes.

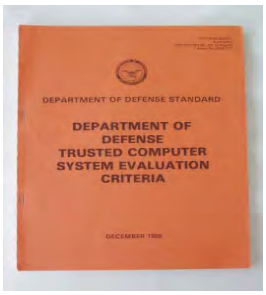


Ilustración 7: El libro naranja.

3. Aproximación combinada. Se refiere a complementar la aproximación de costo-beneficio con la aproximación de línea base.

Antes de continuar con el tema en comento, conviene detenernos para caracterizar un sistema seguro: decimos que un sistema (desde el punto de vista sistémico, no necesariamente informático) es seguro si se puede confiar en que, junto con todos sus componentes, funciona como se espera.[20] Esto quiere decir que, además de permanecer confiable ante situaciones adversas, un sistema seguro debe cumplir adecuadamente con el fin para el que fue creado, cumplir con sus especificaciones técnicas y satisfacer a sus usuarios. Esta definición nos lleva necesariamente a plantear el problema de la seguridad de un sistema como un problema de *calidad*. La siguiente sección del presente trabajo abunda sobre este particular.

El panorama planteado hasta este punto no es alentador. La complejidad y número de variables que intervienen durante la consolidación de un sistema de seguridad son numerosos y difíciles de definir. Sin embargo, estamos convencidos de que establecer un esquema de protección de seguridad de la información, integrando una aproximación que trascienda las circunstancias y tecnologías del momento y que enfoque el problema como un problema de calidad es posible y es la manera correcta de hacerlo.

Siempre es recomendable buscar en la industria casos de éxito y creemos que la industria aeronáutica es un ejemplo a seguir. Un avión en vuelo representa un sistema que debe funcionar tal como se espera. A 12,400 metros sobre el nivel del mar, no hay muchas oportunidades para enmendar errores. Y sin embargo, el día de hoy es más seguro viajar en avión que viajar en automóvil. El sistema de calidad/seguridad que da pie a esta situación funciona.

Así pues, creemos que es hacia esa dirección (calidad-seguridad) a donde deben apuntar los esfuerzos al implementar cualquier sistema de gestión de la seguridad de la información.

2.1 Sistemas de Gestión de Calidad

Para poder implantar un esquema de seguridad en el entorno de la información, debemos contemplar un aspecto primordial en el esquema de aseguramiento, la calidad, la cual se basa en evitar que se produzcan

19 Formalmente, el Libro Naranja forma parte de un estándar militar de seguridad estadounidense llamado “Trusted Computer System Evaluation Criteria” (TCSEC). Más que un solo documento de estandarización, el TCSEC define diferentes categorías de seguridad, de acuerdo con la criticidad de la información que maneje un sistema.

20 Cfr. Garfinkey Simson, Spafford Gene. Seguridad práctica en Unix e Internet. Pág. 5.

bienes defectuosos en los sistemas y procedimientos de una organización, para con ello brindar satisfacción al cliente, reducir costos y tener una mejora continua; es por ello que damos un repaso por las diversas etapas para llegar a lo que ahora conocemos como calidad.

1.- Calidad basada en la inspección. Esta etapa estaba orientada al producto y centrada en la inspección después de la producción. Algunas actividades típicas de esta fase son: las auditorias de producto acabado, la resolución de problemas y la inspección por muestreo en la recepción de materiales.[21]

2.- Control de la calidad. Esta etapa se centra en el proceso de fabricación y en ella se usan técnicas de control estadístico de proceso. Estas técnicas desarrolladas por Shewhart en los años 30 se empezaron a aplicar durante la Segunda Guerra Mundial a las grandes producciones en serie. Shewhart introduce gráficos de control. Posteriormente estas técnicas fueron fuertemente impulsadas por los fabricantes de automóviles, que las impusieron a sus proveedores.[22]

3.- Aseguramiento de la calidad. Esta etapa implica a todos los departamentos de la empresa y en muchos casos también a los proveedores. Esta etapa arranca por requerimiento de la industria nuclear en los años 70 y se consolida en 1987 cuando se establece la norma ISO 9000 de aseguramiento de calidad. En esta etapa la atención se dirige hacia la elaboración del manual de calidad, la evaluación de costos de calidad, el control de los procesos y las auditorias del sistema de calidad, insistiendo en las medidas preventivas orientadas a evitar la aparición de las disconformidades.[23]

4.- Optimización del diseño de nuevos productos y procesos. El arranque de esta etapa se puede situar en los años 70 en Japón y en los años 80 en Occidente. En ella se usan técnicas como el diseño de experimentos para mejorar los productos y procesos.[24]

5.- La gestión de la calidad total se introduce en Europa en los años 80. Es una etapa en la que las empresas toman conciencia de que la calidad es algo que afecta a todos los departamentos.[25]

Anteriormente los departamentos de calidad se dedicaban básicamente, a la inspección del producto, enfrentados a menudo con los departamentos de producción. Esta situación duró hasta mediados de los años 50.

Con Shewhart se inicia la teoría actual de la gestión de la calidad a principios de los 30. Shewhart es considerado como el precursor de la calidad, por haber introducido los principios de control estadístico de proceso y diseñado los gráficos de control, en la misma forma en que se usan hoy para aplicar esos principios a la producción en serie. La idea de gestión de la calidad que se extrae de sus escritos se basa en un seguimiento metódico y continuado del proceso productivo para mantener estables (en estado de control) y en la mejora posterior. Shewhart fue el primero en formular el ciclo PDCA.

Deming es el personaje más emblemático en el desarrollo del marco de calidad. Desde el punto de vista metodológico Deming dio una importancia primordial al control de los procesos y al uso de métodos científicos y preferentemente estadísticos.

La adopción de un sistema de gestión de la calidad debería ser una decisión estratégica de la organización. El diseño y la implementación del sistema de gestión de la calidad de una organización están influenciados por diferentes necesidades, objetivos particulares, los productos suministrados, los procesos empleados y el tamaño y estructura de la organización.[26]

Para que una organización funcione de manera eficaz, tiene que identificar y gestionar numerosas actividades relacionadas entre sí. Una actividad que utiliza recursos, y que se gestiona con el fin de permitir que los elementos de entrada se transformen en resultados, se puede considerar como un proceso.

21 Griful Eulalia, Gestión de la Calidad, Pág. 44
22 Ibid.
23 Ibid.
24 Ibid.
25 Ibid.
26 http://www.leon.uia.mx/SA-II/util/ISO_9001_2000.doc

La aplicación de un sistema de procesos dentro de la organización, junto con la identificación e interacciones de estos procesos, así como su gestión, puede denominarse como “enfoque basado en procesos”.

Deming populariza el modelo PDCA, tal como se comentó es un modelo basado en procesos, el cual consiste en: (Ver ilustración 8)

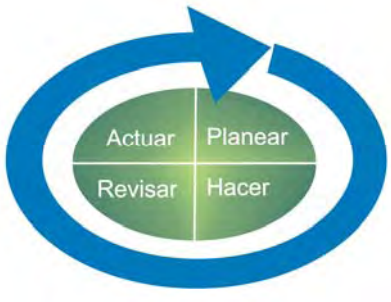


Ilustración 8: El modelo PDCA

- Planificar de qué manera se puede alcanzar una mejora en la empresa.
- Hacer, es decir, poner en práctica el plan.
- Comprobar los resultados obtenidos, usando los indicadores adecuados.
- Actuar, en el sentido de convertir en norma la solución propuesta.

Las metas que nos permite alcanzar un sistema de gestión de calidad es evitar posibles fugas de información al estar basado en procesos documentales, tener la posibilidad de contar con auditorías al sistema y llevar a cabo de forma cíclica mejoras que involucran al personal de todas las áreas corporativas.

El comité técnico ISO/TC 176 se creó en 1980, con la misión de elaborar un modelo de aseguramiento de la calidad. En 1987 aparecen las primeras normas de la serie ISO 9000. A partir de entonces han aparecido dos versiones más, una en 1994 y la actual en el 2000.

2.2 Sistemas de Gestión de Seguridad de la Información.

En los inicios de la década de los años noventa, del siglo pasado, se inició el desarrollo de un modelo de sistema de gestión de seguridad de información en Inglaterra. El British Standards Institute fue el promotor. En 2005 la Organización Internacional para la Normalización, ISO, oficializó la norma denominándola “Sistema de Gestión de Seguridad de Información” ISO/IEC 27001:2005.

Un Sistema de Gestión de Seguridad de Información (ISMS, por sus siglas en inglés) puede definirse de varias maneras:

- “Establecimiento de un sistema que determine qué requiere ser protegido y por qué, de qué debe ser protegido y cómo protegerlo” (Alberts, Donofree, 2003)
- “Es la preservación de la confidencialidad, integridad y disponibilidad de la información (Peltier, 2001)”

El modelo ISO/IEC 27001:2005 define a un ISMS como:

- La parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información[27]

En la tabla 2 se ilustra la cronología que ha sufrido la norma ISO/IEC 27001:2005 para llegar a lo que es hoy en día:

Año	*Suceso*
1995	DS 7799-1:1995 (norma británica) que fue la antecesora del código para la práctica de la gestión de la seguridad de la información
1999	BS 7799-2:1999 (norma británica antecesora del ISO 27001:2005). Esta norma se creó para que las empresas pudiesen certificarse. Fue creada para que fuese auditable.
1999	Revisión del BS 7799-1:1999
2000	La organización ISO adopta el BS 7799-1:1999 y lo oficializa como norma ISO/IEC 17799:2000 como código para la práctica de la gestión de la seguridad de la información.
2002	Revisión al BS 7799-2:1999 y se convierte en el BS 7799-2:2002
2005	Revisión del ISO 17799:2000 y se convierte en el ISO 17799:2005
2005	Revisión al BS 7799-2:2002 y se convierte en el ISO 27001:2005, como norma internacional certificable

Tabla 2: Cronología de la norma ISO 27001:2005[28]

Un Sistema de Gestión de Seguridad de Información nos permite determinar con objetividad:

- Qué requiere ser protegido.
- Por qué.
- De qué debe ser protegido.
- Cómo protegerlo.

Así mismo, nos ayuda a consolidar una visión de la seguridad de la información en la que los incidentes de seguridad dejan de ser considerados como recurrentes; éstos tienen que visualizarse como el “efecto” de una “causa” que reside en el pasado. Todos tienen una causa que debe investigarse y las acciones deben ser diseñadas para evitar que aparezcan de nuevo.

Un Sistema de Gestión de Seguridad de la Información establece pues *procedimientos* para evitar que los eventos de seguridad se conviertan en incidentes de seguridad. Los ISMS tienen memoria, se guardan registros de todas las ocurrencias de incidentes de seguridad significativos, relacionados con el ISMS.

A la fecha de la elaboración del presente trabajo, el estándar ISO/IEC 27001:2005 es el estándar aceptado internacionalmente para la gestión de la seguridad de la información; aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad. A continuación comentaremos este estándar.

27 Alexander G., Alberto. Sistema de Gestión de Seguridad de la Información. Pág. 19.
28 Ibid. Pág. 20.

2.3 El estándar ISO/IEC 27001:2005, "Information technology — Security techniques — Information security management systems — Requirements"

La Organización Internacional para la Estandarización (ISO, por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés) constituyen cuerpos especializados en la creación de estándares a nivel mundial. Cada una de estas organizaciones, está compuesta a su vez de grupos de estandarización procedentes de varios países que participan en el desarrollo de los estándares internacionales en campos particulares de actividad técnica a través de comités establecidos por cada uno de los países.

En su conjunto, los comités técnicos ISO/IEC colaboran en campos de mutuo interés.[29]

El estándar ISO/IEC 27001:2005 "*Tecnología de la información – Técnicas de Seguridad – Sistemas de Administración de la Seguridad de la Información – Requerimientos*" ha sido preparado para proveer un modelo que permita establecer, implantar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

El diseño e implantación del concepto de ISMS está concebido para que se alinee con los objetivos del negocio de cada organización, los requerimientos de seguridad, los procesos empleados y el tamaño y la estructura de la organización. Adicionalmente, se espera que la implementación de un ISMS pueda ser escalada de acuerdo con las necesidades de la organización a lo largo del tiempo.[30]

Fundamentos del ISO/IEC 27001:2005

El estándar ISO/IEC tiene dos pilares fundamentales: por una parte *adopta* el modelo Deming (PDCA) para estructurar una aproximación orientada a procesos del ISMS y por otro lado refleja los principios de los lineamientos de seguridad establecidos por la Organización para el Desarrollo y Cooperación Económico (OECD, por sus siglas en inglés). [31]

La Organización para la Cooperación y el Desarrollo Económico (OECD), es la organización de cooperación internacional, compuesta por 30 países, cuyo objetivo es coordinar sus políticas económicas y sociales. Fue fundada en 1961 y su sede central se encuentra en la ciudad de París, Francia. La OECD se ha constituido como uno de los foros mundiales más influyentes, en el que se analiza y se establecen orientaciones sobre temas de relevancia internacional como economía, educación y medio ambiente.

En 1992, la OECD desarrolló un conjunto de lineamientos (Ver Tabla 3 "*Lineamientos de la Seguridad de la Información de la OECD*") con la intención de servir como fundamento durante la elaboración de marcos de trabajo, políticas, medidas técnicas y administrativas y educación. La última versión de estos estándares fue publicada en el 2002.

Los objetivos de los lineamientos de la seguridad de la información de la OECD son[32]:

- Promover una cultura de la seguridad entre los participantes, como medio de protección de los sistemas y redes de información
- Hacer conciencia acerca de los riesgos que afectan los sistemas y redes de información; las políticas, prácticas, medidas y procedimientos disponibles para hacer frente a esos riesgos; y la necesidad de su adopción e implantación.

29 Cfr. International Organization for Standarization and International Electrotechnical Commission, ISO/IEC 27001:2005, pág. IV.
30 Ibid. pág. V.
31 Idem.
32 Organisation For Economic Cooperation and Development, OECD Guidelines for the Security of Information Systems and Networks. Págs. 9,10.

- Generar mayor confianza en los sistemas y redes de información y en la manera en que se proveen y utilizan.
- Generar un marco de referencia general que apoye a los participantes a entender los problemas de seguridad y apoye con la observación de valores éticos durante el desarrollo e implantación de políticas coherentes, prácticas, medidas y procedimientos para la seguridad de los sistemas y redes de información.
- Promover la cooperación e intercambio de información entre todos los participantes involucrados en el desarrollo e implantación de políticas de seguridad, prácticas, medidas y procedimientos.
- Promover la consideración de la seguridad como un objetivo importante entre todos los participantes involucrados en el desarrollo o implantación de estándares.

Cabe mencionar que al ser documento rector durante la creación del ISO/IEC 27001, los objetivos planteados para la creación de lineamientos de la OECD son observados y plasmados en cualquier esquema de gobierno de la seguridad alienado al estándar en comento.

	Principio	***Descripción***
1	Concienciación	Los participantes deben ser conscientes de la necesidad de asegurar los sistemas y redes de información y de qué pueden hacer para contribuir con la seguridad.
2	Responsabilidad	Todos los participantes son responsables de la seguridad de los sistemas y redes de información.
3	Respuesta	Los participantes deben actuar oportuna y activamente para prevenir, detectar y responder a los incidentes de seguridad.
4	Ética	Los participantes deben respetar los legítimos intereses de otros.
5	Democracia	La seguridad de los sistemas y redes de información deben ser compatibles con los valores esenciales de una sociedad democrática.
6	Evaluación de riesgos	Los participantes deben realizar evaluación de riesgos.
7	Diseño e implantación de la Seguridad	Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.
8	Administración de la Seguridad	Los participantes deben adoptar una aproximación global para administrar la seguridad.
9	Evaluación periódica	Los participantes deben revisar periódicamente la seguridad de los sistemas y redes de información, y hacer las modificaciones apropiadas a las políticas, prácticas, medidas y procedimientos de seguridad.

Tabla 3: Lineamientos de la Seguridad de la Información de la OECD[33]

El otro pilar del estándar ISO/IEC 27001:2005 es el ciclo de calidad. Dado que el modelo ya se trató en la sección anterior del presente capítulo, a continuación solamente se enunciarán las particularidades de su aplicación al ISO/IEC 27001:2005[34].

33 Ibid., págs. 9-12
34 Ibid, pág. VI.

Modelo PDCA aplicado al ISMS.	
Planear (Establecer el ISMS)	Establecer la política, objetivos, procesos y procedimientos del ISMS relativos a la administración de riesgos y la mejora de la seguridad de la información para entregar resultados de acuerdo con las políticas y objetivos generales de la organización.
Hacer (implantar y operar el ISMS)	Implantar y operar la política, controles, procesos y procedimientos del ISMS.
Verificar (supervisar y revisar el ISMS)	Auditar y de ser posible medir el rendimiento de los procedimientos tomando como referencia la política del ISMS, los objetivos y la experiencia práctica y reportar los resultados a la alta dirección para su revisión.
Actuar (mantener y mejorar el ISMS)	Tomar las acciones correctivas y preventivas, basados en los resultados de la auditoría del ISMS y la retroalimentación de la alta dirección, para lograr una mejora continúa del ISMS.

Tabla 4: Modelo PDCA aplicado al ISMS.

En esencia, siguiendo las fases del ciclo Deming, en la fase de “Establecimiento” el estándar da las pautas para determinar el alcance del modelo en la organización, identificar los activos de información, así como hacer el análisis y la evaluación del riesgo. En la segunda fase, la llamada fase de “Implementación”, se dan los fundamentos para posibilitar la elaboración del plan de tratamiento del riesgo. En la fase de “Monitoreo y Supervisión”, se establecen las rutinas y procedimientos con los que debe contar la organización para – con ayuda de métricas acordadas – revisar el desempeño del ISMS. Finalmente, en la fase de “Mejora Continua”, se toman las acciones pertinentes para reaccionar a incidentes y establecer las acciones preventivas que se requieran.[35]

En el desarrollo de las cláusulas que se hace a continuación se trata la aplicación del ciclo Deming de manera más detallada.

Cláusulas del ISO/IEC 27001:2005

La estructura del estándar ISO/IEC 27001, se define de acuerdo con las siguientes secciones:

0. Introducción
1. Alcance
2. Referencias Normativas
3. Términos y definiciones
4. Sistema de Gestión de la Seguridad de la Información
5. Responsabilidad de la dirección
6. Auditorías Internas del ISMS
7. Revisión del ISMS por parte de la dirección
8. Mejoras al ISMS
9. Anexo A (normativo): Objetivos de Control y Controles
10. Anexo B (informativo): Principios de la OECD y este estándar Internacional

35 Op. Cit. Alexander, Alberto G. Pág. 22.

11. Anexo C (informativo): Correspondencia entre ISO 9001:2000, ISO 14001:2004 y éste estándar Internacional
12. Bibliografía

En la sección *0. Introducción*, se plantean las generalidades del estándar: se establece que el propósito del documento es proveer un modelo para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la información. Así mismo, se plantea la aproximación basada en procesos como el método que será utilizado a lo largo del documento. En este contexto, se considera que una actividad gestionada y que haga uso de recursos con el fin de habilitar la transformación de entradas en salidas puede considerarse como un proceso.

La sección *1.Alcance*, se destaca que el ISMS está diseñado para asegurar la selección de controles de seguridad adecuados y proporcionados para proteger los activos de información críticos y den confianza a los clientes y otras partes interesadas.[36] También se establece en esta sección la generalidad del estándar y su intención de ser aplicado a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. Es muy importante comentar que en la sección *1.2 Aplicación* se establece que la exclusión de ciertos controles es válida siempre y cuando no se afecte la capacidad y/o la responsabilidad de la organización en relación con la seguridad de la información que maneja. Sin embargo, para declarar que una organización cumple con el estándar, no se pueden excluir las cláusulas de las secciones 4,5,6,7 y 8. Cabe mencionar, que es precisamente a través de estas cláusulas (4, 5,6,7 y 8) que se implementa el ciclo de calidad PDCA; así mismo estas cláusulas persiguen el cumplimiento con los referidos principios de seguridad de la OECD.

En la sección *2. Referencias Normativas*, se hace mención del estándar ISO/IEC 17799 como una guía de implantación que puede utilizarse para el diseño de los controles de seguridad. Este estándar será tratado con cierto detalle en la siguiente sección del presente capítulo.

La sección *3. Términos y Definiciones*, presenta una serie de conceptos ampliamente referidos durante todo el estándar. Para entender los requerimientos que plantea la norma, es necesario conocer los términos y sus definiciones respectivas. El Anexo B lista estos términos.

La sección *4. Sistema de Gestión de Seguridad de la Información*, presenta los requerimientos que deben cumplirse para decir que se cumple con el estándar. De acuerdo con la naturaleza orientada a procesos y con el apego al ciclo Deming, se tiene la siguiente equivalencia para esta sección: (Ver tabla 5)

36 Op. Cit. International Organization for Standardization and International Electrotechnical Commission, Pág. 1.

Modelo ISO/IEC 27001:2005.	
Planear	4.2.1 Establecer y administrar el ISMS Como parte de la fase de planeación, se requiere que la organización: a. Defina el alcance del ISMS b. Defina la política del ISMS c. Defina la aproximación al análisis de riesgos que utilizará la organización d. Identifique los riesgos e. Analice y evalúe los riesgos f. Identifique y evalúe las opciones para tratamiento de riesgos g. Seleccione los objetivos de control y los controles para el tratamiento de riesgos h. Obtenga aprobación por parte de la dirección para los riesgos residuales propuestos i. Obtenga aprobación por parte de la dirección para implantar y operar el ISMS j. Preparar el documento "Declaración de Aplicabilidad"
Hacer	4.2.2 Implantar y operar el ISMS A través de esta cláusula, se puntualizan los requerimientos para la fase "Hacer" del ciclo Deming: formulación del plan para tratamiento de los riesgos, ejecución de dicho plan con el objeto de cumplir con los objetivos de control identificados, implantación de procedimientos y otros controles que sean capaces de establecer una detección oportuna de eventos de seguridad, etc.
Verificar	4.2.3 Supervisar y revisar el ISMS En esta cláusula se hace mención de los requerimientos para establecer un esquema de supervisión que incluya los procedimientos de revisión necesarios y que nos permita detectar errores, brechas de seguridad. Así mismo, se puntualiza sobre la necesidad de llevar a cabo revisiones de la efectividad del ISMS, tomando en cuenta los resultados de auditorías de seguridad, histórico de brechas e incidentes de seguridad, así como sugerencias de las partes involucradas. De igual importancia, esta cláusula establece que se deben establecer un esquema que permita que el análisis de riesgos sea realizado periódicamente en intervalos regulares planeados con antelación.
Actuar	4.2.4 Mantener y mejorar el ISMS Aquí se hace mención de los procedimientos y controles de supervisión que posibiliten la implantación de las mejoras identificadas al ISMS.

Tabla 5: Modelo PDCA y requerimientos de la cláusula 4.

Adicionalmente, en el rubro *4.3 Requerimientos de Documentación* se mencionan los requerimientos documentales y de control de documentos y registros requeridos por el estándar.

La sección *5. Responsabilidades de la Dirección* está dirigida a la gerencia de la organización, a efecto de puntualizar sus responsabilidades en relación con el ISMS. Cabe destacar que la norma es muy clara en este sentido: la dirección debe desempeñar un papel protagónico en el manejo de un ISMS. Especial mención merecen los rubros de provisión y capacitación de recursos que son cubiertos en el rubro *5.1 Administración de recursos.*

En relación con las auditorías a realizar al ISMS, la cláusula *6.0 Auditorías Internas del ISMS,* es muy precisa al especificar que la organización debe realizar auditorías a intervalos planeados, con el fin de determinar si los objetivos, controles, procesos y procedimientos cumplen con los requerimientos planteados por el estándar, así como el cumplimiento con requerimientos adicionales (por ley, por ejemplo) y con las propias necesidades de seguridad de la información, de acuerdo con los resultados del análisis de riesgos. Es importante comentar que

el término *auditoría interna* es manejado de acuerdo con el ISO 9000:2000 (Sistemas para la gestión de la calidad – Fundamentos y vocabulario). Así mismo, es de vital importancia rescatar un principio fundamental para el practicante de la seguridad de la información: ***La selección del cuerpo de auditores y la conducción de la auditoría debe garantizar la imparcialidad del proceso de auditoría. Por este motivo, los auditores no deben revisar su propio trabajo.***

En nuestra experiencia hemos visto equipos de seguridad que se dedican a implementar soluciones (tanto técnicas como normativas) que después son revisadas por el mismo grupo de trabajo, creando así conflicto de intereses. La recomendación que podemos hacer a este respecto, es consolidar un cuerpo de seguridad de la información que sea responsable de integrar y establecer los objetivos de control y controles que sean requeridos – *siempre* de acuerdo con un análisis de riesgos – mismos que deberán ser implantados y/o instrumentados por las áreas responsables de los activos (el área de administración de servidores, o el área de telecomunicaciones, por mencionar un ejemplo). Una vez finalizada la tarea de las respectivas áreas técnico-administrativas, será responsabilidad del grupo de seguridad de la información la tarea de revisar que los controles hayan observado las especificaciones iniciales.

En relación con las revisiones del ISMS, la sección *7. Revisión Gerencial* plantea que la dirección de la organización debe revisar el ISMS de la organización a intervalos planeados, para asegurarse de su continua idoneidad, conveniencia y efectividad. Así mismo, nos da una guía tanto de los insumos que deben presentarse a un comité gerencial que revisará el ISMS como las salidas que se esperan como entregable de la reunión de dicho comité.

Por último, la sección *8. Mejoramiento del ISMS,* nos da pie para el perfeccionamiento del ISMS a lo largo del tiempo. En este sentido, la mejora continua es visualizada como el conjunto de acciones emprendidas por la organización para aumentar la probabilidad de incrementar la satisfacción de las partes interesadas.

2.4 El estándar ISO 27002:2005 (ISO/IEC 17799:2005), "Information technology — Security techniques — Code of practice for information security management"

El Instituto de Estándares Británico (BSI, por sus siglas en inglés), es un proveedor de servicios multinacional cuya principal actividad es la producción de estándares. Fundado desde 1901, y como primera entidad de normalización a nivel mundial, el BSI es responsable de la publicación de importantes normas que han pasado a convertirse actualmente en estándares internacionales. (Ver tabla 6).

Año de publicación	*Publicación*	*Actualmente*
1979	BS 5750	ISO 9001
1992	BS 7750	ISO 14001
1995	BS 7799-2	ISO 27001
1995	BS 7799-1	ISO 17799
1996	BS 8800	OHSAS 18001

Tabla 6: Estándares generados por la BSI.

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa,

británica o no, un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es la guía de buenas prácticas, para la que no se establece un modelo de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (ISMS) para ser certificable por una entidad independiente.

Los objetivos del estándar BS7799-1 son[37]:

- Capacitar a una organización para que implemente de manera apropiada la seguridad de la información.
- Proveer una guía común de mejores prácticas.
- Facilitar el comercio entre compañías, proporcionando confianza en la seguridad de la información compartida
- Brindar a los practicantes de la seguridad de la información un marco de trabajo para desarrollar políticas y procesos de seguridad.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adopta por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. A la fecha de elaborar éste trabajo, la versión reciente del estándar sufrió una actualización, de ser ISO/IEC 17799:2005, se le conoce como ISO 27002:2005, "Tecnología de la Información — Técnicas de Seguridad — Código de práctica para la administración de la seguridad de la información".

Para comprender la funcionalidad del ISO 27002:2005, hemos encontrado muy útil la analogía de pensar en este estándar como un "supermercado de controles de seguridad":[38] Una vez que se cuenta con un sistema de ponderación que nos permita establecer las prioridades de la organización en materia de seguridad, acudimos al ISO/IEC 17799:2005 para identificar e implantar los controles de seguridad que nos permitirán cubrir las necesidades detectadas.

De manera enunciativa, en el Anexo A se listan a los controles de seguridad incluidos en el estándar comentado[39].

Es importante mencionar que el esquema de gestión de la seguridad de la información se consolidará en la medida en que el conjunto de controles, los cuales pueden ser de naturaleza normativa, documental o tecnológica, se implementen tomando en cuenta las necesidades de la organización, los activos de información más importantes y los riesgos que afecten dichos activos.

En nuestra experiencia como practicantes de la seguridad de la información, hemos visto gran número de iniciativas que fracasan debido a que no se toma en cuenta el giro del negocio, o las necesidades reales de la organización. Por este motivo, decidimos incluir un último estándar en esta sección: CobiT.

2.5 Alineando la estrategia de seguridad con los objetivos del Negocio: CobiT 4.0, "Control Objectives for Information and related Technology"

Para muchas empresas, la información y las tecnologías que la soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las necesidades del aseguramiento del valor de las tecnologías de información (TI), la administración de riesgos asociada, así como el incremento de requerimientos para controlar la misma se entienden ahora como elementos clave del *gobierno*[40] de una empresa.

37 Quezada, Cintia. Metodología para la aplicación de la norma ISO/IEC 17799. pág. 8
38 Cfr. Valenzuela, Ismael. Integrating ISO 17799 into your Software Development Lifecycle. (In)secure Magazine. No. 11.
39 International Organization for Standardization and International Electrotechnical Commission, op. cit., pág. 13-35.
40 Del término en inglés governance. Se refiere a la conducción de los asuntos y políticas de una organización.

Más aún, el *gobierno de la TI* integra e institucionaliza las buenas prácticas existentes para garantizar que la infraestructura de una empresa u organización sirve como base a los objetivos del negocio. De esta manera, se facilita que la empresa aproveche al máximo su información [41]

El IT Governance Institute fue establecido por ISACA (Information Systems Audit and Control Association) en 1998 para aclarar y orientar en cuestiones actuales y futuras relativas a la administración, seguridad y aseguramiento TI. Como consecuencia de su rápida difusión internacional, ambas instituciones disponen de una amplia gama de publicaciones y productos diseñados para apoyar una gestión efectiva de las TI en el ámbito de la empresa.

Uno de sus documentos más conocidos, referencia a nivel mundial, es CobiT (Objetivos de control de información y tecnologías relacionadas).

Se trata de un marco compatible con el ISO/IEC 17799:2005 que incorpora aspectos fundamentales de otros estándares relacionados; de tal manera que aquellas empresas y organizaciones que hayan evolucionado según las prácticas señaladas por CobiT están más cerca de adaptarse y lograr la certificación en ISO 27001.

Para que la TI tenga éxito en satisfacer los requerimientos del negocio, CobiT brinda un marco referencial de buenas prácticas, organizadas en dominios y procesos. CobiT se estructura en cuatro partes; la principal de ellas se divide de acuerdo con 34 procesos de TI. Cada proceso se cubre en cuatro secciones (objetivo de control de alto nivel para el proceso, los objetivos de control detallados, directrices de gestión y el modelo de madurez para el objetivo) que dan una visión completa de cómo controlar, gestionar y medir el proceso. Al igual que los estándares que se han revisado en esta sección, CobiT utiliza un ciclo de vida de tipo PDCA que lo integra en los procesos de negocio. (Ver ilustración 9)

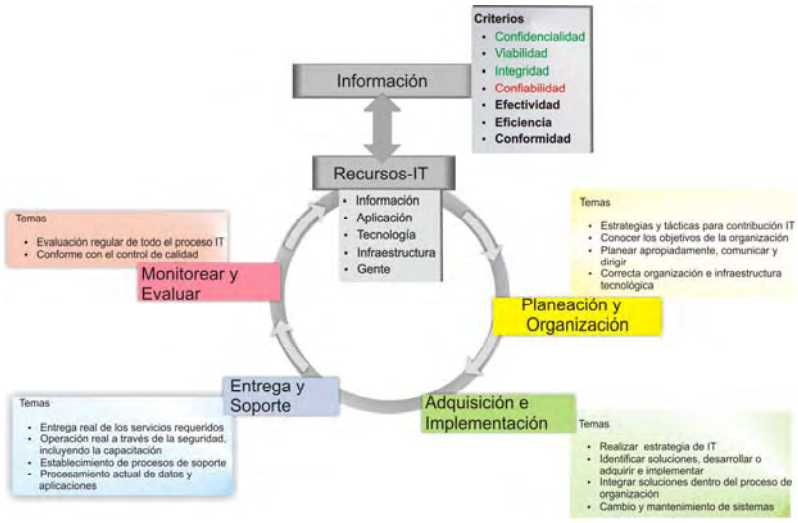


Ilustración 9: Estructura de CobiT.

Con la gran cantidad de estándares, recomendaciones y buenas prácticas que hoy día tratan con los diferentes aspectos de la Tecnología de la Información, hemos encontrado que CobiT juega un papel primordial como elemento integrador de todos estos elementos. Más aún, a partir de la estrategia de gobierno que se plantea, es posible conjuntar los esfuerzos para dirigirlos de manera puntual a cumplir con los objetivos de la empresa u organización.

41 IT Governance Institute, CobiT 4.0., pág. 6

Adicionalmente, hemos encontrado a lo largo de la práctica un gran valor al tomar como referencia este estándar para definir un esquema de niveles de madurez en distintos contextos, así como apoyo primordial para la definición y establecimiento de indicadores de seguridad.

Los nivel de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la información, y va desde un nivel *no existente* (*nivel 0*) hasta un nivel *optimizado* (*nivel 5*). (Ver ilustración 10)

Ilustración 10: Niveles de Madurez en CobiT

Los niveles de madurez están definidos de tal manera que la administración de una empresa reconozca descripciones de estados posibles actuales y futuros, posibilitando así que se entre en un esquema de mejora continua a lo largo del tiempo.

2.6 Conclusiones

La implantación de un sistema de gestión de la seguridad de la información depende en gran medida de la concepción y elaboración de un marco de trabajo que posibilite atacar el problema de una manera sistemática, organizada, que contemple la totalidad del problema y que permita el desprendimiento de métricas e indicadores para medir la eficiencia de la solución que se establezca.

La teoría maneja diferentes tipos de aproximaciones para establecer dicho marco de trabajo: una aproximación basada en un análisis del costo-beneficio que permite establecer un sistema de ponderación del que se desprenderán los criterios para tomar decisiones en relación a la prioridad y alcance del sistema de gestión de la seguridad de la información que se quiere implantar. Un punto a favor de este esquema, radica en que se puede involucrar a la alta dirección de las organizaciones, pues la seguridad de la información se traduce a una gestión de riesgos, disciplina que lleva arraigada mucho tiempo en las empresas. La gran desventaja de esta aproximación es que no da resultados a corto plazo, por lo que se abre una *ventana de exposición a vulnerabilidades* mientras se trabaja en implantar los controles de seguridad que se hayan seleccionado.

Otra aproximación se enfoca principalmente en cerrar las brechas tecnológicas que, de manera apremiante,

hacen vulnerable a la información a partir de la infraestructura tecnológica que la soporta. Este tipo de actividades a corto plazo permiten establecer un nivel *mínimo* de seguridad que, sin embargo, no deja de ser una visión reactiva ante la problemática de la seguridad de la información: cambian las tecnologías y cambian las amenazas, por lo que nuevamente se requiere revisar la estrategia de *línea base* planteada en determinado punto del pasado. Esto hace de esta aproximación una solución poco robusta.

Existe una tercera opción que mezcla las mejores características de las aproximaciones mencionadas con anterioridad: se trata de establecer rápidamente un nivel mínimo de seguridad, que sirva como base para impulsar una estrategia a mediano y largo plazo que se base en los modelos de calidad y mejora continua que son familiares para la mayoría de los corporativos hoy en día.

Es importante resaltar que la seguridad de la información y los procesos de calidad de las empresas llevan mucho en común, por que se considera que un sistema seguro es un sistema que funciona tal y como se espera que funcione. De hecho, encontramos mucho mas valor en integrar una propuesta que abarque controles de seguridad documentales y normativos (procedimientos de control de cambios, procedimientos de generación y verificación de respaldos, políticas de uso aceptable de sistemas internos, etc.) que una propuesta basada puramente en soluciones tecnológicas.

Para auxiliar en el establecimiento del esquema de gestión de la seguridad de la información, se han desarrollado diversos estándares internacionales que nos dicen *qué* se debe hacer. En este capítulo se revisaron muy brevemente las características y estructura de dos publicaciones de la ISO/IEC: ISO/IEC 27001:2005 e ISO/IEC 17799:2005. El primer estándar nos apoya al *traducir* los requerimientos de un sistema de calidad a un esquema de seguridad de la información, dando pie a la supervisión de las actividades mediante el ciclo Deming de calidad.

Una vez establecida la estrategia de protección apegada al ISO/IEC 27001:2005, llega la hora de ejecutar las actividades planeadas. Entra a la escena entonces el ISO/IEC 17799:2005, ya que constituye un “supermercado de los controles de seguridad”. Dado que ya contamos con un alcance claro y bien definido, será muy sencillo seleccionar aquellos controles que apoyen al fortalecimiento de la seguridad dentro de la organización.

CAPÍTULO III

ANÁLISIS DE RIESGOS

Capítulo III. Análisis de Riesgos

"La mentira más común es aquella con la que un hombre se engaña a sí mismo."

Nietzsche.

La seguridad es tanto una realidad como una percepción.[42]

La parte *real* de la seguridad es matemática, basada en la probabilidad de los diferentes riesgos y en la efectividad de las correspondientes salvaguardas. A partir de datos estadísticos e indicadores estratégicos se puede indicar de manera objetiva si una ciudad es más segura que otra, o si existen menos probabilidades de tener un accidente en automóvil o en avión. Si se cuentan con los datos suficientes, no será muy difícil precisar este tipo de información.

La parte subjetiva de la seguridad, por otro lado, tiene que ver con la percepción que las personas tienen en relación a las amenazas y la efectividad de las salvaguardas que se implementen para mitigar dichos riesgos. Tómese por ejemplo, el caso del puente de la bahía de Tay.

En 1878, Thomas Bouch diseñó el entonces más largo puente del mundo en la bahía de Tay en Dundee, Escocia. Bouch utilizó un diseño innovador, mezclado acero económico (*cast iron)* con acero puro. La noche del 28 de Diciembre de 1879, a menos de dos años después de su construcción, el puente colapsó al paso de un ferrocarril con 75 personas a bordo. El accidente fue considerado como la tragedia tecnológica más grande de su época. A raíz de este incidente, otro proyecto que Bouch tenía asignado en la bahía de Forth fue cancelado. (Ver ilustración 11).

Ilustración 11: El desastre del puente de la Bahía de Tay.

A la muerte de Bouch, el plan de construcción de un puente en la bahía Forth fue retomado por John Fowler y Benjamín Baker. Con el recuerdo del desastre todavía presente, los diseñadores no sólo pusieron mayor cantidad de acero en el nuevo puente para hacerlo más seguro, sino que se preocuparon de que el diseño hiciera *parecer* más segura la construcción.[43] Al día de hoy, más de un siglo después el puente de la bahía de Forth es considerado una de las obras más grandes de la ingeniería.

Este caso nos deja dos lecciones para reflexionar. Primero: si un sistema falla, se debe replantear la estrategia e intentar nuevamente con una aproximación más conservadora, sin sacrificar la seguridad en aras de la

42 Schneier, Bruce, The Psychology of Security.
43 *Cfr.* Schneier, Bruce. Practical Cryptography. Pág. 2.

eficiencia[44]. Por otra parte, nos indica que la *percepción* de la seguridad de un sistema es tan importante como la seguridad real que se llegue a implantar en el mismo, y debe ser considerada durante la concepción e implantación del sistema.

Recordemos del capítulo anterior que una de las aproximaciones para atacar el problema de establecer un esquema de protección de la seguridad de la información involucra establecer un esquema de ponderación que nos permita clasificar y dar prioridades a los riesgos y salvaguardas requeridas para administrar aquellos.[45]

La base de este sistema de ponderación, descansa en la creación y consolidación de los *criterios* que nos permitan realizar una buena toma de decisiones en materia de seguridad. Esta no es una actividad nueva, realmente. Tomamos decisiones de seguridad todo el tiempo. Decidimos si cerrar con doble llave la puerta al salir de casa, decidimos la ruta más segura a tomar para llegar al trabajo y decidimos si el artículo que se comprará vía Internet se pagará con cheque o directamente con tarjeta de crédito. Hacemos consideraciones intuitivas de seguridad todo el tiempo[46]. Sin embargo, en muchas de las situaciones que nos presenta la modernidad tecnológica, el mecanismo de percepción de los riesgos *humano* no funciona adecuadamente, llevándonos a tomar decisiones erróneas.

Evaluar y reaccionar ante los riesgos es una de las cosas más importantes que una criatura debe aprender a hacer bien, y dentro del cerebro humano, existe una zona muy primitiva que es la encargada de este trabajo: la amígdala cerebral. [47] (Ver ilustración 12).

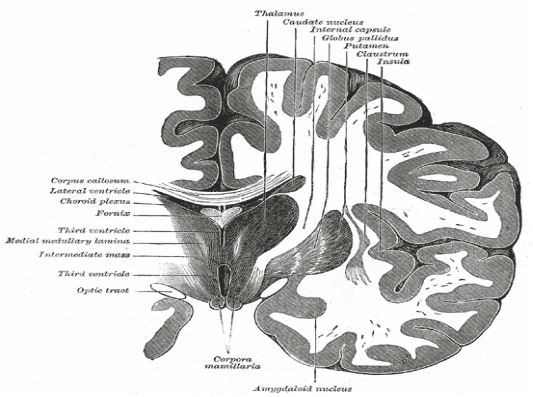


Ilustración 12: Amígdala cerebral.

La amígdala cerebral es responsable de procesar y generar emociones básicas (furia, miedo, etc.) a partir de la información sensorial recibida. Cuando un animal ve, escucha o siente un peligro potencial, la amígdala cerebral reacciona inmediatamente, causando que la adrenalina y otras hormonas sean inyectadas en la sangre. Este mecanismo funciona perfectamente si estamos cazando (o siendo cazados) en la sabana africana. El mundo actual, sin embargo, es más complicado.

Esta realidad neurológica no debe ser tomada a la ligera, porque para el análisis exitoso de problemas complicados, se requiere el uso de la capa más avanzada del cerebro: un área conocida como *neocórtex.* Sin embargo por razones evolutivas, al evaluar riesgos el cerebro toma una *ruta* completamente distinta, actuando por *instinto*.

De acuerdo con Schneier, existen algunos patrones patológicos que surgen de manera continua al realizar un

44 Desafortunadamente, en la industria del software ésta no es una práctica muy común. Si el software falla se entra en una dinámica de instalación de actualizaciones que intentan *parchar* las fallas a medida que se van detectando.

45 *Vid Supra*, pág. 7.

46 *Cfr.* Schneier Bruce, The Psychology of Security.

47 *Idem.*

análisis de riesgos[48]:

- Las personas tendemos a exagerar riesgos espectaculares y a minimizar los riesgos presentes en el día a día
- La personas tenemos problemas al identificar riesgos que se dan en contextos que no son familiares
- Los riesgos *personalizados* se perciben como mayores en comparación a los riesgos *anónimos*
- Las personas tendemos a menospreciar riesgos que deseamos aceptar, y tendemos a sobre estimar riesgos que se dan en situaciones que no controlamos
- Las personas tendemos a sobre estimar los riesgos que son objeto del escrutinio público

Para intentar mitigar esta situación, se requiere estructurar una aproximación sistemática al análisis de riesgos. Así el practicante de la seguridad de la información debe asegurarse de que se tomen en cuenta los siguientes aspectos:

- La severidad del riesgo
- La probabilidad del riesgo
- La magnitud de los costos
- La efectividad de la salvaguarda para mitigar el riesgo
- Cómo comparar riesgos y salvaguardas que son dispares

Si la percepción de cualquiera de estos puntos se aleja de la realidad, la decisión en relación al compromiso costo-beneficio que se tome será incorrecta. Por ejemplo, si se piensa que el riesgo es más grande de lo que realmente es, se perderán recursos (humanos, económicos, etc.) tratando de mitigar un riesgo que no es tan importante. Si, por otro lado, se considera incorrectamente que la efectividad de una salvaguarda no es la adecuada entonces no se aplicará en su momento, dando pie a vulnerabilidades que pueden ser aprovechadas por un atacante en potencia.

Con estos antecedentes como bagaje, podemos decir que la tarea de definir criterios que nos permitan identificar y dar prioridades los riesgos de una manera objetiva, sistemática, con resultados que se puedan repetir y medir, se antoja como un problema que por sí mismo, tiene una magnitud similar a la de establecer un esquema de gestión para la seguridad de la información.

Creemos que, en gran medida, así es. De hecho, estamos convencidos de que la piedra angular para establecer una estrategia de calidad, radica precisamente en un exitoso análisis de riesgos. A continuación, presentaremos una metodología que nos sirve para atacar el problema de establecer la estrategia de protección que se comenta, en el contexto de seguridad de la información.

3.1. Una propuesta para ejecutar análisis de riesgos: el método OCTAVE

Para contar con un marco de referencia probado y aceptado por la industria, el análisis de riesgos a comentar se basará en la metodología que propone el Instituto de Ingeniería de Software (SEI, por sus siglas en inglés) de la Universidad de Carneige Mellon, llamado: Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). OCTAVE es una técnica de planeación y evaluación estratégica de riesgos de seguridad; constituye además una evaluación flexible que permite ser adaptada por la mayoría de las organizaciones.

Aunque los sistemas de información se han vuelto esenciales para la operación eficiente de las organizaciones, las estrategias de protección que existen hoy día están enfocadas solamente a las vulnerabilidades de la infraestructura tecnológica; omitiendo establecer previamente el efecto de un incidente de seguridad sobre los *activos* de información que son más importantes para las empresas y organizaciones. (Ver ilustración 13).

48 Schneier, Bruce. Beyond Fear. p.40-41

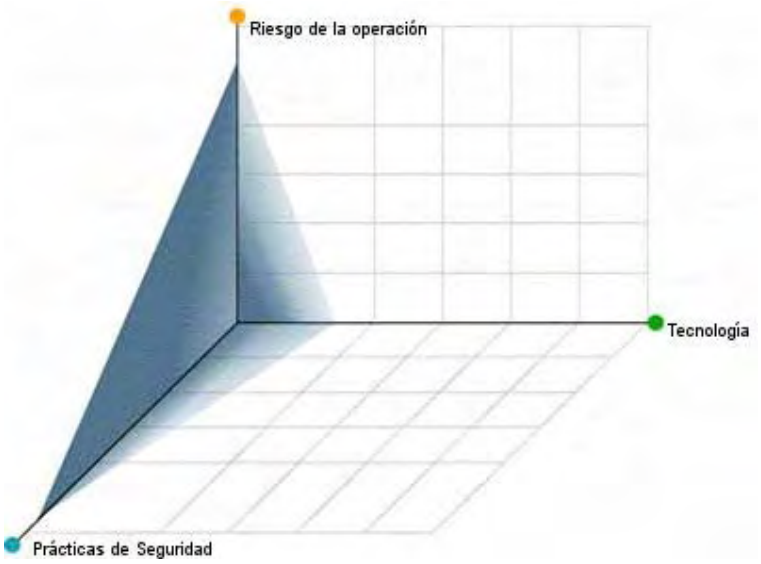


Ilustración 13: Las dimensiones del riesgo de acuerdo con OCTAVE.

Esto ha llevado a una situación en la que existe una brecha entre los requerimientos de seguridad reales de las organizaciones y los requerimientos de seguridad de Tecnología de la Información. La estrategia actual de análisis de riesgos es pues incompleta si no se está incluyendo la totalidad de los componentes al realizar el análisis: activos, amenazas y vulnerabilidades.[49]

Al gestionar el riesgo, el primer paso es entender cuáles son los riesgos existentes. Una vez que se han identificado dichos riesgos, se procede con el diseño de una estrategia de mitigación. El método OCTAVE nos permitirá elaborar una estrategia de administración de riesgos de esta naturaleza.

Cabe mencionar en este punto que OCTAVE es una aproximación a la evaluación de riesgo integral, sistemática, dependiente del contexto y auto-implementada. El método está sustentado en un conjunto de parámetros que definen los elementos de una evaluación del riesgo orientado a los activos.

El método OCTAVE requiere que la evaluación sea conducida y llevada a cabo por un grupo de análisis interdisciplinario, que incluya tanto al personal de las áreas operacionales de las organizaciones como a personal de las unidades de tecnología de la información. Los miembros del equipo deben trabajar juntos para tomar decisiones basadas en los riesgos asociados a los activos críticos de información que se identifiquen.

Así mismo, el método OCTAVE requiere de catálogos de información para medir las prácticas de la organización relativas a la seguridad de la información, análisis de amenaza y para la construcción de estrategias de protección. Estos catálogos son:

2 Catálogo de prácticas: Colección de prácticas de seguridad estratégicas y operacionales

- Perfil genérico de amenazas: Colección de las mayores fuentes de amenaza

k. Catálogo de Vulnerabilidades: Colección de vulnerabilidades basadas en la plataforma y la aplicación en ejecución

Constituido por tres fases que permiten examinar tanto los puntos operacionales de las organizaciones como los puntos tecnológicos de la infraestructura de información, OCTAVE ayuda a ensamblar un panorama integral

49 http://www.cert.org/octave

de las necesidades de seguridad de la información de la empresa.

El método consta de talleres de trabajo en donde se fomenta la discusión abierta y el intercambio de información acerca de los activos, las prácticas de seguridad y las posibles estrategias. De esta manera, se busca atacar la percepción subjetiva que cada uno de los participantes puedan tener acerca de los riesgos y sus prioridades relativas. (Ver ilustración 14).

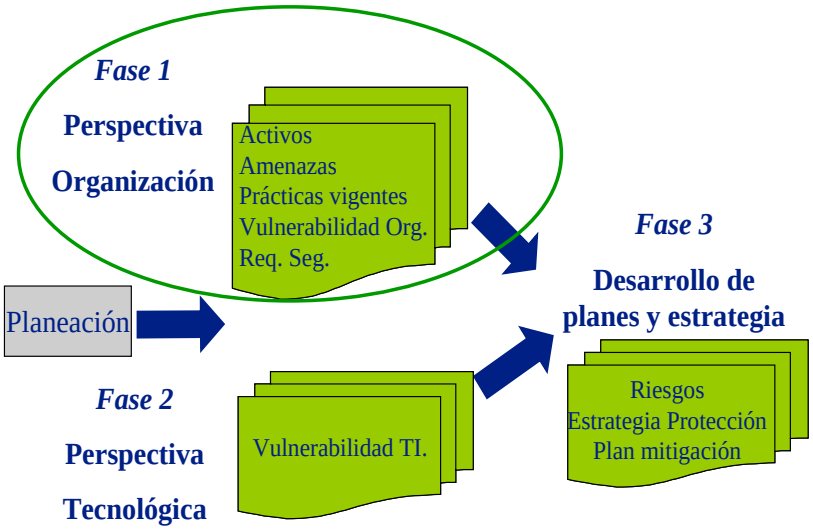


Ilustración 14: Proceso OCTAVE.

A continuación se describen estas tres fases y sus procesos correspondientes:

Fase 1: Construcción de perfiles de amenaza basados en los activos. Consiste en una evaluación de la organización. Un equipo de análisis determinará cuáles son los activos críticos para la organización e identificará las actividades que se llevan a cabo para proteger esos activos. Los procesos de la Fase 1 son:

> Proceso 1: Identificar el conocimiento de la alta dirección – Los directores seleccionados identificarán los activos importantes, las amenazas relacionadas, los requerimientos de seguridad, prácticas de seguridad que se llevan a cabo actualmente y vulnerabilidades de la organización.
>
> Proceso 2: Identificar el conocimiento de los administradores de las áreas operacionales – Los administradores de las áreas operacionales identificarán los activos importantes, las amenazas relacionadas, los requerimientos de seguridad, prácticas de seguridad que se llevan a cabo actualmente y vulnerabilidades de la organización.
>
> Proceso 3: Identificar el conocimiento del personal operativo – Los miembros seleccionados de las áreas operativos (áreas de operación y áreas de TI) identificarán los activos importantes, las amenazas relacionadas, los requerimientos de seguridad, prácticas de seguridad que se llevan a cabo actualmente y vulnerabilidades de la organización.
>
> Proceso 4: Creación de los perfiles de amenaza – El equipo de análisis consolidará la información recopilada en los procesos 1 a 3, seleccionan los activos críticos, refinan los requerimientos de seguridad asociados e identifican las amenazas a esos activos, creando los perfiles de amenaza.

Fase 2: Identificar las vulnerabilidades de la infraestructura – Esta es una evaluación de la infraestructura de comunicación. El equipo de análisis examina los componentes clave en busca de vulnerabilidades tecnológicas que puedan derivar en acciones no autorizadas en detrimento de los activos críticos. Los procesos

de la Fase 2 son:

Proceso 5: Identificación de los componentes clave – El equipo de análisis identifica los sistemas y componentes clave para cada activo crítico. Los componentes específicos son seleccionados para evaluación.

Proceso 6: Evaluación de los componentes seleccionados – El equipo de análisis examina los componentes clave en busca de vulnerabilidades tecnológicas. Durante esta fase se utilizan herramientas de escaneo de vulnerabilidades. Los resultados son examinados y consolidados, basando el análisis en la relevancia para los activos críticos y los perfiles de amenaza.

Fase 3: Desarrollo de estrategia y plan de seguridad – Durante esta etapa de la evaluación, el equipo de análisis identifica los riesgos asociados a los activos críticos y decide qué hacer para mitigarlos. Los procesos de la Fase 3 son:

Proceso 7: Conducir el Análisis de Riesgos – El equipo de análisis identifica el impacto de las amenazas sobre los activos críticos, define el criterio para evaluar los riesgos identificados y evalúa los impactos con base en los criterios definidos. La información obtenida se plasma en un perfil de riesgo para cada activo crítico.

Proceso 8: Desarrollo de una estrategia de protección – El equipo de análisis crea una estrategia de protección para la organización y planes de mitigación para los activos críticos, basados en el análisis de la información recopilada. La alta dirección revisa, refina y aprueba la estrategia y los planes.

Para integrar una evaluación exitosa, se requiere considerar los siguientes puntos fundamentales:

- Obtener el patrocinio de la alta dirección – Este es el factor más importante para lograr una evaluación exitosa. Si la dirección apoya el proceso, las personas pertenecientes al área participarán de manera activa.
- Seleccionar al equipo de análisis – Los miembros del equipo de análisis requieren tener las habilidades suficientes para dirigir la evaluación.
- Alcance de OCTAVE – La evaluación debe incluir las áreas operacionales que se consideren más importantes. Si el alcance es muy amplio, será muy difícil analizar toda la información. Si el alcance se queda corto, no se tendrán resultados significativos.
- Selección de los participantes – Se requiere que miembros de múltiples áreas de la institución contribuyan con su conocimiento y punto de vista. Es importante que estas personas entiendan el funcionamiento de su propia área.

Cabe señalar, para finalizar con la presentación de la metodología, que los riesgos son evaluados para proveer información adicional para ayudar a las personas responsables con la toma de decisiones. Una organización no puede mitigar cada riesgo debido a los costos, el personal y las restricciones que enfrenta durante su operación. Por lo tanto, es necesario determinar las respectivas prioridades.

En muchos procesos de administración de riesgos, tanto el impacto como la probabilidad son evaluados como un medio para determinar qué riesgos tratar primero .Considérese un ejemplo simple. Un director puede decidir tratar solamente los riesgos con alto-impacto, alta-probabilidad de riesgos; tener vigilados a los riesgos con mediano-impacto, mediana-probabilidad de riesgos; e ignorar los riesgos con bajo-impacto y con baja-probabilidad de riesgos. Por lo tanto, el director está usando el impacto y la probabilidad para guiar sus elecciones.

Para los riesgos de seguridad de la información, la probabilidad es una variable más complicada e imprecisa de lo que normalmente es encontrada en otros dominios de administración de riesgos. Es irrazonable, por ejemplo, intentar calcular la probabilidad de un adolescente desconocido de un país desconocido con las motivaciones desconocidas llevando a cabo un escaneo de puerto sobre su servidor y encontrando un camino. Incluso si la probabilidad pudiera ser calculada, cambiaría minuto a minuto basado en numerosos factores. Por esta razón en OCTAVE, solamente se evalúa el impacto de un riesgo.

3.2. Estrategias posibles para el tratamiento del riesgo

Es muy conveniente que a lo largo de la consolidación y ejecución del análisis de riesgos, el practicante de la seguridad de la información tenga en mente el posible tratamiento que se dará a los riesgos una vez que sean identificados. Se optará por una de las siguientes alternativas: mitigación del riesgo, aceptación del riesgo, transferencia del riesgo o evitar el riesgo. Incluso después de realizar la selección de los controles que ayuden a combatir el riesgo, en algunas ocasiones no será posible eliminar las situaciones potencialmente indeseables totalmente. En estos casos, se tratará el concepto de riesgo residual.

Mitigación del riesgo

Supongamos que como resultado del análisis de riesgo, se identifica que una organización que posee un sitio de comercio electrónico está expuesta a las amenazas más severas como resultado de basar su infraestructura en un sistema operativo que es blanco frecuente de los hackers. El grupo de seguridad de la información ha recomendado que la infraestructura sea migrada para que haga uso de un sistema operativo más conservador y seguro. Sin embargo, la gerencia de la compañía de nuestro ejemplo no está en posibilidades de realizar un cambio de tamaño magnitud en el corto o mediano plazo. ¿Qué hacer?

Para todas aquellas situaciones en que se decida que no es posible eliminar el riesgo en su totalidad, se puede trabajar la alternativa de mitigación del mismo. En este caso, se deben condensar un nivel que se defina con aceptable e implantar los controles apropiados en consecuencia. Los controles pueden reducir el riesgo estimado de la siguiente manera:

- Reduciendo la posibilidad de que una vulnerabilidad sea explotada por una amenaza
- Reduciendo el posible impacto si el riesgo se materializa, detectando de manera oportuna la ocurrencia de un evento no deseado, reaccionando y recuperándose en el tiempo que se haya establecido como aceptable.

Es tarea de la organización adoptar la postura que le sea conveniente, de acuerdo con los requerimientos del negocio, el ambiente y las circunstancias en las que la organización opera de manera cotidiana.[50]

Aceptación del riesgo

Siguiendo con el caso hipotético del sitio de comercio electrónico, podemos suponer que la gerencia de la organización, decide que los fondos requeridos para tomar una postura de mitigación del riesgo tampoco estarán disponibles a corto o mediano plazo.

Muchas veces se presenta la situación en la cual una organización no encuentra controles para mitigar el riesgo, debido a que el costo que representa el establecimiento de los mismos supera con mucho el costo derivado de la materialización de un riesgo. En estas circunstancias, la decisión de aceptar el riesgo y vivir con las consecuencias es la más adecuada. Es importante recalcar que cuando se toma una decisión de esta índole, se deben documentar de manera detallada, así como definir de manera precisa el criterio de aceptación del riesgo.

Adicionalmente, aconsejamos que una persona con la jerarquía suficiente se responsabilice por la toma de la decisión. De esta manera, el equipo de seguridad de la información garantiza que la decisión se tome de manera *realmente* objetiva, y no por ser la solución más sencilla o la que menos trabajo implica.

Transferencia del riesgo

Estamos convencidos de que la pobre situación en materia de seguridad de la información en la llamada *era de Internet* puede achacarse en gran medida a las malas prácticas que históricamente han venido realizando los

[50] *Op. Cit.* Alexader, Alberto G. Pág. 56

fabricantes de software. Basta con revisar las licencias de los programas en boga, para darse cuenta que la responsabilidad que los programadores asumen es siempre la mínima posible.

Así mismo, creemos que un catalizador que ayudará en años venideros a resolver esta situación tiene que ver con el manejo de riesgos mediante la transferencia de los mismos. El razonamiento que nos ha llevado a esta conclusión tiene el siguiente tenor: considérese que nuestra organización ficticia está expuesta a una miríada de virus y gusanos informáticos debido a que el fabricante del sistema operativo está mas interesado en la apariencia gráfica y en la facilidad de uso de su sistema operativo que en construir software seguro. A partir de un concienzudo análisis de riesgos, el equipo de seguridad de la información recomienda que se defina una estrategia para tratar esta situación.

Durante el proceso de la toma de decisión, una de las grandes compañías aseguradoras a nivel mundial hace llegar información a la gerencia de nuestra organización ficticia sobre un nuevo seguro contra virus informáticos. Si se adquiere esta póliza contra virus informáticos, en caso de presentarse un incidente de infección la compañía aseguradora asumirá un porcentaje de la pérdida, mismo que será compensado a la feliz poseedora de dicho seguro. Pues bien, nuestra gerencia programa una reunión con el representante de la aseguradora sólo para enterarse de que el costo anual de la póliza depende en gran medida del sistema operativo que se esté utilizando. Desafortunadamente para nuestro caso, el uso de un sistema operativo que no tiene dentro de sus prioridades el diseño de una estrategia de seguridad robusto eleva demasiado el costo de la póliza.

A partir de este momento, la selección de una versión de sistema operativo tendrá repercusiones que las directivas de las organizaciones a nivel mundial entienden perfectamente. En este escenario, creemos que las empresas que apuesten por la funcionalidad sobre la seguridad, tendrán una vida bien corta.

La transferencia de riesgos, es pues, una opción cuando para la compañía es difícil reducir o controlar el riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante estas circunstancias.

Existe una serie de mecanismos para transferir los riesgos a otra organización; como en el ejemplo citado, se puede utilizar una aseguradora. Otra opción es la *tercerización (outsourcing)* para manejar activos o procesos críticos, en la medida en que tengan la capacidad de hacerlo.

Evitar el riesgo

Al seleccionar la estrategia de evitar el riesgo, entendemos que las acciones están orientadas a cambiar las actividades o la manera de desempeñar una actividad en particular, para así evitar la presencia del riesgo. El riesgo puede evitarse por medio de:

- No desarrollar ciertas actividades comerciales (por ejemplo, la no utilización de Internet)
- Mover los activos amenazados a un área libre de riesgo (por ejemplo, mover el centro de cómputo a una zona libre de huracanes)
- Decidir no procesar información especialmente sensitiva

Como puede apreciarse, la estrategia de evitar el riesgo debe sopesarse contra las necesidades financieras y comerciales. Puede ser que evitar el riesgo coloque en una posición de desventaja a una organización frente a sus competidores, por ejemplo.

Riesgo residual

Después de implantar las decisiones relacionadas con el tratamiento del riesgo, por lo general encontraremos remanentes del mismo. Justamente ese riesgo que se queda después de llevar a cabo un plan de protección de la información se denomina *riesgo residual*.

Si el riesgo residual se considera inaceptable, deben tomarse decisiones para atacarlo. Una opción es identificar diferentes aproximaciones, o seleccionar otro grupo de controles de seguridad. A veces, reducir los riesgos a un nivel aceptable pudiera no ser posible o financieramente aceptable.

En cualquier caso, la gerencia de la organización debe ser informada siempre del riesgo residual. Y no sólo eso. Se debe contar con la aceptación documentada de los riesgos residuales por parte de la dirección antes de comenzar a implantar una estrategia de protección.

3.3. Conclusiones

Se mencionó ya que la seguridad de un sistema debe considerarse desde todas sus aristas para tener la posibilidad de plantear una estrategia de protección que sea *realmente* efectiva.[51] Y esto no excluye la consideración de las personas como parte de dicho sistema. De hecho, la mayor parte de las intrusiones de seguridad involucran al componente humano, por que muchas veces representan el eslabón más débil del sistema. Las personas, pues, no deben ser nunca relegadas en aras de panaceas tecnológicas que prometen la solución total en materia de seguridad de la información.

Durante el análisis de riesgos, se hace más patente que nunca este hecho. Porque la evolución del ser humano no nos ha preparado para lidiar con las situaciones que las amenazas modernas representan, se debe contar con una aproximación estructurada al análisis de riesgos que permita minimizar las deficiencias que nos son inherentes y poder identificar de manera efectiva los activos, amenazas e impactos que se ciernen sobre nuestro sistema.

En el presente capítulo, se propone estructurar un análisis de riesgos basado en dinámicas grupales, en contraste con aproximaciones al análisis de riesgos que utilizan herramientas para automatizar el proceso. Basada en una metodología desarrollada por el Carnegie Mellon, se planteó una propuesta de trabajo que tiene como objetivo:

- Integrar una estrategia de protección que permita la visualización oportuna de los problemas potenciales, para poder estructurar de manera anticipada las defensas que se requieran.
- Considerar la seguridad de una organización como un problema interdisciplinario, involucrando a los empleados de las áreas involucradas en todos los niveles.
- Consolidar una estructura *interna* para el análisis de riesgos que permita a la organización adaptarse y responder rápidamente a los cambios en la tecnología y a las necesidades de seguridad.
- Iniciar un esfuerzo continuo y sustentable que permita a una organización mantener y mejorar su postura en relación a la seguridad de la información.

De esta manera, contamos con una sólida base sobre la cual se puede comenzar con la estructuración de una estrategia de protección que cumpla con las características que se han destacado a lo largo del presente trabajo.

51 *Vid. Supra.*, Pág.7.

CAPÍTULO IV

UN CASO PRÁCTICO

Capítulo IV. Un caso práctico.

"La práctica hace al maestro"
Anónimo.

En los capítulos anteriores se ha presentado la naturaleza de un Sistema de Gestión de Seguridad de la Información; a continuación se muestra una propuesta de los pasos para llevar a cabo la implantación de dicho sistema en una organización ficticia.

4.1. Metodología propuesta

Unas palabras de advertencia: la implantación de un modelo de seguridad de la naturaleza que se va a proponer, altera el *status quo* y por lo tanto, de manera natural, desarrollará rechazo al cambio. Así pues, antes de comenzar con la revisión de la metodología, es requisito fundamental la participación activa de la alta gerencia, cuyo apoyo y papel protagónico será clave para llevar a cabo de manera exitosa la implantación del SGSI.

De acuerdo con Alexander Alberto[52], en la tabla 7 se presenta el ciclo metodológico para implantar un SGSI basado en el modelo que presenta el ISO/IEC 27001:2005. Si se cumple a cabalidad con los pasos que se muestran, se es susceptible a ser auditado y certificado de acuerdo con el ISO/IEC 27001:2005. Cabe mencionar que la tabla 7 que se muestran a continuación, servirá solamente como referencia para enmarcar la propuesta – mucho más breve - que es objeto de esta tesis.

FASES	ACTIVIDADES
I. Entendimiento de los requerimientos del modelo	1. Taller con varios niveles estratégicos y tácticos
II. Determinación del alcance	2. Etapa estratégica
	3. Etapa táctica
III. Análisis y evaluación del riesgo	4. Realización del análisis y evaluación del riesgo
	5. Definición de política de seguridad y objetivos
	6. Evaluación de las opciones para el tratamiento del riesgo
	7. Selección de controles y objetivos de control
	8. Elaboración de la declaración de aplicabilidad
IV. Elaboración del plan de continuidad del negocio	9. Realizar el Análisis de Impacto al negocio
	10. Efectuar el análisis de riesgo e identificar escenarios de amenaza
	11. Elaborar estrategias de continuidad

[52] *Op. Cit.*, Alexander, Alberto G.

	12. Diseñar el plan de reanudación de operaciones
	13. Diseñar procesos de ensayos
V. Implantar y operar el SGSI	14. Elaborar el plan de tratamiento del riesgo
	15. Determinar la efectividad de los controles y las métricas
VI. Supervisar y Operar el SGSI	16. Detección de incidentes y eventos de seguridad
	17. Realización de revisiones periódicas al SGSI
VII. Mantener y mejorar el SGSI	18. Implantar las acciones correctivas y preventivas
VIII. Desarrollo de competencias organizacionales	19. Entrenamiento en documentación del SGSI
	20. Entrenamiento en manejo de la acción correctiva y preventiva
	21. Entrenamiento en el manejo de la auditoria interna
IX. Redacción del Manual de Seguridad de Información	22. Redacción del Manual de Seguridad de Información
X. Ejecución de las auditorias internas	23. Realización de las auditorias internas
XI. Obtención de la Certificación Internacional	24. Búsqueda de la empresa certificadora
	25. Realización de la auditoria por parte de la empresa certificadora
	26. Obtención de la certificación

Tabla 7 Metodología para implantar el SGSI ISO/IEC 27001:2005

Enmarcados en esta metodología general, presentamos a continuación los pasos que se detallarán en el resto de este trabajo. Ver la tabla 8.

FASES	ACTIVIDADES
I. Desarrollo del Análisis de Riesgos	1. Construcción de los perfiles de amenaza
	2. Identificación de Vulnerabilidades a la Infraestructura
	3. Desarrollo de la Estrategia y Planes de Seguridad
II. Identificación y selección de los controles de seguridad utilizando el ISO/IEC 17799:2005	4. Selección de controles y objetivos de control
	5. Elaboración de la declaración de aplicabilidad
III. Desarrollo de los controles de seguridad seleccionados	6. Diseño de los controles de seguridad
	7. Desarrollo de los controles de seguridad

Tabla 8 Metodología propuesta

Aunque mucho más escueta que una metodología que contempla incluso la certificación del SGSI, consideramos que las actividades que comprenden nuestra propuesta cumplen la esencia de las fases del ciclo Deming, de acuerdo con la tabla 9:

FASES DEL CICLO DEMING	FASES DE LA METODOLOGÌA PROPUESTA
Planeación: • Determinar el alcance del modelo • Identificar los activos de información • Realizar el análisis y la evaluación del riesgo	Desarrollo del análisis de riesgos: ✓ Identifica los activos de información ✓ Realiza el análisis y evaluación de riesgos
Implantación: • Elaborar el plan del tratamiento del riesgo	Desarrollo del análisis de riesgos: ✓ Elabora el plan de tratamiento del riesgo
Monitoreo y revisión: • Establecer los procedimientos y rutinas para revisar el desempeño del SGSI	Identificación y selección de los controles de seguridad utilizando el ISO/IEC 17799:2005 ✓ Selección de controles y objetivos de control
Mejora Continua: • Reaccionar a los incidentes de seguridad y tomas las acciones preventivas	Desarrollo de los controles de seguridad seleccionados ✓ Diseño de los controles de seguridad ✓ Desarrollo de los sistemas de seguridad

Tabla 9 Alineación de la Metodología propuesta con el Ciclo Deming

Es importante señalar, que a efectos de hacer práctica la propuesta, no estamos incluyendo aspectos para determinar el alcance del modelo, como pueden ser la identificación de los riesgos principales de un proyecto, identificación de funciones del negocio, etcétera. Todos estos dominios son parte de estándares de planeación de proyectos.

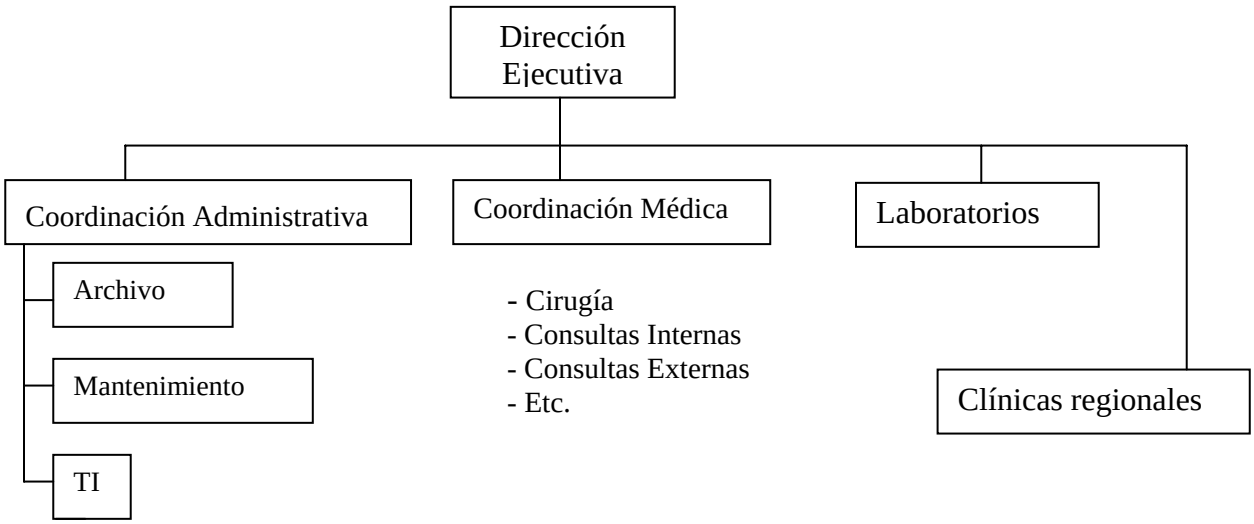
4.2. Introducción al escenario ejemplo.

Para ejemplificar los conceptos que se han venido manejando en los capítulos anteriores, haremos uso de una organización médica ficticia, llamada MedSite[53].

Las instalaciones de tratamiento de MedSite constan de un hospital central con laboratorios y clínicas regionales, estas últimas distribuidas en locaciones a lo largo de todo el país.

Entre las principales áreas de operación de MedSite encontramos:

- Un cuerpo de personal administrativo permanente
- Personal médico, con carácter personal y permanente, incluyendo doctores, enfermeras y cirujanos.
- Un pequeño departamento de tecnología de la información, responsable de la operación y mantenimiento del equipo de cómputo y la infraestructura de comunicaciones, así como prestar servicios de Mesa de Ayuda.



Uno de los principales sistemas de información es el Sistema de Manejo de Datos de los Pacientes (SMDP), por sus siglas). El SMDP incluye los dispositivos de red, equipos personales de cómputo y aplicativos requeridos para vincular e integrar un conjunto de pequeñas bases de datos legadas, que incluyen tratamiento de los pacientes, resultados de laboratorio e información para realizar el cobro de los tratamientos. La información sobre los pacientes puede introducirse directamente en alguna de las bases de datos desde cualquier estación de trabajo. Las personas que ingresan la información son técnicos del laboratorio, personal del cuerpo de enfermería y doctores. Las estaciones de trabajo se localizan en las áreas de oficina, estaciones de enfermería, laboratorios y oficinas administrativas. Actualmente se está permitiendo el ingreso de equipos personales de cómputo móviles (laptop) y asistentes personales digitales. El desarrollo del SMDP fue realizado por un tercero, “Sistemas ABC”. El hospital cuenta con un pequeño equipo de TI que provee soporte a los usuarios del sistema y lleva a cabo rutinas básicas de mantenimiento para el hospital, las clínicas regionales y los laboratorios. El personal de TI interno cuenta con un entrenamiento básico en el uso del SMDP por parte de “Sistemas ABC”.

[53] http://www.cert.org/octave/

Se muestra a continuación el diagrama topológico de nuestra organización ejemplo; ver Ilustración 15:

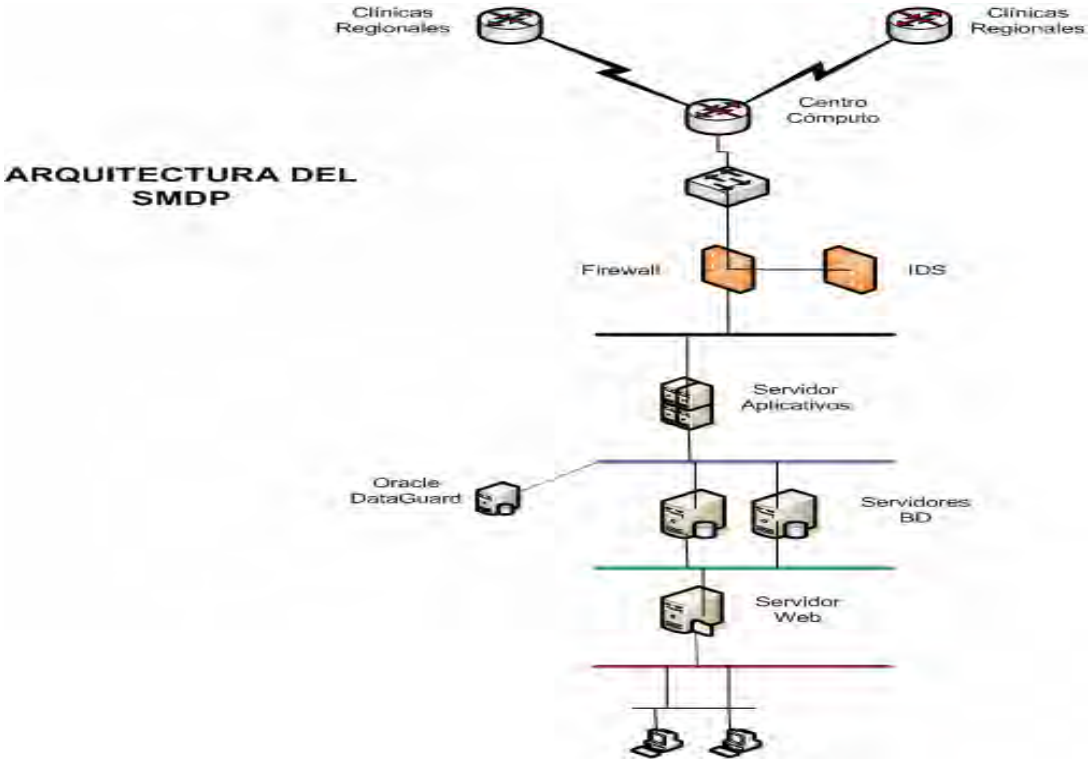


Ilustración 15 Arquitectura del SMDP

4.3. Fase I: Desarrollo del Análisis de Riesgos.

Como ya hemos mencionado, para que un programa de seguridad de la información sea exitoso debe basarse en un análisis de riesgos que nos permita identificar los procesos críticos de la organización, la tecnología que soporta a dichos procesos, las principales amenazas que los asechan, las vulnerabilidades técnicas y administrativas de los activos críticos y el impacto que causaría en caso de ocurrir algún evento no deseado. Con la obtención de la información anteriormente descrita, se puede generar un esquema que nos permita ponderar los riesgos y las salvaguardas correspondientes, lo que a su vez dará pie a la estrategia de seguridad para hacer frente a dichos riesgos identificados.

Para el proyecto de seguridad informática que se llevará a cabo en MedSite, se ejecutará un análisis de riesgos que nos permita identificar los escenarios de amenaza más probables y las vulnerabilidades relacionadas.

El método a seguir para el análisis de riegos se visualizó bajo los requerimientos específicos, prácticas exitosas de la organización, regulación existente en relación al manejo de datos de pacientes y la infraestructura tecnológica previamente diseñada para soportar los sistemas de MedSite. Así mismo, se tomó como base que la infraestructura tecnológica y las prácticas administrativas de seguridad tendrán que ser desarrolladas en caso de que no se encuentran implantadas como parte de la operación cotidiana de la organización.

Se definió además que el éxito de la organización consiste en operar de manera íntegra, confiable y continua durante las 24 horas los 365 días del año.

El análisis de riesgos se enfocó en identificar las amenazas y crear escenarios de intrusión que asecharán al Sistema de Manejo de Datos de los Pacientes (SMDP) en toda la infraestructura que lo soportará, y por consiguiente se identificarán aquellos controles que se tendrán que desarrollar e implementar para que minimicen la probabilidad de que dichas amenazas se materialicen.

Utilizando los criterios de cada una de las Fases de la metodología Octave y la información recolectada se muestran los resultados del análisis a continuación:

Actividad 1: Construcción de los perfiles de amenaza

Para el caso de MedSite el proceso crítico que la organización desea fortalecer de manera puntual es propiamente el Sistema de Manejo de Datos de los Pacientes (SMDP). Por esta razón no se hizo necesario realizar formalmente las actividades propias de la identificación y clasificación de los procesos críticos de la organización. Sin embargo, se recolectó toda aquella información relacionada con dicho proceso tal como posibles requerimientos de regulación, entradas y salidas de información del proceso, diagramas de la infraestructura tecnológica, gente involucrada en todo el proceso, tiempos en que la organización dará el servicio, ubicación física del centro de cómputo, etc.

Con dicha información fue posible identificar los requerimientos de seguridad del SMDP y construir los escenarios de amenazas y de riesgo en la infraestructura tecnológica.

Activos Críticos

La metodología OCTAVE específica que un activo es algo que tiene valor para la organización y es importante para lograr su misión, dichos activos son clasificados de la siguiente forma:

- Información. – información documentada (electrónica o en papel) o activos intelectuales utilizados para cumplir con la misión de la organización.
- Sistemas. – sistema que procesa y almacena información. Los sistemas son una combinación de software, hardware e información.
- Software. – aplicaciones de software (sistemas operativos, aplicaciones de bases de datos, software de red, aplicaciones de oficina, aplicaciones personalizadas, entre otras).
- Hardware. – dispositivos tecnológicos físicos (servidores, estaciones de trabajo, etc.)
- Gente. – gente de la organización, incluyendo sus habilidades, conocimiento, entrenamiento y experiencia.

Para el caso particular del MedSite se ha identificado de inicio el Sistema de Manejo de Datos de los Pacientes (SMDP) como activo crítico , el cual es una combinación de software, hardware e información de acuerdo con lo que define OCTAVE. Ver tabla 10.

Información del Activo Crítico	
Activo	Sistema de Manejo de Datos de los Pacientes (SMDP)
Razón de ser activo crítico	El departamento de tecnologías de información es responsable de mantener el SMDP en buen estado y disponible. La Coordinación Médica es el propietario de la información del SMDP. El personal médico requiere la información proporcionada por el SMDP para brindar tratamiento y medicamentos correctamente. Las áreas administrativas también requieren de información del SMDP para llevar a cabo sus tareas. El SMDP se utiliza para dar información estadística a los proveedores de medicamentos y durante la atención de emergencias. .

Tabla 10: Activos críticos para el Hospital.

Requerimientos de Seguridad

Los requerimientos de seguridad delinean las cualidades del activo que se pretende proteger, además de ser un insumo muy importante para la creación de la estrategia de seguridad a seguir, ya que se especifica la importancia de cada servicio de seguridad. A continuación se muestran los requerimientos de seguridad del sistema SMDP. Ver tabla 11.

Servicios de seguridad	**Prioridad**	**Requerimientos Específicos**
DISPONIBILIDAD	ALTA	Se determinó que el sistema SMDP requiere estar disponible sin interrupción las 24 horas del día durante los 365 días del año. La disponibilidad abarca todos los dispositivos tecnológicos relacionados al sistema SMDP.
INTEGRIDAD	ALTA	El SMDP necesita ser altamente íntegro, ningún usuario interno y/o externo no autorizado debe alterar los datos. La integridad de los datos se debe considerar desde su captura hasta su uso por parte del personal médico.
AUTENTICIDAD	ALTA	Este es un servicio de seguridad altamente importante ya que se procesarán datos confidenciales de índole personal, por lo cual es necesario contar con la garantía de que provienen de fuentes legítimas, evitando así diagnósticos erróneos. En este sentido es necesaria la autenticidad del origen de los datos.

Tabla 11: Requerimientos de Seguridad identificados

Amenazas al SMDP

Este proceso dentro de la metodología OCTAVE especifica que se debe identificar cuáles son las amenazas a las que los activos críticos están sujetos, recordando que una amenaza es un evento que puede causar un efecto no deseado en la infraestructura crítica que se ha identificado previamente. La siguiente lista de amenazas son las que OCTAVE reconoce como las principales fuentes de amenaza:

- Acciones deliberadas por el personal.- esta fuente de amenaza incluye a personal tanto interno como externo del hospital, quienes pueden tomar acciones en contra de los activos críticos.

- Acciones accidentales por el personal.- esta fuente de amenaza incluye a personal tanto interno como externo del hospital, quienes pueden dañar accidentalmente los activos críticos.

- Problemas de Sistemas.- esta fuente de amenaza son problemas con la tecnología de información, por ejemplo: defectos de hardware, defectos de software, no disponibilidad de los componentes, virus, código malicioso, y otros tipos de problemas de sistemas.

- Otros problemas.- esta fuente de amenaza son los problemas que están fuera del control del hospital, por ejemplo: desastres naturales, indisponibilidad de mantenimiento de sistemas por otras organizaciones, interrupciones de energía, rotura de tubos y/o pipas de agua e interrupciones en las comunicaciones.

Los efectos resultantes de los escenarios anteriores normalmente caen dentro de las siguientes categorías:

- Divulgación de información sensitiva.

- Modificación de información importante o sensitiva.

- Destrucción o pérdida de información, hardware o software importante.

- Interrupción en el acceso a información, software, aplicaciones o servicios.

La tabla 12 muestra los efectos adversos al SMPD que se pueden tener en caso de que las fuentes de amenaza se materialicen:

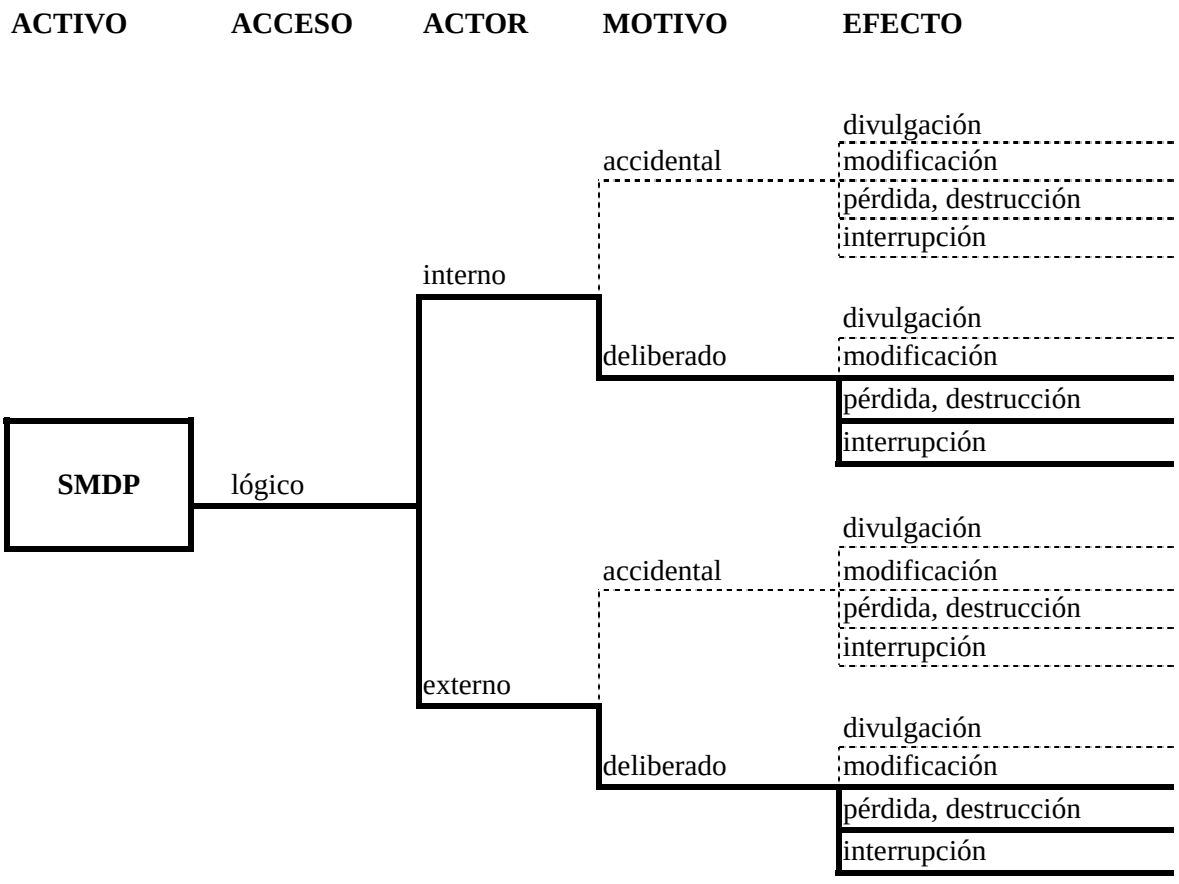
Tipo de Amenaza	Amenazas al sistema crítico SMPD
Acciones ejecutadas por la gente (acceso lógico)	Modificación, Pérdida/Destrucción Al estar interconectado a la infraestructura de que comunica a las clínicas regionales y al permitir el acceso de personal desde las mismas, es posible que una persona interna o externa a MedSite, se introduzca a la infraestructura tecnológica y vulnere el SMPD, pudiendo modificar la información almacenada en la base de datos. Interrupción Una persona interna o externa al hospital puede hacer una denegación de servicio sobre la página de publicación de resultados del SMPD, el impacto que se tendría es de disponibilidad el cual es altamente crítico, ya que el SMPD debe estar disponible durante todo el año.
Acciones ejecutadas por la gente (acceso físico)	Pérdida/Destrucción, Modificación En caso de no contar con procedimientos de seguridad formales y probados es posible que exista pérdida o modificación de información por error humano. Si el personal tiene acceso indiscriminado al centro de cómputo y no existe una vigilancia de las acciones que se lleven a cabo dentro del mismo, es posible que se produzca un daño físico a los equipos que conforman el SMDP.

Tipo de Amenaza	Amenazas al sistema crítico SMPD
Problemas de Sistemas	Interrupción, Pérdida/Destrucción Si se presenta un defecto del hardware de los dispositivos tecnológicos, se puede afectar la disponibilidad de la infraestructura ya que los diferentes sistemas están interrelacionados y están encaminados al mismo objetivo. Interrupción Los virus informáticos no es algo que afecte directamente a los servidores del SMDP, ya que éstos tendrán sistemas Linux; sin embargo, la expansión de virus y/o código malicioso en la red interna del Hospital puede afectar la disponibilidad de la red, denegando el servicio de consulta. Pérdida/Destrucción, Interrupción, Modificación El SMDP puede tener defectos en su diseño, desarrollo y/o implementación. Interrupción, Pérdida/Destrucción Las malas configuraciones de los sistemas pueden denegar el servicio.
Otros Problemas	Interrupción, Pérdida/Destrucción La inundación, fallas de energía eléctrica y otros eventos externos pueden denegar el servicio del SMDP. Esto esencialmente tiene un impacto crítico de disponibilidad. Divulgación La falta de consciencia en cuanto a prácticas seguras de administración de dispositivos pueden dejar vulnerable al sistema en períodos de tiempo largo. El no contar con una clasificación de la información, posibilita que un atacante conozca información de configuración que le permitan perpetrar futuros ataques.

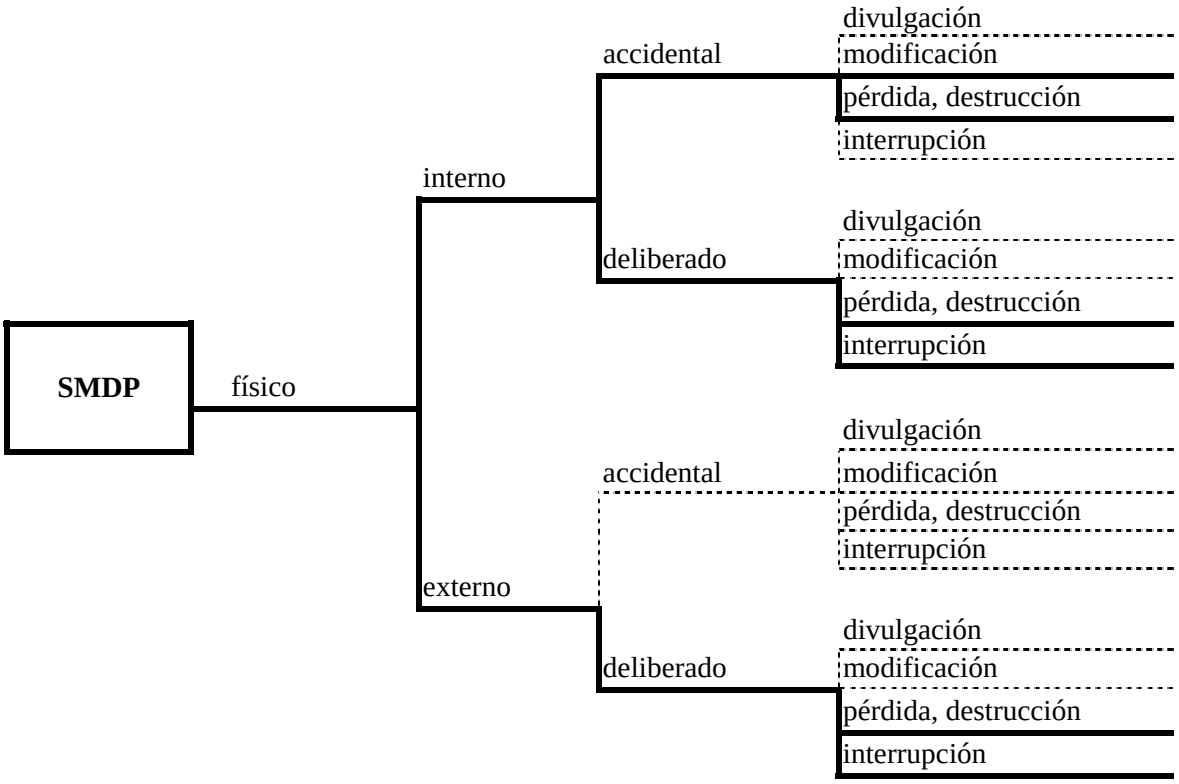
Tabla 12: Amenazas y áreas de preocupación identificadas.

Perfiles de Amenaza

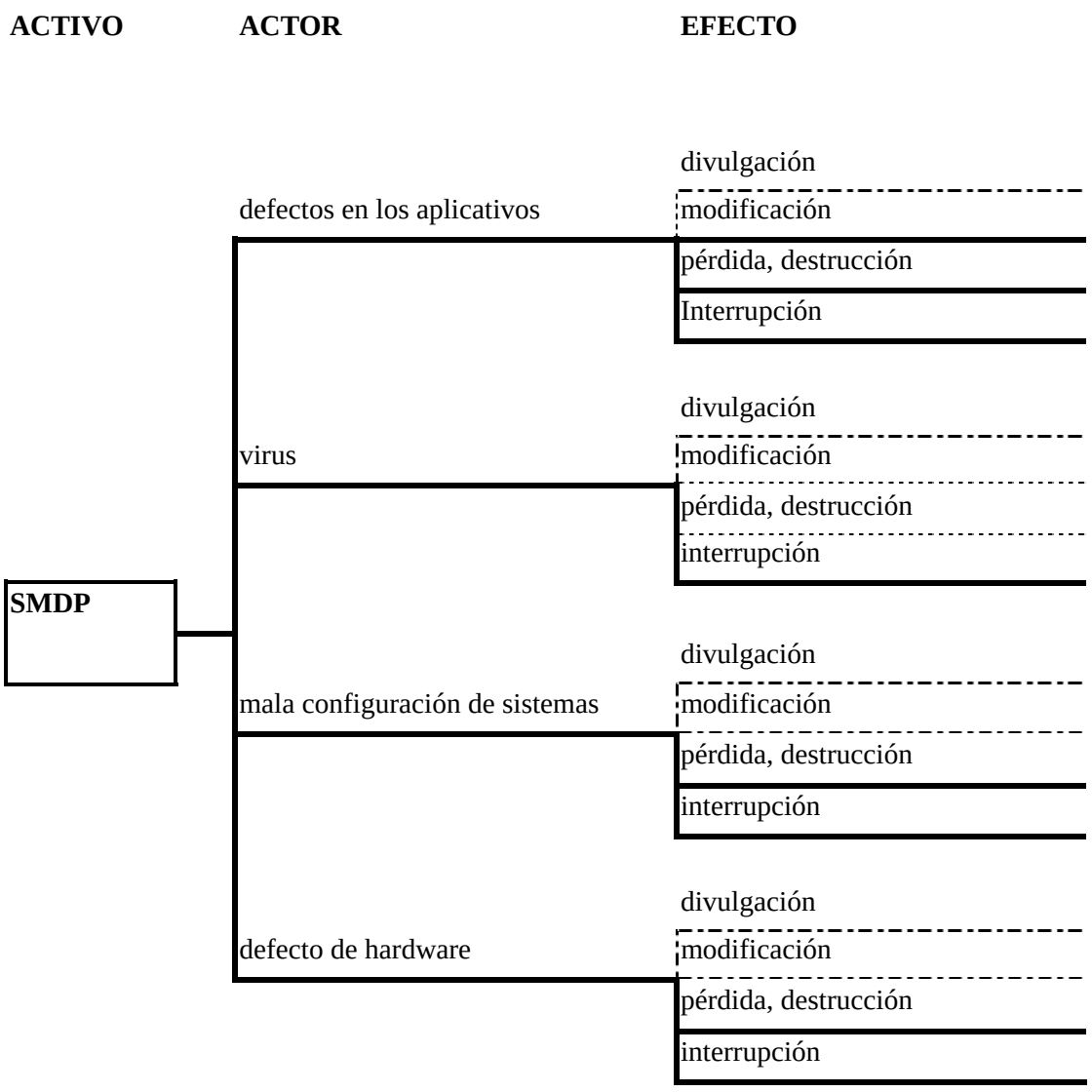
ACCIONES EJECUTADAS POR LA GENTE (ACCESO LÓGICO)



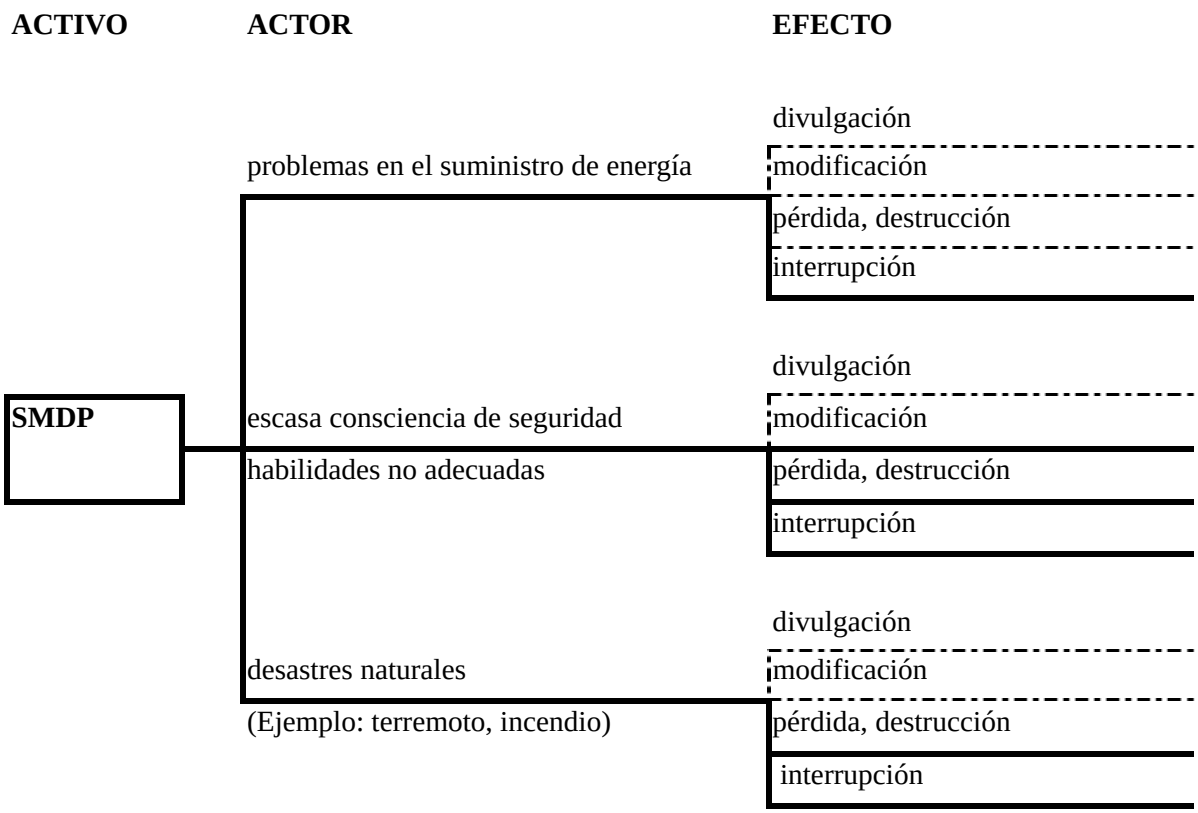
ACCIONES EJECUTADAS POR LA GENTE (ACCESO FÍSICO)



PROBLEMAS DE SISTEMAS



OTROS PROBLEMAS



Actividad 2: Identificación de Vulnerabilidades a la Infraestructura

Identificación de Componentes Críticos

A continuación, en la tabla 13 se presentan los componentes que forman parte de la infraestructura tecnológica del sistema SMDP:

HARDWARE - INFRAESTRUCTURA SMDP		
DISPOSITIVO	**UBICACIÓN**	**CANTIDAD**
Ruteador 2801	Clínicas a nivel nacional	30
Ruteador 7206	Centro de Cómputo	1
Switch 2950	Clínicas a nivel nacional	30
	Centro de Cómputo	3
Servidor de Aplicación		1
Servidor de Base de Datos		1
Servidor de Publicación (Web)		1
Switch Fibre Channel		1
Controladora EVA		1
Switchintercom Clusters - Arreglo de discos EVA 6000		1
Balanceador 11503		1

Tabla 13 Componentes

Las tablas 14 y 15 especifican el software y las aplicaciones necesarias para el SMDP:

SOFTWARE
Oracle 10g Clusterware
Oracle Data Guard
Red Hat Linux Enterprise Server 4
Enterprise Virtual Array (EVA) 6000
Apache
Tomcat
Java - JDK 1.6

APLICACIONES
Aplicativo Central SMDP

Tabla 14 Software y aplicaciones

Los componentes de seguridad que forman parte de la infraestructura del sistema SMDP son:

DISPOSITIVOS DE SEGURIDAD SMDP		
DISPOSITIVO	**UBICACIÓN**	**CANTIDAD**
Cisco PIX 515	Infraestructura tecnológica	1
IDS Cisco 4215	Infraestructura tecnológica	1

Tabla 15 Dispositivos de seguridad

Identificación de Componentes a Examinar

Esta sección hace una exploración en las listas de correo de seguridad de mayor reconocimiento a nivel internacional. Con esto se pretende buscar las vulnerabilidades detectadas en los equipos que se van a implementar en el site central.

A continuación se muestra una tabla con los resultados de esta búsqueda. Los vínculos llevan a la página Web donde se encuentran reportadas dichas vulnerabilidades. Cabe resaltar que la validez de estos resultados está sujeta a un período de tiempo determinado. Ver tablas 16 y 17.

Dispositivo	Fecha	Reportes - Full-disclosure
Firewall PIX 515 IOS 6.3	Marzo-06	http://seclists.org/lists/fulldisclosure/2006/Mar/0144.html http://seclists.org/lists/fulldisclosure/2006/Mar/0145.html http://seclists.org/lists/fulldisclosure/2006/Mar/0146.html http://seclists.org/lists/fulldisclosure/2006/Mar/0175.html
Firewall PIX 515 IOS 6.3	Ene-06	http://seclists.org/lists/fulldisclosure/2006/Jan/0655.html
Routers IOS 12.4 (03) 12.04(5)	Ene-06	http://seclists.org/lists/fulldisclosure/2006/Jan/0655.html
Routers IOS 12.4 (03) 12.04(5)	Dic-05	http://seclists.org/lists/fulldisclosure/2005/Dec/0053.html
Firewall PIX 515 IOS 6.3	Nov-05	http://seclists.org/lists/fulldisclosure/2005/Nov/0412.html
Routers IOS 12.4 (03) 12.04(5)	Sep-05	http://seclists.org/lists/fulldisclosure/2005/Sep/0145.html
IDS 4215 5.0	Sep-05	http://seclists.org/lists/fulldisclosure/2005/Aug/0721.html

Tabla 16 Vulnerabilidades reportadas en la lista de correo "Full-Disclosure"

Dispositivo	Fecha	Reportes - Bugtraq
IDS 4215 5.0	Feb-06	http://seclists.org/lists/bugtraq/2006/Feb/0221.html
Routers IOS 12.4 (03) 12.04(5)	Ene-06	http://seclists.org/lists/bugtraq/2006/Jan/0325.html
Routers IOS 12.4 (03) 12.04(5)	Dic-05	http://seclists.org/lists/bugtraq/2005/Dec/0020.html
Firewall PIX 515 IOS 6.3	Nov-05	http://seclists.org/lists/bugtraq/2005/Nov/0276.html
Routers IOS 12.4 (03) 12.04(5)	Nov-05	http://seclists.org/lists/bugtraq/2005/Nov/0010.html http://seclists.org/lists/bugtraq/2005/Nov/0160.html
Routers IOS 12.4 (03) 12.04(5)	Sep-05	http://seclists.org/lists/bugtraq/2005/Sep/0090.html

Tabla 17 Vulnerabilidades reportadas en la lista de correo "Bugtraq"

Con esta búsqueda se pudo comprobar que aunque han aparecido vulnerabilidades en los equipos, también se cuenta con medidas que pueden solucionarlos. Lo anterior indica que la tecnología en cuanto a equipos de comunicación es adecuada y garantiza seguridad en el manejo de la información.

Actividad 3: Desarrollo de la Estrategia y Planes de Seguridad

Identificación de Riesgos

Con la información recolectada en las fases anteriores es posible construir los perfiles de riesgo para el activo crítico del hospital. Los perfiles de riesgo son una extensión de los perfiles de amenaza, agregando una medida cualitativa (Bajo, Medio, Alto) del impacto que puede producir que una de las amenazas identificadas se materialice. Cabe destacar que la metodología OCTAVE no utiliza la probabilidad como medida del riesgo, la probabilidad de cualquier efecto identificado en los perfiles de riesgo se toma como la misma. A continuación en la tabla 18 se detallan los impactos hacia el sistema SMDP.

IMPACTO AL HOSPITAL "MedSite"		
Efecto	**Descripción del Impacto**	**Valores**
Divulgación	Cualquier fuga de información pone en riesgo la privacidad de los pacientes. Esto conlleva a demandas potenciales y a pérdida de credibilidad ante la sociedad.	ALTO
Modificación	Cualquier tipo de modificación ya sea ésta con dolo o sin intención, afectará el registro personal del paciente, ocasionando una publicación errónea de resultados en el módulo de consultas. Esto conlleva a poner en riesgo la vida del paciente por un mal tratamiento.	ALTO
Destrucción/ Pérdida	La destrucción o pérdida hardware y/o software conlleva a una "caída del sistema".	ALTO
	La pérdida de información afecta la publicación de resultados del módulo de consultas, poniendo en riesgo la disponibilidad ante emergencias. Se cuenta sin embargo, con registros en papel que posibilitan una consulta vía telefónica.	MEDIO
Interrupción	La publicación de resultados de manera oportuna es vital para el módulo de consultas, de lo contrario se está poniendo en riesgo la disponibilidad ante emergencias. Se cuenta sin embargo, con registros en papel que posibilitan una consulta vía telefónica.	ALTO

Tabla 18 Tabla de impactos

Criterios de Evaluación de Riesgos

Los criterios de evaluación son medidas mediante las cuales se pueden comparar y evaluar el impacto que se describió en la actividad anterior. Ver tabla 19 a 24. Los criterios de evaluación son creados de una gran gama de tipos o categorías de impactos. Estas categorías de impactos de las cuales se crearán los criterios de evaluación alineándose a la metodología de OCTAVE son:

- Reputación / Confianza del Cliente
- Vida / Salud de los Clientes
- Productividad
- Multas / Penas Legales
- Financiero
- Otros

Criterios para Evaluar los Impactos de los Riesgos			
Área de Impacto	**ALTO**	**MEDIO**	**BAJO**
Reputación / Confianza de los clientes	• Reputación irrevocablemente destruida o dañada • Pérdida del rango en clasificación o acreditación por parte de cuerpos de auditoria y certificación • Más del 30% de disminución de los clientes debido a la pérdida de confianza	• Reputación dañada; se requieren algunos esfuerzos y gastos para recuperarla • Reducción o advertencia de reducción del rango en clasificación o acreditación por parte de cuerpos de auditoria y certificación • Del 10 al 30% de disminución de los clientes debido a la pérdida de confianza • El paciente busca atención de otra fuente	• Reputación mínimamente afectada; se requiere poco o ningún esfuerzo o gasto para recuperarla • Sin cambios del rango en clasificación o acreditación por parte de cuerpos de auditoria y certificación • Menos del 10% de disminución de los clientes debido a la pérdida de confianza

Tabla 19 Criterio de Evaluación de Riesgos para Reputación

Criterios para Evaluar los Impactos de los Riesgos			
Área de Impacto	**ALTO**	**MEDIO**	**BAJO**
Vida / Salud de los Clientes	• Pérdida de la vida del cliente • Discapacidad permanente de uno o más aspectos importantes de la salud del cliente (por ejemplo, pérdida del uso de una o más extremidades, ceguera, daño cerebral) • No se puede prestar atención a los pacientes durante más de una semana • Seguridad violada	• La vida del cliente es amenazada, pero recuperable con tratamiento adicional • Deficiencia transitoria o recuperable de la salud del cliente (por ejemplo, recuperación de la utilización de las extremidades por medio de terapia física) • No se puede prestar atención a los pacientes de uno a dos días • Seguridad afectada	• No hay pérdida o una amenaza significativa para la vida del cliente • Mínimo, de inmediato tratables en la degradación de los clientes con la recuperación de la salud dentro de los cuatro días • Degradación mínima e inmediatamente curable en la salud del cliente con una recuperación dentro de cuatro días • Para dar continuidad del cuidado se requiere incrementar la comunicación entre los proveedores en las diferentes instalaciones • Seguridad en duda

Tabla 20 Criterio de Evaluación de Riesgos para Vida / Salud de los clientes

Criterios para Evaluar los Impactos de los Riesgos			
Área de Impacto	**ALTO**	**MEDIO**	**BAJO**
Productividad	• Los médicos y / o el personal de enfermería no pueden cumplir los aspectos de trabajo críticos durante dos o más días (por ejemplo, no hay cirugías, terapias físicas, atención especializada a los pacientes) • Se requiere un incremento del 40% o más en las horas de trabajo de al menos el 10% del personal general (por ejemplo, el manual de re-creación de los registros de tratamientos o el manual de correlación de los resultados de laboratorio y los planes) • Pérdida irrecuperable de los registros y la información de los pacientes	• El trabajo de los médicos y / o del personal de enfermería ha incrementado en un 10-40% durante un día (por ejemplo, la localización de registros en papel, la verificación verbal de todas las decisiones, no pueden acceder a los resultados de laboratorio o de prueba) • Incrementos en el trabajo del personal general del 10-40% durante un día (por ejemplo, duplicando registros escritos, re-creando registros de facturación del paciente, recuperando y verificando los respaldos de datos) • Continuidad ineficiente de la atención; demoras mientras se recupera información extraviada	• Los médicos y / o el personal de enfermería es incomodado durante menos de un día, pero no hay un incremento considerable en el esfuerzo de trabajo (por ejemplo, el retraso en las horas de las citas, el laboratorio debe ser llamado para obtener los resultados) • Otros inconvenientes para el personal de menos de un día, pero no mensurable aumento en el trabajo se produce el esfuerzo • Personal general es incomodado durante menos de un día pero no hay un aumento considerable en el esfuerzo de trabajo

Tabla 21 Criterio de Evaluación de Riesgos para Productividad

Criterios para Evaluar los Impactos de los Riesgos			
Área de Impacto	**ALTO**	**MEDIO**	**BAJO**
Multas / Penas Legales	• Multas impuestas de más de $100,000 • Una o más demandas no frívolas de más de $3,000,000 presentadas por los clientes • El gobierno u otra organización de investigación inicia una investigación de alto perfil y a fondo de las prácticas organizacionales	• Multas impuestas de $10,000 a $100,000 • Una o más demandas judiciales no frívolas entre $ 250,000 y $ 3,000,000 presentadas por los clientes • El gobierno u otra organización de investigación requiere información o registros (de bajo perfil)	• No hay multa o hay una de menos de $10,000 impuestos • Demanda judicial de menos de $250,000 o una demanda frívola (existe una probabilidad del 95% de que se pueda vencer) presentadas por los clientes • Sin preguntas del gobierno o de otras organizaciones de investigación

Tabla 22 Criterio de Evaluación de Riesgos para Multas / Penas Legales

Criterios para Evaluar los Impactos de los Riesgos			
Área de Impacto	**ALTO**	**MEDIO**	**BAJO**
Financiero	• Anualmente los gastos de operación son de hasta el 15% (por ejemplo, agregar trabajadores temporales para la recuperación de registros, añadiendo más software para disuadir a los intrusos) • 20% de la pérdida anual de los ingresos (por ejemplo, reubicación del 20% de los pacientes a otros sitios debido a la pérdida de energía) • Por una sola vez los costos financieros son mayores a $1M (por ejemplo, la sustitución de sistemas dañados por el agua, la contratación de 25 empleados temporales para volver a capturar los registros) • Errores incorregibles en la financiación y el personal	• Anualmente los gastos de operación son de 2 % y hasta el15% (por ejemplo, la contratación de empleados temporales por tres meses para llevar a mano los resultados de laboratorio varias veces al día) • Hay desde un 5% hasta un 20% de pérdida anual de los ingresos (por ejemplo, demorar cirugías rentables debido a la pérdida y recuperación de archivos) • Por una sola vez el costo financiero es de $25K hasta $1M (por ejemplo, la adición de un servidor y la re-asignación de activos) • Errores parcialmente corregibles en la financiación y el personal	• Aumento de menos del 2% en los gastos de operación (por ejemplo, una semana de tiempo extra para cuatro miembros del personal para documentar los cambios en los planes de tratamiento) • Menor al 5 % en la pérdida del ingreso anual (por ejemplo, $50K en fondos de investigación si no hay acceso remoto a la universidad) • Por una sola vez los costos financieros son de menores a $ 25K (por ejemplo, el re-entrenamiento de 20 funcionarios) • Errores inconvenientes, pero corregibles en la financiación y el personal

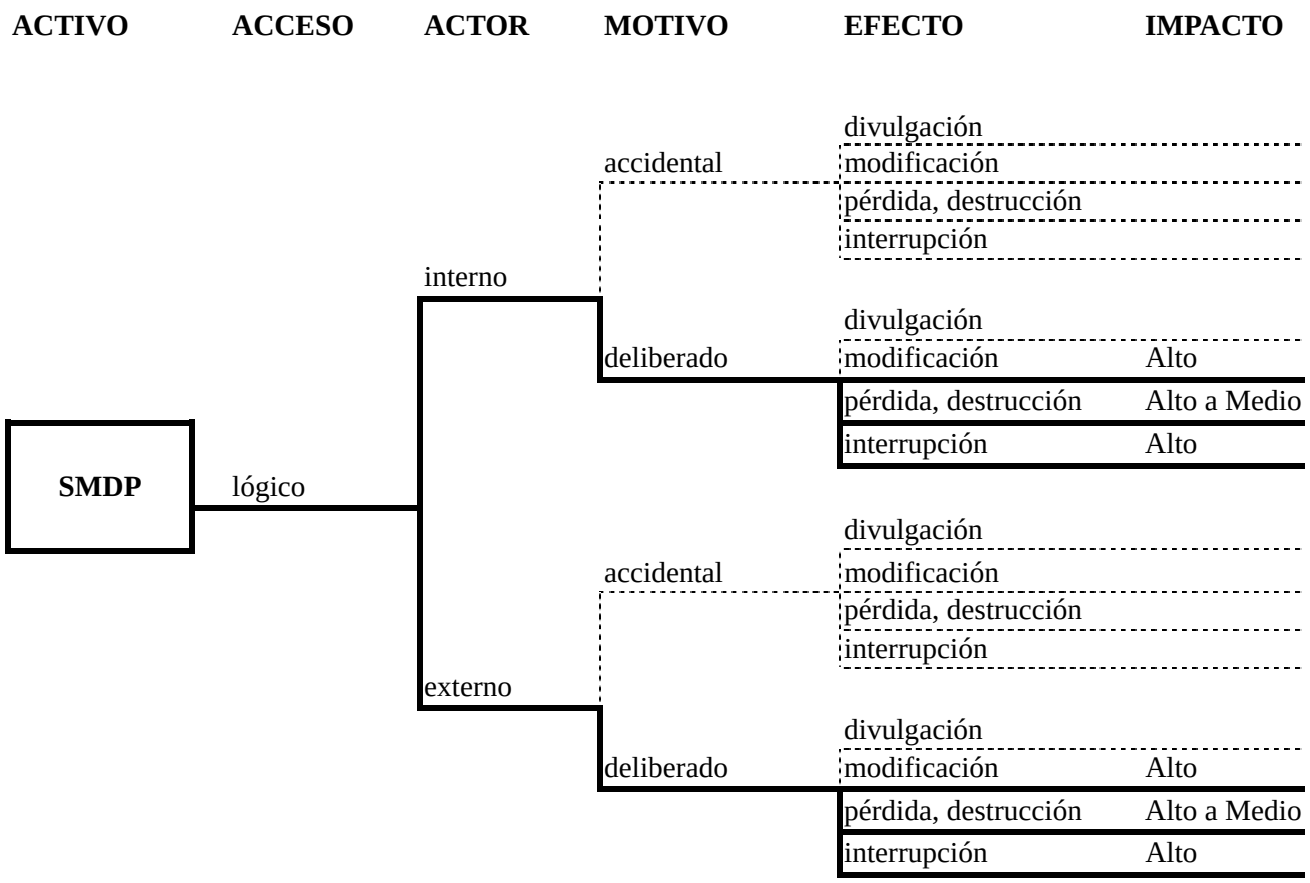
Tabla 23 Criterio de Evaluación de Riesgos para el rubro Financiero

Criterios para Evaluar los Impactos de los Riesgos			
Área de Impacto	**ALTO**	**MEDIO**	**BAJO**
Otros	• Pérdida total de una instalación o edificio debido a un incendio • Proveedores o personal médico falsamente acreditado causan daños a los pacientes	• Los daños a una instalación o edificio implican la reubicación temporal de los pacientes • No se han podido verificar las credenciales de los proveedores o el personal médico • No es posible realizar el seguimiento preciso de la ejecución de las instalaciones o proveedores	• Pérdida de aire acondicionado durante dos semanas • Impacto insignificante en las operaciones diarias

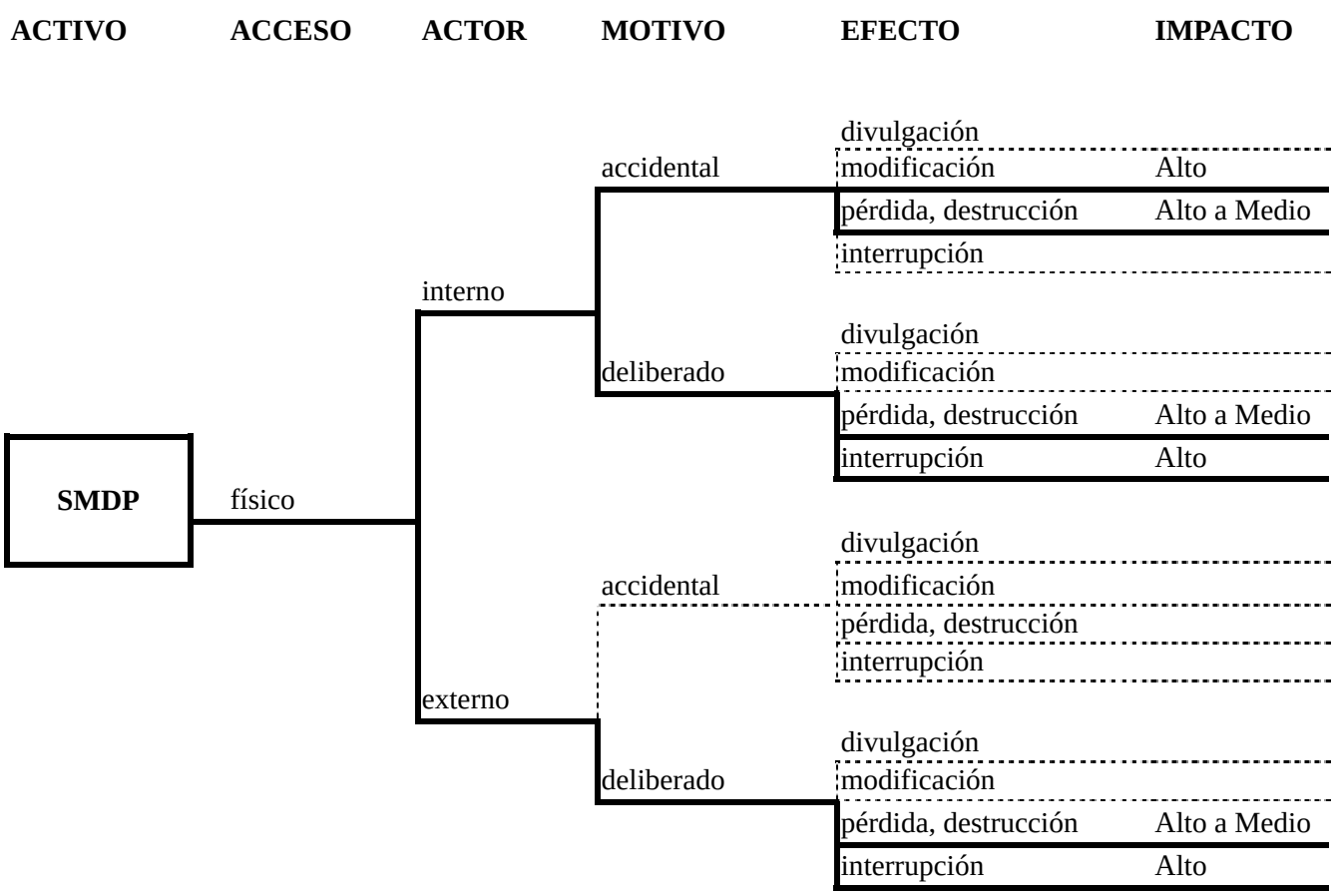
Tabla 24 Criterio de Evaluación de Riesgos para el rubro Otros

Perfiles de Riesgo

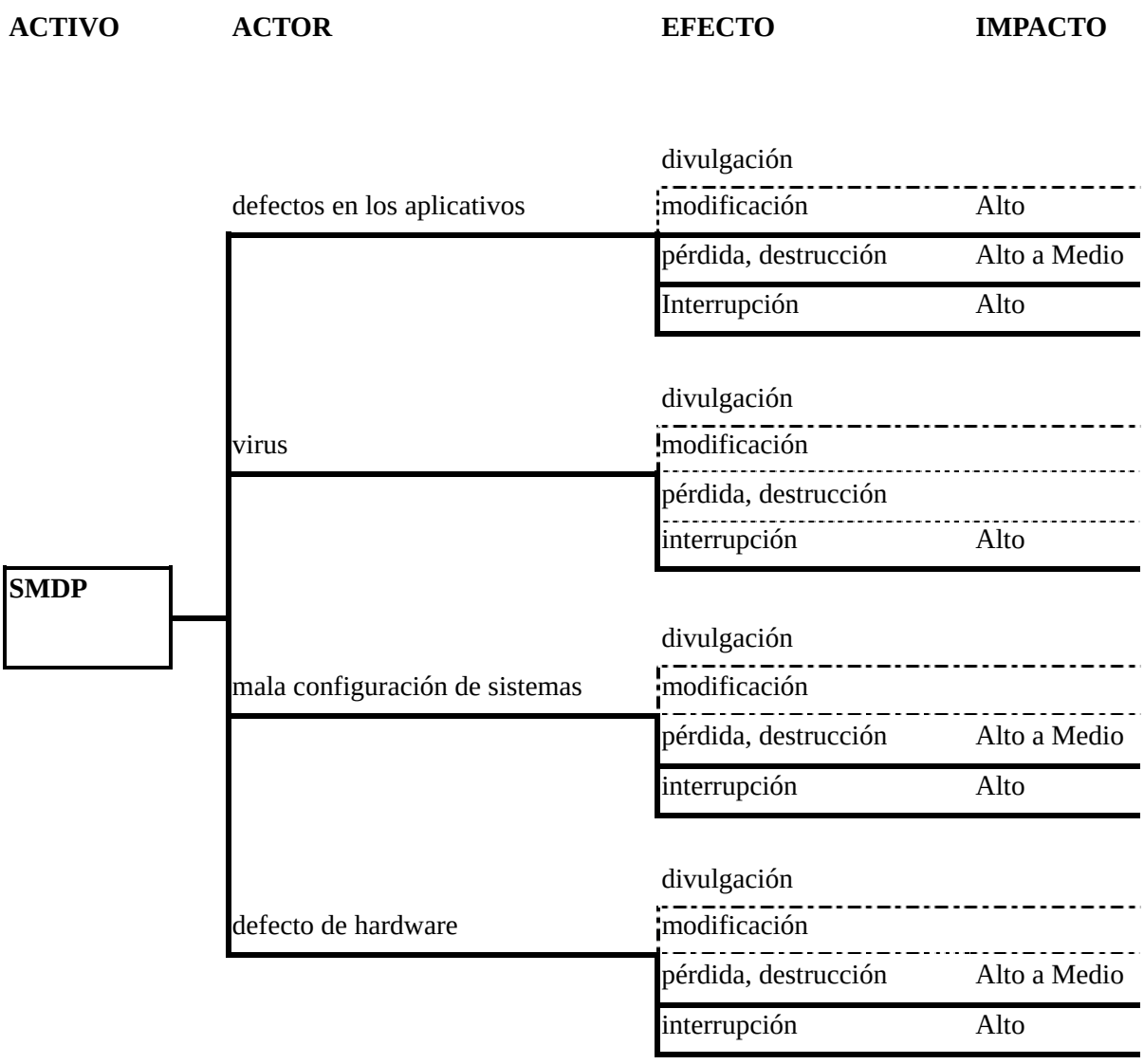
ACCIONES EJECUTADAS POR LA GENTE (ACCESO LÓGICO)



ACCIONES EJECUTADAS POR LA GENTE (ACCESO FÍSICO)



PROBLEMAS DE SISTEMAS



OTROS PROBLEMAS

ACTIVO	ACTOR	EFECTO	IMPACTO
SMDP	problemas en el suministro de energía	divulgación	
		modificación	
		pérdida, destrucción	
		interrupción	Alto
	escasa consciencia de seguridad	divulgación	
		modificación	Alto
	habilidades no adecuadas	pérdida, destrucción	Alto a Medio
		interrupción	Alto
	desastres naturales	divulgación	
		modificación	
	(Ejemplo: terremoto, incendio)	pérdida, destrucción	Alto a Medio
		interrupción	Alto

Desarrollo de la Estrategia de Protección

El desarrollo de la estrategia de protección se lleva a cabo mediante dos posturas, las cuales se detallan a continuación:

1. Estrategia de Protección.- basado en el catálogo de prácticas lo que se especifica como vulnerabilidades organizacionales; se enfoca principalmente en reforzar la seguridad en todo el entorno del sistema SMDP.

   El catálogo de prácticas que se utilizará estará basado completamente en el ISO 17799:2005 con el fin de alinearse a un estándar de seguridad de la información internacionalmente reconocido por la industria.

   Por otro lado, se debe crear una Declaración de Aplicabilidad (SoA por sus siglas en inglés) indicando los controles del estándar ISO que aplican, los que no aplican, los que se implementarán y los que no serán implementados, con su debida justificación y observaciones.

2. Planes de Mitigación para los activos críticos.- estos planes son específicos y tienen como objetivo mitigar los riesgos identificados de los activos críticos, basado en los perfiles de amenaza y riesgos identificados anteriormente. Ver tabla 25.

Plan de Mitigación de Riesgos	
Tipo de Amenaza	**Acciones**
Acciones ejecutadas por la gente (acceso lógico)	La comunicación entre el hospital y las clínicas regionales se llevará a cabo a través de la tecnología Frame Relay la cual permite establecer un circuito virtual de comunicación directa y permanente a través de una red compartida entre dos puntos distintos a lo largo de todo el país. Esta tecnología opera sobre la capa física y de enlace del modelo de referencia OSI.
	Se implementará Firewall Cisco PIX 515 con lo que se pretende contar con una herramienta que pueda filtrar todo el tráfico que proviene de las clínicas regionales. Verificando que solo se pueda acceder a los servicios definidos por la aplicación los host y/o dispositivos autorizados, evitando así que agentes no permitidos entren y realicen actividades que no sean propias a las actividades del sistema SMDP. Este dispositivo cumple con las certificaciones Common Criteria nivel EAL4, ICSA nivel Firewall, 4.1 Corporate, así como FIPS 140-2 nivel 2.
	Se implementará IDS 4215 con el que se analizará el tráfico proveniente de la comunicación con las clínicas regionales. Los IDS permiten analizar el trafico de red en busca de actividad anómala lo que pude indicar que se esta ejecutando un ataque. Esto permitirá tener una serie de alertas las cuales se ejecutarán de manera oportuna, con el objetivo de dar aviso de manera anticipada cuando un ataque este en vías de ser ejecutado. Este dispositivo cuenta con la certificación Comon Criteria nivel EAL2.
	Se implementarán firewalls OpenBSD en los servidores de aplicación y base de datos, con el que se pretende evitar que haya tráfico de información proveniente de las clínicas regionales evitando de esta manera que agentes maliciosos logren tener acceso al SMDP y puedan ejecutar cualquier tipo de ataque.
	Se contará con bitácoras centralizadas de toda la información generada mediante un servidor Syslog para concentrar y analizar la información generada por los dispositivos tanto de comunicaciones como de procesamiento de la información.
	Serán desarrollados Baselines de seguridad basados en mejores prácticas de la industria para la configuración de todos los dispositivos de la infraestructura tecnológica del SMDP.
	Se supervisará toda la actividad que tenga el SMDP mediante Nagios, el cual es una herramienta de software libre que permite monitorear una gran variedad de las propiedades de los sistemas que forman parte de una red. Se monitoreará el comportamiento de los servidores que forman parte de las clínicas regionales, con el objetivo de determinar si están trabajando de manera adecuada, observando entre otras cosas, cual es el estado de los recursos.
Acciones ejecutadas por la gente (acceso físico)	Se implementará video vigilancia (20 cámaras de CCTV) en el centro de cómputo.
	Se implementarán controles de acceso biométrico para el centro de cómputo.
	Se reforzará la seguridad mediante guardias de protección civil en el site central.
	Se generarán acreditaciones para todo el personal del hospital y gafetes de visitantes. No se permitirá el acceso desde la entrada a cualquier persona que no porte gafete.

Plan de Mitigación de Riesgos	
Tipo de Amenaza	**Acciones**
Problemas de Sistemas	Para combatir las fallas de hardware y software que forman parte de la infraestructura tecnológica del sistema SMDP, se contará con redundancia de dichos dispositivos; es decir, se tendrán dobles equipos por capa de comunicación.
	Se implementará el dispositivo ASA 5500 como infraestructura de respaldo a la red de Frame Relay, para que se cuente con una red vía MODEM telefónico (tipo PSTN) y garantizar la operación de todas las transacciones que se lleven a cabo. Este dispositivo cuenta con la certificación FIPS 140-2 nivel 2.
	Se desarrollarán procedimientos de manejo de incidentes, entre ellos de contención de código malicioso. Se instalará y configurará el antivirus institucional a los usuarios de las instalaciones de MedSite.
	Se creará un área de Calidad de sistemas para identificar los posibles errores del sistema SMDP.
	Se realizarán pruebas locales y nacionales de unidad e integrales de la infraestructura tecnológica del sistema SMDP.
Otros Problemas	Se contará con un centro de cómputo espejo alterno para recuperarse en caso de desastre
	Se implementarán plantas de energía eléctrica alternas y sistemas UPS en el site central.
	Se llevará a cabo una campaña (reducida) de concienciación en materia de seguridad de la información para todo el personal del Hospital.
	Se implementará tecnología de almacenamiento de información centralizada como lo es la tecnología Storage Area Network (SAN).

Tabla 25 Plan de Mitigación de Riesgos

Identificación de Riesgos Residuales

Aún y con la implementación de una estrategia de seguridad informática exitosa, no es posible decir que se está 100% seguro o que se es invulnerable; ya que, aún con la implementación de los controles de seguridad existen todavía riesgos, a los que se le conocen como riesgos residuales, que aunque la probabilidad de ser explotados es pequeña, es importante conocerlos.

La metodología OCTAVE no considera la identificación de riesgos residuales, sin embargo, para el proyecto de seguridad del sistema SMDP se ve la necesidad de identificarlos. De esta manera, los riesgos residuales identificados se dividieron de acuerdo con la Estrategia de Protección y a los Planes de Mitigación de Riesgos, creados anteriormente.

Es importante señalar que los controles implementados en la Estrategia de Protección minimizan la mayoría de los riesgos identificados como residuales descritos en la Tabla 26 “Estrategias de protección”; sin embargo, durante el análisis de riesgos se identificó que al no contar con políticas de seguridad y la normativa relacionada a dichos controles se queda expuesto a incumplimientos por parte del personal del Hospital. Por tal motivo en la siguiente tabla se especifican los riesgos residuales por falta de normativa (controles que sí fueron implementados) y los riesgos residuales por la no implementación de controles.

Estrategia de Protección	
Cláusula	**Riesgo Residual**
Políticas de Seguridad	*Riesgos por falta de normativa* • Mal uso de los activos de TI. • No cumplimiento con los controles y recomendaciones de seguridad. • Posibles errores por parte de los usuarios. • Configuraciones vulnerables en los equipos de la infraestructura tecnológica. • Malas prácticas administrativas de seguridad.
Seguridad Organizacional	*Riesgos por falta de normativa* • Mal uso de los activos de TI y/o robo de información confidencial. • Posibles errores por parte de los usuarios. *Riesgos por no implementación* • Inadecuados contratos de seguridad de terceras partes.
Administración de Activos	*Riesgos por no implementación* • Acceso a la información sensible por personal no autorizado. • Mal uso de la información. • Niveles y/o privilegios de acceso otorgados de manera errónea. • Extravío de información confidencial.
Seguridad en los Recursos Humanos	*Riesgos por falta de normativa* • Posibles errores por parte de los demás usuarios al no tener una delimitación en sus actividades al no existir un documento formal con las responsabilidades y roles. • Desconocimiento de las responsabilidades y roles por parte de los usuarios. • Contratación de personal no capacitado para las funciones específicas a desempeñar.
Seguridad Física y Ambiental	*Riesgos por no implementación*. • Robo de equipo de oficina.
Administración de Comunicaciones y Operaciones	*Riesgos por falta de normativa* • No acatamiento de las reglas por parte de los usuarios. • Control de los medios informáticos no establecido adecuadamente.

Estrategia de Protección	
Cláusula	**Riesgo Residual**
	Riesgos por no implementación • Perdida de información y/o equipo en tránsito.
Control de Acceso	*Riesgos por falta de normativa* • Mala aplicación o ejecución de los procedimientos en los sitios remotos. • Indisposición de los usuarios al no contar con políticas que avalen alguna tarea o función específica dentro de sus actividades cotidianas. • Ejecución de actividades malintencionadas dentro de los sistemas.
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	*Riesgos por falta de normativa* • Indisposición de los usuarios al no contar con políticas que avalen alguna tarea o función específica dentro de sus actividades cotidianas.
Incidentes de Seguridad de la Información	*Riesgos por falta de normativa* • No aplicación del proceso disciplinario a los usuarios por posibles actividades mal intencionadas.
Administración de la Continuidad del Hospital	*Riesgos por falta de normativa* • Desconocimiento por parte de los usuarios de la comprensión de los procesos de continuidad del Hospital o de actividades relacionadas. • Al no existir una política de continuidad de las operaciones del Hospital, es posible que no se lleve a cabo el plan de continuidad con el mismo formalismo para las siguientes elecciones.
Cumplimiento	*Riesgos por falta de normativa* • Imposibilidad de obtener información del uso inadecuado de los recursos de cómputo por parte de los usuarios. • No acatamiento de reglas o indisposición de los usuarios al no contar con políticas que avalen alguna tarea o función específica dentro de sus actividades cotidianas.

Tabla 26 Estrategia de protección

Los riesgos residuales identificados de los Planes de Mitigación de Riesgos se muestran en la tabla 27 “Planes de Mitigación de Riesgos”:

Planes de Mitigación de Riesgos	
Descripción	**Riesgo Residual**
Comunicación de las clínicas regionales hacia el site central mediante Frame Relay, PSTN y enlaces dedicados	*Interrupción:* • Es posible que el proveedor del servicio no pueda continuar brindando dicho servicio o es probable que ocurra una falla en los dispositivos de comunicación que comunican a las clínicas regionales y el site central con dicha red. • Se podría realizar un ataque de Denegación de Servicio comprometiendo alguno de los host que forman parte de la red Interna de cada clínica regional, que a pesar de que existen controles para de alguna forma controlarlo, no se sabe la magnitud del ataque; es decir, es posible que sea una Denegación de Servicio Distribuida y no se pueda contener por mucho tiempo. *Intercepción:* • Los datos que viajan a través de estas redes podrían ser interceptados por un agente extraño, y hacer mal uso de dicha información. *Modificación:* • La información original transmitida por las clínicas regionales podría ser modificada por algún agente externo y enviar información no válida hacia el site central. *Suplantación:* • Algún agente extraño podría intentar hacerse pasar por un cliente valido y tratar de enviar información falsa hacia el site central.
Storage Area Network	• Se pueden comprometer los servidores de bases de datos permitiendo el acceso a la información que se encuentra en los medios de almacenamiento masivo, lo que puede producir el robo o modificación de la información.

Tabla 27 Planes de mitigación de riesgos

Es importante hacer notar que perpetrar los ataques anteriormente identificados como riesgos residuales es muy POCO PROBABLE debido a la necesidad de una combinación de factores como:

- Tecnología necesaria.
- Conocimiento formal y/o conocimiento del entorno.
- Tiempo necesario para perpetrar el ataque.

Tomando como base los puntos anteriores y los riesgos residuales identificados, se mencionan los medios necesarios para lograr perpetrar los ataques mencionados en la tabla de riesgos residuales. Ver tabla 28.

Planes de Mitigación de Riesgos	
Descripción	**Medios Necesarios**
Comunicación de las clínicas regionales hacia el site central mediante Frame Relay, PSTN y enlaces dedicados	• Para que un atacante pudiera tener éxito requeriría tener acceso físico y/o lógico a la infraestructura del proveedor de estos servicios, para poder ejecutar desde ahí su ataque. Esto requeriría de un gran conocimiento del entorno tecnológico y de tecnología especializada para llevar a cabo esta acción, además de esperar que el proveedor sea altamente vulnerable, además de requerir un tiempo considerable en caso de lograrlo. • Tener acceso físico a las instalaciones en las clínicas regionales para instalar herramientas de software malicioso que comprometa cualquiera de los host conectados a la red con el objetivo de lanzar un ataque desde cualquiera de estos puntos, la necesidad de hacerse pasar por una dirección IP válida y dirección física (MAC) válida para lograr burlar la ACL del router. Aún teniendo éxito el único ataque que pudiera perpetrar es un DoS y al no ser distribuido el daño sería imperceptible. • Conectar un dispositivo comprometido directamente a cualquiera de estas redes con el objetivo de suplantar la identidad de un dispositivo valido para lanzar un ataque, teniendo las restricciones comentadas en el punto anterior. • Conectar un host malicioso directamente a cualquier dispositivo instalado para establecer la comunicación entre las clínicas regionales y el site central como son: – Dispositivos de comunicación ubicados del lado de las clínicas regionales – Dispositivos que reciben la acometida de las clínicas regionales del lado del site central Al igual que el punto anterior las restricciones son las suficientes para minimizar la probabilidad de dicho ataque. • Colocar una herramienta de captura de tráfico en alguno de los host conectados a cualquiera de los dispositivos mencionados en el punto anterior para analizar el tráfico de red y poder interceptar contraseñas o información sensible
Storage Area Network	• Tener acceso lógico a los switches que permiten el funcionamiento de la SAN con el objetivo de modificar su información. Para que un atacante pudiera obtener acceso lógico a los switches requeriría haber obtenido ya el acceso al servidor de bases de datos y haber vulnerado los segmentos de red (VLAN) que son implementados. Esto que representa una baja probabilidad debido a la dificultad técnica que esto representa y al tiempo necesario para que se pudiera lograr en todo caso, por otro lado el esfuerzo necesario para vulnerar un switch es alto ya que los conocimientos requeridos para manejar un switch de esta naturaleza son elevados.

Tabla 28 Medios necesarios para realizar un ataque existoso

4.4. Fase II: Identificación y selección de los controles de seguridad utilizando el ISO/IEC 17799:2005.

Para la identificación y selección de los controles de seguridad se tomará como base el Estándar Internacional ISO/IEC 17799:2005, adicionalmente se ilustra el esquema que será utilizado que muestra el proceso general de cómo se llevará a cabo el análisis para lograr la identificación y selección de los controles aplicables que entrarían dentro del sistema SMDP.

Cabe mencionar que a la fecha de elaboración del presente trabajo, el estándar en comentó ya fue renombrado como ISO/IEC 27002. Al igual que el estándar antecesor, el ISO/IEC 27002 es un código de práctica para la información de seguridad, detallando mecanismos de control que pueden implantarse tomando como base la guía que provee el ISO 27001.

Así pues, este esquema nos da el enfoque general para llevar de forma ordenada, controlada y planeada la identificación, selección e implementación de los objetivos de control con sus respectivos controles dentro del sistema SMDP en comento. En general, se deben observar los siguientes pasos durante la implementación de una estrategia de seguridad alineada al ISO/IEC 17799:2005:

a) Elaboración de la matriz de identificación de controles generales del ISO/IEC 17799:2005.-

La matriz desarrollada contiene todos los dominios del ISO 17799 y sus controles respectivos, adicionalmente fueron identificadas y agregadas mejores prácticas para cada control.

b) Identificación de los Controles.-

Con base en el Análisis de Riesgos, se deben identificar los controles definidos dentro del ISO/IEC 17799:2005, los cuales podrían ser aplicables al sistema SMDP.

c) Análisis de la información.-

Este análisis fue realizado con base en la documentación actual con que se contaba y las entrevistas realizadas en las diferentes áreas de MedSite, la cual fue analizada con el fin de ver si cumplía o estaba relacionada con algún objetivo de control del ISO/IEC 17799:2005.

d) Selección e Implementación de Controles.-

Una vez finalizado el análisis de información fueron identificados y seleccionados aquellos controles de seguridad del ISO/IEC 17799:2005 que serían implementados dentro sistema SMDP, así como aquellos controles que no aplicarían, debido a que la actividad o proceso que tenía el control no entraba dentro del SMDP.

e) Análisis de Resultados.-

Se detallarán de forma general los resultados generados de la identificación, selección e implementación de los controles de seguridad del ISO/IEC 17799:2005 que fueron enfocados al SMDP.

f) Informe Declaración de Aplicabilidad (SoA[54]).-

Se debe generar un informe correspondiente con todas las justificaciones y declaraciones de la selección e implementación de los controles de seguridad, así como de aquellos controles que no fueron seleccionados

54 Por sus siglas en inglés: *Statement of Applicability*

debido a que su alcance no se consideraba dentro del SMDP.

Ejemplo de identificación y selección de los controles a Implementar

Los controles identificados y seleccionados serán implementados con base en las mejores prácticas que abarca cada control específico del ISO/IEC 17799:2005.

Por otro lado es importante mencionar que aquellos controles y mejores prácticas que no son considerados para ser implementados, son debido a que se consideró que no están enfocados a las operaciones SMDP o por que su implementación actual no será posible ejecutarla dentro del periodo de tiempo con el que se cuenta.

A continuación, de manera ilustrativa se listan las justificaciones generales de los controles a implementar para las siguientes cláusulas del estándar en comento:

- A.5 Política de Seguridad
- A.7 Administración de Activos
- A.10 Gestión de Comunicaciones y Operaciones

El esquema de numeración utilizado hace referencia a las cláusulas del ISO/IEC 17799:2005 y al tipo de control de seguridad identificado; en seguimiento la numeración que se presenta en el Anexo A.

A.5 Política de Seguridad.

Objetivo

Proveer soporte y dirección de seguridad de información a la alta gerencia con base en los requerimientos de la organización, leyes y regulaciones relevantes. Ver tabla 29.

5. Políticas de Seguridad			
Control	**¿Será Implementado?**		**Justificación**
	Sí	**No**	
5.1.1 Documentación de la Política de Seguridad de Información		×	No se cuenta con el tiempo necesario para el desarrollo, revisión y aprobación de la política corporativa dentro del SMDP por parte de la alta gerencia. No estaba contemplado dentro del alcance del proyecto
5.1.2 Revisión de la Política de Seguridad de Información		×	

Tabla 29: Aplicabilidad para la cláusula 5.

A.7 Administración de activos

Objetivo

Lograr y mantener la adecuada protección sobre los activos de TI de la organización, definiendo los niveles de protección adecuados para el manejo de la información. Ver tabla 30.

7. Administración de Activos			
Control	**¿Será Implementado?**		**Justificación**
	Sí	**No**	
7.1.1 Inventario de Activos	✔		La coordinación administrativa de MedSite no está llevando a cabo una asignación de los inventarios como parte del proceso de alta y baja de empleados al Hospital.
7.1.2 Dueño de los Activos		✕	Actualmente no es posible realizar la clasificación de la información debido a que debe hacerse un análisis detallado de la información que es manejada dentro del SMDP para la identificación del Dueño, Custodio o usuario de la información. Por el tiempo limitado actualmente y este tipo de análisis se omite todo lo referente al control.
7.1.3 Aceptación del uso de los Activos		✕	No existe un acuerdo documentado en donde se especifiquen de manera explícita los derechos y responsabilidades de los usuarios en relación a los Activos de MedSite.
7.2.1 Pautas de Clasificación		✕	No es posible llevar a cabo el proceso de las pautas a seguir para clasificar la información, ni tampoco el etiquetado y rotulado de la información, debido a que no se cuenta previamente con una clasificación previa de la información, ya que de este análisis se derivan los aspectos necesarios para llevar a cabo la implementación de estos controles.

Tabla 30: Aplicabilidad para la cláusula 7.

A.10. Gestión de comunicaciones y operaciones.

Objetivo

Proteger las actividades de procesamiento de información de manera correcta, implementando niveles adecuados de protección a la información y a la infraestructura de redes para prevenir el acceso no autorizado, mal uso o destrucción de los activo s de TI por personal no autorizado, así como minimizar las fallas en los sistemas y detectar actividades no autorizadas en los equipos de cómputo. Ver tabla 31.

10. Gestión de Comunicaciones y Operaciones			
Control	**¿Será Implementado?**		**Justificación**
	Sí	**No**	
10.1.1 Documentación de los procedimientos operativos	✔		Aunque el departamento de IT del Hospital conoce y opera adecuadamente la infraestructura, no se tiene una administración orientada a procesos ni los registros documentados de los mismos.
10.1.2 Control de cambios en las operaciones	✔		El equipo de TI de MedSite maneja un control de cambios rudimentarios en diversos archivos. Esto no está documentado.
10.1.3 Separación de funciones		✕	Dado que el equipo de TI MedSite es muy pequeño, no es posible asignar roles específicos.
10.1.4 Separación entre instalaciones de desarrollo e instalaciones operativas	✔		No se cuenta con un ambiente para el desarrollo y pruebas de los sistemas que se llegan a desarrollar en el Hospital.
10.2.1 Entrega de Servicios	✔		No existen puntos de seguridad acordadas entre el personal de MedSite y la empresa “Sistemas ABC”.
10.2.2 Monitoreo y validación de los servicios de terceras partes		✕	Con base a la supervisión, validación y administración de los cambios de los servicios de las terceras partes no se implementará este control debido a que los servicios por parte del proveedor de servicio de “Sistemas ABC” no contemplan este rubro.
10.2.3 Administrando cambios en los servicios de terceras partes		✕	Con base a la supervisión, validación y administración de los cambios de los servicios de las terceras partes no se implementará este control debido a que los servicios por parte del proveedor de servicio de “Sistemas ABC” no contemplan este rubro.
10.3.1 Planificación de la capacidad	✔		Durante la concepción de servicios y sistemas no se están tomando en cuenta aspectos básicos como requerimientos de almacenamiento a mediano y largo plazo.
10.3.2 Aprobación del sistema	✔		No existe un método formal para liberación y/o aprobación de los servicios o sistemas.

10. Gestión de Comunicaciones y Operaciones			
Control	**¿Será Implementado?**		**Justificación**
	Sí	**No**	
10.4.1 Controles contra software malicioso	✔		Aunque se cuenta con antivirus instalados en los equipos personales de cómputo, no se cuenta con una plataforma homogénea antivirus. La solución no cuenta con un único punto de administración.
10.4.2 Controles contra software móvil malicioso		✕	En lo que respecta a los controles contra software móvil malicioso no aplica debido a que una vez aprobada y revisada la aplicación del SMDP no se contemplará el uso de módulos especiales dentro de ella para su instalación o actualización, por lo que no se permitirá realizar la inserción de código adicional en la misma, una vez ya instalada.
10.5.1 Respaldo de la Información	✔		Aunque se llevan a cabo respaldos, no existe un procedimiento formal.
10.6.1 Controles de redes	✔		No existen roles ni responsabilidades formalmente asignados para las tareas de fortalecer la seguridad en la red. Se llevan a cabo labores en base a la experiencia del personal.
10.6.2 Seguridad en los servicios de red	✔		No existen roles ni responsabilidades formalmente asignados para las tareas de fortalecer la seguridad en la red. Se llevan a cabo labores en base a la experiencia del personal.
10.7.1 Administración de medios informáticos removibles		✕	Debido a la falta de normatividad no serán establecidos niveles de autorización para la administración de los medios removibles ya que esto implicaría el desarrollo de políticas, por lo que se ha menciona que no se desarrollarán dentro del proyecto.
10.7.2 Disposición de los medios informáticos	✔		No existen procedimientos para disponer de equipos de cómputo obsoletos, así como dispositivos de almacenamiento móviles o extraíbles.
10.7.3 Procedimientos de manejo de la información		✕	El tiempo actual dentro del SMDP no permite desarrollar a tiempo este tipo de procedimientos, debido a su análisis de desarrollo y su periodo de implantación.

10. Gestión de Comunicaciones y Operaciones			
Control	**¿Será Implementado?**		**Justificación**
	Sí	**No**	
10.7.4 Seguridad de la documentación del sistema	✔		La documentación técnica (ejemplo: archivos de configuración y documentación relativa al diseño y desarrollo de sistemas) no está siendo resguardada de la manera apropiada.
10.8.1 Procedimientos y Políticas de Intercambio de Información	✔		No existen procedimientos para garantizar un correcto intercambio de información con otros hospitales.
10.8.2 Acuerdos de Intercambio de Información		✕	Para el sistema SMDP no existirá acuerdos de intercambio de información debido al proceso actual con se esta llevando a cabo, por lo que este tipo de acuerdos no serían considerados dentro de este proyecto.
10.8.3 Seguridad de los medios de transito		✕	No será implementado debido a que no se hizo una adecuada búsqueda y/o integración de los servicios de mensajería correspondientes desde un inicio, por lo que en este momento ya no es conveniente la implementación de este control.
10.8.4 Seguridad del Comercio Electrónico		✕	Actualmente dentro del sistema SMDP no se lleva acabo ningún tipo de comercio electrónico por lo que no hace transacciones de ventas en línea ni nada relacionado a sistemas de información de negocio, debido a que el SMDP no es un sistema de venta, por lo que los controles referentes a esto no serán involucrados dentro de las actividades del SMDP.
10.8.5 Sistemas de Información de Negocios		✕	No se cuenta con el tiempo (personal/recursos) para implementar este control.
10.9.1 Comercio Electrónico		✕	No aplica, dado que no es el giro del Hostpital.
10.9.2 Transacciones en línea		✕	El sistema no realiza transacciones de ventas en línea por lo que este control queda descartado para se implementado dentro del SMDP.
10.9.3 Sistema de Información a disposición del Público		✕	La información del SMDP no será puesta a disposición del público.

10. Gestión de Comunicaciones y Operaciones			
Control	**¿Será Implementado?**		**Justificación**
	Sí	**No**	
10.10.1 Registro de Eventos		✕	Los sistemas están ejecutando utilerías del sistema operativo Linux y se valido que dichas herramientas ya cumplen con lo marcado por este punto del estándar.
10.10.2 Monitoreo del Uso de los Sistemas	✔		Aunque se cuentan con herramientas para realizar monitoreo de los sistemas, no está establecido un procedimiento documentado para realizar las actividades de supervisión.
10.10.3 Protección de los Registros de Información.	✔		No se ha habilitado un mecanismo de protección para los registros que brindan los programas de monitoreo de actividades.
10.10.4 Registros de Operador y Administrador	✔		Aunque se están registrando las actividades de los usuarios y las actividades propias de los sistemas, no se está supervisando la actividad del personal de TI.
10.10.5 Registro de fallas	✔		Se están generando bitácoras referentes a fallos en el sistema, sin embargo no existe un procedimiento para revisar y tomar acciones basados en dichos registros.
10.10.6 Sincronización de relojes		✕	Se identificó que la sincronización de relojes está configurada de manera adecuada.

Tabla 31: Aplicabilidad para la cláusula 10.

4.5. Fase III: Ejemplo del desarrollo de los controles de seguridad seleccionados.

Cabe mencionar que en este punto se han logrado consolidar ya los fundamentos que nos ayudarán a integrar una estrategia de seguridad efectiva: se cuenta con un análisis de riesgos que incorpora las necesidades tecnológicas y la visión de la organización. A partir de este análisis, se ha establecido además un esquema de ponderación que nos permitió establecer las prioridades durante la fase siguiente: la selección de controles de seguridad.

Como ya ha sido mencionado, la oferta tecnológica en materia de seguridad de la información crece rápidamente y en respuesta a las situaciones de riesgo que se presentan en el momento. Así pues, una de las tareas más complicadas para el practicante de la seguridad de la información - integrar una propuesta técnico

normativa con vigencia a corto y mediano plazo – queda reducida a una selección basada en un análisis costo-beneficio que *además* es posible analizar con el personal directivo y administrativo de la organización.

A partir de este punto, siguiendo con el sistema SMDP como escenario de aplicación, se integrará una breve reseña, a manera de ejemplo, del desarrollo de controles de seguridad en los rubros tanto normativos como tecnológicos.

Desarrollo de controles ejemplo: “Baseline de Seguridad para servidores Linux” y “Baseline de Seguridad para dispositivos de comunicaciones”.

Como ya se mencionó, la aproximación de *línea base* a los problemas de seguridad, nos permite establecer rápidamente una solución a riesgos que, de manera puntual, se han identificado como prioritarios. Es importante recalcar, sin embargo, que esta aproximación al problema de seguridad no permite establecer planes a más largo plazo.

De tal suerte que mediante esta perspectiva estamos estableciendo un control *reactivo*, que es válido solamente en determinado intervalo del tiempo. Si se requiere revisar y actualizar el control de acuerdo con los cambios en la tecnología y en las amenazas, se recomienda hacer un análisis más profundo e incluir las tareas relativas al control un ciclo de calidad PDCA que nos permitan establecer un plan de mejora continua.

Dicho lo anterior, procederemos a revisar cómo se elabora un documento de configuración mínima de seguridad (que llamaremos *baseline*) para dispositivos de procesamiento y almacenamiento de seguridad así como para dispositivos de comunicaciones.

Para integrar un documento base que especifique las consideraciones mínimas de seguridad se requieren observar las siguientes fases:

1. Como primera actividad, el practicante de seguridad de la información se da a la tarea de revisar los estándares y mejores prácticas existentes en la industria y en las comunidades de seguridad de la información.

   En este sentido, para la integración de actividades por área y por dispositivo, se recomienda hacer uso de los siguientes recursos:

   - NIST: El Instituto Nacional de Estándares y Tecnologías (NIST) es una agencia del Departamento de Comercio de los Estados Unidos, cuya misión es promover la innovación y competitividad industrial.

     La División de Seguridad en Cómputo (CSD, por sus siglas en inglés) desarrolla y publica estándares que apoyan en el establecimiento de requisitos mínimos de seguridad para diversos sistemas.

     En el contexto SMDP, se utilizaron estas recomendaciones para generar líneas base de configuración segura para los dispositivos de comunicaciones, servidores de aplicativos, servidores Web y bases de datos.

   - CERT: Establecido en 1988, el CERT es parte del Instituto en Ingeniería del Software, en la Universidad Carnegie Mellon. Entre otras actividades, el CERT es responsable de analizar y reducir las amenazas y vulnerabilidades informáticas, difundir información de advertencia sobre las más recientes amenazas y coordinar actividades de respuesta a incidentes en cómputo.

     El CERT también cuenta con publicaciones que documentan las mejores prácticas para configuración y administración de dispositivos de tecnología de información. Así, se han tomado aquellas recomendaciones que son aplicables a los distintos componentes tecnológicos del SMDP

2006 como insumos para generar listas de configuraciones mínimas seguras.

- SANS: El Instituto SANS es uno de los principales centros de certificación y entrenamiento para profesionales de la Seguridad Informática a nivel mundial. Como parte de sus tareas desarrolla, mantiene y pone a disposición de la comunidad de Internet documentos que cubren aspectos varios de la seguridad informática.

  Las recomendaciones que se consideraron pertinentes para el SMDP fueron integradas para la elaboración de configuraciones mínimas de seguridad para los distintos dispositivos de la infraestructura tecnológica.

De manera adicional, cabe mencionar que los controles de seguridad aplicados al ciclo de vida del desarrollo del sistema SMDP (planeación, análisis de requerimientos, diseño, desarrollo y pruebas) se basaron en COBIT. Dado que la aplicación de controles de seguridad al ciclo de desarrollo de software representa un tema muy amplio, no se tocará en el presente trabajo.

2. A partir de los insumos obtenidos de las distintas fuentes, el practicante debe integrar una lista de requerimientos de seguridad (*checklist*) en donde se plasmen las medidas mínimas requeridas para mitigar un riesgo.
3. Con la lista de requerimientos de seguridad, se procede a entrevistar a los administradores del componente, para acordar con ellos qué controles aplican para la situación particular de un dispositivo.

   Este es un paso de vital importancia, por que a partir de esta entrevista se integra un muy rudimentario y acotado análisis costo-beneficio de la implantación del control.

   Por ejemplo, las mejores prácticas de seguridad nos indican que los protocolos utilizados para la administración remota de equipos de comunicación deben ir *montados* sobre un protocolo que brinde los servicios de seguridad (OpenSSL, TLS, etc.). Sin embargo, existen situaciones en las que debido al tipo de licencia adquirida, no es posible bloquear puertos o protocolos.
4. Finalmente, se procede con la elaboración del propio documento de configuración básica de seguridad. Se debe incluir en el cuerpo de este documento, los detalles de las configuraciones establecidas, así como indicar claramente el por qué alguna de ellas no ha podido ser implantada de manera total o tal como lo solicitó el practicante de la seguridad de la información.

Para referencia y apoyo durante la dimensión en tiempo de este tipo de tareas, se muestran en la tabla 32 los tiempos estimados para el desarrollo de algunos controles como parte del proyecto de fortalecimiento de seguridad del SMDP.

Creación de baselines de seguridad	Tiempo
Crear baseline para servidores Linux Red Hat AS	5 días
Crear baselines para servidores de bases de datos Oracle	5 días
Crear baselines para servidores web	5 días
Crear baselines para equipo de comunicaciones (Firewalls, Switches, Routers, Redes)	20 días
Crear baselines para equipo Windows XP	10 días
Crear baseline para servidor DNS	5 días
Crear baseline para SAN	5 días
Crear baseline para Firewalls (servidores linux)	5 días
Entregables	

• Baselines de seguridad de los servidores	0 días
• Baselines de equipos de comunicación	0 días
• Baseline de SAN	0 días
• Baseline de DNS	0 días
• Baseline de Firewall de host	0 días

Tabla 32: Tiempos invertidos para realizar los baseline.

Se muestra a continuación el proceso de desarrollo de estos controles mediante un par de ejemplos:

Desarrollo de Baseline de Seguridad para Servidores Linux.

1. Revisión de estándares y mejores prácticas de seguridad.

   Para el desarrollo de este documento se consultaron las siguientes referencias:

   a) Unix Security Checklist v2.0
   http://www.cert.org/tech_tips/usc20.html#3.2

   b) IT Baseline Protection Manual.
   http://www.bsi.bund.de/english/index.html

   c) Red Hat Enterprise 3: Security Guide.
   https://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/security-guide/

   d) TCP-IP Stack Hardening.
   http://www.cromwell-intl.com/SECURITY/security-stack-hardening.html

2. Integración de la lista de requerimientos de seguridad para servidores Linux (checklist).

ID	Configuración	Implantación		Comentarios y/o Justificación
		Sí	No	
Seguridad Física del Servidor				
1	El servidor se debe ubicar en un site con acceso controlado.	✓		
2	Contar con UPS (Unninterrumpible Power Supply).	✓		

ID	Configuración	Implantación		Comentarios y/o Justificación
		Sí	No	
3	Contar con doble fuente de alimentación y cada una conectada a diferente línea.	✓		
4	Identificar con etiqueta o algún otro medio al servidor.	✓		
	Conocer la ubicación exacta del equipo (site, rack, posición).	✓		
5	Asignar contraseña al BIOS del servidor.	✓		Se agregará también contraseña para el arranque del equipo
6	Deshabilitar la opción para bootear desde CD una vez que el servidor haya sido instalado.	✓		
Instalación del Servidor				
1	Contar con un esquema de particionamiento bien definido de acuerdo a las necesidades del sistema.	✓		Verificar el esquema de particionamiento a utilizar en la SAN.
2	Contar con particiones independientes para cada file system.	✓		
3	Generar un kernel personalizado, no utilizar el que se instala por default. Deshabilitar la opción *firewall packet netlink device* para evitar conflictos con iptables. Habilitar los módulos necesarios de Netfilter (iptables). Hacer un aseguramiento general de la implementación de la pila TCP/IP como: Deshabilitar la opción de *ip_forwarding*. Deshabilitar la respuesta a paquetes icmp de broadcast. Deshabilitar los mensajes de redirección de IP (Puede ser modificada la tabla de ruteo local). Deshabilitar la opción de *syn_cookies* para evitar ataques de DoS:	✓		Aplicará a todos los servidores con excepción de los que tendrán Oracle donde se irá el kernel por default de Red Hat, esto por las cuestiones relativas al soporte de los productos de Oracle sobre Red Hat.
4	Proteger el bootloader (grub) mediante el uso de contraseña.	✓		
5	Evitar dentro de lo posible la instalación del servidor X.	✓		Aplicará a todos los servidores con excepción de los que tendrán Oracle.
6	Actualizar el sistema en su totalidad con las últimas actualizaciones de seguridad (kernel y aplicaciones).	✓		Se definirá una fecha previa donde se dejará de actualizar el sistema para evitar que alguna actualización afecte las aplicaciones. En caso de surgir una vulnerabilidad crítica después de esta fecha se debe instalar previa definición del esquema a seguir (Maqueta de pruebas, etc).
7	Descargar los parches de actualización del sitio oficial de Red Hat, así como verificar el checksum y las firmas electrónicas de los paquetes descargados.	✓		
8	Establecer esquema de cuotas en el sistema de archivos.	✓		
9	Habilitar el uso del directorio /shadow	✓		
Servicios				
1	Identificar qué servicios se están ejecutando en el servidor.	✓		
2	Deshabilitar aquellos servicios que no son necesarios (cups, kudzu, lpd, etc.).	✓		
3	Utilizar versiones seguras de los servicios si es que existen (ssh, sftp, https, etc.).	✓		
4	De ser posible ejecutar los servicios con un usuario diferente a root.	✓		
5	Los servicios deberán estar debidamente	✓		Se deshabilitarán los banners en todos los servicios excepto

ID	Configuración	Implantación		Comentarios y/o Justificación
		Sí	No	
	configurados y no mostrar información innecesaria. (el banner no deberá mostrar la versión del software, sistema operativo, opciones de compilación,etc).			Oracle que se dejará por default.
	En caso de que el servidor cuente con un servidor web (Apache), seguir las recomendaciones baseline relativo a servidores WEB.	✓		
6	Habilitar el envío de eventos relevantes a bitácoras. Accesos a servicios, autenticaciones exitosas y fallidas, alta, baja y reinicio del servicio, intentos continuos de conexión, número de conexiones activas, etc.	✓		
7	Deshabilitar, de ser posible, el servicio de portmap. (Este servicio no se requiere si no se está utilizando NIS o NFS).	✓		No se utilizará NFS en ninguno de los servidores.
8	Habilitar los mecanismos de control de acceso (iptables, tcpwrappers).	✓		
9	Sincronizar la hora y fecha del equipo con el servidor NTP del Hospital.	✓		Se utilizará el servidor por defecto.
	Cuenta de root			
1	Habilitar el uso de contraseñas con MD5	✓		
2	Las características de la contraseña serán: ▪ 16 caracteres como mínimo ▪ Emplear al menos un carácter especial. ▪ Emplear al menos una letra mayúscula o minúscula. ▪ Cambiar la contraseña mensualmente. ▪ Contener letras mayúsculas y letras minúsculas Contener *al menos* uno de los siguientes símbolos especiales: !, @, #, $, %, &, /, (,), ?, _, \, +, “ ▪ Contener *al menos* un dígito (0-9) ▪ Evitar reciclar la contraseña <u>La contraseña no debe:</u> ▪ Estar basada en palabras que se encuentren en el diccionario ▪ Estar basada en información personal. Esto incluye palabras tales como nombres de familiares, nombres de mascotas, nombres de lugares, fechas de cumpleaños, números de teléfono. ▪ Estar basada en patrones simples de letras del teclado, tales como *aaaaa*, *qwerty*, *123321*, etc. ▪ Estar basada en cualquiera de las anteriores deletreadas hacia atrás. Por ejemplo: *oterces*, *elcaro*, etc.	✓		Aún falta definir la matriz de las personas que tendrán la contraseña de root y el período en que se cambiarán.
3	Contar con un esquema bien definido de cambio periódico de contraseña.	✓		
4	Restringir el comando *su* a un grupo específico de usuarios (P.ej. wheel).	✓		
5	Hacer uso de la utilería *sudo* para control de acceso y ejecución de comandos	✓		

ID	Configuración	Implantación		Comentarios y/o Justificación
		Sí	No	
	administrativos.			
6	Restringir el acceso directo con la cuenta de root excepto desde la consola del servidor.	✓		
7	La ejecución de comandos cuando se es root se debe hacer empleando rutas absolutas.	✓		
8	Verificar que los archivos o scripts que son ejecutados por el cron de root pertenezcan a él.	✓		
	Autenticación y usuarios			
1	Saber con exactitud cuántos usuarios están dados de alta en el sistema mediante un documento formal.	✓		Ya se cuenta con una matriz de usuarios, se debe actualizar y dejar a punto.
2	Contar con algún criterio para limitar el uso de recursos del sistema a los usuarios; podría ser mediante el uso de perfiles.	✓		
3	Definir un criterio para la asignación de contraseñas a los usuarios se propone el siguiente: • Tener una longitud mínima de 8 caracteres • Contener letras mayúsculas y letras minúsculas • Contener *al menos* uno de los siguientes símbolos especiales: !, @, #, $, %, &, /, (,), ?, _, \, +, “ • Contener *al menos* un dígito (0-9) <u>La contraseña no debe:</u> • Estar basada en palabras que se encuentren en el diccionario • Estar basada en información personal. Esto incluye palabras tales como nombres de familiares, nombres de mascotas, nombres de lugares, fechas de cumpleaños, números de teléfono. • Estar basada en patrones simples de letras del teclado, tales como *aaaaa*, *qwerty*, *123321*, etc. • Estar basada en cualquiera de las anteriores deletreadas hacia atrás. Por ejemplo: *oterces*, *elcaro*, etc.	✓		
4	Definir una estructura de grupos del sistema con sus respectivos privilegios y restricciones.	✓		
5	Deshabilitar los esquemas que no requieren de contraseña (borrar /etc/host.equiv, .rhost, etc).	✓		
6	Emplear SSH para sesiones remotas	✓		
7	No permitir el uso de sesiones remotas sobre canales no cifrados como rlogin,	✓		

ID	Configuración	Implantación		Comentarios y/o Justificación
		Sí	No	
	rsh, telnet, ftp, etc.			
8	Deshabilitar el acceso remoto como root.	✓		
	Monitoreo			
1	Verificar que el servicio de syslog esté activado.	✓		
2	Contar con un servidor centralizado y remoto de bitácoras.	✓		Definir la política de envío de bitácoras, a qué servidor se enviarán.
3	Contar con algún mecanismo automático de monitoreo de bitácoras (logwatch, swatch, etc.).	✓		Se utilizará logwatch en su configuración básica.
4	Contar con algún mecanismo de integridad de archivos del sistema (tipo tripwire).	✓		Se monitorearan aplicaciones y archivos de configuración.
5	Instalar el monitoreo de accouting del sistema (uso de recursos del sistema).	✓		Una vez instaladas todas las aplicaciones se integrará el sistema de accounting para verificar consumo de recursos y performance de los equipos, hasta este momento se valorará si es posible o no tenerlo habilitado por cuestiones de desempeño.
6	Llevar un control y monitoreo de los trabajos calendarizados (cron, at).	✓		
7	Monitorear todos los servicios instalados en el servidor.	✓		Se instalará un servidor de monitoreo con Nagios donde se estarán monitoreando los servicios importantes.
8	Dentro de lo posible contar con un IDS tipo snort para detectar eventos de seguridad.	✓		Se tiene con el uso de un IDS de CISCO, verificar si esto es posible.
	Red			
1	Asignar una dirección IP bien definida	✓		
2	La asignación de la IP deber ser de manera estática.	✓		
3	Configurar firewall de host (iptables) con política restrictiva.	✓		
4	Configurar TCP-Wrappers de manera restrictiva y enviando alertas de intento de accesos	✓		
5	Replicar las reglas de filtrado de paquetes en iptables y tcp wrappers.	✓		
6	Verificar qué servicios de red están activos (netstat –na| grep LISTEN). Validar que sean los correctos y/o autorizados.	✓		Se estarán monitoreando con Nagios en lugar de con netstat, se define un período de 1 hora para estar monitoreando los servicios.
7	Deshabilitar el acceso como root vía SSH.	✓		
8	Configurar el banner de acceso en SSH.	✓		
9	Sólo acceder por el protocolo 2 de SSH.	✓		
10	En caso de contar con algún sistema de archivos en red (NFS), habilitar algún mecanismo de control de acceso a este recurso. Por ejemplo: Filtrar el puerto 111 udp y 2049 tcp en el firewall o router del perímetro para que sólo accedan equipos de la red local. Montar los sistemas de archivos como solo lectura. Evitar exportar el sistema de archivos a todos, usar la opción *access=host.*		☒	No aplica, no se contará con ningún sistema de archivos de red. Aplicar las reglas de filtrado en equipos de comunicaciones.
11	Todas las sesiones gráficas remotas deberán hacerse utilizando SSH.	✓		No habrá sesiones gráficas remotas, todas las sesiones gráficas serán vía consola.
12	Deshabilitar el ip_forwarding a nivel kernel. Se verifica cat /proc/sys/net/ipv4/ip_forward debe ser 0.	✓		

ID	Configuración	Implantación		Comentarios y/o Justificación
		Sí	No	
13	Controlar el acceso vía remota usando SSH mediante usuario@dirección_ip	✓		
	Recuperación			
1	Definir un esquema de respaldos, y contar con los procedimientos necesarios.	✓		Falta definir esquema de respaldos, se realizarán en DVD.
2	Verificar el funcionamiento del esquema de respaldos. Probar si se puede recuperar la funcionalidad del sistema con los respaldos que se realizan.	✓		Se verificará en la prueba y puesta en marcha del DRP.
3	Se cuenta con el expertise y/o la documentación necesaria para reparar el servidor desde desperfectos físicos hasta la puesta en producción de los servicios.	✓		Se verificará en la prueba y puesta en marcha del DRP.
	Permisos			
1	Verificar que el umask default de todos los archivos sea 022.	✓		
2	Revisar que el directorio y archivos bajo /var/log puedan ser sólo escritos por root	✓		
3	Verificar que el archivo /etc/services/ pertenece a root y sus permisos son 644	✓		
4	Verificar que el archivo /etc/login.defs pertenece a root y sus permisos son 600	✓		
5	Verificar que el archivo /etc/crontab pertenece a root y permisos 600. Si es posible, deshabilitar el uso de cron a usuarios.	✓		
6	Verificar que los permisos de los archivos /etc/motd y /etc/mtab sean 644	✓		
7	Verificar que el archivo /etc/exports pertenece a root y sus permisos sean 644.	✓		
8	Verificar que los permisos de los archivos /var/run/syslog.pid sean 644	✓		
9	Considerar el deshabilitar el acceso a lectura a archivos de configuración del sistema. Dejar el permiso sólo a root. (p.ej. /etc/hosts.allow, etc.)	✓		
10	Verificar que la imagen del kernel /boot/vmlinuz pertenece al grupo 0, su dueño es root y sus permisos sean 644.	✓		
11	Verificar que los directorios /etc /usr/etc /bin /usr/bin /sbin /usr/sbin /tmp y /var/tmp pertenecen a root y el sticky-bit se encuentra sólo en los directorios /tmp y /var/tmp	✓		
12	Verificar que todos los archivos bajo /dev sean archivos especiales (de carácter o bloque).	✓		
13	Hacer una revisión de los archivos que cuentan con SUID y GID, validar que dichos archivos realmente lo requieren y eliminar el sticky-bit de aquellos en los que no sea necesario. A continuación los que son necesarios: /bin/ping /bin/su /usr/bin/at /usr/bin/chage /usr/bin/chfn /usr/bin/chsh	✓		Verificar que estos comandos son los necesarios y no afecta a ninguna aplicación.

ID	Configuración	Implantación		Comentarios y/o Justificación
		Sí	No	
	/usr/bin/crontab /usr/bin/gpasswd /usr/bin/newgrp /usr/bin/passwd /usr/sbin/postdrop /usr/sbin/postqueue /usr/sbin/utempter			
NFS				
1	Deshabilitar NFS si no es necesario		☒	No se cuenta con ningún NFS no aplican ninguno de estos controles.
2	Verificar que en el archivo /etc/exports no se encuentre ninguna entrada como "localhost".		☒	
3	Utilizar nombres completos o IP's bien definidas e identificadas en el archivo /etc/exports.		☒	
4	Ejecutar showmount –e para verificar que sistemas de archivos se están exportando y verificar que sean los correctos.		☒	

3. Integración del baseline.

Baseline:

El sistema operativo Linux ha demostrado ser una opción viable para sistemas críticos y de alta disponibilidad siendo utilizado en centros de investigación reconocidos como la NASA y en un gran número de instituciones académicas a nivel mundial. Como cualquier otro sistema operativo, cuenta con vulnerabilidades que lo hacen susceptible de ataques sin embargo, también puede ser configurado para ser un sistema estable, seguro y con una gran disponibilidad. En este sentido, se ha logrado que la distribución de Linux Red Hat Enterprise que será la utilizada en los servidores del SMDP, haya alcanzado el nivel de seguridad EAL3 que establecen los Criterios Comunes.

Las recomendaciones de seguridad que a continuación se listan están basadas en estándares reconocidos internacionalmente como los Criterios Comunes, los estándares de seguridad BS779/ISO 17999, recomendaciones de configuración emitidas por el CERT, el IT Baseline Protection Manual y todo esto complementado con la experiencia de los administradores que mantienen los sistemas del Hospital.

Los aspectos considerados son lo siguientes:

Seguridad Física del Servidor.

La seguridad física de los servidores es el último perímetro de seguridad del sistema SMDP, y requiere contar con condiciones ambientales óptimas (temperatura, humedad), suministros de energía adecuados y mecanismos de control de acceso para su óptimo desempeño y funcionamiento; todo esto con el firme objetivo de prevenir accesos no autorizados, daños e interferencia en los sites donde se

ubiquen físicamente los servidores e información tratada por el sistema SMDP.

Instalación del Servidor.

Se generará un kernel personalizado para el servidor dependiendo de los servicios con que contará a excepción de los servidores de bases de datos Oracle en cuyo caso se utilizará el kernel por default de Red Hat; esto con el fin de evitar que se encuentren habilitadas opciones no necesarias que consuman recursos o bien que permitan la explotación de alguna vulnerabilidad.

Se habilitarán los módulos necesarios para las aplicaciones que se ejecutarán, por ejemplo:

- Habilitar todos los módulos de Netfilter.
- Deshabilitar el módulo *firewall packet netlink device* para evitar conflictos con el firewall generado por iptables.
- Deshabilitar la opción *ip_forwarding* que evita la redirección de paquetes hacia otros destinos diferentes al original.
- Deshabilitar la respuesta a paquetes icmp de broadcast lo que evitará que el equipo responda a una petición de ping hecha al broadcast de la red en que se encuentra.
- Deshabilitar los mensajes de redirección de IP, que puede dar la opción a modificar la tabla de ruteo local.
- Deshabilitar la opción *syn_cookies* que evita exponer el equipo a ataques de denegación de servicio basadas en esta técnica.

El esquema de particionamiento estará definido de acuerdo con el tipo de aplicaciones que se ejecutarán en el servidor con el fin de dimensionar el espacio en disco necesario que evite de alguna manera la saturación de una partición y mantener la disponibilidad del sistema o bien el desperdicio de recursos finitos, esto se logra estableciendo límites al uso de espacio en disco mediante cuotas para evitar el uso ilimitado de recursos del sistema

En cualquier proceso de instalación y/o actualización de alguna nueva aplicación o RPM, será descargado del sitio oficial de Red Hat https://rhn.redhat.com y siempre se verificará que el cheksum coincida con el proporcionado por el proveedor del paquete.

En esta etapa, se deshabilitarán servicios que se sabe de entrada no se estarán ejecutando en el servidor como:

- cups
- kudzu
- lpd

Servicios

Los servicios son parte esencial de un sistema, son quienes proporcionan la funcionalidad misma al servidor, como su nombre lo indica es el servicio que se proporciona a través del servidor, por lo que debemos ocuparnos del control de acceso, la disponibilidad y generación de bitácoras de eventos relevantes que suceden con determinado servicio.

Con la documentación de los servicios que se están ejecutando en el servidor y su plena identificación, se permite tener un conocimiento a fondo del equipo y así poder deshabilitar servicios no necesarios que pueden ser puertas de entrada hacia nuestro sistema, reduciendo así, el abanico de posibilidades de un posible ataque.

El acceso a servicios será única y exclusivamente para los equipos de la red del Hospital MedSite, es decir, ninguna dirección IP que no pertenezca a esta red podrá consultar o acceder a alguno de los servidores que conforman el SMDP.

Lo anterior se complementa con una buena definición de las reglas de un firewall a nivel de host que esté basado en una política restrictiva,"Todo lo que no esté explícitamente permitido está prohibido", y habilitando mecanismos de control de acceso a servicios de red como TCP-Wrappers que permiten, de alguna manera, tener un segundo nivel de control de acceso dando la posibilidad de alertar al administrador de posibles accesos no permitidos mediante el envío de un correo electrónico.

Como parte del control de acceso a servicios, se debe habilitar el envío a bitácoras de información relevante como accesos, salidas del sistema, intentos fallidos de conexión y autenticación, alta, baja y reinicio del servicio, etc., todo esto para poder hacer a los servicios objetos de monitoreo y auditoria.

Se hará una personalización de los banners que muestran los servicios cuando se accede a ellos, esto para evitar que se muestre información innecesaria de software y versiones que están siendo ejecutadas que permita la ejecución de ataques remotos a ciertas versiones de aplicaciones. El banner a utilizar será el siguiente:

```
+--------------------------------------------------------------------------+
|                        HOSPITAL MEDSITE                                  |
+--------------------------------------------------------------------------+

  Este es un sistema Privado propiedad del Hospital MedSite.

  El  acceso  a  este sistema  está reservado exclusivamente a personal
  autorizado  por  el  Hospital MedSite  para la realización
```

de tareas administrativas y de mantenimiento.

Todas las actividades que se realicen durante la sesión serán registradas y monitoreadas; los intentos de conexión no autorizados serán motivo de investigación y remitidos a las autoridades competentes.

+---+
| Departamento de TI |
+---+

==========

La sincronización de todos los equipos en fecha y hora es de vital importancia en el sistema SMDP, todos los componentes del sistema estarán sincronizados en fecha y hora permitiendo la puesta en producción de todos los componentes sincronizados entre sí. La sincronización deberá realizarse con un servidor de tiempo, en este caso con el servidor por defecto de la red del Hospital MedSite.

Cuenta de root

La cuenta de superusuario en sistemas Linux root es de vital importancia para la administración y acceso de recursos del servidor en general, ya que tiene los privilegios suficientes y necesarios para dar de baja en su totalidad al sistema. Para cumplir con las recomendaciones de seguridad al respecto el Jefe del Departamento de TI, será la persona que configure y tenga conocimiento de dicha contraseña, también se almacenaran en sobre cerrado y dentro de una caja fuerte, con el objetivo de tenerla disponible en caso que la persona mencionada anteriormente no se encuentre disponible, sólo personal autorizado tendrá acceso a dicho sobre. Se deberá tener un control a detalle de los usuarios que tengan permiso de ejecutar el comando “su” para convertirse en superusuario así como algunas buenas prácticas como la ejecución de comandos utilizando rutas absolutas cuando se es root.

Dentro de las características con que deberá contar la contraseña de root se encuentran:

- 16 caracteres como mínimo
- Emplear al menos un carácter especial.
- Emplear al menos una letra mayúscula o minúscula.
- Cambiar la contraseña mensualmente.
- Contener letras mayúsculas y letras minúsculas
- Contener *al menos* uno de los siguientes símbolos especiales: !, @, #, $, %, &, /, (,), ?, _, \, +, “

- Contener *al menos* un dígito (0-9)

La contraseña no debe:

- Estar basada en palabras que se encuentren en el diccionario
- Estar basada en información personal. Esto incluye palabras tales como nombres de familiares, nombres de mascotas, nombres de lugares, fechas de cumpleaños, números de teléfono.
- Estar basada en patrones simples de letras del teclado, tales como *aaaaa*, *qwerty*, *123321*, etc.
- Estar basada en cualquiera de las anteriores deletreadas hacia atrás. Por ejemplo: *oterces*, *elcaro*, etc.

De la mano con un esquema definido de roles y permisos de usuarios y archivos, se configurará restrictivamente la herramienta sudo, asignando la menor cantidad de privilegios a usuarios para evitar así el uso indiscriminado de privilegios en el sistema.

Autenticación y usuarios

Controles de seguridad a nivel sistema operativo para restringir el acceso a los recursos del sistema para lograr identificar y verificar la identidad y ubicación desde donde se está teniendo acceso a los recursos; tanto a nivel autenticación de usuarios como accesos remotos.

Todos los usuarios tendrán un UID único identificable de uso personal e intransferible y su autenticación con el sistema será a través del uso de contraseñas; además, pertenecerán a un grupo válido dentro del sistema y se contará con una matriz de usuarios que defina el rol de usuario y permisos de acceso a recursos del sistema.

Una vez instaladas todas las aplicaciones, se procederá a la instalación del sistema de contabilidad del sistema SAR[55]. El sistema de accounting permitirá identificar qué usuario o procesos está consumiendo la mayor cantidad de recursos y por qué.

Monitoreo

El proceso de monitoreo es necesario para asegurar que se está haciendo uso correcto y realizando las actividades permitidas sobre los recursos del sistema, se incluirá monitoreo de:

- Acceso al sistema
- Usuario que ingresa

[55] SAR. System Accounting Resources. El comando sar produce informes de utilización del sistema basado en los datos reunidos por sadc. Los informes sar, se pueden generar interactivamente o se pueden escribir a un archivo para un análisis más intensivo. De acuerdo con la configuración en Red Hat Enterprise Linux, SAR es ejecutado automáticamente para procesar los archivos reunidos automáticamente por sadc. Los archivos de informes se escriben a /var/log/sa/ y son nombrados sar<*dd*>, donde <*dd*> son las representaciones de dos dígitos de la fecha del día anterior.

- Fecha y hora del acceso
- Tipo de eventos realizados
- Comandos ejecutados
- Acceso a archivos
- Programas o aplicaciones utilizadas.
- Se tendrá un monitoreo detallado de las actividades de la cuenta de administrador
- Inicio y apagado del sistema
- Accesos no autorizados
- Intentos de acceso fallidos
- Calendarización de trabajos.

Dentro del proceso de monitoreo se encuentra el envío y análisis de éstos eventos a bitácoras. Se tendrá también un contenedor central de bitácoras remoto donde en caso de pérdida o alteración de las bitácoras en el servidor se cuente con el respaldo en un servidor externo. Además, dentro del análisis de bitácoras, está el uso de herramientas como logwatch para generar un resumen de todos los eventos ocurridos en el sistema y que han sido enviados a bitácoras, con el fin de tener un mecanismo de análisis de información más digerible para su análisis.

Red

Estas configuraciones están orientadas al uso seguro de los servicios de red que esté prestando el servidor y van desde la asignación de la dirección IP hasta la configuración de algunos servicios de red.

La asignación de la dirección IP será de manera estática, es decir, no estará dado por un servidor DHCP lo que provocaría la dependencia de un servicio extra que en este caso por ser un ambiente plenamente identificado y controlado no es necesario. Como se mencionó, la habilitación de todos los servicios y en especial aquellos que puedan ser vistos a través de la red, estarán controlados por un firewall de host que sólo permitirá el acceso a servicios previamente definidos y bien identificados, además de contar con una replicación de control de acceso a servicios mediante tcp-wrappers donde se definirán las direcciones IP válidas para conectarse o acceder a cierto servicio.

Se hará un monitoreo continuo de aquellos servicios que abren algún puerto. Esto se hará mediante la configuración de un servidor con Nagios dedicado a monitorear algunos servicios del sistema SMDP.

También, dado que el acceso remoto al servidor será única y exclusivamente vía Secure Shell (ssh), es necesario asegurar que dichas sesiones sean lo más seguras posibles. De entrada, haciendo uso de este servicio, garantizamos un canal seguro de comunicación, sin embargo; hay que hacer algunas consideraciones en la configuración de este servicio como:

- Deshabilitar el acceso remoto como root al servidor

- Usar solamente protocolo 2 de SSH
- Definir y habilitar el banner que se mostrará al hacer una conexión vía este servicio.
- Controlar mediante la pareja usuario-ip el acceso por secure shell al servidor, con el fin de evitar que se acceda al servicio desde algún equipo externo.

En cuanto las sesiones gráficas, se ha definido que las sesiones gráficas por ningún motivo serán remotas así que no se permitirá la exportación del display y se filtrará desde la configuración del servicio de ssh, hasta la implementación de esta restricción en las reglas del firewall de host.

Recuperación

Dentro de la sección de recuperación se tratan los aspectos relacionados con el esquema de respaldos que se utilizará así como la documentación y puesta en marcha del plan de recuperación de desastres que deberá realizarse para recuperar el servidor en su totalidad.

Permisos

Los permisos en el sistema de archivos de un sistema Linux son parte esencial del control de acceso a recursos del sistema, una buena gestión de los roles y permisos de usuarios blindará todos y cada uno de los controles antes mencionados. En particular, se deberá tener cuidado con aquellos archivos que dentro de sus permisos tengan habilitado el sticky bit que permite la ejecución de dicho archivo con privilegios administrativos entre los archivos que deben tener habilitado el sticky bit se encuentran:

- /bin/ping
- /bin/su
- /usr/bin/at
- /usr/bin/chage
- /usr/bin/chfn
- /usr/bin/chsh
- /usr/bin/crontab
- /usr/bin/gpasswd
- /usr/bin/newgrp
- /usr/bin/passwd
- /usr/sbin/postdrop
- /usr/sbin/postqueue
- /usr/sbin/utempter

Existen directorios que tienen ya definidos una serie de permisos y dueños y que por ningún motivo deben variar, para tener control sobre esto, se hará uso de la herramienta de control de integridad de archivos tripwire y estará funcionando en específico sobre archivos de configuración tanto del sistema como de aplicaciones y archivos binarios que una vez terminada la etapa de pruebas no deberán tener variaciones de permisos, dueño, tamaño o contenido durante todo el ciclo de vida del sistema.

También se protegerán archivos que puedan mostrar información sobre la configuración de los sistemas, este tipo de archivos sólo pertenecerán, serán leídos y serán modificables por el usuario root.

Desarrollo de Baseline de Seguridad para Equipos de Comunicación.

1. Revisión de estándares y mejores prácticas de seguridad.

a) Documento CERT
Deploying Firewalls
http://www.cert.org/security-improvement/modules/m08.html

b) Fundamentos de Seguridad de Redes.
CiscoPress.
Traducción: José Manuel Díaz.

c) Documento desarrollado por DISA (Defense Information Systems Agency) y por el DoD (Department of Defense of United States of America)
Network Infrastructure
Security Technical Implementation Guide
Version 6, Release 3
5 Julio 2005.
http://csrc.nist.gov/pcig/STIGs/network-stig-v6r3.pdf

2. Integración de la lista de requerimientos de seguridad para dispositivos de comunicaciones (checklist).

ID	Configuración	Implantación		Observaciones.
		SI	NO	
Documentación de la Red.				

1	Generar y mantener un diagrama actualizado de la red, que incluya todos los enlaces externos e internos, subredes, y todo el equipo de red.	✓		Se generaran diagramas para la red del Hostpital MedSite y se incluirán direcciones IPs y MACs de todos los equipos.
Conexiones Externas.				
2	Asegurar que todas las conexiones externas estén validadas y aprobadas antes de la conexión.	✓		
3	Bloquear o desconectar conexiones que sean inapropiadas.	✓		
Conexiones que puedan ser usadas como puertas traseras.				
4	Asegurarse que no existen conexiones que puedan servir de puertas traseras.	✓		Se revisarán y depurarán cuentas de MODEM, y se asegurará que cuenten con contraseñas seguras.
Direccionamiento IP.				
5	Asegurarse que todas las direcciones usadas en la infraestructura son direcciones autorizadas y han sido registradas y asignadas.	✓		
NAT.				
6	Asegurarse que las direcciones IP de la LAN no son reveladas al público implementando NAT en el firewall o router.	✓		Se considerara la utilización de NAT en la red
Monitoreo.				
7	Asegurarse de implementar mecanismos de análisis de rendimiento de los equipos y enlaces de la red de MedSite	✓		Se analizará cuáles son los requerimientos necesarios para que un equipo pueda monitorear todo el tráfico y equipos de red de MedSite (oficinas centrales y clínicas regionales). Definir qué es lo que se va a monitorear y con qué software. Analizar opciones de monitoreo como nagios, cricket, mrtg, netflow, etc.
QoS.				
8	Implementar QoS para asegurar un ancho de banda a las aplicaciones del SMDP.	✓		
IDS.				
	Se implementarán NIDS que nos permitan identificar en tiempo real cualquier intento de intrusión.	✓		

3. Integración del baseline.

***Antecedentes**:*

Uno de los retos de cualquier red es cómo mitigar los ataques. Desarrollando estrategias de seguridad para piezas críticas de la infraestructura de la red es uno de los mecanismos a través de los cuales se

puede lograr dicho reto.

Cualquier infraestructura de red o comunicación debe mantener seguros, disponibles y confiables los datos de los usuarios.

***Objetivo**:*

Ayudar a conocer los mínimos requerimientos estándares, controles y opciones de configuración que deben implementarse para asegurar la operación de la red.

***Alcance**:*

La información que se presenta aquí ayudará para controlar el acceso, resistir ataques, protegerse de otras redes y proteger la integridad y confidencialidad del tráfico de la red.

Siguiendo las recomendaciones en este baseline no garantiza un entorno seguro o que el administrador va prevenir todas las intrusiones. Sin embargo, el administrador puede alcanzar una seguridad razonable estableciendo buenas políticas de seguridad, manteniéndose actualizado sobre los últimos desarrollos de las comunidades de hackers y de seguridad, y manteniendo y monitoreando todos los sistemas.

El carácter de este documento es obligatorio, lo cual quiere decir que se deberá cumplir cabalmente con lo especificado a continuación.

Baseline:

Infraestructura de Red

Sin documentación exacta y actualizada, cualquier cambio en la infraestructura de red puede afectar la integridad de la red. Para ayudar a la administración, auditoria, y seguridad de la red, se harán diagramas y mapas topológicos de red. Los mapas topológicos mostrarán el esquema general de la infraestructura de red y donde los dispositivos de red estarán físicamente localizados. También mostrarán la relación entre los dispositivos interconectados que nos ayudará a identificar dónde podría haber un posible ataque.

Conexiones Externas

Las conexiones a redes externas son una de las áreas más complejas de diseño, implementación y administración de la red. Una red externa es conectada a la red interna a través de conexiones externas que pueden incluir circuitos dedicados, dial-on-demand Integrated Services Digital Network (ISDN), etc.

Sin importar la tecnología usada, cada conexión externa a la red interna será asegurada para no introducir ningún riesgo a la red. Cada site tendrá políticas de seguridad que filtren tráfico de dichas conexiones.

Es por ello que se implementaran las siguientes medidas:

- Asegurar que todas las conexiones externas estén validadas y aprobadas antes de la conexión.

- Bloquear o desconectar conexiones que sean inapropiadas.

NAT

En una red segura, es importante que sus direcciones IP internas permanezcan ocultas al exterior, de forma que ningún atacante potencial puede obtener información referente a la topología de la red y su diseño.

NAT puede ocultar estas direcciones, lo que dificulta que esos atacantes obtengan información importante sobre la red y la utilicen para explotar sus vulnerabilidades. Por tal motivo se implementará NAT en la red perimetral.

Detección de Intrusos

Como intrusión se entiende la realización de un acto no autorizado, como puede ser el acceso a un sistema, la ejecución de programas no autorizados o el ataque a una red informática.

La detección de intrusos es un área aplicada de la seguridad informática encargada de informar eventos que puedan tener lugar en un sistema informático y puedan ser considerados como parte de un intento de intrusión.

Tipos de Detectores de Intrusos

IDS. (Host). Capturan alertas ocurridas en el host local donde están instalados.

NIDS. (Network Intrusion Detection System). Detectan alertas analizando (mediante un sniffer) el tráfico que pasa por su tarjeta de red. Si son colocados en lugares estratégicos (firewalls, gateways, etc.) detectan ataques producidos a cualquiera de los hosts de nuestra red.

DIDS (Distributed Intrusion Detection System). Son NIDS donde los sensores están distribuidos en diferentes puntos de la red.

Por tal motivo:

Se implementarán NIDS que nos permitan identificar en tiempo real cualquier intento de intrusión.

QoS

Los últimos años han sido testigos del rápido crecimiento del tráfico de redes informáticas. Los administradores agregan continuamente nuevos recursos para tratar de responder al ritmo de la creciente demanda. Incluso los clientes de redes no están, a menudo, satisfechos con el rendimiento de la red. El uso creciente de un nuevo tipo de aplicaciones multimedia ávidas de recursos va a agudizar esta situación. Los mecanismos de QoS (Calidad del Servicio, por sus siglas en inglés) proporcionan un conjunto de herramientas que el administrador de redes puede utilizar para administrar el uso de recursos de red de una forma controlada y eficaz. Como resultado, se obtendrá un servicio mejor a las aplicaciones y a usuarios de misiones críticas, al mismo tiempo que se va frenando el ritmo al que es necesario aumentar la capacidad.

Con el fin de poder garantizar un ancho de banda a las aplicaciones críticas que estarán corriendo para el sistema del SMDP se implementará QoS.

Desarrollo de control ejemplo: “Procedimiento para Control de Cambios”.

Desde la perspectiva de la organización, la empresa o institución tiene formulados objetivos muy claros. Para alcanzar dichos objetivos, se requiere que los *procesos* de negocio tengan lugar en tiempo y forma. A su vez, los procesos requieren como insumo principal a la *información.* De esta manera, las organizaciones se hace cada día más dependientes de una fuente de información que funcione correcta y eficientemente. En otras palabras, las organizaciones son cada día más dependientes de la *Tecnologías de la Información* que funcionen con la calidad requerida para apoyar al negocio a cumplir con sus objetivos.

En este contexto, la seguridad de la información no es una meta por si misma, sino que forma parte de un sistema más amplio que tienen por misión alcanzar los objetivos del negocio.

Hemos encontrado en repetidas ocasiones, que los controles considerados (ya no digamos implantados) por los practicantes de la seguridad de la información solamente están enfocados al aspecto tecnológico de la misma. Estamos convencidos de que esto es un *graso* error.

No se requiere proteger un activo de hardware (un servidor, por ejemplo) si no la información que posibilita los procesos que el negocio u organización requieren ejecutar para subsistir.

Desde este punto de vista, las buenas prácticas manejan como punto de partida la correcta *organización* de la

seguridad de la información, es decir: responsabilidades, derechos y deberes deben ser especificados claramente para reducir los niveles de abstracción durante la implantación de una estrategia de protección.

En este sentido, los siguientes puntos son *cruciales* para lograr este cometido:

- Políticas y/o códigos de conducta (nos dicen *qué* objetivos estamos persiguiendo)
- Procesos (nos dicen *qué* tenemos que hacer para alcanzar esos objetivos)
- Procedimientos (nos dice *quién* hace qué y *cuándo*)
- Instrucciones de trabajo (nos dicen *cómo* hacer cada actividad)

Para el caso práctico que estamos tratando, a continuación se presentará un procedimiento de seguridad, en el que tratamos de ejemplificar la importancia de contar con un documento que detalle los roles y las responsabilidades, el flujo de información durante el desarrollo de las actividades, así como el momento en el que se deben realizar.

Conviene dejarlo claro de una vez: nuestra postura es que una aproximación a un problema de seguridad de la información que no considere procesos y procedimientos, es una aproximación *trunca*. Y el brindar un falso sentido de seguridad a partir de un plan incompleto, beneficia solamente a los atacantes en potencia.

Recomendaciones para el desarrollo de los procedimientos.

Para el desarrollo de los procedimientos, se requiere invariablemente que el practicante de la seguridad se involucre en la cotidianidad de las operaciones del negocio en todas sus facetas. A partir de técnicas de extracción de información (entrevistas personales, encuestas, cuestionarios vía Web) debe ser capaz de desarrollar una visión general que permita identificar el proceso del negocio y el flujo de información dentro del mismo.

Igualmente, es primordial para el éxito de los procedimientos que el practicante de seguridad asuma en una primera iteración la responsabilidad (actualizaciones, revisión, supervisión) del documento. De esta manera, las áreas involucradas no tendrán la percepción de que se les están asignando tareas adicionales. En nuestra experiencia, una vez que se han desarrollado un par de procedimientos, es posible comenzar a delegar la responsabilidad de los mismos a las áreas que lo ejecutan, de acuerdo con las mejores prácticas.

Con esta recomendación como último punto, procedemos a mostrar un diagrama de flujo de información en el contexto de control de cambios de configuraciones para dispositivos de red; ver ilustraciones 16, 17 y 18.

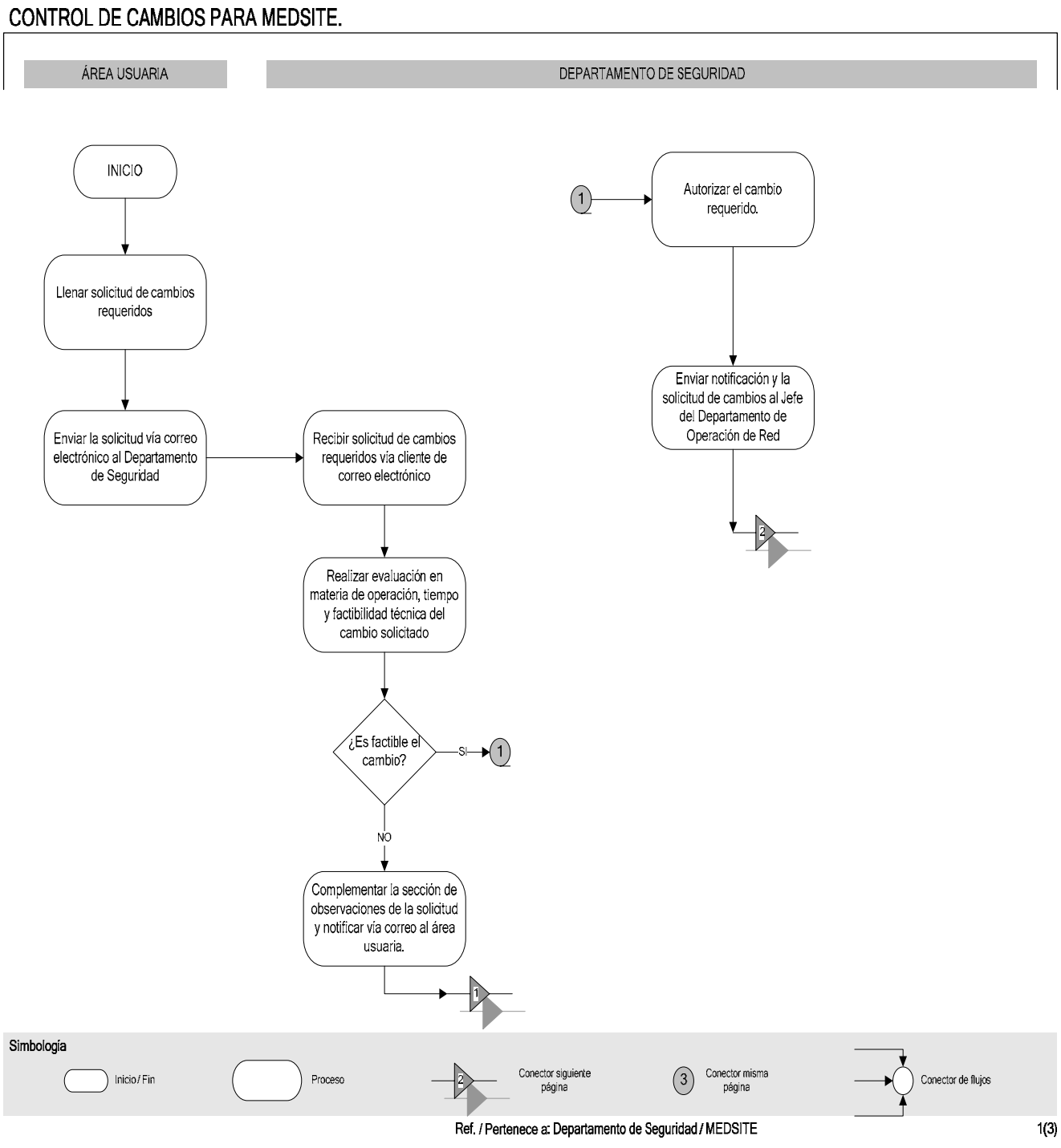


Ilustración 16 Diagrama de flujo de información (1/3)

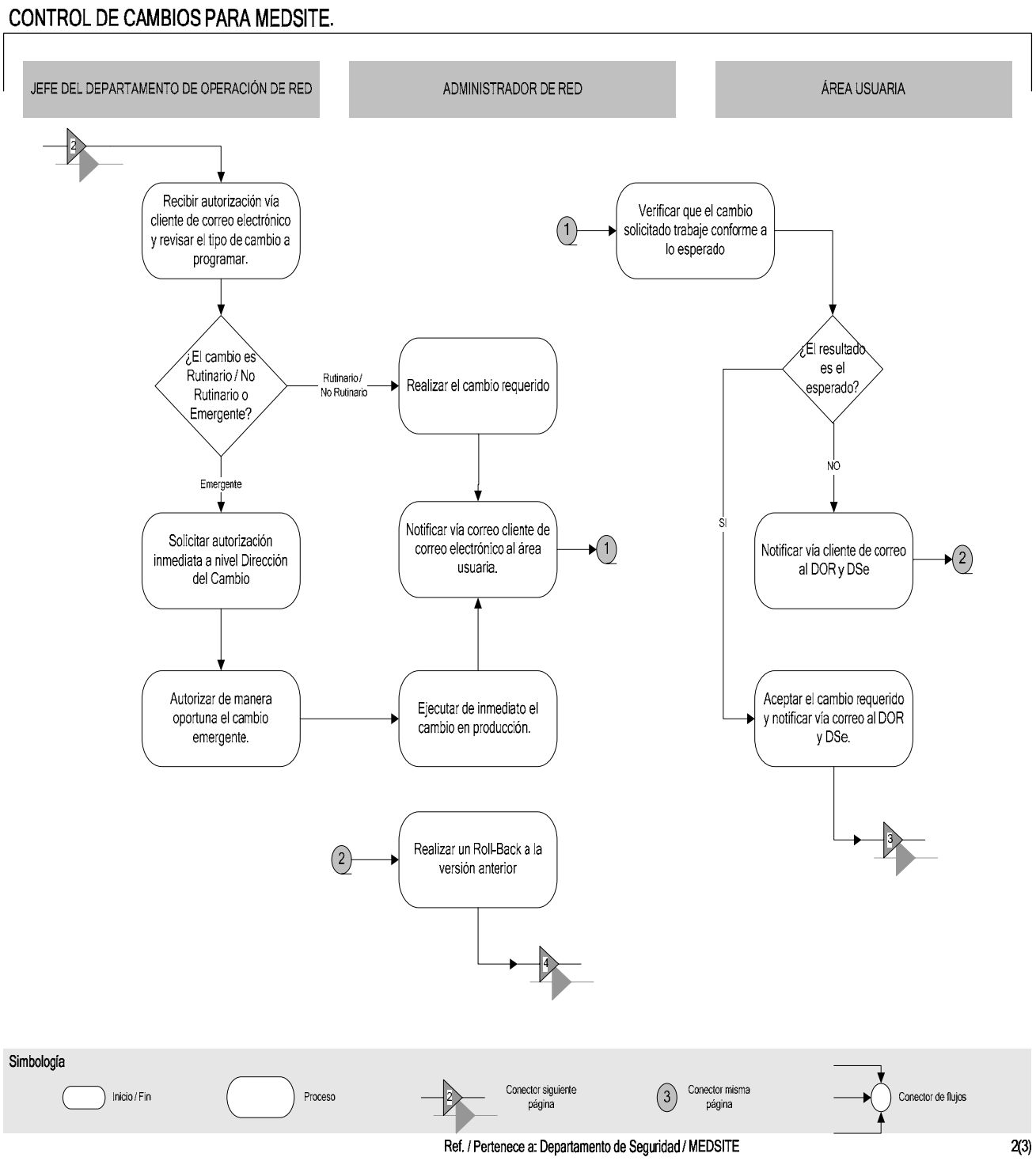


Ilustración 17 Diagrama de flujo de información (2/3)

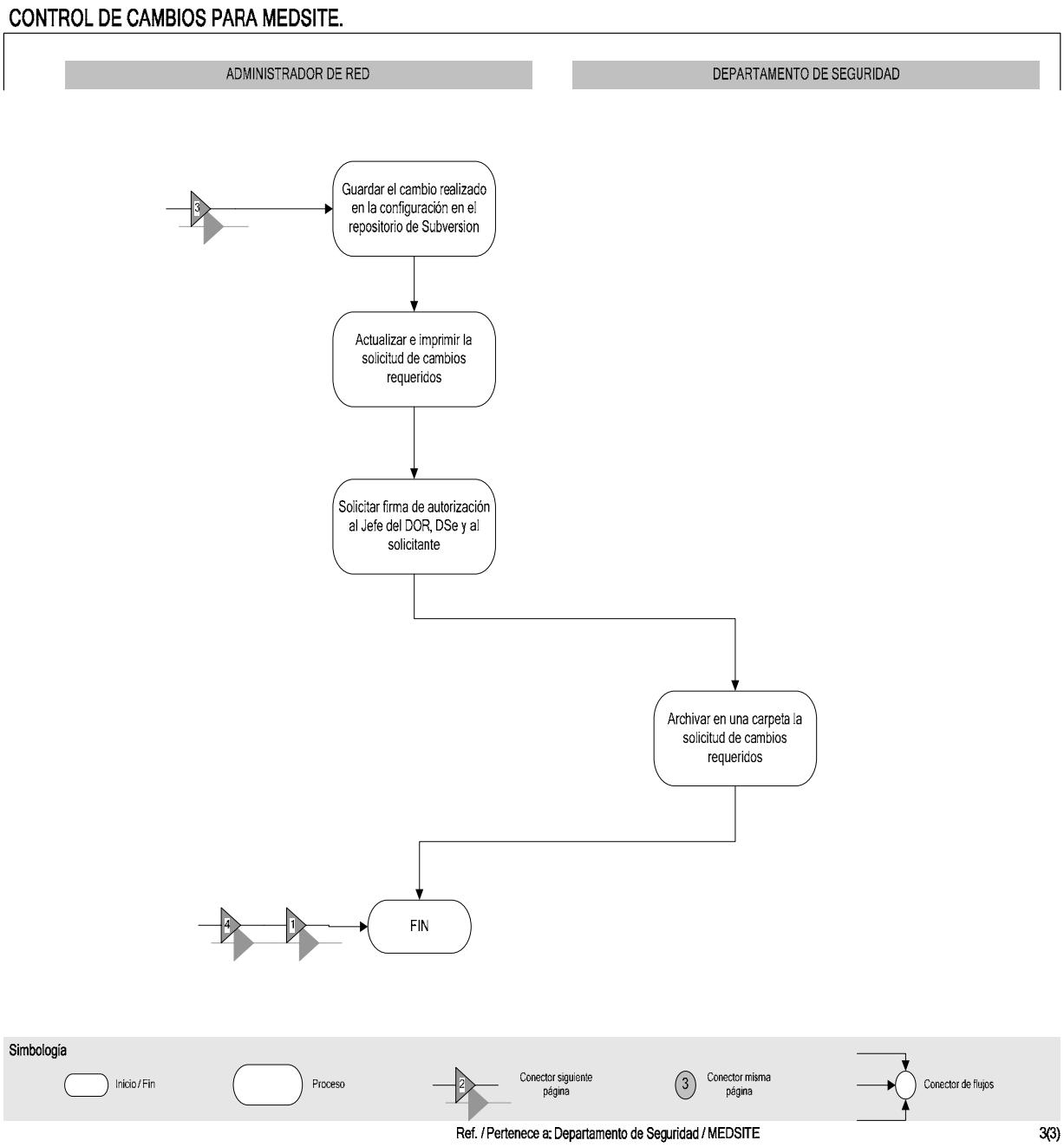


Ilustración 18 Diagrama de flujo de información (3/3)

Una vez detectado el flujo de información, se requiere corroborar quién es el responsable de cada actividad, así como cuál es el alcance de sus tareas y en qué orden se ejecutan. Una vez finalizado este reconocimiento, se puede proceder con la documentación exhaustiva y detallada del flujo de información:

Act: 010 **SOLICITUD DE CAMBIOS**

Paso	Tarea	Responsable	Formatos / Sistema
01	Llenar el formato de Solicitud de Cambios Requeridos	Área usuaria	Solicitud de Cambios Requeridos
02	Solicitar el cambio al departamento de Operación de Redes vía Cliente de correo anexando la Solicitud de Cambios Requeridos.	Área usuaria	Solicitud de Cambios Requeridos / Cliente de correo

Act: 020 **RECEPCIÓN DE SOLICITUD CAMBIOS**

Paso	Tarea	Responsable	Formatos / Sistema
01	Recibir la Solicitud de Cambios Requeridos por parte del área usuaria vía Cliente de correo.	Administrador de Red	Solicitud de Cambios Requeridos / Cliente de correo
02	Realizar una evaluación técnica del cambio solicitado, si es factible enviar la solicitud de Cambios requeridos al Jefe de Departamento de Operación de Redes y Jefe de Departamento de Seguridad vía Cliente de correo.	Administrador de Red	Solicitud de Cambios Requeridos / Cliente de corre
03	De lo contrario notificar al área usuaria completando la sección de Observaciones del formato enviándolo vía Cliente de correo y dirigirse al Paso 04 de la Act: 070.	Administrador de Red	Solicitud de Cambios Requeridos / Cliente de correo

Act: 030 **AUTORIZACIÓN DEL CAMBIO REQUERIDO**

Paso	Tarea	Responsable	Formatos / Sistema
01	Recibir la solicitud de Cambios Requeridos por parte del Administrador de Red	Jefe de Departamento de Operación de Redes y Jefe de Departamento de Seguridad	Solicitud de Cambios Requeridos / Cliente de correo
02	Revisar el cambio requerido en materia de impacto a la operación, tiempo y factibilidad técnica.	Jefe de Departamento de Operación de Redes y Jefe de Departamento de Seguridad	
03	Si no es factible el cambio requerido pasar al paso 03 de la Act: 020.	Jefe de Departamento de Operación de Redes y Jefe de Departamento de Seguridad	
04	De ser factible el cambio requerido autorizar el cambio.	Jefe de Departamento de	

		Operación de Redes y Jefe de Departamento de Seguridad	
05	Notificar vía Cliente de correo, la autorización para el control de cambios requerido al Administrador de Red.	Jefe de Departamento de Operación de Redes y Jefe de Departamento de Seguridad	Solicitud de Cambios Requeridos / Cliente de correo

Act: 040 **PROGRAMACIÓN DEL CAMBIO REQUERIDO**

Paso	Tarea	Responsable	Formatos / Sistema
01	Recibir la autorización del cambio requerido vía Cliente de correo por parte del Jefe de Departamento de Operación de Redes y Jefe de Departamento de Seguridad.	Administrador de Red	Solicitud de Cambios Requeridos / Cliente de correo
02	Revisar el tipo de cambio requerido: Rutinario, No-Rutinario o Emergente.	Administrador de Red	
03	Si el cambio es Rutinario o No-Rutinario se programará el cambio llenándose el campo de observaciones en el formato establecido y dirigirse al paso 01 de la Act: 050.	Administrador de Red	
04	De lo contrario el cambio es emergente y solicitar la autorización inmediata del cambio requerido al Jefe de Departamento de Operación de Redes.	Administrador de Red	.
05	Solicitar autorización de manera inmediata a nivel Dirección.	Jefe de Departamento de Operación de Redes	
06	Autorizar de manera oportuna el cambio emergente al Administrador de Red.	Jefe de Departamento de Operación de Redes	
07	Ejecutar de inmediato en el ambiente de Producción y dirigirse al paso 01 de la Act: 070.	Administrador de Red	

Act: 050 **EJECUCIÓN DEL CAMBIO REQUERIDO**

Paso	Tarea	Responsable	Formatos / Sistema
01	Realizar el cambio requerido.	Administrador de Red	

Act: 060 **ACEPTACIÓN DEL CAMBIO REQUERIDO**

Paso	Tarea	Responsable	Formatos / Sistema
01	Verificar que el cambio solicitado se vea reflejado y trabaje conforme a lo esperado.	Área Usuaria y Administrador de Red	
02	De no ser el resultado esperado notificar vía Cliente de correo al departamento de Operación de Redes y realizar un Roll-Back a la versión anterior de configuración	Área Usuaria	Cliente de correo
03	De lo contrario notificar al departamento de Operación de Redes y al departamento de Seguridad que el cambio es aceptado.	Área Usuaria	Cliente de correo

Act: 070 **LIBERACIÓN DEL CAMBIO REQUERIDO**

Paso	Tarea	Responsable	Formatos / Sistema
01	Guardar el cambio realizado en el script o en la configuración en la herramienta “Subversion” utilizando la guía de subversión.	Administrador de Red	control-de-cambios (Guía de Subversion) / Subversion
02	Actualizar e imprimir el formato de Solicitud de Cambios Requeridos.	Administrador de Red	Solicitud de Cambios Requeridos
03	Solicitar firma de autorización al Jefe de Departamento de Operación de Redes, Jefe de Departamento de Seguridad y al Solicitante.	Administrador de Red	Solicitud de Cambios Requeridos
04	Archivar en una carpeta la solicitud autorizada de Cambios Requeridos.	Administrador de Red	Solicitud de Cambios Requeridos
05	Finalizar Procedimiento.	Administrador de Red	Solicitud de Cambios Requeridos

4.6. Conclusiones.

Siguiendo la metodología propuesta, durante el análisis de la información fueron identificados y seleccionados los controles de seguridad para llevar a cabo su implantación dentro del SMDP.

Los dominios o cláusulas del ISO/IEC 17799:2005 que se ejemplificaron son mostrados en la “Tabla General de Resultados” (tabla 33) a continuación:

ID	Dominio ISO	Controles Implementados
A.5	**Política de Seguridad**	0
A.7	**Administración de Activos**	1
A.10	**Administración de Comunicaciones y Operaciones**	20

Tabla 33 Tabla General de Resultados

Cláusula ISO
A.5. Política de Seguridad

Objetivo

Proveer soporte y dirección de seguridad de información a la alta gerencia con base a los requerimientos de la organización, leyes y regulaciones relevantes.

Total de Controles = **2**

Controles Implementados	Controles NO Implementados
0	**2**

Tabla 34 Cumplimiento cláusula 5

Ilustración19. Cumplimiento cláusula 5

Fortalezas de la implementación de los controles y Mejores Prácticas

- Establecimiento de un marco normativo de referencia asociados con los objetivos del hospital MedSite en materia de seguridad de la información.
- Entendimiento de los aspectos generales de seguridad por parte de los usuarios.
- Elevación de la cultura de seguridad dentro de los usuarios de MedSite.
- Cumplimiento de los controles de seguridad implementados.

- Identificación de responsables en la implementación de seguridad en diferentes áreas.

Posibles Riesgos

- Mal uso de los activos de TI.
- No cumplimiento con los controles y recomendaciones de seguridad.
- Posibles errores por parte de los usuarios.
- Configuraciones vulnerables en los equipos de la infraestructura tecnológica.
- Malas prácticas administrativas de seguridad.

Cláusula ISO
A.7. Administración de Activos

Objetivo

Lograr y mantener la adecuada protección sobre los activos de TI de la organización, definiendo los niveles de protección adecuados para el manejo de la información.

Total de Controles = **5**

Controles Implementados	Controles NO Implementados
1	4

Tabla 35 Cumplimiento cláusula 7

Ilustración 20 Cumplimiento cláusula 7

Fortalezas de la implementación de los controles y Mejores Prácticas

- Identificación de los todos los activos de TI con base a un inventario definido.
- Establecimiento del dueño de los activos de TI.
- Establecimiento adecuado de los niveles de protección de los activos de TI.
- Implementación de políticas y/o guías para el adecuado uso de los recursos de TI por parte de los usuarios.
- Realización de la clasificación de la información con base en su criticidad.
- Identificación adecuada de la información a utilizar mediante su adecuado etiquetado y rotulado según sea el tipo de clasificación dada.

Posibles Riesgos

- Inadecuado uso de los equipos de procesamiento de información.
- Acceso a la información sensible por personal no autorizado.
- Mal uso de la información.
- Niveles y/o privilegios de acceso otorgados de manera errónea.
- Extravío de información.

Cláusula ISO
A.10. Administración de Comunicaciones y Operaciones

Objetivo

Proteger las actividades de procesamiento de información de manera correcta, implementando niveles adecuados de protección a la información y a la infraestructura de redes para prevenir el acceso no autorizado, mal uso o destrucción de los activo s de TI por personal no autorizado, así como minimizar las fallas en los sistemas y detectar actividades no autorizadas en los equipos de cómputo.

Total de Controles = **32**

Controles Implementados	Controles NO Implementados
20	**12**

Tabla 36 Cumplimiento cláusula 10

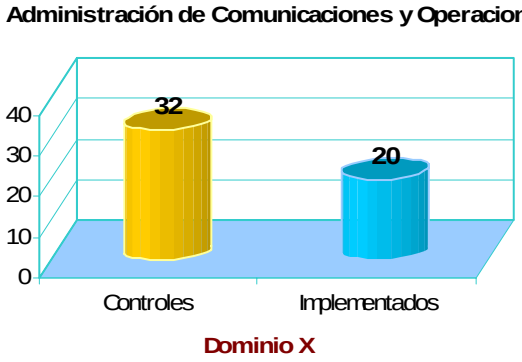


Ilustración 21 Cumplimiento cláusula 10

Fortalezas de la implementación de los controles y Mejores Prácticas

- Establecimiento e implementación de procedimientos operativos.
- Aprobación del sistema.
- Adecuada definición de los ambientes de pruebas.
- Limitación de acceso al sistema.
- Establecimiento de Acuerdos de Niveles de Servicio (SLA) con proveedores.

- Implementación de controles contra software malicioso.
- Ejecución adecuada de los respaldos de información.
- Establecimiento e implementación de controles de redes.
- Establecimiento de la Seguridad en las redes.
- Implementación de mecanismos de seguridad (IDS, Firewall, etc.).
- Implementación de controles de autenticación y cifrado de los servicios de red.
- Implementación de baselines sobre los equipos de cómputo y servidores.
- Adecuada configuración de los equipos de cómputo y servidores.
- Generación de registros de auditoria.
- Implementación de Listas de Control de Accesos “ACL”.
- Monitoreo del uso de las instalaciones de procesamiento de información.
- Protección de los registros de información.

Posibles Riesgos

- No acatamiento de las reglas por parte de los usuarios.
- Acceso no autorizado a las instalaciones de área y entrega por personal no autorizado.
- Control de los medios informáticos no establecido adecuadamente.
- Perdida de información y/o equipo en tránsito.

CONCLUSIONES GENERALES

Conclusiones Generales

"No estudio por saber más,
sino por ignorar menos."

Sor Juana Inés de la Cruz.

En nuestra época como estudiantes universitarios y como personas interesadas desde entonces en la disciplina de la seguridad de la información, se nos presentó un primer reto importante: ¿a qué fuentes acudir para comenzar el aprendizaje en este apasionante tema?

Entonces era necesario asistir a primera hora a la biblioteca de la Facultad de Ciencias para encontrar disponible la única copia de *Applied Cryptography 1st. Ed.*, o para leer sobre la implantación de controles y mecanismos[56] en sistemas operativos "arcanos" (*léase UNIX-HP)* y con una muy pronunciada curva de aprendizaje.[57]

Otra de las fuentes de consulta - mucho más llamativa y excitante - era constituida por los *e-zines* (revistas digitales en línea) desarrollados por los autodenominados *hackers.* Pasamos muchas horas explorando los excelentes artículos escritos por *aleph0ne* y *fyodor* en sitios como *www.phrack.org* o *www.2600.com*.

El día de hoy, más de una década después, encontramos que el problema de información en relación a la seguridad se presenta nuevamente pero en un sentido completamente opuesto.

Existe un abundante flujo de información que parece provenir de todos lados: los propios gigantes de la industria de la seguridad (Symantec, Websense, Computer Associated, etc.), grandes fabricantes de software, medios especializados, revistas orientadas a administradores de negocio, memorias de congresos matemáticos y así por el estilo, en una sucesión que parece ser interminable. Por otra parte, se está presentando en estos momentos un parte aguas en tecnología, que apunta por un lado a la convergencia de servicios de telecomunicaciones y apunta a la *virtualización* de dispositivos que hasta ahora estábamos acostumbrados a tener de manera física dentro de los centros de cómputo.

Esta es la situación actual de la industria de la Tecnología de Información, y henos aquí: practicantes de la seguridad de la información armados con un pensamiento estructurado, orientado a "sistemas lineales, de parámetros concentrados e invariantes en el tiempo" que nos fue moldeado durante los años de aprendizaje en la Facultad de Ingeniería.

No es de extrañar, bajo esta óptica, que estén en auge las certificaciones de ésta o aquella tecnología, que permiten a las personas "integrarse a la industria" de manera "óptima", presentando "resultados inmediatos" y brindando un máximo "retorno de la inversión" a la feliz organización que tuvo a bien contratarlos.

¡Que impertinencia!

Porque hemos tenido la inmensa fortuna de estar presentes durante las fases de planeación, implantación de estrategias y solución de problemas de grandes magnitudes; presentes en situaciones de presión y encarando factores que van mucho más allá de la mera propuesta técnica para su solución, podemos decir que es justamente lo contrario.

Ante los grandes retos, no conocemos al día de hoy una técnica más efectiva que esperar a que los seguidores de la tecnología en boga agoten sus argumentos y se ahoguen en las limitaciones propias de su formación, para proceder con lo que sabemos hacer y regresar a lo básico: plantear un esquema del modelo OSI en la pizarra de la sala de juntas y comenzar, paso a paso, a definir cuál es el alcance del problema, cuáles son los

56 Satan era la herramienta de moda

57 Se tenía la ventaja, eso sí, que la sala UNIX de UNICA en el edificio principal de Ingeniería todavía estaba más o menos vacía.

factores que intervienen y cuáles merecen ser tomados en cuenta.

Se trata, pues, de la capacidad de *modelar* y *abstraer* configuraciones físicas complejas para proceder con la aplicación de una aproximación estructurada, disciplinada y basada en consideraciones técnicas sólidas. No queríamos empezar esta parte final, que abre también una etapa en nuestra vida como profesionales, sin mencionar que estamos convencidos de que la educación que hemos recibido nos ha permitido desarrollar esta capacidad. Por ello, estaremos siempre en deuda con *la Facultad*.

A lo largo del trabajo, se integró un marco de referencia que posibilita la consolidación, integración y ejecución exitosa de un plan de aseguramiento de la información para una organización. Dicho marco, garantizará que la solución que se conforme esté orientada por los objetivos de la organización y alineado a los estándares mundiales y buenas prácticas existentes.

En el mismo sentido, se presentaron los formatos consolidados para la elaboración de normatividad en materia de seguridad de la información en los rubros de análisis de riesgos y creación de procedimientos de seguridad, incluyendo el desarrollo de algunos controles de seguridad que involucren los dispositivos tecnológicos de transmisión, almacenamiento y procesamiento de la información.

Durante el primer capítulo de este trabajo se abordó la perspectiva de seguridad de la información desde una óptica histórica, aludiendo a los retos de magnitud mayor que quedan representados por los conflictos bélicos.

Esperamos que esta perspectiva presente al lector una renovada dimensión de los alcances y la importancia de esta disciplina: no se trata ya sólo de impedir que un usuario tenga acceso a los archivos personales de un tercero, cuando hablamos de seguridad de la información estamos hablando *ya* de guerra cibernética, de terrorismo cibernético y del derecho de la privacidad que tenemos todos como ciudadanos y que día a día se ha ido mermando ante el nuevo Leviatán tecnológico.

¿Estamos preparados para afrontar el reto de mantener segura nuestra información? ¿Como individuos? ¿Como sociedad? ¿Como país?

Si parece que el punto que expresamos es exagerado, basta considerar que Internet ha venido a revolucionar no sólo las tecnologías de información, sino paradigmas sociales, culturales y políticos que nos rigieron hasta finales del siglo pasado.

Ante un reto de esta magnitud, se hace necesaria la consolidación de un grupo mínimo de *parámetros de diseño* que nos permitan realizar el modelado del problema, trascendiendo modas y tecnologías. Encontramos y señalamos en el primer capítulo que las dimensiones básicas a considerar al atacar un problema son tres:

- La oportuna identificación de los *activos* de información.
- El pronto reconocimiento de las principales *amenazas* que los asechan.
- El *impacto* en caso de ocurrir algún evento indeseable.

Atribuir el reconocimiento de estos puntos básicos a la disciplina de la seguridad de la información sería pecar de arrogancia. Desde muchos años atrás, la industria del manejo de riesgos (léase aseguradoras) conocen y administran este tipo de factores.

Es muy importante comentar aquí que, ante la velocidad a la que se presentan los cambios, se requiere que hagamos un alto y veamos lo que se está haciendo en otras áreas del conocimiento: ¿Puede servirme lo que se está haciendo en el campo de la virología?, ¿tiene alguna utilidad revisar lo que se ha hecho en los centros de prevención de epidemias?, ¿vale la pena revisar las técnicas para administración de portafolios?

La propuesta que hacemos es: utilicemos el conjunto de técnicas y conocimientos que ya han evolucionado en otras áreas y utilicémoslas en nuestro campo.

Acorde con el comentario inicial de estas conclusiones, en el segundo capítulo del presente trabajo se planteó la estructuración de una aproximación al problema de la seguridad de la información que intenta incorporar las principales características y ventajas de disciplinas de la ingeniería mucho más consolidadas.

En este sentido, la teoría de la calidad ha sido rescatada por los expertos del ISO/IEC y se nos ha proveído con una serie de documentos que nos dicen *qué* hacer para poder integrar una solución que se enfoque exclusivamente las necesidades del momento, sino que permita darle una vigencia a mediano plazo a la

solución propuesta (como mínimo) y que posibilite además el entrar en un ciclo de mejora continua del que podamos extraer indicadores y figuras para justificar la inversión de la organización en tecnologías de seguridad de la información.

Cabe mencionar que a través de nuestra historia como *especie* en este planeta, nos hemos distinguido y desarrollado por la excepcional capacidad que tenemos para almacenar y transmitir conocimientos. ¿Por qué, entonces, cuesta tanto aceptar estándares y lineamientos generados por expertos para basar nuestro propio plan de protección? Aunque parezca risorio, hemos visto con tristeza que muchos proyectos de seguridad no llegan a buen término porque se quiere comenzar desde *cero*. Anotamos aquí que esto es un error, porque no sólo no basamos nuestra solución en conocimientos y experiencias consolidadas, sino que nos echamos a hombros la titánica tarea de convencer a nuestros colegas, superiores y usuarios que la solución que proponemos es la mejor.

Se mencionó a lo largo de este trabajo que la seguridad de la información es ante todo un compromiso: ganamos confidencialidad, pero perdemos disponibilidad. O ganamos disponibilidad, pero nuestra privacidad se ve afectada. La pregunta (*errónea)* que se hace es: ¿qué tan efectiva es una salvaguarda contra un riesgo?, cuando en realidad lo que debemos preguntarnos es: ¿la implantación de esta salvaguarda representa una buena decisión costo-beneficio?

Y si personalmente ya implica cierta dificultad hacer decisiones de esta naturaleza, al hablar de establecer la estrategia para un ente corporativo, el problema escala de manera exponencial. A este respecto, en el capítulo II Se hizo la introducción del estándar CobiT. Aunque no es el objetivo de este trabajo desarrollar más respecto a éste, quedó mencionado que hemos encontrado en él una invaluable referencia que nos permite alinear objetivos de los proyectos tecnológicos con la misión de la organización.

Aquí conviene hacer la siguiente observación: la normatividad existente al día de hoy, está *sesgada* de manera perceptible para mentes anglo-sajonas. Sin detrimento de culturas o creencias, es muy distinto tratar de establecer un programa para evitar que los usuarios vean sitios Web recreativos en sus áreas de trabajo en México o en Europa.

Vemos la necesidad, de trabajar y adaptar la normatividad existente. No solamente haciendo una traducción de los estándares, sino realmente integrando una visión latino-americana en los mismos, que permita al practicante de la seguridad una aproximación mas fácil a las personas. El doctor Daltabuit, experto mexicano de la seguridad de la información, ha manejado el término de “*tropicalización de los ISO”*, y es un término que nos gusta para resumir esta necesidad.

El problema de la seguridad, ya quedó patente, es un problema humano, no tecnológico. Este hecho se tiene que tomar en cuenta durante todo momento, so pena de encontrarse con dificultades no previstas. Considérese a manera de ejemplo, que dentro de las tecnologías para autenticación de personal mediante biometría, el análisis del iris es la más efectiva. Sin embargo, está distante de ser la tecnología más popular. Esto se debe en parte al alto costo de la solución (hay que decirlo), pero también influye mucho que las personas encuentren esta técnica como *intrusiva* y poco confiable.

En el capítulo III, presentamos una breve semblanza de la psique humana y sus reacciones ante la percepción del riesgo. Al igual que el caso de la normatividad, encontramos estudios que documentan la reacción humana ante los riesgos, pero no nos fue posible localizar un estudio de la misma naturaleza para México o Latinoamérica. Es nuestro deseo, que en un futuro cercano los académicos nacionales de esta disciplina establezcan los programas necesarios que nos permita establecer un *perfil* genérico del mexicano, y nos facilite en este sentido la actividad de análisis y evaluación de riesgos.

Finalmente, el capítulo IV presenta un caso simulado, aunque acotado en alcance y ejemplos, sobre el cual se aplicaron los conceptos hasta ahora mencionados. Cabe destacar que un solo vistazo a los resultados que arroja la metodología propuesta, nos habla de indicadores, y nos habla de planes para retomar y para realizar mejoras al proyecto, sin necesidad de iniciar desde cero una y otra vez.

A futuro, vemos un cambio importante en esta disciplina de la ingeniería: la tendencia es “sacar” la información de las fronteras de la empresa. Creemos que estamos viendo el final de las tecnologías de información como “islas” disjuntas de información. Paradigmas nuevos de cómputo como las Aplicaciones Orientadas a Servicios

(SOA, por sus siglas en inglés) están consolidando una vasta infraestructura de organizaciones y compañías que podrán realizar operaciones de cómputo mucho más rápido de lo que cualquier ente individual podrá. Dichos servicios serán puestos a disposición del público, y si no hacemos uso de ellos estaremos en franca desventaja ante nuestros competidores.

Esto planteará un problema de seguridad: ¿cómo procesar la información de mi empresa en un sistema ajeno? Toda la criptografía, elementos de protección en frontera y filtrados de paquete seguirán siendo un sustento muy importante, pero el control principal para proteger la información será contractual.

ANEXOS

Anexo A: Objetivos de control y controles del ISO/IEC 270001:2005.

A.5 Política de Seguridad

A.5.1 Política de Seguridad de la Información

Objetivo: Proporcionar dirección y soporte para la seguridad de la información de acuerdo con la empresa.

A.5.1.1	Documento de la política de seguridad de la información	Control Un documento de política de seguridad de la información será aprobado por la dirección, publicado y comunicado a todos los empleados y partes externas relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información será revisada en intervalos definidos o si ocurren cambios importantes para asegurar su correcta continuidad, adecuación y efectividad.

A.6 Organización de la seguridad de información

A.6.1 Organización interna

Objetivo: Administrar la seguridad de la información dentro de la organización.

A.6.1.1	Compromiso de la dirección para la seguridad de la información	Control La dirección respaldará activamente la seguridad dentro de la organización a través de una clara administración, demostrando compromiso, misión explícita y reconocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de seguridad de la información	Control Las actividades de la seguridad de la información serán coordinadas por representantes de diferentes partes de la organización con roles y funciones de trabajo importantes.
A.6.1.3	Asignación de responsabilidades de seguridad de la información	Todas las responsabilidades de la seguridad de la información deberán ser claramente definidas
A.6.1.4	Proceso de autorización para los servicios/instalaciones de procesamiento de la información	Control Un proceso de autorización de la dirección para nuevos servicios de procesamiento de la información será definido e implementado.
A.6.1.5	Contratos de confidencialidad	Los requisitos para la confidencialidad o contratos de no divulgación que reflejarán las necesidad para la protección de la información de la organización serán identificados y examinados con regularidad.
A.6.1.6	Contacto con las autoridades	Control Se establecerán los contactos apropiados con las autoridades relevantes.

A.6.1.7	Contacto con grupos de interés especial.	Se establecerán los contactos apropiados con los grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
A.6.1.8	Evaluación independiente de la seguridad de la información	Control El enfoque de la organización para dirigir la seguridad de la información y su implementación (Ejemplos. Los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información) serán examinados por separado en intervalos definidos o cuando ocurran cambios importantes para la implementación de la seguridad.

A.6.2 Partes externas

Objetivo: Mantener la seguridad de la información de la organización y los servicios/instalaciones de procesamiento de la información que son accedidos, procesados, comunicados a, o dirigidos por partes externas.

A.6.2.1	Identificación de los riesgos relacionados con las partes externas.	Los riesgos a la información de la organización y los servicios/instalaciones de procesamiento de la información que vienen de procesos de negocio que involucran a participantes externos deberán ser identificados y los controles apropiados implementados antes de permitir el acceso
A.6.2.2	Requerimientos de seguridad con el manejo de los clientes	Todos los requisitos de seguridad identificados serán atacados antes de dar acceso a los clientes a la información o activos de la organización.
A.6.2.3	Requerimientos de seguridad en contratos con terceros	Contratos con terceros que pretenden acceder, procesar, comunicar o administrar la información o servicios/instalaciones de procesamiento de información de la organización, o añadir productos o servicios a los servicios de procesamiento de la información cubrirán todos los requisitos importantes de seguridad.

A.7 Administración de activos

A.7.1 Responsabilidad con los activos

Objetivo: Conseguir y mantener la protección apropiada de los activos organizacionales.

A.7.1.1	Inventario de activos	Todos los activos serán claramente identificados y se hará y mantendrá un inventario de todos los activos importantes.
A.7.1.2	Posesión de activos	Toda la información y los activos asociados con los servicios/instalaciones de procesamiento de la información serán poseídos por una parte designada de la organización.
A.7.1.3	Uso aceptable de activos	Se identificarán, documentarán e implementarán reglas para el uso aceptable de la información y los activos relacionados con servicios/instalaciones de procesamiento de la información.

A.7.2 Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel apropiado de protección.

A.7.2.1	Indicaciones de clasificación	La información será clasificada de acuerdo a su valor, requisitos legales, sensibilidad y que tan crítica sea para la organización.
A.7.2.2	Manejar y etiquetar la información	Un conjunto apropiado de procedimientos para etiquetar y manejar la información será desarrollado e implementado de acuerdo con el esquema de clasificación adoptado por la organización.

A.8 Seguridad de recursos humanos

A.8.1 Prioridad en el empleo

Objetivo: Asegurar que los empleados, contratistas y terceros usuarios entiendan sus responsabilidades y que sean las adecuadas a los roles para los que fueron considerados, y reducir el riesgo de robo, fraude o mal uso de las instalaciones.

A.8.1.1	Roles y responsabilidades	Se debe desarrollar un documento donde se definan los roles y responsabilidades del usuario considerando las responsabilidades generales por la implementación o el mantenimiento de la política de seguridad, así como las responsabilidades específicas por la protección de cada uno de los activos, o por la ejecución de procesos o actividades de seguridad específicos.
A.8.1.2	Proyección	Se deben llevar a cabo controles de verificación del personal permanente en el momento en que se solicita el puesto, considerando: Disponibilidad de certificados de buena conducta satisfactorios, por ej. uno laboral y uno personal. Comprobación (de integridad y veracidad) del curriculum vitae del aspirante. Constatación de las aptitudes académicas y profesionales alegadas. Verificación de la identidad (pasaporte o documento similar).
A.8.1.3	Términos y condiciones de empleo	Como parte su obligación contractual, los empleados, contratistas y terceros usuarios acordarán y firmarán los términos y condiciones de su contrato de empleo, el cual declarará sus responsabilidades y las de la organización para la seguridad de la información.

A.8.2 Durante el empleo

Objetivo: Asegurar que todos empleados, contratistas y terceros usuarios estén conscientes de las amenazas de seguridad de la información, sus responsabilidades y que estén equipados para respaldar la política de seguridad organizacional en el transcurso de su trabajo normal y para reducir el riesgo del error humano.

A.8.2.1	Responsabilidades de dirección.	La dirección exigirá que empleados, contratistas y terceros usuarios apliquen la seguridad de acuerdo con las políticas y los procedimientos establecidos por la organización.

A.8.2.2	Concienciación, educación y entrenamiento de seguridad de la Información.	Todos empleados de la organización, los contratistas y terceros usuarios recibirán el entrenamiento de concienciación apropiado y las actualizaciones regulares en políticas y procedimientos organizacionales, tan importante para su función de trabajo.
A.8.2.3	Proceso disciplinario	Control Habrá un proceso disciplinario formal para empleados que han cometido un incumplimiento de seguridad.

A.8.3 Terminación o cambio de empleo

Objetivo: Asegurar que los empleados, contratistas y terceros usuarios salgan de la organización o cambien de empleo de manera organizada.

A.8.3.1	Responsabilidades de terminación.	Las responsabilidades para llevar a cabo la terminación o cambio de empleo serán claramente definidas y asignadas.
A.8.3.2	Devolución de activos	Control Todos empleados, contratistas y tercero usuarios devolverán todos los activos de la organización que tengan en su posesión sobre la terminación de su empleo, contrato o acuerdo.
A.8.3.3	Retirar los derechos de acceso	Control Los derechos de acceso de todos empleados, contratistas y tercero usuarios a la información e instalaciones de procesamiento de la información les serán quitados o ajustados al terminar su empleo, contrato o acuerdo.

A.9 Seguridad física y ambiental

A.9.1 Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a las instalaciones de la organización y a la información.

A.9.1.1	Perímetro de seguridad física	Control Perímetros de seguridad (barreras como paredes puertas de entrada tarjeta controladas por o recepciones tripuladas) serán use proteger áreas que contienen la información y las instalaciones de procesamiento de la información.
A.9.1.2	Controles de acceso físico	Áreas seguras estarán protegidas por controles de entrada apropiados para asegurar que sólo el personal autorizado tenga permitido el acceso.
A.9.1.3	Protección de oficinas, recintos e instalaciones	Control La seguridad física para oficinas, recintos e instalaciones será diseñada y aplicada.
A.9.1.4	Protección contra amenazas externas y ambientales	Será diseñada y aplicada la protección física contra los daños del fuego, inundación, sismo, explosión, el descontento civil, y otras formas de desastre natural o hecho por el hombre.

A.9.1.5	Desarrollo de tareas en áreas protegidas	Serán diseñadas y aplicadas protección física y pautas para trabajar en áreas seguras.
A.9.1.6	Aislamiento de las áreas de entrega y carga	Los puntos de acceso como las áreas de entrega y carga, y otros puntos donde las personas no autorizadas pueden entrar a las instalaciones serán controlados y, si posible, aislados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.

A.9.2 Seguridad del equipo

Objetivo: Prevenir la pérdida, daño, robo o la puesta en peligro de activos y la interrupción de las actividades de la organización.

A.9.2.1	Ubicación y protección del equipo	Control El equipo será ubicado o protegido para reducir los riesgos de las amenazas ambientales, los peligros y las oportunidades para el acceso no autorizado.
A.9.2.2	Suministros de energía	Control El equipo será protegido de los cortes de electricidad y otras interrupciones causadas por los fallos en utilidades de soporte.
A.9.2.3	Seguridad del cableado	Control Será protegido de daños o intercepciones el cableado de la electricidad y las telecomunicaciones transporta datos o respalda servicios de información.
A.9.2.4	Mantenimiento de equipos	Control El equipo será mantenido correctamente para asegurar su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera del ámbito de la organización	Control Se aplicará seguridad al equipo exterior teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.9.2.6	Baja segura o reutilización de equipo	Control Todos los artículos del equipo que contengan medios de almacenamiento serán revisados para asegurar que cualquier información confidencial y software autorizado han sido eliminados o bien sobrescritos antes del traspaso.
A.9.2.7	Retiro de Bienes	Control El equipo, la información o el software no serán llevados al exterior sin previa autorización.

A.10 Gestión de las comunicaciones y operaciones.

A.10.1 Procedimientos y responsabilidades operativas

Objetivo: Asegurar la operación correcta y segura de servicios/instalaciones de procesamiento de la información.

A.10.1.1	Documentación de los procedimientos operativos	Control Los procedimientos operativos serán documentados, mantenidos, y puestos a disposición de todos los usuarios que los necesiten.
A.10.1.2	Control de cambios en las operaciones	Control Los cambios para servicios/instalaciones de procesamiento de la información y sistemas serán controlados.
A.10.1.3	Separación de funciones	Control Los servicios y áreas de responsabilidad serán separados para reducir las oportunidades para la modificación no autorizada o involuntaria o el mal uso de los activos de la organización.
A.10.1.4	Separación entre instalaciones de desarrollo e instalaciones operativas	Control Desarrollo, prueba e instalaciones en funcionamiento serán separados para reducir los riesgos del acceso no autorizado o cambios al sistema operativo.

A.10.2 Administración de Entrega de Servicio de Terceros

Objetivo: Implementar y mantener el nivel apropiado de la seguridad de la información y la entrega del servicio de acuerdo con los contratos de entrega de los contratos de con terceros.

A.10.2.1	Entrega de servicios	Control Se asegurará que los controles de seguridad, las definiciones del servicio y niveles de entrega incluidos en el contrato de entrega del servicio a los terceros sean implementados, operados y mantenidos por la tercera parte.
A.10.2.2	Monitoreo y validación de los servicios de terceras partes	Control Los servicios, los informes y registros proveídos por la tercera parte serán monitoreados y examinados con regularidad y las auditorías se llevarán a cabo con regularidad.
A.10.2.3	Administrando cambios en los servicios de terceras partes	Control Los cambios para la previsión de servicios, incluyendo mantener y mejorar políticas de seguridad de la información existentes, procedimientos y controles, serán administrados tomando en cuenta la criticidad de los sistemas de la empresa, los procesos complicados y reexaminación de los riesgos.

A.10.3 Planeación y Aceptación de Sistemas

Objetivo: Minimizar el riesgo de fallo de los sistemas.

A.10.3.1	Planificación de la capacidad	Control El uso de recursos será monitoreado, afinado y las proyecciones hechas de futuros requisitos de capacidad para asegurar el rendimiento de sistema requerido.

A.10.3.2	Aprobación del sistema	Control El criterio de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones estarán establecidas y se llevarán a cabo las pruebas apropiadas de (los) sistema (s) durante el desarrollo y antes de la aprobación.

A.10.4 Protección contra código malicioso y móvil

Objetivo: Proteger la integridad del software y la información.

A.10.4.1	Controles contra código malicioso	Control La detección, prevención y los controles de recuperación para proteger contra código malicioso y los procedimientos de conocimiento apropiados de usuario serán implementados.
A.10.4.2	Controles contra código móvil	Control Donde sea autorizado el uso de código móvil, la configuración asegurará que el código móvil autorizado opere de acuerdo a la política de seguridad claramente definida y se impedirá que el código no autorizado sea ejecutado.

A.10.5 Respaldo

Objetivo: Mantener la integridad y disponibilidad de la información y los servicios/instalaciones de procesamiento de la información.

A.10.5.1	Respaldo de la Información	Control Las copias de seguridad de la información y el software serán tomadas y evaluadas con regularidad de acuerdo con la política de copia de seguridad aceptada.

A.10.6 Administración de Seguridad en la Red

Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

A.10.6.1	Controles de redes	Control Las redes estarán adecuadamente dirigidas y controladas, para estar protegidas de las amenazas y mantener la seguridad para los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad en los servicios de red	Control Características de seguridad, niveles del servicio y requisitos de dirección de todos servicios de la red serán identificados e incluidos en cualquier acuerdo de servicios de la red, ya sea que estos servicios sean proveídos en la empresa o por un subcontrato (fuentes externas a la empresa).

A.10.7 Manejo de los medios de almacenamiento

Objetivo: Prevenir la revelación no autorizada, la modificación, la eliminación o destrucción de activos la interrupción de las actividades de la empresa.

A.10.7.1	Administración de medios informáticos removibles	Control Habrá procedimientos en su lugar para la dirección de medios removibles.
A.10.7.2	Disposición de los medios informáticos	Se deben tener procedimientos adecuados para la disposición de los medios informáticos para evitar su disposición por personal no autorizado.
A.10.7.3	Procedimientos de manejo de la información	Control Los procedimientos para el manejo y el almacenamiento de la información serán establecidos para proteger esta información de la revelación no autorizada o el mal uso.
A.10.7.4	Seguridad de la documentación del sistema	Control La documentación del sistema será protegida contra el acceso no autorizado.

A.10.8 Intercambio de Información

Objetivo: Mantener la seguridad en el intercambio de información y software entre una organización y cualquier entidad externa.

A.10.8.1	Procedimientos y Políticas de Intercambio de Información	Control Políticas de intercambio formales, procedimientos, y controles estarán en el lugar para proteger el intercambio de la información a través del uso de todo tipo de instalaciones de comunicación.
A.10.8.2	Acuerdos de Intercambio de Información	Control Los contratos serán establecidos para el intercambio de la información y el software entre la organización y las partes externas.
A.10.8.3	Seguridad de los medios de transito	Control Los medios que contienen la información estarán protegidos contra accesos no autorizados, el mal uso o la corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Seguridad del Comercio Electrónico	Control La información involucrada en el intercambio de mensajes electrónicos estará protegida apropiadamente.
A.10.8.5	Sistemas de Información de Negocios	Control Las políticas y los procedimientos serán desarrollados e implementados para proteger la información relacionada con la interconexión de sistemas de información de la empresa.

A.10.9 Servicios de comercio electrónico

Objetivo: Asegurar la seguridad de servicios de comercio electrónicos, y su uso seguro.

A.10.9.1	Comercio Electrónico	Control La información involucrada en el paso de comercio electrónico sobre redes públicas será protegida de la actividad fraudulenta, la disputa de contrato y la revelación no autorizada y modificaciones.
A.10.9.2	Transacciones en línea	Control La información involucrada en las transacciones en línea estará protegida para prevenir la transmisión incompleta, alteración no autorizada de mensaje, revelación no autorizada y duplicación o repetición no autorizado del mensaje.
A.10.9.3	Sistema de Información a disposición del Público	Control El software, los datos y demás información que requiera un alto nivel de integridad, y que esté disponible en un sistema de acceso público, deben ser protegidos, mediante mecanismos adecuados, por Ej. firmas digitales

A.10.10 Monitoreo

Objetivo: Detectar las actividades de procesamiento de la información no autorizadas

A.10.10.1	Registro de Eventos	Control Deben generarse registros de auditoria que contengan excepciones y otros eventos relativos a seguridad, y deben mantenerse durante un periodo definido para acceder en futuras investigaciones y en el monitoreo de control de accesos.
A.10.10.2	Monitoreo del Uso de los Sistemas	Control Los procedimientos para monitorear el uso de las instalaciones de procesamiento de la información serán establecidos y los resultados de las actividades de monitoreo revisadas periódicamente.
A.10.10.3	Protección de los Registros de Información.	Control Se deben establecer los privilegios de los usuarios para la revisión de los registros de información.
10.10.4	Administrador y operador de registros	Control Las actividades del administrador y del operador del sistema serán registradas.
A.10.10.5	Conexiones Preestablecidas	Control Se deben generar reportes de las conexiones por default establecidas dentro del sistema, así como generar los privilegios de conexión para las cuentas por default a ser utilizadas dentro del sistema.
A.10.10.6	Sincronización de relojes	Control Los relojes de todos los sistemas importantes de procesamiento de la información dentro de una organización o dominio de seguridad serán sincronizados con un origen de tiempo exacto aceptado.

A.11 Control de acceso

A.11.1 Requerimientos de negocio para el Control de Acceso
Objetivo: Controlar el acceso a la información.

A.11.1.1	Política de control de acceso	Control Una política de control de acceso será establecida, documentada y revisada basándose en los requisitos de seguridad para el acceso.

A.11.2 Administración de acceso a usuarios
Objetivo: Asegurar el acceso a usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.

A.11.2.1	Registro de usuarios	Control Debe existir un procedimiento formal de registro y des-registro de usuarios para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Administración de privilegios	Control La asignación y uso de privilegios será restringido y controlado.
A.11.2.3	Administración de contraseñas de usuario	Control La asignación de contraseñas será controlado mediante un proceso de administración formal.
A.11.2.4	Revisión de derechos de acceso de usuario	Control La dirección examinará los derechos de acceso de los usuarios en intervalos regulares usando un proceso formal.

A.11.3 Responsabilidades de Usuario
Objetivo: Prevenir el acceso a usuarios no autorizados y el robo de información o de instalaciones de procesamiento de la información.

A.11.3.1	Uso de contraseñas	Control Se exigirá a los usuarios seguir buenas prácticas de seguridad en la selección y el uso de contraseñas.
A.11.3.2	Equipos desatendidos en áreas de usuarios	Control Los usuarios deben garantizar que los equipos desatendidos sean protegidos adecuadamente con controles de seguridad adecuados.
A.11.3.3	Política de pantalla clara y escritorio limpio	Control Se adoptará una política de escritorio limpio de papeles y medios de almacenamiento removibles y una política de pantalla clara para instalaciones de procesamiento de la información.

A.11.4 Control de acceso a la red
Objetivo: Prevenir el acceso no autorizado a servicios conectados a la red.

A.11.4.1	Política sobre el uso de servicios de la red	Control A los usuarios sólo se les dará acceso para los servicios que se les ha autorizado usar.
A.11.4.2	Autentificación del usuario para conexiones externas.	Control Se usarán métodos de autentificación apropiados para controlar el acceso a usuarios por medios remotos.
A.11.4.3	Identificación de equipos en la red	Control Se debe establecer un identificador único a cada uno de los equipos conectados a la red para identificar si el equipo tiene permitido conectarse a la red.
A.11.4.4	Diagnóstico remoto y protección de puerto de configuración	Serán controlados los accesos físicos y lógicos para diagnosticar y configurar puertos.
A.11.4.5	Subdivisión de redes	Control Debe ser establecida una subdivisión de redes de dominios de red interna y externa, cada una de ellas protegidos por un perímetro de seguridad adecuado.
A.11.4.6	Control de conexión a redes	Control Para redes compartidas, especialmente aquellas que se extiendan al otro lado de los límites de la organización, la capacidad de usuarios para conectarse a la red estará restringida, de acuerdo con la política de control de acceso y los requisitos de las aplicaciones de la empresa (ver 11.1).
A.11.4.7	Control de direccionamiento de la red	Control Los controles de direccionamiento serán implementados para redes para asegurar que las conexiones de computadora y los flujos de información no violan la política de control de acceso de las aplicaciones de la empresa.

A.11.5 Control de acceso del sistema operativo

Objetivo: Prevenir el acceso no autorizado a los sistemas operativos

A.11.5.1	Procedimientos de entrada en el sistema seguros	Control El acceso para los sistemas operativos será controlado por un procedimiento seguro de entrada al sistema.
A.11.5.2	Autentificación e identificación de usuarios	Control Todos usuarios tendrán un identificador único (clave del usuario) para su uso personal y se elegirá una técnica de autentificación adecuada para que comprobar la identidad de un usuario.
A.11.5.3	Sistema de administración de contraseña	Control Los sistemas para administrar contraseñas serán interactivos y asegurarán la calidad de las contraseñas.
A.11.5.4	Uso de utilidades de sistema	Control Se deben tener documento con los perfiles de usuario para el uso de las utilidades del sistema definiendo a los usuarios autorizados de su uso.

		Control
A.11.5.5	Sesiones expiradas	Las sesiones inactivas se apagarán después de un período definido de la inactividad.
		Control
A.11.5.6	Limitación del tiempo de conexión	Las restricciones en tiempo de conexión serán utilizadas para brindar seguridad adicional para aplicaciones de alto riesgo.

A.11.6 Control de acceso a la información y a la aplicación

Objetivo: Prevenir el acceso no autorizado para la información sujeta en sistemas de aplicación.

		Control
A.11.6.1	Restricción de acceso a la información	El acceso a la información y a las funciones del sistema de aplicación por usuarios y el personal de soporte será restringido de acuerdo con la política de control de acceso definida.
		Control
A.11.6.2	Aislamiento de sistemas sensibles	Se deben tener identificados y acordados los sistemas de aplicación con los cuales compartirá recursos, cuando una aplicación sensible ha de ejecutarse en un ambiente compartido.

A.11.7 Cómputo móvil y trabajo remoto

Objetivo: Garantizar la seguridad de la información cuando se usa informática móvil e instalaciones de trabajo remotas.

		Control
A.11.7.1	informática y comunicaciones móviles	Se debe adoptar una política formal que tome en cuenta los riesgos que implica trabajar con herramientas informáticas móviles, en particular en ambientes no protegidos.
		Control
A.11.7.2	Trabajo Remoto	Una política, planes operativos y procedimientos serán desarrollados e implementados para actividades remotas.

A.12 Adquisición de Sistemas de Información, Desarrollo y Mantenimiento

A.12.1 Requerimiento de Seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad es una parte integral de los sistemas de información

		Control
A.12.1.1	Análisis y especificaciones de los requerimientos de seguridad	Se debe contar con un documento formal que defina los requerimientos de seguridad de los sistemas de información y el método bajo el cual se desarrollara la aplicación.

A.12.2 Procesamiento adecuado en las Aplicaciones

Objetivo: Prevenir errores, pérdidas, modificaciones no autorizadas o el mal uso de la información en aplicaciones.

A.12.2.1	Validación de datos de entrada	Control Los datos de entrada en los sistemas de aplicación deben ser validados para asegurar que sea correctos, apropiados y confiables.
A.12.2.2	Controles de procesamiento interno	Deben ser contempladas revisiones de verificación dentro de la aplicación para detectar cualquier tipo de anomalía en la información a través de errores de procesamiento o actos deliberados.
A.12.2.3	Autenticación de mensajes	Debe ser implementado un dispositivo físico de autenticación de mensajes o un algoritmo de software en hardware o software que lo soporte.
A.12.2.4	Validación de los datos de salida	Control Los datos de salida de una aplicación serán validados para asegurar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.

A.12.3 Controles Criptográficos

Objetivo: Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos

A.12.3.1	Política de utilización de controles criptográficos	Se debe contar con una política documentada e implementada para el uso de los controles criptográficos para la protección de la información.
A.12.3.2	Administración de claves	Deben ser implementadas técnicas de cifrado dentro de la administración de las claves.

A.12.4 Seguridad en los Archivos de Sistema

Objetivo: Garantizar la seguridad de los archivos de sistema.

A.12.4.1	Control del software operativo	Control Debe haber procedimientos para controlar la instalación del software sobre sistemas operativos
A.12.4.2	Protección de los datos de prueba del sistema	Deben ser realizadas pruebas de aceptación del sistema considerando volúmenes grandes de datos prueba, estos datos deben ser protegidos y controlados.
A.12.4.3	Control de acceso a las bibliotecas de programa fuente	Será restringido el acceso al código fuente del programa.

A.12.5 Seguridad en los procesos de desarrollo y soporte

Objetivo: Mantener la seguridad del software del sistema de aplicación y de la información.

A.12.5.1	Procedimientos de control de cambios	La implementación de cambios será controlada con un procedimiento formal de control de cambios
A.12.5.2	Revisión técnica de los cambios en el sistema operativo	Cuando se realizan los cambios, los sistemas de aplicación deben ser revisados y probados para garantizar que no se produzca un impacto adverso en las operaciones o en la seguridad

A.12.5.3	Restricción del cambio en los paquetes de software	Las modificaciones para paquetes de software estarán limitados a los cambios necesarios y todos cambios serán estrictamente controlados
A.12.5.4	Fuga de información	Se prevendrá de las oportunidades para la fuga de información
A.12.5.5	Desarrollo externo de software	Control El desarrollo externo de software será supervisado y monitoreado por la organización.

A.12.6 Administración de vulnerabilidad técnica

Objetivo: Reducir riesgos que resulten de la explotación de las vulnerabilidades técnicas anunciadas.

A.12.6.1	Control de vulnerabilidades técnicas	Control Deben ser establecidas revisiones de seguridad para el análisis de vulnerabilidades iniciando con la creación de un inventario de los activos a ser analizados.

A.13 Administración de Incidente de Seguridad de la Información

A.13.1 Reporte de Eventos de Seguridad de la Información y Debilidades

Objetivo: Asegurar que los eventos de seguridad de la información y las vulnerabilidades relacionadas con los sistemas de información sean comunicados de manera que se permita que la acción correctiva sea ejecutada en el momento oportuno.

A.13.1.1	Reporte de Incidente de Seguridad de Información	Control Los eventos de seguridad de la información serán reportados a través de los canales de administración apropiados tan rápido como sea posible.
A.13.1.2	Reporte de vulnerabilidades de seguridad	Control Se pedirá a todos los empleados, contratistas y terceros usuarios que tengan acceso a los sistemas de información y servicios que apunten y reporten cualquier sospecha de vulnerabilidad en los sistemas o servicios.

A.13.2 Administración de los Incidentes de Seguridad de la Información y Mejoras

Objetivo:

13.2.1	Procedimientos y Responsabilidades	Control Las responsabilidades de administración y procedimientos serán establecidos para asegurar una reacción rápida, eficaz y ordenada a los incidentes de seguridad de información.
13.2.2	Aprendizaje de los incidentes de seguridad de información	Control Se deben implementar mecanismos que permitan monitorear y cuantificar los incidentes o anomalías detectadas con anterioridad para identificar o anomalías recurrentes o de alto impacto.

A.13.2.3	Recolección de evidencia	Debe existir un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización.

A.14 Administración de la Continuidad del Negocio

A.14.1 Aspectos de Seguridad de la Información de la Administración de la Continuidad del Negocio

Objetivo: Contrarrestar las interrupciones a las actividades de la empresa y proteger procesos críticos de la empresa de los efectos de fracasos mayores de sistemas de información o desastres y asegurar su reanudación en el momento oportuno.

A.14.1.1	Proceso de administración de la continuidad de los negocios	Control Un proceso dirigido será desarrollado y actualizado para la continuidad de la empresa en toda la organización que aborda los requisitos de seguridad de información necesarios para la continuidad de la empresa de la organización.
A.14.1.2	Continuidad del negocio y análisis de Riesgo	Se identificarán los eventos que puedan causar interrupciones a los procesos de la empresa, también se identificará la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Elaboración e implementación de planes de continuidad de los negocios	Control Se desarrollarán e implementarán planes para mantener o restituir las operaciones y asegurar la disponibilidad de la información en el nivel y tiempo requeridos, escalar a la interrupción siguiente o al fracaso de procesos siguiente.
A.14.1.4	Marco para la planificación de la continuidad de los negocios	Será elaborado un marco de planes de continuidad de la empresa para asegurar que todos planes sean consistentes para dirigir razonablemente los requisitos de seguridad de la información y para identificar las prioridades para la prueba y el mantenimiento.
A.14.1.5	Prueba, mantenimiento y reevaluación de los planes de continuidad de los negocios	Control Los planes de continuidad del negocio serán evaluados y actualizados con regularidad para asegurar que están actualizados y que son eficaces.

A.15 Cumplimiento

A.15.1 Cumplimiento de Requerimientos Legales

Objetivo: Evitar los incumplimientos de cualquier ley, obligaciones reguladoras o contractuales y de algunos requisitos de seguridad.

A.15.1.1	Identificación de la legislación aplicable	Control Todos los requisitos legales, reguladores y contractuales y el enfoque de la organización para cubrir estos requisitos serán explícitamente definidos, documentados y guardado hasta la fecha para cada sistema de información y la organización.

A.15.1.2	Derechos de propiedad intelectual (dpi)	Control Se implementarán los procedimientos apropiados para asegurar el acatamiento a requisitos legislativos, reguladores y contractuales sobre el uso del material con respecto a el que puede tener derechos de propiedad intelectual y sobre el uso de productos de software de propietario.
15.1.3	Protección de los registros de la organización	Se debe llevar una clasificación de los registros en diferentes tipos, por ej. registros contables, registros de base de datos, “logs” de transacciones, “logs” de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento.
A.15.1.4	Protección de datos y privacidad de la información personal	Control Se asegurará la protección y privacidad de datos requerida en la legislación, las reglas y, si es aplicables en cláusulas contractuales.
A.15.1.5	Prevención del uso inadecuado de los recursos de procesamiento de información	Deben ser establecidas políticas donde se indique que el usuario no podrá realizar actividades para propósitos no autorizados.
A.15.1.6	Regulación de controles para el uso de criptografía	Control Los controles criptográficos serán usados de acuerdo con todos los contratos relevantes, leyes y reglas.

A.15.2 Cumplimiento con Políticas de Seguridad y Estándares y Cumplimiento Técnico

Objetivo: Asegurar el acatamiento de sistemas con las políticas de seguridad organizacionales y los padrones.

15.2.1	Cumplimiento con políticas y estándares de seguridad	Control Los directores asegurarán que todos los procedimientos de seguridad dentro de su área de responsabilidad son llevados correctamente para conseguir el acatamiento de las políticas de seguridad y los padrones.
A.15.2.2	Revisar el cumplimiento técnico	Control Las sistemas de información serán examinadas regularmente en busca del cumplimiento con los padrones de implementación de seguridad.

A.15.3 Consideraciones de Auditoría de Sistemas de Información

Objetivo: Maximizar la eficacia de y minimizar la interferencia a/de los procesos de auditoria a los sistemas de información.

A.15.3.1	Controles de auditoria de sistemas	Los requisitos y las actividades de auditoría para examinan los sistemas operativos serán cuidadosamente planeadas y aceptadas para minimizar el riesgo de las interrupciones a procesos de la empresa.

A.15.3.2	Protección de las herramientas de auditoría de sistemas	Control El acceso para herramientas de auditoría de sistemas de la información será protegido para prevenir cualquier posible mal uso o acuerdo.

Anexo B: Términos y definiciones del ISO/IEC 270001:2005

Activo

Cualquier cosa que tiene valor para la organización.

Disponibilidad

La propiedad de ser accesible y estar a disposición de uso bajo demanda por parte de una entidad autorizada.

Confidencialidad

La propiedad mediante la cual la información no se hace disponible o se revela a individuos, entidades o procesos no autorizados.

Seguridad de la información

Trata de la preservación de la confidencialidad, integridad y disponibilidad de la información; adicionalmente, otras propiedades como la autenticidad, responsabilidad, confiabilidad y no repudio también pueden estar involucradas.

Evento de seguridad de la información

La ocurrencia identificada de un sistema, servicio o estado de red que indica una posible brecha a la política de seguridad de la información o una falla en las salvaguardas, o una situación previamente desconocida que sea relevante desde el punto de vista de seguridad.

Incidente de seguridad de la información

Un evento o serie de eventos indeseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenazar la seguridad de la información.

Sistema de Gestión de la Seguridad de la Información

La parte del sistema de gestión global, basada en aproximación de riesgos del negocio, para establecer, implantar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Integridad

La propiedad mediante la cual se salvaguarda la precisión y el estado completo de los activos.

Riesgo residual

El riesgo remanente después del tratamiento del riesgo.

Aceptar el riesgo

La decisión de aceptar un riesgo.

Análisis de riesgo

El uso sistemático de información para identificar fuentes y estimar el riesgo.

Tasación del riesgo

El proceso general comprendido por el análisis y evaluación del riesgo.

Evaluación del riesgo

El proceso de comparar el riesgo estimado contra unos criterios dados para determinar la importancia del riesgo.

Administración del riesgo

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Tratamiento del riesgo

El proceso de seleccionar e implantar medidas para modificar el riesgo.

Declaración de aplicabilidad

Declaración documentada en donde se describen los objetivos de control y los controles que son relevantes y aplicables al ISMS de la organización.

GLOSARIO

Glosario

ACL: Una **Lista de Control de Acceso** o **ACL** (del inglés, ***Access Control List***) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Activo informático: Involucra datos, información, sistema, software, hardware o cualquier elemento de tecnología de información

Amenaza: Cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema

Autenticidad: Se refiere a establecer con seguridad el origen de la información.

Broadcast: Broadcast, en castellano **difusión**, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CERT: Un CERT es una organización a nivel nacional o regional que actúa como centro de coordinación para responder a incidentes de seguridad en materia de cómputo y redes de datos.

Checksum: Una **suma de verificación** o **checksum** es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corrompidos. Es empleado para comunicaciones (internet, comunicación de dispositivos, etc.) tanto como para datos almacenados (archivos compresos, discos portátiles, etc.)

COBiT: Control Objectives for Information and Related Technology (Objetivos de Control para la Información y Tecnologías Relacionadas)

Control: salvaguarda o mecanismo: Medida de protección (técnica o normativa) de los activos informáticos

Criterios Comúnes: Los Criterios Comúnes para la Evaluación de la Seguridad de la Tecnología de Información (**Common Criteria for Information Technology Security Evaluation)** es un estándar internacional para la seguridad en cómputo.

Cron: En el sistema operativo Unix, **cron** es un administrador regular de procesos en segundo plano (*demonio*) que ejecuta programas a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el archivo `crontab`.

DIDS: DIDS (*DistributedIDS*): sistema basado en la arquitectura cliente-servidor compuesto por una serie de NIDS (IDS de redes) que actúan como sensores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar unas reglas de control especializándose para cada segmento de red.

DISA: La Agencia de Defensa de los Sistemas de Información es una agencia de combate responsable por la planeación, ingeniería, adquisición, implantación y soporte de soluciones céntricas con alcance global para servir a las necesidades de la Secretaría de Defensa de los Estados Unidos de América.

Disponibilidad: La propiedad de ser accesible y estar a disposición de uso bajo demanda por parte de una entidad autorizada

DNS: El **Domain Name System** (DNS) es la asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS.

DoS: En seguridad informática, un **ataque de denegación de servicio**, también llamado **ataque DoS** (de las siglas en inglés *Denial of Service*), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima

DRP: Un **plan de recuperación ante desastres** (del inglés *Disaster Recovery Plan*) es un proceso de

recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos. Esto también debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave, aunque esto no sea cubierto en este artículo, el propósito es la protección de datos.

Guerra asimétrica: Conflicto violento donde existe una gran desproporción entre las fuerzas de los bandos implicados, y que por lo tanto obliga a las partes a utilizar medios fuera de la tradición de guerra común

Firewall: Un **cortafuegos** (o ***firewall*** en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red

ICMP: El **Protocolo de Mensajes de Control de Internet** o **ICMP** (por sus siglas de ***I**nternet **C**ontrol **M**essage **P**rotocol*) es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP).

IDS: Un **sistema de detección de intrusos** (o **IDS** de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional)

Impacto: El efecto de una amenaza sobre la misión y objetivos de una organización

Información: Conjunto organizado de datos procesados

Integridad: La propiedad mediante la cual se salvaguarda la precisión y el estado completo de los activos

Iptables: Netfilter es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho framework permite realizar el manejo de paquetes en diferentes estados del procesamiento

MODEM: Un **módem** es un dispositivo que sirve para modular y demodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada *portadora* mediante otra señal de entrada llamada *moduladora*.

Netfilter es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux. El componente más popular construido sobre *Netfilter* es **iptables**, una herramientas de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log.

NFS: El **Network File System** *(Sistema de archivos de red)*, o **NFS**, es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local

NIS: Network Information Service (conocido por su acrónimo **NIS**, que español significa *Sistema de Información de Red*), es el nombre de un protocolo de servicios de directorios cliente-servidor desarrollado por Sun Microsystems para el envío de datos de configuración en sistemas distribuidos tales como nombres de usuarios y hosts entre computadoras sobre una red

ISMS: Information Security Manager System (Sistema de Gestión de Seguridad de la Información)

ISO: Organización Mundial para la Estandarización

MAC: En redes de computadoras la dirección MAC *(Media Access Control address* o dirección de control de acceso al medio) es un identificador de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

MD5: En criptografía, **MD5** (acrónimo de *Message-Digest Algorithm 5*, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado

Necortex: Neocórtex, "corteza nueva" o la "corteza más reciente" es la denominación que reciben las áreas más evolucionadas de un área del cerebro. Estas áreas constituyen la "capa" neuronal que recubre los lóbulos prefrontales y, en especial, frontales de los mamíferos. Se encuentran muy desarrolladas en los primates y destaca el desarrollo en el homo sapiens.

NIDS: NIDS (*NetworkIDS*): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.

NIST: El **Instituto Nacional de Normas y Tecnología** (**NIST** por sus siglas en inglés) es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida

OCTAVE: Operationally Crtical Threat, Asset, and Vulnerability Evaluation (Evaluación de Amenazas, Activos y Vulnerabilidades Criticas para la Operación)

OECD: Organisation for Economic Co-operation and Development (Organización para la Cooperación y el Desarrollo Económico)

Outsourcing: **Subcontratación** (del inglés **outsourcing**), también llamado **tercerización** o **externalización**, es el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.

Perpetrar: Cometer, consumar un delito o culpa grave

PDCA: Ciclo PDCA de mejora continua de la calidad, basado en 4 pasos, planear, hacer, revisar y actuar

Políticas de seguridad: Es el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema.

QoS: QoS o **Calidad de Servicio** (*Quality of Service*, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio.

Riesgo: Algo que puede causar un daño o la probabilidad de que una amenaza pueda explotar una vulnerabilidad

RPM: ***RPM Package Manager*** (o **RPM**, originalmente llamado ***Red Hat Package Manager***) es una herramienta de administración de paquetes pensada básicamente para Linux. Es capaz de instalar, actualizar, desinstalar, verificar y solicitar programas. RPM es el formato de paquete de partida del Linux Standard Base

SAN: Una **red de área de almacenamiento**, en inglés **SAN** (Storage Area Network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de respaldo principalmente, está basada en tecnología **fibre channel** y más recientemente en **iSCSI**. Su función es la de conectar de manera rápida, segura y confiable los distintos elementos que la conforman.

SAR: El comando sar produce informes de utilización del sistema basado en los datos reunidos por sadc. Los informes sar, se pueden generar interactivamente o se pueden escribir a un archivo para un análisis más intensivo. De acuerdo con la configuración en Red Hat Enterprise Linux, SAR es ejecutado automáticamente para procesar los archivos reunidos automáticamente por sadc. Los archivos de informes se escriben a /var/log/sa/ y son nombrados sar<dd>, donde <dd> son las representaciones de dos dígitos de la fecha del día anterior

SEI: Software Engineering Institute (Instituto de Ingeniería del Software)

Seguridad informática: Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización

SoA: Declaración documentada en donde se describen los objetivos de control y los controles que son relevantes y aplicables al ISMS de la organización

SSH: SSH (**S**ecure **SH**ell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X arrancado.

Sudo: El programa **sudo** (de las siglas en inglés de ***s****uper****u****ser* -o ***s****ubstitute* ***u****ser*- ***do***) es una utilidad de los sistemas operativos tipo Unix, como Linux, BSD, o Mac OS X, que permite a los usuarios ejecutar programas

con los privilegios de seguridad de otro usuario (normalmente el usuario root) de manera segura

TCP/IP: La **familia de protocolos** de Internet es un conjunto de protocolos de red en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se la denomina *conjunto de protocolos **TCP/IP***, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia.

TCP Wrapper: TCP Wrapper ("*Envolvedor de TCP*") es un sistema de red ACL que trabaja en terminales y que se usa para filtrar el acceso de red a servicios de protocolos de Internet que corren en sistemas operativos (tipo UNIX), como ser Linux o BSD. Permite que las direcciones IP, los nombres de terminales y/o respuestas de consultas ident de las terminales o subredes sean usadas como *tokens* sobre los cuales filtrar para propósitos de control de acceso

UID: En sistemas tipo Unix, los usuarios son representados por un identificador de usuario, normalmente abreviado como UID. Las características básicas son:

- El rango de los valores de los UID's varía entre los diferentes sistemas.
    - Como mínimo los UID's deben estar comprendidos entre 0 y 32767.
- El superusuario debe tener siempre UID 0.
- Al usuario nobody siempre se le asignada por tradición el UID más alto posible (como oposición al superusuaio). Normalmente, se le asigna el 32767

VLAN: Una **VLAN** (acrónimo de ***Virtual LAN***, 'red de área local virtual') es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de colisión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador)

Vulnerabilidad: Cualquier debilidad que puede explotarse para causar pérdida o daño al sistema

WTC: Centro Mundial de Comercio, en el texto referido como complejo ubicado en Manhatan, Nueva York, donde se situaban las torres gemelas

BIBLIOGRAFÍA

Bibliografía

- Alexander G., Alberto. *Diseño de un Sistema de Gestión de Seguridad de la Información.* Ed. Alfaomega. Colombia, 2007.
- Amoroso, Edward. *Cyber Security*. Silicon Press, E.U., 2007. Consultado en línea en http://acm.books24x7/
- Báez, Fernando. *Fuego y pillaje en la biblioteca de Bagdad.* La Nación, 2003**,** Suplemento Cultura en http://www.lanacion.com.ar/Archivo/Nota.asp?nota_id=498289
- Báez, Fernando. *Historia universal de la destrucción de libros: de las tablillas sumerias a la guerra de Irak*. Ed. Debate 1ra edición, Barcelona 2004, 386 páginas
- Daltabuit, Enrique. *La información y su seguridad.* Nexos, 2005. No. 334 en http://www.nexos.com.mx/articulos.php?id_article=646&id_rubrique=203
- Daltabuit, Enrique, Hernández, Leobardo, Mallen, Guillermo y Vázquez José de Jesús. *La Seguridad de la Información,* Ed. Limusa. 1ra. Edición, México, 2007. 774 págs.
- Garfinkey Simson, Spafford Gene. *Seguridad práctica en Unix e Internet*. Ed. McGrawHill. México, 1999.
- Griful Eulalia, *Gestión de la Calidad.* Ediciones UPC 1ra edición, Barcelona 2002, 234 páginas
- International Organization for Standarization and International Electrotechnical Commission, *ISO/IEC 27001:2005 "Information Technology – Security techniques – Information security management systems – Requirements"*.
- IT Governance Institute, *CobiT 4.0*. IT Governance Institute, E.U. 2005., 209 Págs.
- Kessler, Gary. Levine, D. *Computer Security Handbook*, Ed. John Wiley & Sons, E.U. 2002.
- Quezada, Cintia. *Metodología para la aplicación de la norma ISO/IEC 17799.* Postgrado en Ciencia e Ingeniería de la Computación. México, 2005.
- Organization For Economic Cooperation and Development, *OECD Guidelines for the Security of Information Systems and Networks*. OECD, 2002. 30 Págs.
- Sagan, Carl. *El mundo y sus demonios.* Editorial Planeta. México, 2007. 469 págs.
- Schneier, Bruce. *Beyond Fear*, Ed. Springer-Verlag. E.U. 2003. 296. Págs.
- Schneier, Bruce. Ferguson, Niels. *Practical Cryptography*.Wiley Publishing, Inc., E.U., 2003. 384 págs.
- Schneier, Bruce. *The Psychology of Security.* 2008. Consultado en http://www.schneier.com/essay-155.html.
- Staten, Clark. *Asymmetric Warfare, the Evolution and Devolution of Terrorism* en http://www.emergency.com/
- Summers, Rita C. *Secure Computing. Threats and Safeguards.* Ed. McGraw-Hill, E.U. 1996. 654 págs.
- The 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Superintendent of Documents, U.S. Government en http://www.9-11commission.gov/
- Valenzuela, Ismael. *Integrating ISO 17799 into your Software Development Lifecycle.* (In)secure Magazine. No. 11. en http://www.net-security.org/insecuremag.php.