UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

Una Metodología para la formulación de políticas en seguridad informática

T E S I S

QUE PARA OBTENER EL TITULO DE

A C T U A R I O

P R E S E N T A :

JUAN CARLOS HIDALGO CABALLERO

DIRECTOR DE TESIS: MAT. SALVADOR LOPEZ MENDOZA

2004

UNIVERSIDAD NACIONAL
AVENSA TI
MEXI

ACT. MAURICIO AGUILAR GONZÁLEZ
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:

"Una Metodología para la formulación de políticas en seguridad informática"

realizado por Juan Carlos Hidalgo Caballero

con número de cuenta 7408058-6 , quien cubrió los créditos de la carrera de: Actuaría

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Mat. Salvador López Mendoza
Propietario	M. en C. José Antonio Flores Díaz
Propietario	M. en A.P. María del Pilar Alonso Reyes
Suplente	Mat. María Concepción Ana Luisa Solís González-Cosio
Suplente	Dra. Amparo López Gaona

Consejo Departamental de Matemáticas

Act. Jaime Vázquez Alamilla

FACULTAD DE CIENCIAS
CONSEJO DEPARTAMENTAL
DE
MATEMATICAS

Dedicatoria

A mi familia, que son lo que mas amo en la vida:
Guadalupe, Sara, Lucía y Carlos

A mi hermana Maru, A mi madre

A Fer, A Marce, A Don Dani

A mi muy querida Universidad, con todo mi reconocimiento y agradecimiento. A la Facultad de Ciencias. A los profesores de quienes aprendí no sólo infinidad de conocimiento, sino actitud perseverante, pensamiento riguroso y entrega

Prefacio

El presente trabajo está fundamentado en 20 años de experiencia profesional en el área de Tecnologías de la Información.

Se ha realizado buscando entregar un documento que sirva de referencia y guía práctica a quien quiera consultarlo, buscando aprovechar el conocimiento de la industria, las necesidades del mercado y las aportaciones que diversas personas han hecho al tema de la seguridad, desde la academia, hasta prestigiados organismos de investigación.

Quisiera agradecer a mi director de tesis, Mat. Salvador López Mendoza su dedicación y paciencia para orientar mi trabajo, ayudándome a darle forma a un caudal de ideas que brotaban de mi mente en forma espontánea, pero desordenada. Agradezco también a los sinodales sus puntos de vista y opiniones.

Finalmente quiero expresar la enorme satisfacción que tiene para mi llegar a este punto, después de haber dejado la facultad por tantos años. Ha sido una experiencia muy gratificante, y espero que los lectores encuentren de provecho esta aportación al tema.

México D.F., mayo de 2004

INTRODUCCIÓN.

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan plenamente sus objetivos, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática y su cumplimiento.

Esta situación ha llevado a que muchas empresas con activos muy importantes se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen su información confidencial y por ende el resguardo de sus documentos confidenciales. Ante esta situación los directivos de las organizaciones deben confirmar que las personas entiendan la importancia estratégica de la seguridad, conozcan sus alcances y estén de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas deben integrarse a las estrategias de la empresa, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencia en las proyecciones y utilidades de la organización.

Finalmente, es importante señalar que las políticas constituyen un marco para la seguridad de las organizaciones, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la administración de la información.

La seguridad informática ha tomado gran auge debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes mundiales ha abierto nuevos horizontes a las

empresas para mejorar su productividad y poder interactuar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas, y recomendaciones para obtener el mayor provecho de estas ventajas y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

Es así como las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación el proponer o identificar una política de seguridad se vuelve prioritario ya que se requiere un alto compromiso con la organización, agudeza técnica para identificar vulnerabilidades y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las empresas modernas.

El objetivo de este trabajo es resaltar la importancia que tiene el establecer y mantener un nivel óptimo de seguridad de la información dentro de las organizaciones a través del establecimiento de un manual que contenga las políticas y los lineamientos en seguridad informática. Así mismo analizar los riesgos y los efectos en las organizaciones de no contar con una política de seguridad informática.

ÍNDICE

CAPÍTULO 1

LA SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO 1

LA SEGURIDAD DE LA INFORMACIÓN

Actualmente, el uso de las computadoras se ha vuelto una herramienta imprescindible para las empresas de cualquier ramo de la industria, que pretenden mejorar su competitividad ante el mercado. La información que se genera a través de este tipo de herramientas es uno de los activos más importantes dentro de una empresa, ya que a partir de ésta se pueden obtener infinidad de datos y estadísticas que son insumos muy valiosos en las empresas para la toma de decisiones. Por lo tanto, es de vital importancia que se cuente con esquemas de seguridad informática, por muy básicos que sean, de tal manera que se pueda garantizar no sólo a los clientes sino a los empleados y a los propietarios de la empresa que su información está protegida. Con un buen esquema de seguridad de información la empresa limita el acceso y evita fugas, daños o pérdida de la misma además de ofrecer confidencialidad, integridad y disponibilidad de la información a sus clientes.

Para poder establecer un buen esquema de seguridad es necesario analizar las amenazas o riesgos a los que está expuesta la información. Para este fin se utilizan diversas técnicas, entre ellas se encuentra el análisis de riesgo, herramienta que sirve para cuantificar los riesgos a que están sujetos los activos de una empresa, la pérdida esperada y el costo de tomar medidas para controlar la situación. Si no se lleva a cabo una evaluación periódica de los esquemas de seguridad, o no se toman las acciones adecuadas en base a los resultados de estos, es posible que la información no esté totalmente protegida.

"La tecnología de la información nos está introduciendo rápidamente en una nueva era, posterior a la industrial, la cual se encuentra en sus etapas iniciales.

Se ha dicho que el elemento básico en esta tecnología, el microprocesador, cobrará mayor importancia que la máquina de vapor, la cual en su propio tiempo puso los cimientos para la revolución industrial." [1]

Según datos de Microsoft se ha calculado que el volumen total de información se está incrementando a una tasa aproximada de 20% anual. En forma paralela a este crecimiento, los especialistas en tecnología de la información, deben mantenerse actualizados, de manera que se disponga de los conocimientos y la capacidad para tomar las decisiones correctas. Esto significa que se debe tener la capacidad de manejar y administrar información en forma segura y confiable; significa también que se deben tener sistemas que estén disponibles siempre que se los necesite y que produzcan información en la cual se pueda confiar.

¿Qué tan segura está la información que utiliza y necesita la sociedad? El hecho de que los grandes desastres no se produzcan todos los días y sean más bien ocasionales no significa que se tenga totalmente controlada la situación. Todos los días pueden ocurrir robos de información, incendios y aun sabotaje contra instalaciones de procesamiento electrónico de datos. Esto puede no representar una catástrofe para la sociedad, pero seguramente si es lo suficientemente serio para los afectados. También pueden ocurrir desastres naturales, tales como terremotos, inundaciones, erupciones volcánicas, etc. en este caso, representarían una catástrofe para toda la sociedad afectando, entre otras cosas, a los sistemas de información.

Cada día más funciones vitales para la sociedad están basando su ejecución y su futuro en la tecnología de la información. Mientras mejor se aproveche este poderoso recurso e se integren sistemas de cómputo a los procesos operativos

[1] Braun, Unda. M. Apuntes de la materia Ciencias y técnicas de la información, UNAM, ENEP Acatlán, 2000.

y administrativos, mayor relevancia tendrá la seguridad de la información. Así, hay una necesidad real para incrementar el conocimiento de los temas referentes a seguridad y vulnerabilidad de la información.

1.1 ¿QUÉ ES LA SEGURIDAD?

La función del procesamiento de datos es un servicio de toda organización que apoya no sólo a los sistemas de información administrativa sino también a las operaciones funcionales, por lo tanto, la seguridad de la información es un aspecto de gran importancia para la correcta administración informática.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos, dispositivos y de los ambientes en que éstos se encuentren.

La seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar incluso a la vida privada de las personas, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto por parte de la nueva sociedad informática.

Cuando se habla de seguridad, se habla también de tres aspectos que se deben contemplar siempre: confidencialidad, integridad y disponibilidad

- "La confidencialidad, se cumple cuando solamente las personas autorizadas pueden conocer los datos o la información correspondiente.
- La integridad, consiste en que sólo los usuarios autorizados puedan alterar los datos.

- La disponibilidad, se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas."[2]

Además de estos tres aspectos, también deben existir las autorizaciones necesarias para que los usuarios puedan ingresar a las bases de datos en las que sólo ellos puedan hacer uso.

1.2 ¿QUÉ ES LA INFORMACIÓN?

Información es una palabra usada de muchas maneras, pero en relación con el procesamiento electrónico de datos (EDP por sus siglas en ingles), significa "datos recopilados y presentados de modo que contengan un significado".[3]

Un sistema efectivo de información basado en EDP que puede producir la información correcta para la persona indicada en el tiempo necesario, apoyando la toma de decisiones correcta, se ha vuelto uno de los factores competitivos más importantes en estos días.

Manejo de la Información

La información y los sistemas de información son muy valiosos. Por lo tanto, deberían ser tratados como un recurso estratégico, como el capital o la infraestructura y se les debería dar la misma protección. Toda la información debe ser protegida para asegurar credibilidad junto con calidad y precisión al usuario. El responsable de la seguridad de la información es el "propietario" de la información.

---

[2] Información presentada en el seminario "Construyendo un servidor Internet seguro" del Instituto para la Seguridad en Internet http://www.intise.com, 2001.

[3] Bohlander George y Sherman Arthur. Administración de la Información. México. Ediciones Thomson. 1999. p. 87

El principal desafío y riesgo para la seguridad está representando no por la tecnología sino por la gente involucrada. Por lo tanto es necesario decidir que información no debería estar disponible para todos, pero sí para personal con cierto perfil. La clasificación de información sensitiva requiere ser formalizada, a fin de preservar la seguridad de la información bajo condiciones más extremas. En el caso de los sistemas de información automatizados, se debe establecer la jerarquía de autorización formal antes de que los sistemas sean puestos en producción.

1.3 ¿DE QUIÉNES SE PROTEGEN LAS EMPRESAS?

Según Russell, la seguridad en Informática tiene su nacimiento con la aparición de los ataques a la información por parte de intrusos interesados en el contenido de ésta. Los tipos de ataque en la seguridad de una computadora o una red de datos se pueden caracterizar por la inspección realizada sobre una computadora que funciona como proveedora de información. Los tipos de ataque se pueden categorizar de la siguiente manera

a) "Interrupción: La información del sistema es destruida o llega a ser inutilizable. Este es un ataque sobre la disponibilidad. En este ataque se puede incluir ejemplos de destrucción de hardware, como un disco duro o el corte de una línea de comunicación.
b) Intercepción: Una participación sin autorización por parte de una persona, computadora o programa en una comunicación. Éste es un ataque sobre la confidencialidad. Un ejemplo podría ser la copia ilegal de programas, números de cuenta o archivos.
c) Modificación: Una participación sin autorización, pero no sólo accediendo a la información sino que también alterándola. Este es un ataque sobre la integridad. Los ejemplos podrían ser los cambios de

valores en archivos y programas o la modificación de mensajes transmitidos en una red.

d) Fabricación: Introducción de objetos falsificados en un sistema sin autorización. Este es un ataque sobre la autenticidad. Un ejemplo sería la introducción de mensajes falsos en una red."[4]

Estas categorías de ataques se pueden resumir en dos tipos: ataques pasivos y activos.

Ataques Pasivos

Los ataques pasivos son simplemente observaciones de datos reservados durante una transmisión. La finalidad del intruso es la obtención de la información transmitida y se pueden clasificar en dos tipos de ataque: a) la observación del contenido del mensaje y b) el análisis de tráfico.

El primero sería el entendimiento por parte de un intruso del contenido de una transmisión que contiene información confidencial, como una conversación telefónica o correo electrónico.

El análisis de tráfico sería la observación por parte del intruso sobre la longitud del mensaje, la identificación de los usuarios y la frecuencia de transmisión, pero en ningún caso puede entender la información, pues va encriptada. Los ataques pasivos son difícilmente detectables porque no producen una alteración de la información, no obstante son posibles de prevenir.

[4] Russell Deborah. "Some Security History". Computer Security Basic. Oreilly & Assoc. Inc. 1993. p. 8-9

Ataques Activos

Los ataques activos incluyen alguna modificación del mensaje o la creación de mensajes falsos. Hay varios tipos de ataques[5]:

- Cambiar la identidad del emisor o receptor: ocurre cuando una entidad pretende hacerse pasar por otra, lo cual se conoce como usurpación.
- Manipulación de datos
- Repetición: capturar una información, guardarla un tiempo y volverla a enviar, produciendo un efecto de no autorización.
- Denegación de servicio: impedir una comunicación, una respuesta, causar un rechazo de usuarios.
- Enrutamiento incorrecto: atacan a los nodos dentro de la red, pues no están tan protegidos como los terminales.

1.4 SEGURIDAD LÓGICA

"En la situación actual de criminología, los delitos de "cuello blanco" han incluido la modalidad de los delitos hechos mediante la computadora o los sistemas de información de los cuales el 95% de los detectados han sido descubiertos por accidente y la gran mayoría no han sido divulgados para evitar dar ideas a personas mal intencionadas. Es así como la seguridad de la información no solo está en manos de quien la usa."[6]

Según un estudio reciente de la compañía Ernst &Young[7], firma internacional dedicada a la consultoría de negocios, el 25% de las empresas

---

[5] Matthews Don Q. Diseño de sistemas de información administrativa., Argentina., El Ateneo. 1997, p. 89

[6] Rodríguez Luis Ángel "La seguridad de la Información". Seguridad de la Información en Sistemas de Computo Ediciones Ventura. 1995. p. 34-38.

[7] Ernst &Young. Datos estadísticos. América Latina. 2003.

norteamericanas que operan con redes de trabajo sufrieron ataques a su información entre 1998 y 2000, provocando pérdidas económicas que ascienden a los US $250,000.

En la actualidad y principalmente con el uso de las computadoras personales, se ha dado otro fenómeno que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se diseña como paquetes que son copiados sin autorización y son capaces de borrar toda la información que se tenga almacenada en un equipo de cómputo. Se trata de pequeñas subrutinas escondidas en los programas, las cuales son activadas automáticamente en cuanto se cumple alguna condición.

"Un ejemplo es la destrucción de la información de la compañía USPA & IRA de Forth Worth, Texas, Estados Unidos; cuando despidieron a un programador en 1985, este dejó una subrutina que destruía mensualmente la información de ventas. Este incidente provocó el primer juicio en Estados Unidos contra una persona por sabotaje a través de un equipo de cómputo."[8]

El crecimiento de los fraudes por computadora se ha desarrollado de una manera importante, además de cada vez ser más costoso (se estima que en los Estados Unidos se han cometido crímenes por computadora por más de tres mil millones de dólares). Smith[9] considera que existen cuatro factores que han permitido el incremento en los crímenes por computadora:

---

[8] Información publicada en la pagina web del Instituto Nacional de Estadística e Informática de Perú http://www.iei.gob.pe. "Plan de Contingencias y seguridad de la información". Metodologías Informáticas 1997.

[9] N. Smith, Joe, Sistemas de control de acceso del Proyecto Salt River, en Phoenix, Arizona, Presidente del Comité Permanente para Seguridad de Empresas de Servicios Públicos, USA, 2002. p. 90

1. El aumento del número de personas que se encuentran estudiando computación.
2. El aumento del número de empleados que tienen acceso a los equipos principales.
3. La facilidad en el uso de los equipos de cómputo.
4. El incremento en la concentración del número de aplicaciones y, consecuentemente, de la información.

"El uso inadecuado de una computadora comienza desde su utilización para usos ajenos a la organización, copia de programas para fines de comercialización sin reportar los derechos de autor, hasta el acceso por vía telefónica a bases de datos con el fin de modificar la información con propósitos fraudulentos."[10]

El tipo de seguridad puede comenzar desde la simple clave de acceso (password o contraseña) hasta sistemas más complicados, aunque se debe evaluar que entre más complejos y completos sean los sistemas de seguridad, serán más costosos. Por lo tanto, se deberá mantener una adecuada relación de seguridad-costo en los sistemas de información.

Los sistemas de seguridad generalmente no contemplan la posibilidad de fraude cometido por los empleados de la propia empresa. La introducción de información confidencial a una sola computadora o equipo puede provocar que esté concentrada en las manos de unas cuantas personas y una alta dependencia en caso de pérdida de los registros.

"El más común de estos delitos está dado en el momento de programación, en el cual por medio de ciertos algoritmos se manda borrar un archivo. Por ejemplo, en un sistema de nómina al momento de programarlo se puede incluir

[10] Russell Deborah. Op Cit. p. 55-56

una rutina que verifique si dentro del archivo de empleados existe el registro federal de causantes del programador, en caso de existir, continúa el proceso normalmente, si no existe significa que el programador que elaboró ese sistema renunció o fue despedido y en ese momento borra todos los archivos indicados. Esta rutina, aunque es fácil de detectar, puede provocar muchos problemas en caso de que no se tengan los programas fuente o bien no se encuentre debidamente documentado."[11]

La seguridad de la información tiene dos aspectos principales:

El primero consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, el cual también se le puede llamar protección de la privacidad, si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.

Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a aquellas personas que ejerzan adecuadamente este privilegio, las cuales tienen la responsabilidad de proteger los datos que se les han confiado.

En general, la protección de los datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la seguridad se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la preservación del secreto. Éste se logra cuando no existe acceso a todos los datos sin autorización. La privacidad adecuada puede lograrse cuando los datos que puedan obtenerse no pueden enlazarse a individuos específicos o no pueden utilizarse para imputar hechos acerca de ellos.

---

[11] Fine Leonard. "Seguridad de la s Aplicaciones". Seguridad en Centros de Computo, políticas y procedimientos Editorial Trillas. 1990. p. 70-75

Por otro lado es importante incorporar dispositivos de seguridad durante el diseño del sistema en vez de desarrollarlas después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes, como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un sistema de información.

Los puntos básicos que cualquier esquema de seguridad lógica debe abarcar son:

- Sistemas de control de acceso a la información
- Procedimientos de respaldo
- Encripción o cifrado, autentificación y firmas digitales
- Correo electrónico seguro
- Políticas claras y firmes con el personal: clasificación de los puestos, procedimientos de contratación, procedimientos de terminación de contrato, procedimientos electrónicos, transferencia y entrenamiento del personal.

1.5 SEGURIDAD FÍSICA

Debido a que muchas veces las empresas no cuentan con una guía para establecer las medidas de seguridad del área donde se encuentra la información más importante es frecuente que esta área esté expuesta a diversos riesgos, como incendios, desastres naturales, ataque por intrusos, condiciones ambientales no satisfactorias, fallas de la corriente eléctrica, fallas en el sistema de aire acondicionado, robo de equipo e información, etc., por lo tanto debe contarse con medidas de seguridad para el establecimiento adecuado del área de sistemas. El objetivo es establecer políticas,

procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos o información

Los puntos básicos que un esquema de seguridad física debe contemplar son:[12]

- Control de acceso a las áreas
- Control del medio ambiente
- Seguridad en redes y comunicaciones
- Seguros para equipos
- Controles generales de la seguridad informática
- Planes de contingencia.

En cuanto al control de acceso a las áreas, así como el control del medio ambiente, son tópicos tratados tradicionalmente por el diseño de centros de cómputo o bien el diseño de las distintas áreas de la organización. Sin embargo recientemente algunas empresas de Software han anunciado soluciones que abarcan estos tópicos, compartiendo la información del personal de la organización, así como su ubicación física en las instalaciones, con los accesos autorizados definidos centralmente.

1.6 SEGURIDAD EN REDES Y COMUNICACIONES

En la actualidad, es muy común la necesidad de compartir recursos, utilizar el trabajo de otros y compartir esfuerzos. Sin embargo esto implica un mayor riesgo en cuanto a pérdida, destrucción de información, revelación de datos a personas no autorizadas, etc. Por lo tanto, es importante mantener un

[12] Fine Leonard. "Seguridad de la s Aplicaciones". Seguridad en Centros de Computo, políticas y procedimientos Editorial Trillas. 1990. p. 70-75

esquema eficiente de seguridad en redes y comunicaciones, el cual debería incluir[13]:

- Un sistema de disponibilidad para asegurar que los activos de la red están listos para ser usados por los usuarios autorizados
- Un sistema de control de acceso que permita que los datos restringidos sean usados únicamente por personas autorizadas
- Un sistema de integridad que protege contra modificación de datos, ya sea accidental o intencional.

En general, los objetivos de la seguridad en redes y comunicaciones son[14]:

1. Preservar la confidencialidad de los datos que pasan a través de cualquier canal de comunicación.
2. Asegurar que el mensaje permanezca inalterado durante su transmisión.
3. Asegurar que un usuario está conectado con la persona con quien cree que está.
4. Garantizar que solamente los usuarios autorizados tienen acceso a la red, esto se logra controlando el acceso a los componentes de la red y a los passwords.
5. Garantizar la disponibilidad de la información para los usuarios autorizados, cuando y desde donde lo requieran.

En el intento de proteger una red de computadoras, existen varias funciones comunes a las cuales deben dirigirse. Se identifican tres problemas básicos:

---

[13] Rodriguez Luis Ángel "La seguridad de la Información". Op Cit. P. 102-103
[14] Ibid p. 104

- EL anfitrión promiscuo
- La autorización de cliente y servidor
- Contabilidad de cliente y servidor

El anfitrión promiscuo.

El anfitrión promiscuo es el que se introduce sin permiso a el sistema o a la red de una empresa, es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red. Si un intruso es paciente, él puede simplemente mirar que los paquetes fluyen de aquí para allá a través de la red. No toma mucha programación el análisis de la información que fluye sobre la red.

Un ejemplo simplemente es un procedimiento de login remoto. En el procedimiento login, el sistema pedirá y recibirá el nombre y contraseña del usuario a través de la red. Durante la transmisión, esta información puede no estar codificada o encriptada de cualquier forma. Una persona paciente simplemente puede esperar, y así recolectar toda la información que necesita para romper cualquier cuenta.

Autenticación

El procedimiento de login remoto ilustra el problema de autenticidad. ¿Cómo una persona se identifica ante el anfitrión remoto para probar que es realmente quien dice ser?

¿Cómo puede realizarse esta identificación, de forma que no se repita por el mecanismo simple de una jornada registrada?

Contabilidad

Finalmente, se debe considerar el problema de contabilidad. Hay que recordar que se debe asumir que hay otros con un conocimiento mayor de sistemas ¿Cuánta contabilidad tiene que hacer el sistema para crear una pista de revisión y luego examinar?

1.7 SEGUROS PARA LOS EQUIPOS

Los seguros de los equipos en algunas ocasiones se dejan en segundo término aunque son de gran importancia. Se tiene poco conocimiento de los riesgos que envuelven a la computación, ya que muchas veces el riesgo no es claro para los vendedores de seguros, debido a lo nuevo de la herramienta y la poca experiencia existente sobre desastres. Adicionalmente, se deben verificar las fechas de vencimiento de las pólizas, pues puede suceder que se tenga la póliza adecuada pero vencida.

El seguro debe cubrir todo el equipo y su instalación, por lo que es probable que una sola póliza no pueda cubrir todo el equipo con las diferentes características, por lo que tal vez convenga tener dos o más pólizas por separado, cada una con las especificaciones necesarias.

El costo de los equipos puede variar, principalmente en aquellos países que tienen grandes tasas de inflación o de devaluación, por lo que las sumas aseguradas deben estar a precio de compra (valor de adquisición de nuevo equipo con iguales características) y no con precio del momento de contratación del seguro.

"El seguro debe cubrir tantos daños por factores externos (terremoto, inundación) como por factores internos (daños ocasionados por negligencia o

falta de pericia de los operadores, daños debidos al aire acondicionado, etc.)".[15]

1.8 CONTROLES GENERALES PARA LA SEGURIDAD INFORMÁTICA

Los controles son técnicas específicas, procedimientos y políticas que permiten que los objetivos de las empresas se lleguen a cumplir, sin importar si estos controles son financieros o de tecnología de la información. Enfocándose en el área de tecnología de la información, el hecho de desarrollar controles o mecanismos de control, permite que los sistemas sean acordes a los objetivos corporativos, los cuales son acordes con los financieros. Dentro del área de tecnología de la información, se puede considerar tres tipos de controles:

- "Preventivos, aseguran que las vulnerabilidades de seguridad no sean expuestas.
- De detección, identifican deficiencias en la seguridad que han sido descubiertos y que muy posiblemente, han sido utilizados en contra de la organización.
- Correctivos, corrigen las deficiencias en la seguridad que han sido descubiertos y que muy posiblemente, han sido utilizados en contra de la organización."

A continuación se presenta un cuadro sinóptico con los principales controles de seguridad en tecnología de la información, su descripción y sus objetivos[16].

[15] Fine Leonard. Seguridad de las Aplicaciones". Op cit. P. 37-40
[16] G. Jumes James. "IT Security Control Model". Microsoft Windows NT 4.0 Security.Audit and Control Microsoft Press. 1999. p. 6-7

Controles de seguridad	Descripción de los controles de seguridad	Objetivos
Habilidad para recuperar funcionalidad después de fallas en la operación	Los controles deben asegurar que la operación del negocio continúe si los sistemas fallan por ellos mismos o por desastres naturales o de otro tipo.	Disponibilidad
Asegurar los sistemas en general	Los controles deben asegurar que los accesos a los sistemas de computadoras, programas y datos están restringidos apropiadamente.	Confidencialidad
Asegurar el acceso físico a sistemas críticos	Los controles deben asegurar el acceso físico a las instalaciones de cómputo y que los datos estén restringidos apropiadamente	Confidencialidad e integridad
Administración efectiva de la seguridad	Los controles deben asegurar que el sistema de seguridad está siendo administrado y mantenido de manera correcta. Los controles implementados deben incluir el desarrollo de políticas y procedimientos de seguridad que ayuden a los empleados a darle la importancia necesaria a la seguridad.	Confidencialidad, integridad y disponibilidad
Monitoreo efectivo de la seguridad	Los controles deben monitorear la manera en que los sistemas manejan la seguridad.	Confidencialidad, integridad y disponibilidad

1.9 DELITOS INFORMÁTICOS MÁS USUALES

Robo de equipos y de Información

En los centros de cómputo se encuentran activos de gran valor monetario, que resultan susceptibles de ser sustraídos. Más grave aun puede resultar la sustracción de información, parte de la cual tiene carácter de confidencialidad.

A continuación analicemos algunos de los delitos más usuales, considerando que la lista puede ser mucho más extensa, y que seguimos añadiendo nuevas variantes de los delitos señalados.

Actos Destructivos Premeditados

Un ejemplo de actos destructivos premeditados son los actos terroristas de los cuales México ha estado prácticamente exento, pero no por eso se puede decir que sea inmune.

Piratería de Software

En años recientes, la piratería de software (el robo de copias de software comparado), se ha vuelto un nuevo riesgo de seguridad, esto se debe a la proliferación de las microcomputadoras personales, en ellas los programas que corren en una, corren fácilmente en otra.

Crimen por computadora

Es un término general para describir cualquier uso de sistemas computarizados y llevar cabo actos ilegales. Se piensa, y es correcto en parte, que los crímenes por computadora, (sabotaje y espionaje) son relativamente poco frecuentes. De la misma manera, probablemente la mayoría de los directores de las empresas tienden a pensar que "un desastre nunca me tocará a mí". Pero esta actitud ha probado muchas veces ser peligrosa. Desafortunadamente no podemos confiar en que todos sean honestos.

El problema parece estarse incrementando con el uso creciente de computadoras, ya que la aplicación de la tecnología está llevando rápidamente hacia una sociedad sin dinero en efectivo. Los sistemas de punto de venta, cajeros automáticos (ATM), sistemas de pago por teléfono y sistemas de trasferencia electrónica de fondos se están volviendo parte de la vida diaria, con la posibilidad de usarlos en forma indebida.

Sabotaje

"Los saboteadores no tratan de robar nada. En lugar de esto, tratan de invadir y dañar hardware, software, información o datos. Pueden ser "hackers" (aunque ellos no tratan de hacer daño, en ocasiones lo hacen por error), empleados con privilegios de acceso, o espías. Existen inclusive, algunas organizaciones con el objetivo expreso de dañar computadores. El año 2002 la Comisión Federal de Comercio de EE UU recibió 219,000 quejas y espera que aumente 10 veces para el 2005."[17]

Espionaje Industrial

En forma natural el espionaje tiene hoy a las computadoras como uno de sus objetivos principales. Los espías trataran de obtener información de medios de almacenamiento magnéticos en lugar de otras fuentes tradicionales. Es conocido que la información guardada en medios magnéticos es fácilmente identificada, ordenada y copiada, en ocasiones sin dejar rastro.

Tipos de Delitos Informáticos Conocidos por Naciones Unidas[18]

Delitos	Caracteristicas
Fraudes cometidos mediante manipulación de computadoras	
Manipulación de los datos de entrada	Este tipo de fraude informático conocido también como sustracción de datos, representa el delito Informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

[17] Revista Newsweek no. 48, vol 8, de diciembre de 2003, p40-45.
[18] www.onu.org/delitosinformaticos Cita obtenida en enero del año 2004.

La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de computo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones Informáticas	
Como Objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada
Como instrumentos	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados	
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legitima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco pare que transfiera continuamente dinero a una cuenta ilícita.
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.
Acceso no autorizado a Sistemas o Servicios	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático.
Piratas informáticos o Hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El

	delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
Reproducción no autorizada de programas informáticos de protección Legal.	Esta puede entrañar una perdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el trafico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

1.10 PRINCIPALES VULNERABILIDADES EN EL ÁREA DE SISTEMAS

Se ha presentado una serie de contingencias relacionadas con los sistemas. Para desarrollar medidas efectivas de seguridad contra estos riesgos, es necesario entender bien sus causas. Aunque cada desastre implica una situación particular, es posible identificar condiciones que incrementan la vulnerabilidad a cada tipo de contingencia, o a varios tipos de estas (ver Tabla)

TABLA

Condiciones que Incrementan la Vulnerabilidad a Desastres

	CONTINGENCIA	CONDICIONES QUE INCREMENTAN LA VULNERABILIDAD

Desastres no intencionales	Error del operador	Dificultad para prever como funcionarán los sistemas y como se adaptaran los sistemas y como se adaptarán a ellos los usuarios. Complacencia al suponer que el sistema operará como se espera Falta de trabajo y cuidado para asegurar que los sistemas funcionen correctamente
	Falla de hardware	No creer que el hardware puede fallar Dificultad para decir si la falla esta en el hardware o en el sistema
	Errores de software	Diseño y pruebas inadecuadas Factores no esperados que afectan la operación del sistema
	Errores en los datos	Fallas en los procedimientos Falta de capacidad en el software para detectar muchos tipos de errores. Falta de cuidado Respaldos no adecuados Seguridad física contra fenómenos naturales no adecuada. Protección no adecuada contra fallas en los sistemas de apoyo a la computadora
	Daño a las instalaciones y medios de almacenamiento	Mal diseño Demanda de trabajo no prevista Diseño no adecuado del sistema de computo

Desastres intencionales	Desempeño no adecuado de los sistemas	Existencia de muchos objetivos fáciles para el robo Sistemas distribuidos
	Robo	Prevención no adecuada de accesos no autorizados (a sistemas e instalaciones)
	Vandalismo y sabotaje	Procedimientos no adecuados de seguridad en toda la empresa

En forma general, la información computarizada es particularmente vulnerable porque:

- Está más concentrada. Una computadora, o algunas veces una base de datos o grupos de archivos, puede almacenar o contener información de muchos departamentos, los cuales fueron compilados anteriormente de kardex individuales en diversas áreas.
- Es más accesible. En el pasado solamente unos pocos empleados tenían acceso a sus archivos. Hoy en día, miles de empleados usan computadoras y, a menos que se hayan tomado medidas apropiadas de seguridad, la información confidencial puede ser fácilmente accedida.
- Está sujeta a daños no detectables o uso indebido. No es posible ver físicamente los daños almacenados en una computadora, así, los cambios y eliminaciones no deseados son menos obvios. Un solo error puede dañar o eliminar un archivo, y un comando puede borrar todos los archivos contenidos en un disco duro.

1.11 PLANES DE CONTINGENCIA

Es posible que en cualquier organización existan instalaciones y aplicaciones consideradas de alto riesgo, causando severos trastornos a la funcionalidad general de la organización o de la comunidad en caso de que el servicio se interrumpa cierto periodo de tiempo; o que pueden fácilmente continuar sin afectar grandemente a la organización gracias a la utilización de medios alternos.

Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo/beneficio entre el costo por perdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

- Clasificar la instalación en términos de riesgo: alto, mediano y bajo.
- Identificar aquellas aplicaciones que tengan un alto riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo
- Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera
- Justificación del costo de implantar las medidas de seguridad

Una vez que se ha definido el grado de riesgo, hay que elaborar una lista de los sistemas con las medidas preventivas que se deben tomar, así como las correctivas en caso de desastre señalándole a cada uno su prioridad.

En caso de desastres, se recomienda trabajar los sistemas de acuerdo a sus prioridades, ya que no se podrán trabajar los sistemas en otra instalación, en la misma forma en la que se venían trabajando en la instalación original.[19]

El plan de contingencia es uno de los subtemas que están comprendidos dentro de seguridad de la información. Cada uno de los puntos es independiente de los demás, ya que puede existir sin importar si existen los demás. Sin embargo, para maximizar la seguridad de la información, es necesario que se trabaje de manera integral en todos los aspectos. Por ejemplo, no serviría de mucho tener una perfecta clasificación de la información y no tener nada de seguridad física. Así, para que el plan de contingencia pueda ser mejor y de los mejores resultados, debe existir conjuntamente con planes de seguridad física, lógica, aseguramiento, etc.

Inclusive, es necesario que el coordinador de recuperación de desastres se involucre en algunas de las áreas de seguridad de la información, por ejemplo en el control de acceso físico al centro de procesamiento de datos. Un gran número de desastres son el resultado de daño intencional o acceso indebido, y pueden reducir significativamente el riesgo de desastres provocados por el hombre. En general, es importante que el equipo, o al menos quien elabora el plan de contingencia, entienda bien de los sistemas de seguridad instalados, y que sepa que es lo que está siendo salvaguardado por las medidas de seguridad, y así determine si esto debe permanecer diariamente en la instalación o si estaría mejor guardado fuera del *site*.

Puede ser necesario que el encargado de la seguridad sea miembro de los equipos de recuperación, ya que es importante que cuando se reacondicione o reconstruya el centro de cómputo, se reinstalen los controles de seguridad al mismo tiempo. Los anteriores construyen de ejemplos de la relación entre

[19] Fine Leonard."Planes y Simulacros para la recuperación en caso de desastres". P. 92-100.

seguridad de información y plan de contingencia, al cual se le considera como el principal elementos requerido para alcanzar el objetivo de la continuidad del negocio.

En suma, incrementar la seguridad significa incrementar las posibilidades de salvaguardar los activos de una compañía, reduciendo el riesgo de pérdida financiera. En un momento dado se podría probar que puede resultar mucho más caro no invertir en todas las medidas en si mismas. De hecho invertir en seguridad de la información debería considerarse una forma de aseguramiento. Por otro lado, obviamente, estas medidas nunca pueden ser por si mismas garantía contra daños y accidentes. Estas medidas deben estar en armonía con todo el perfil y el medio ambiente de la empresa, Aun así, un cierto grado de riesgo tendrá que ser aceptado, y desde luego no hay que ver cualquier pequeña irregularidad como un gran problema, todo debe dimensionarse adecuadamente con respecto a la organización.

Beneficios de un plan de contingencia para la seguridad

Las ventajas de crear y contar con un plan de contingencia abarcan lo tangible e intangible así:

- Reducción de los costos por perjuicios si ocurre un siniestro.
- Las primas de seguro de bajo costo.
- Mayor comunicación y mejores relaciones entre los departamentos.
- Una mayor conciencia entre el personal de seguridad sobre la importancia de la seguridad y el valor de la propiedad que se está protegiendo.

Etapas clave en la elaboración de planes de contingencia

Las partes involucradas en el desarrollo de un plan de contingencia deben saber escuchar y comunicarse. Aunque existen algunas etapas importantes de

desarrollo, mantener un buen plan significa repetir continuamente estas etapas, volver a evaluar el plan y revisarlo.

1. **Determinación del objetivo:** El punto de partida para el desarrollo de un plan de contingencia es determinar un objetivo claro. El departamento de Tecnología Informática (TI) y los funcionarios de nivel ejecutivo deben identificar el objetivo operativo en caso de una emergencia en materia de seguridad. Por ejemplo, determinar si el objetivo es proteger cierta información y bienes, es mantener operaciones comerciales o brindar un excelente servicio al cliente. El objetivo ayudará al departamento de TI a definir un plan estratégico de acción y determinar los recursos que se deben proteger primero.

2. **Realización de un inventario completo:** Se deben identificar las principales herramientas de TI, los recursos y las tareas prioritarias para realizar negocios y atender las funciones críticas establecidas en el objetivo de la elaboración de planes de contingencia. El inventario debe incluir recursos auxiliares como suministros de energía y recursos de respaldo.

3. **Análisis de riesgos:** Evalúe los perjuicios financieros, técnicos jurídicos y operativos totales que pudieran ocurrir como resultado de una brecha del sistema de seguridad. El riesgo abarcaría perjuicios potenciales a los clientes y compañías. También analice amenazas a la seguridad y los perjuicios que potencialmente podrían ocasionar a varios departamentos y operaciones. El software de administración de riesgos a la seguridad puede ayudar al personal de TI a evaluar el impacto de las amenazas a la seguridad de la compañía.

4. **Desarrollo de un plan de acción:** Repase los escenarios detallados de "qué pasaría si..." que implican diferentes amenazas a la seguridad y los efectos posibles en las operaciones. Para cada escenario potencial de

disminución de riesgos, tenga en cuenta a las personas involucradas, sus responsabilidades, las consideraciones presupuestales, etc.

5. **Prevea un "Plan B":** Aunque los mejores planes de contingencia en el momento de su ejecución encuentran problemas técnicos, trate de anticiparse a estos problemas y crear soluciones alternas.

6. **Planeación de las comunicaciones y compras:** Los mejores planes son efectivos solo si los empleados tienen en cuenta su importancia y entienden sus mensajes y procesos. Los departamentos de recursos humanos, de aspectos jurídicos y finanzas deben revisar y responder a los planes de contingencia de seguridad en cada etapa de desarrollo.

CAPÍTULO 2
METODOLOGÍA PARA LA EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

CAPÍTULO 2

METODOLOGÍA PARA LA EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada rama que la integra, desde su diseño de ingeniería hasta el desarrollo de software, y por supuesto la auditoria informática.

Una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno solo, por lo que resulta habitual el uso de metodologías de empresas auditoras profesionales, desarrolladas por los expertos para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

"La proliferación de metodologías en el mundo de la auditoría y el control informativos surgen en la década de los ochenta, paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas, como el software de análisis de riesgos. Pero el uso de métodos de auditoría es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas cuyo uso de metodologías constituye una práctica común. Una de ellas es la seguridad informática."[20]

El nivel de seguridad informática en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la información de la entidad y sus

[20] Rodríguez Luis Ángel. Seguridad de la información en sistemas de cómputo. Ediciones Ventura, México 1995. p. 35

medios de proceso. Cuando se evalúa el nivel de seguridad de sistemas en una empresa se están evaluando los siguientes factores: normatividad de la empresa, organización, metodologías, objetivos de control, procedimientos de control, tecnología de seguridad y herramientas de control, para después plantar un plan de seguridad nuevo que mejore todos los factores, aunque conforme se vayan realizando los distintos proyectos del plan no irán mejorando todos por igual. Al finalizar el plan, se habrá conseguido una situación nueva en la que el nivel de control sea superior al anterior[21].

En el mundo de la seguridad informática se utilizan todas las metodologías necesarias para realizar un plan de seguridad además de las de auditoría informática. Las dos metodologías de evaluación de sistemas por antonomasia son las de análisis de riesgos y las de auditoria informática. La auditoría informática sólo identifica el nivel de exposición por la falta de controles, mientras que el análisis de riesgo facilita la evaluación de los riesgos y recomienda acciones en base al costo-beneficio de las mismas[22].

2.1 TIPOS DE METODOLOGÍAS

"Todas las metodologías existentes desarrolladas y utilizadas en la auditoría y el control informáticos, se pueden agrupar en dos grandes familias: cuantitativas y cualitativas".[23]

Metodologías Cuantitativas

[21] González Zubieta José María. "Metodologías de control interno, seguridad y auditoría informática". Auditoría Informática: Un Enfoque Practico. Alfaomega grupo Editor. 1998. p. 45-48
[22] Hernández Enrique. "La auditoría informativa y su entorno". Auditoria en Informática: Un Enfoque Metodológico. CECSA. 1999. p. 21-22
[23] González Zubieta José María. Op. Cit. P. 51-52

Diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados valores numéricos. Estos valores, en el caso de metodologías de análisis de riesgos, son datos de probabilidad de ocurrencia (riesgo) de un evento que se debe extraer de un registro de incidencia donde el número de incidencias tienda al infinito o sea suficientemente grande. Sin embargo, esto no pasa en la práctica, y se aproxima ese valor de forma subjetiva restando así rigor científico al cálculo. Pero dado que el cálculo se hace para ayudar a elegir el método entre varias contramedidas se podría aceptar, y al mismo tiempo, por los cálculos obtenidos, permite identificar los puntos más vulnerables.

Se indican dos inconvenientes que presentan este tipo de metodologías; por una parte la debilidad de los datos de la probabilidad de ocurrencia por los pocos registros y la poca significación de los mismos a nivel mundial, y por otro la imposibilidad o dificultad de evaluar económicamente todos los impactos que pueden acaecer frente a la ventaja de poder usar un modelo matemático para el análisis.

Metodologías Cualitativas.

Precisan de la involucración de un profesional experimentado, pero requieren menos recursos humanos y tiempo que las metodologías cuantitativas.

La tendencia de uso en la realidad es una mezcla de ambos. A continuación se muestra un cuadro comparativo entre ambos tipo de metodologías[24].

[24] González Zubieta José María. Op. Cit. P. 52

	Cuantitativa	Cualitativa
Pros	Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnerabilidades muy distintas Proporciona una cifra justificante para cada contramedida.	Enfoque lo amplio que se desee. Plan de trabajo flexible y reactivo Se concentra en la identificación de eventos. Incluye factores intangibles
Contras	Estimación de probabilidad depende de estadísticas fiables inexistente. Estimación de perdidas potenciales solo si son valores cuantificables. Metodologías estándares. Difícil de mantener o modificar Dependencia de un profesional	Depende en gran medida de la habilidad y calidad del personal involucrado. Puede excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list). Identificación de eventos reales más claros al no tener que aplicar probabilidades complejas de calcular. Dependencia de un profesional.

2.2 TIPOS DE RIESGOS

Entre otros, los tipos de riesgo que deben considerarse en cualquier metodología de análisis de riesgo son riesgos externos e internos.

Riesgos Externos

Son todos aquellos que se presentan en el ambiente físico y social que rodea a una instalación de procesamiento de información. Si bien no es posible eliminarlos, si es factible tomar las medidas necesarias que minimicen la probabilidad de pérdida de información o destrucción de las instalaciones. Pueden ser naturales u ocasionados por el hombre.

En los ocasionados por desastres naturales se consideran, entre otros: inundaciones, temblores, tornados, tormentas eléctricas, huracanes, erupciones volcánicas, etc.

En los propiciados por el hombre se encuentran: incendios, explosiones, accidentes laborales, bombas, destrucción intencional, sabotaje, robos, fraude, contaminación ambiental, etc.

Riesgos internos

Se generan dentro de la misma empresa. Por su origen, son más sencillos de prever. Sin embargo y aun cuando parezca contradictorio, será más fácil que se presenten, ya que el conocimiento de los procedimientos internos de operación hará más sencillo el camino de alguna persona interesada en dañar a la empresa. Por ejemplo: robo de material, de recursos o de información, sabotaje, destrucción de datos o recursos, huelgas, fraudes, etc.

Una vez determinados los riesgos, es importante que se realice una evaluación del presupuesto asignado para reducirlos. Se deben considerar los siguientes puntos[25]:

a) Objetivo, ¿qué se busca con un plan de reducción de riesgos?
b) Alcance y recursos, determinar la magnitud de las necesidades de la empresa y los recursos de la organización para satisfacerlas
c) Planeación profunda, el plan debe considerar todas las posibilidades y evaluar hasta el más mínimo riesgo existente.
d) Organización del proyecto, es necesario contar con un responsable de los trabajos realizados, que tenga pleno cocimiento de lo que se ha hecho
e) Esfuerzo conjunto.

[25] Rodríguez, Luis Ángel "La seguridad de la Información". Op. Cit. P. 148-150

2.3 METODOLOGÍA DE ANÁLISIS DE RIESGOS

El objetivo general del análisis de riesgos es cuantificar los riesgos a que están sujetos los activos de una empresa, la pérdida esperada y el costo de tomar medidas de control.

Los objetivos específicos del análisis de riesgo son:

1. *Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas.* El tiempo y los recursos necesarios para atacar los problemas dependerán del tipo de riesgo considerado. Se debe tomar en cuenta que muchas veces se incrementa la pérdida por la interrupción de labores o bien que puede existir una pérdida de oportunidades para la empresa en caso de que la restricción tome mucho tiempo. Los recursos actuales disponibles ayudaran a contrarrestar los gastos y deben considerarse dentro del análisis.

2. *Determinar cuales son los activos existentes.* Al determinar los activos existentes es recomendable realizar un inventario detallado. Además se deben evaluar los costos de las pérdidas potenciales y cuantificar los costos de reposición y reparación. Se pueden señalar tres áreas de riego básicas instalaciones de proceso de información, información y comunicaciones.

3. *Llevar a cabo un minucioso análisis de riesgos y debilidades.* Identificar las fuentes, alcances, métodos y amenazas potenciales. Estimar la probabilidad de ocurrencia. También se deben identificar las debilidades potenciales y todos los tipos de amenazas y vulnerabilidades.

4. *Identificar, definir y revisar todos los controles de seguridad ya existentes.* Se deben identificar las defensas existentes, así como los recursos del sistema.

5. *Determinar si es necesario incrementar las medidas de seguridad, los costos de riesgo y los beneficios esperados.* El análisis de riesgos deberá definir cuáles son las medidas a implantar y las ventajas y desventajas de cada decisión[26].

Para determinar la probabilidad de que ocurra un evento que dañe las instalaciones se recurre a diversas técnicas. El objetivo del análisis de riesgos, bajo este criterio, se divide en dos:

- Reducir la probabilidad de que ocurra un evento
- Proporcionar los elementos de seguridad y protección adecuados para que, en el caso de que ocurra un desastre, los costos en que se incurra no sean tan altos.

El autor Luis Ángel Rodríguez, propone que el esquema básico de una metodología de análisis de riesgos es en esencia el siguiente:

Etapa 1 Cuestionario

Etapa 2 Identificar los riesgos

Etapa 3 Calcular el impacto

Etapa 4 Identificar las contramedidas y el costo

Etapa 5 Simulaciones

Etapa 6 Creación de los informes

[26] Rodríguez, Luis Ángel "La seguridad de la Información". Op. Cit. P. 150-151

Con base a cuestionarios se identifican vulnerabilidades y riesgos y se evalúa el impacto para más tarde identificar las contramedidas y el costo. La siguiente etapa es la más importante, pues mediante un juego de simulación (el cual puede representarse con la condición "¿Qué pasa si?") se analiza el efecto de las distintas contramedidas en la disminución de los riesgos, eligiendo de esta manera un plan de seguridad que compondrá el informe final de la evaluación[27].

Un análisis de riesgos debe prepararse de forma personalizada para cada área u organización, ya que es muy difícil establecer un estándar de evaluación de seguridad debido las diversas maneras en que se utiliza la información y la manera que se procesa. Según el articulo del The Journal of Information Systems Audit And Control Association, se identifican dos tipos de metodologías para análisis de riesgos: análisis de riesgo basado en misiones y análisis de riesgos orientado a amenazas.

El primer método supone un conjunto predefinido de capacidades en el adversario para determinar si puede explotar los posibles fallos en la seguridad del sistema. En los métodos orientados a amenazas el análisis sólo se puede llevar a cabo cuando el sistema se encuentra bien definido, las capacidades en el adversario para determinar si puede explotar los posibles fallos en la seguridad del sistema. En los métodos orientados a amenazas el análisis únicamente se puede llevar a cabo cuando el sistema se encuentra bien definido.

Este tipo de método es útil cuando, por ejemplo, se desea saber los riesgos que existen con un determinado sistema informático. Un punto débil de este método es que solo se puede demostrar la inseguridad de un sistema, mas no

[27] González Zubieta, José María. Op. Cit. P. 53

la seguridad; por lo que existe desconocimiento sobre operaciones no identificadas adicionales. Por otra parte, los métodos orientados a misión intentan identificar todos los peligros que amenazan a corto plazo dicha misión, entendiéndose como misión los objetivos de la organización. Éstos se utilizan para definir los requisitos básicos de seguridad de los sistemas. Este análisis consta de cuatro elementos:

- **Análisis de fallos en la seguridad.**

Estudiar las computadoras, su software, su localización y utilización con el objeto de identificar los huecos en la seguridad que pudieran poner un peligro para la misión. Por ejemplo, si se instala una PC para recibir informes de inventario vía modem desde otras PCs situadas en lugares remotos, se ha abierto una vía de acceso al sistema, por lo tanto habría que tomar medidas de seguridad para protegerlo, como puede ser la validación de claves de acceso.

- **Análisis de peligros.**

Estudiar la capacidad de los adversarios potenciales para determinar si podrían o no causar o producir fallos en la seguridad.

- **Reducción de riesgos.**

Si el análisis de las debilidades del sistema y de la capacidad de los adversarios revela riesgos que se juzgan innecesarios, se hace necesaria una reducción de riesgos. Se habrán de considerar más medidas de respuesta, con una evaluación de la relación costo-efectividad, cuanto mayores sean las perdidas posibles por un fallo en la seguridad, mayor es la justificación de una reducción de riesgos.

- **Evaluación de la seguridad.**

Debido a que la seguridad absoluta es un objetivo inalcanzable, un conjunto concreto de medidas de seguridad se ha de probar hasta que muestra sus puntos débiles. La evaluación de seguridad del sistema con las protecciones en activo constituye una parte importante del proceso de análisis de riesgos, en el cual se exploran las posibilidades de pérdida, las consecuencias de ésta y las probabilidades de que ocurra[28].

A continuación se abordaran algunos métodos de análisis de riesgos.

2.3.1 MÉTODO MARION

Método documentado en dos libros de los cuales el más actual es "La securite des reseaux-Mathods et Techniques" de JM Lamere y Leroux J. Tourly. Tiene dos productos: MARION AP+ para sistemas individuales y MARION RSX para sistemas distribuidos y conectividad. Es un método cuantitativo y se basa en la encuesta anual de miembros del C.L.U.S.I.F. (base de incidentes francesa). No contempla probabilidades, sino esperanzas matemáticas que son aproximaciones numéricas.

MARION AP+ utiliza cuestionarios y parámetros correlacionados enfocados a la presentación gráfica de las distintas contramedidas en cada uno de los factores (27 factores en seis categorías). Las categorías son: seguridad informática general, factores socioeconómicos, concientización sobre la seguridad informática general, concientización sobre la seguridad de software y materiales, seguridad en explotación y seguridad de desarrollo.
El análisis de riesgo lo hace sobre diez áreas problemáticas a través de cuestionarios. Estas áreas son[29]:

---

[28] Show, Davis. Risk Analysis: Methods and Processes. The Journal of information system Audit and Control association. EUA. 1998; Volumen III: p. 35-38.
[29] Rodríguez, Luis Ángel. Op. Cit. P. 156

1. Riesgos materiales
2. Sabotajes físicos
3. Averías
4. Comunicaciones
5. Errores de desarrollo
6. Errores de explotación
7. Fraude
8. Robo de información
9. Robo de software y,
10. Problemas de personal

2.3.2 METODOLOGÍA BS 7799

"BS 7799 es una metodología británica reconocida mundialmente, tiene como principal objetivo la administración de seguridad de la información. Está respaldado por el BSI (British Standard Institute). Desarrollado en demanda del sector público, comercial e industrial para ejercer un marco de trabajo común, cuya finalidad es que las compañías desarrollen, implementen y apliquen medidas efectivas de seguridad, además de proporcionar confidencialidad en la transferencia de información entre compañías. Está basado, de acuerdo al BSI, en las mejores prácticas actuales de seguridad de la información en Inglaterra y en empresas internacionales".[30]

Dada su gran utilización y adopción como código de práctica en varios países europeos, en 1999 se propuso que esta metodología se reconociera como un estándar internacional para seguridad de la información por la ISO (Internacional Organization for Standarization). Finalmente en octubre de 2000

[30] Información publicada en la pagina web del Instituto Nacional de Estadística e Informática de Perú http://www.iei.gob.pe. "Plan de Contingencias y seguridad de la información". Metodologías Informáticas 1997.

fue aprobada como estándar de ISO y actualmente se conoce como ISO 1799[31].

La Metodología está conformada por dos partes:

Primera parte. Código de práctica para sistemas de Administración de Seguridad de la información, contiene más de 100 controles de seguridad divididos en diez secciones, los cuales se adaptan a las necesidades específicas que empresas de diversos sectores pudieran presentar.

1. Políticas de seguridad
2. Organización y control de activos
3. Clasificación y control de activos
4. Seguridad del personal
5. Seguridad física y ambiental
6. Administración de redes y equipo de cómputo.
7. Control de acceso a sistemas.
8. Desarrollo y mantenimiento de sistemas.
9. Planeación para la continuidad del negocio
10. Cumplimiento

Segunda parte. Indica los requerimientos para establecer, implementar y documentar medidas de seguridad de la información. Consta de cuatro fases:

[31] Show, Davis. Risk Analysis: Methods and Processes. The Journal of information system Audit and Control association. EUA. 1998; Volumen III: p. 23-25

evaluación de riesgos, manejo de riesgos, implementación de los dispositivos de seguridad y enunciado de aplicabilidad.

- **Evaluación de riesgos:** es el análisis de lo que puede sucederle la información y el impacto que incide, y que puede tener en los objetivos de la compañía.
- **Manejo de riesgos:** es el plan que la empresa puede utilizar para reducir los riesgos. Los métodos utilizados en el manejo de riesgos no solo comprenden dispositivos de seguridad, como firewalls, sino también seguridad física, procedimientos administrativos, planes de contingencia e iniciativas de los recursos humanos.
- **Dispositivos de seguridad:** son las herramientas actuales y recursos identificados y adoptados por la empresa para minimizar los riesgos.
- **Enunciado de aplicabilidad:** es un plan de seguridad que se requiere para la acreditación BS7799. Este instructivo comprende los controles de seguridad que la empresa ha adoptado y las razones por las cuales se tomaron esas medidas. Además la empresa debe listar los controles que no se han adoptado y de igual forma, indicar la razón[32].

2.3.3 OTRAS METODOLOGÍAS

PRIMA (Prevención de Riesgos Informáticos con Metodología Abierta)

Es un compendio de metodologías españolas con un enfoque subjetivo, desarrolladas a principios de los años 1990. Sus características esenciales son[33]:

---

[32] Russell Deborah. Op Cit. p. 58-60

[33] Ibid p. 60

- Cubrir las necesidades de los profesionales que desarrollan cada uno de los proyectos necesarios de un plan de seguridad
- Fácilmente adaptable a cualquier tipo de herramienta
- Posee cuestionarios de preguntas para la identificación de debilidades o falta de controles.
- Posee listas de ayuda para los usuarios menos experimentados debilidades, riesgos y recomendaciones.
- Permite fácilmente la generación de informes finales
- Las listas de ayuda en los cuestionarios son abiertas y por lo tanto es posible introducir información nueva o cambiar la existente.
- Es cualitativa y con capacidad de aprendizaje al poseer una base de conocimiento o registro de incidentes.

BDSS: Bayesian Decisión Support System, Sistema Bayesiano de Soporte a Decisiones.

Soporta la evaluación de riesgos cuantitativos en un entorno de proceso de datos. Se ejecuta en cualquier PC y soporta todas las tareas de una evaluación de riesgos cuantitativa detallada y completa.

Está diseñado para responder las siguientes preguntas que de acuerdo a sus creadores, engloban un amplio análisis de riesgos:

1. ¿Qué puede ir mal?
2. ¿Con qué frecuencia puede ocurrir?
3. ¿Cuáles serían sus consecuencias?
4. ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

Par responder la primer pregunta, el BDSS desarrolla un modelo de riegos lógico sobre el entorno de procesamiento de la información, basándose en las

respuestas que se den a una serie de preguntas que hace. Una potente lógica interna controla el proceso de obtener la información, de forma que las preguntas que el sistema hace se encuentran determinadas en gran medida por las respuestas a las preguntas anteriores. De esta forma BDSS desarrolla un modelo de riesgos adaptados al entorno de procesamiento de información de la organización cliente.

Para responder a la segunda pregunta, BDSS calcula las distribuciones de probabilidad para varios escenarios de riesgo. Esto se hace integrando información y utilizando complejos algoritmos matemáticos y lógicos.

Para responder a la tercer pregunta, BDSS tiene en cuenta tanto recursos tangibles como intangibles, yendo de las computadoras al impacto en la misión o negocio. Se guía al usuario a través de un proceso que identifica y evalúa el valor de los recursos, además del impacto inmediato y posterior de su pérdida.

La respuesta a la cuarta pregunta, la obtiene BDSS mediante la integración bayesiana de la falta de certeza dentro del análisis del modelo de riesgo lógico. Este retrato realistico de la falta de certeza según valores calculados, constituye el atributo central del análisis de riesgos BDSS.

El sistema BDSS continúa proponiendo protección basadas en su análisis de modelo de riesgos. Se es libre de seleccionar las protecciones que se deseen, y en ese caso el programa calculará la reducción de riesgo atribuible a esa selección. Se representan gráficamente los resultados, mostrando los niveles de riesgo antes y después de aplicar las protecciones. Esto se hace mediante curvas de riesgo, en la que se muestra el rango verdadero de la exposición de pérdida y el rango de probabilidades saciado. Tras revisar estas gráficas, se selecciona la combinación más efectiva de protecciones. Finalmente, BDSS

lleva a cabo, basándose en los parámetros que se le ofrecen, el análisis costo-beneficio de las protecciones que ha identificado como más efectivas[34].

2.4 LA PROTECCIÓN DE LA INFORMACIÓN

"Un estudio realizado por Computing e Information Week muestra que un 59 por ciento de las compañías encuestadas califican a la seguridad como prioridad alta. Sin embargo, las organizaciones se están enfrentando a una media de 14 incidentes, cada año, y adicionalmente casi la mitad no tiene conciencia de cuándo sus redes están sufriendo un ataque electrónico. De esta forma, un 43 por ciento de los encuestados afirma que la mayor barrera para disponer de una seguridad efectiva pasa por la creciente sofisticación de las amenazas y ataques, aunque casi un 25 por ciento de las compañías analizadas no han revisado o medido el verdadero alcance de su política de seguridad en los últimos doce meses."[35]

"Igualmente, los ataques más comunes proceden de explotar vulnerabilidades en sistemas operativos como Microsoft Windows, de forma que cuatro de cada diez incidentes se basan en este método. Blaster, Slammer o Sobig han sido los virus más comunes recientemente, debido a la propagación por medio del correo electrónico."[36]

Como dato relevante, un 42 por ciento de los usuarios de equipos en las empresas no conocen la política de seguridad de su organización. La educación debe así convertirse en vía importante para combatir las amenazas.

---

[34] Información publicada en la pagina web del Instituto Nacional de Estadística e Informática de Perú http://www.iei.gob.pe. "Plan de Contingencias y seguridad de la información". Metodologías Informáticas 2000.

[35] Informe Global Information Security 2003, realizado por Computing, Information Week p. 24

[36] www.microsoft.com/espanol/seguridad. Cita obtenida en enero del año 2004.

Tres de cada cinco entidades consultadas consideran que mejorar estos avisos constituye una prioridad para el próximo año.

Paralelamente, los organismos gubernamentales y asociaciones que luchan contra los delitos informáticos insisten en que los ataques deben hacerse públicos por parte de las empresas. No obstante, más de la cuarta parte de los entrevistados no ha informado de los incidentes sufridos en el apartado de seguridad.

CAPÍTULO 3

PAUTAS Y RECOMENDACIONES PARA ELABORAR POLÍTICAS DE SEGURIDAD INFORMÁTICA

CAPÍTULO 3

PAUTAS Y RECOMENDACIONES PARA ELABORAR POLÍTICAS DE SEGURIDAD INFORMÁTICA

La seguridad informática ha tomado gran auge debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo la aparición de nuevas amenazas para los sistemas de información.

"Estos riesgos que se enfrentan ha llevado a que se desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa."[37]

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva, sin comprometer la información de la organización. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico entorno que rodea las organizaciones modernas.

---

[37] Rodríguez Luis Ángel, Seguridad de la información en sistemas de cómputo, Ediciones Ventura, México 1995. p. 127

3.1 ¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA?

Las políticas de seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

"Una política de seguridad informática (PSI) es aquella que fija los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Si bien existen algunos modelos o estructuras tipo, tiene que diseñarse *a la medida* para así recoger las características propias de cada organización ."[38]

Una buena política de seguridad corporativa debe establecer, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos. Esta visión general resulta vital para asegurar un nivel homogéneo en el grado de seguridad que quiera alcanzarse, y evitar la aparición de "agujeros negros" en determinados puntos del sistema. En definitiva, de nada sirve un excelente cortafuegos si no se encuentra instalado un buen antivirus, o tener un avanzado software de detección de intrusos si se carece de una adecuada política de contraseñas para los usuarios.

Las áreas que contemple la política de seguridad variarán en función de cada empresa y sistema. Como mínimo deberán abordar apartados tales como: [39]

---

[38] Bohlander, George y Sherman, Arthur. Administración de la Información. México. Ediciones Thomson. 1999. p. 39

[39] Matthews, Don Q. Diseño de sistemas de información administrativa., Argentina., El Ateneo. 1997, P. 76

- Evaluación de riesgos
- Protección perimétrica
- Control de acceso a los recursos
- Directrices de uso de Internet
- Correo electrónico
- Antivirus y
- Copias de seguridad

Otra característica importante que no debe olvidarse en las políticas de seguridad es su mantenimiento y revisión periódica. En la práctica, el crecimiento y la modificación de los sistemas de la empresa, así como la continua aparición de nuevas vulnerabilidades y amenazas, exigen que la política de seguridad corporativa sea un elemento vivo que se vaya adaptando a las necesidades que surgen cotidianamente.

"Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal en relación con los recursos y servicios informáticos importantes de la organización. No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de lo que deseamos proteger y el por qué de ello."[40]

[40] Cobb Stephen, Manual de seguridad para PC y redes locales, MacGrawHill, España, 1994. p. 89

Cada PSI es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

Objetivos de las políticas de seguridad:

El objetivo principal de las PSI es informar al mayor nivel de detalle a los usuarios, empleados y directivos de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

Los Componentes principales de una política de seguridad:

- Una política de privacidad
- Una política de acceso
- Una política de autenticación
- Una política de contabilidad
- Una política de mantenimiento para la red
- Una política de divulgación de información

3.2 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

Una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere una disposición de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos[41]:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.

"Las PSI deben ofrecer explicaciones comprensibles sobre porque deben tomarse ciertas decisiones, transmitir por qué son importantes éstos u otros recursos o servicios. De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa."[42]

---

[41] Matthews, Don Q. Diseño de sistemas de información administrativa., Argentina., El Ateneo. 1997, p. 89

[42] Vázquez Torres, Norma Angélica. Seguridad en los sistemas informáticos en las empresas, Editorial Trillas, México, 1993. p. 183

Por otro lado, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y las actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud que pasará cuando algo suceda; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

3.3 PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD

Si bien las características de la PSI que se han mencionado muestran una perspectiva de las implicaciones en la formulación de estas directrices, se propone revisar algunos aspectos generales recomendados para la formulación de las mismas:

- Es necesario que se efectúe un ejercicio de análisis de riesgos informático a través del cual se valoren los activos, el cual permitirá afinar las PSI de la organización.
- El involucrar a las áreas propietarias de los recursos o servicios es prioritario, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- El comunicar a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad, ayudará a que funcione todo de manera correcta.

- Recordar que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Se debe de desarrollar un proceso de monitoreo periódico de las directrices, que permita una actualización oportuna de las mismas
- Un punto importante: no hay que dar por hecho algo que es obvio. Las PSI deben ser explícitas y concretas, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

¿Cómo establecer una política de seguridad?

- **Identificar y evaluar los activos:** ¿Qué activos deben protegerse y cómo protegerlos de forma que permitan la prosperidad de la empresa?
- **Identificar las amenazas:** ¿Cuáles son las causas de los potenciales problemas de seguridad? Considere la posibilidad de violaciones a la seguridad y el impacto que tendrían si ocurrieran.

Estas amenazas pueden ser externas o internas:

"Las amenazas externas: Se originan fuera de la organización y son los virus, gusanos, caballos de Troya, intentos de ataques de los hackers, retaliaciones de ex-empleados o espionaje industrial.

Las amenazas internas: Son las amenazas que provienen del interior de la empresa y que pueden ser muy costosas porque el infractor tiene mayor acceso y perspicacia para saber donde reside la información sensible e importante. Las amenazas internas también incluyen el uso indebido del acceso a Internet por parte de los empleados, así como los problemas que

podrían ocasionar los empleados al enviar y revisar el material ofensivo a través del Web."[43]

Evaluar los riesgos: Éste puede ser uno de los componentes más desafiantes del desarrollo de una política de seguridad. Debe calcularse la probabilidad de que ocurran ciertos sucesos y determinar cuáles tienen el potencial para causar mucho daño. El costo puede ser más que monetario - se debe asignar un valor a la pérdida de datos, la privacidad, responsabilidad legal, atención pública indeseada, la pérdida de clientes o de la confianza de los inversionistas y los costos asociados con las soluciones para las violaciones a la seguridad.

Asignar las responsabilidades: Será necesario seleccionar un equipo de desarrollo que ayude a identificar las amenazas potenciales en todas las áreas de la empresa. Es ideal la participación de un representante por cada departamento de la compañía. Los principales integrantes del equipo serían el administrador de redes, un asesor jurídico, un ejecutivo superior y un representante del departamento de Recursos Humanos.

Establecer políticas de seguridad: El definir una política que apunte a los documentos asociados; parámetros y procedimientos, normas, así como los contratos de empleados, será una tarea fundamental. Estos documentos deben tener información específica relacionada con las plataformas informáticas, las plataformas tecnológicas, las responsabilidades del usuario y la estructura organizacional. De esta forma, si se hacen cambios futuros, es más fácil cambiar los documentos subyacentes que la política en sí misma.

Implementar una política en toda la organización: La política que se escoja debe establecer claramente las responsabilidades en cuanto a la seguridad y reconocer quién es el propietario de los sistemas y datos específicos. También puede requerir que todos los empleados firmen la declaración; si la firman,

[43] Klander, Lars. A prueba de Hackers, Editorial Anaya, España, 1998. p. 56

debe comunicarse claramente. Éstas son las tres partes esenciales de cumplimiento que debe incluir la política: [58]

- **"Cumplimiento:** Es necesario indicar un procedimiento y los indicadores para garantizar el cumplimiento y las consecuencias potenciales por incumplimiento.

- **Funcionarios de seguridad:** El ubicar a las personas que sean directamente responsables de la seguridad de la información. Asegúrese de que no es la misma persona que supervisa, implementa o revisa la seguridad para que no haya conflicto de intereses.

- **Financiación:** hay que cerciorarse de que a cada departamento se le haya asignado los fondos necesarios para poder cumplir adecuadamente con la política de seguridad de la compañía."[45]

Administrar el programa de seguridad: Es necesario establecer procedimientos internos para implementar los requerimientos y hacer obligatorio su cumplimiento.

Consideraciones importantes

En el proceso de elaboración de una política de seguridad, es importante asegurarse de que la política tenga las siguientes características:

- Se pueda implementar y hacer cumplir
- Sea concisa y fácil de entender
- Compense la protección con la productividad

---

[44] Klander, Lars, A prueba de Hackers, Editorial Anaya, España, 1998. p. 67

[45] Ibidem. p. 67

Una vez que la política se aprueba totalmente debe hacerse asequible a todos los empleados porque, en última instancia, ellos son responsables de su éxito. Las políticas deben actualizarse anualmente (o mejor aún cada seis meses) para reflejar los cambios en la organización o cultura.

Se debe mencionar que no puede haber dos políticas de seguridad iguales puesto que cada empresa es diferente y los detalles de la política dependen de las necesidades exclusivas de cada una. Sin embargo, es posible comenzar con un sistema general de políticas de seguridad y luego personalizarlo de acuerdo con sus requerimientos específicos, limitaciones de financiación e infraestructura existente.

Una política completa de seguridad de la información es un recurso valioso que amerita la dedicación de tiempo y esfuerzo. La política que se adopte debe brindar una base sólida para respaldar el plan general de seguridad. Y una base sólida sirve para respaldar una organización sólida.

3.4 RAZONES QUE IMPIDEN LA APLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Según Camilo García Cabeza: "resulta una labor ardua el convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática. Muchos de los inconvenientes se inician por los tecnicismos informáticos y la falta de una estrategia de mercadeo de los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: *más dinero para los juguetes de los ingenieros.*"[46]

---

[46] García Cabeza Camilo, Félix José Pascual, Miguel. Julián Chaparro Pelaéz. "Sistemas de información y comunicaciones para la gestión del conocimiento". Universidad Politécnica de Madrid. España 2001. p. 87

Esta situación ha llevado a que muchas empresas con activos muy importantes se encuentren expuestas a graves problemas de seguridad, que en muchos de los casos lleva a comprometer su información sensitiva y por ende su imagen corporativa.

Ante esta situación los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular la gente debe saber las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una buena intrusión o una travesura puede convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos.

Luego, para que las PSI logren abrirse espacio al interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía. De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas.

En este contexto, el entender la organización, sus elementos culturales y comportamientos deben llevar a reconocer las pautas de seguridad necesarias y suficientes que aseguren confiabilidad en las operaciones y funcionalidad de la compañía.

A continuación algunas recomendaciones para "vender" las preocupaciones sobre la seguridad informática[47]:

- "Desarrollar ejemplos organizacionales relacionados con fallas de seguridad que capten la atención de sus interlocutores.
- Asociar el punto anterior a las estrategias de negocio y la imagen de la empresa en el desarrollo de sus actividades.
- Articular las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información.
- Mostrar una valoración costo-beneficio, ante una falla de seguridad.
- Desarrollar las justificaciones de la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización
- Se debe de ser oportuno para presentar el producto, procurando tener la mayor información del negocio y los riesgos asociados con los activos críticos de la organización."

3.5 LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA COMO BASE DE LA ADMINISTRACIÓN DE LA SEGURIDAD INTEGRAL

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos.

---

[47] Bohlander, George y Sherman, Arthur. Administración de la Información. México. Ediciones Thomson. 1999. p. 90

"Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general."[48]

Las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

3.6 ¿CÓMO CONTROLAR LOS DESAFÍOS ACTUALES A LA SEGURIDAD?

Históricamente las empresas que desean mejorar su sistema de seguridad han tenido que afrontar la ardua tarea de comprar, administrar y mantener las múltiples aplicaciones y dispositivos de seguridad que provienen de muchos fabricantes. Una falta de recursos de TI podría hacerlo incontrolable y el alto costo total de propiedad podría hacer que la seguridad total fuera prohibitiva. El resultado ha sido que muchas empresas e incluso oficinas sucursales de las grandes compañías no han instalado sistemas de seguridad más sofisticados que los básicos, como el antivirus y firewall.

Algunas percepciones comunes que obstaculizan la seguridad total

[48] www.symantec.com/seguridadinformatica.htm Cita obtenida en enero del año 2004.

Ningún fabricante de seguridad ofrece todas las soluciones de seguridad necesarias

Muchos profesionales de TI creen que varios componentes de protección total (firewall, antivirus, detección de intrusos, etc.) se deben obtener de diferentes fabricantes porque creen que ningún fabricante ofrece cubrimiento total de seguridad. Además, el proceso de identificación y adquisición de los productos adecuados requiere tiempo, dinero y experiencia en seguridad de la información que por lo general existen solamente en las grandes organizaciones. Estas percepciones han hecho que muchas empresas no tengan un perímetro seguro.

La administración de todos los componentes por separado requiere más tiempo y por tanto dinero.

"Otro obstáculo para la seguridad total ha sido la percepción de que una vez ésta ha sido identificada y adquirida, cada componente debe instalarse, configurarse y administrarse por separado. Esto requerirá disponer de sistemas operativos múltiples y hardware exclusivo, así como podría generar deficiencias en la protección que harán a la empresa vulnerables a los ataques. Y una vez esté instalado el sistema, el administrador se enfrentaría a entradas (logs) y registros múltiples para llegar a comprender la situación de seguridad. Para muchas empresas, esto significa más tiempo y dinero del que tienen que gastar."[49]

Las amenazas complejas requieren protección total

Tan rápidamente como el mundo empresarial se ha conectado a Internet, así también ha aumentado la manera en que diferentes amenazas a la seguridad pueden atacar las redes, inutilizar las operaciones y comprometer la integridad

[49] http://www.symantec.com/region/mx/enterprisesecurity/content/expert/LAM_1155.html Nota obtenida el 20 febrero año 2004.

de las empresas. La naturaleza y complejidad de las amenazas están cambiando constantemente y está claro que el enfoque según el cual para cada amenaza hay una cura, ya no es suficiente. Por otra parte, las limitaciones a los recursos de TI y al presupuesto también pueden ser una carga para las iniciativas de seguridad.

Es posible que su empresa haya implementado las tecnologías firewall y antivirus. Si comienza a agregar nuevas tecnologías de seguridad, como detección de intrusos, control de vulnerabilidades y tecnologías de filtrado de contenidos, su empresa puede terminar con una serie de productos poco flexibles de diferentes fabricantes, que son difíciles de instalar y de administrar por separado. Además, hay poca confianza en que funcionarán conjuntamente para proteger su red.

A medida que cambian las amenazas, también deben cambiar sus iniciativas de seguridad

Los ataques actuales a Internet son diferentes de lo que eran tan solo hace un par de años. Además de los virus, gusanos y hackers, existe una nueva categoría de amenazas poderosas y sofisticadas que se conocen como "amenazas combinadas". A diferencia de los gusanos o virus anteriores, las amenazas combinadas puede propagarse a través de diferentes caminos, con frecuencia al descubrir rápidamente vulnerabilidades y aprovecharlas. Y pueden dispararse automáticamente sin asistencia humana.

Lo importante es que así como las amenazas actuales tienen más artimañas, la seguridad debe ser más inteligente. Entonces, ¿cómo proteger su red y cómo administrar la protección del gateway de Internet cuando lo atacan?

La solución al problema

Puesto que los virus, gusanos y hackers, así como la nueva generación de amenazas combinadas son un riesgo constante para las puertas traseras y para los gateways desprotegidos, las empresas deben volver a revisar su estrategia de seguridad actual. Éste no es el momento para jugar a la ruleta con la seguridad de su empresa. Pensar en implementar medidas de seguridad que "no son lo suficientemente buenas" o decidir "esperar hasta que algo suceda en realidad" pueden traer consecuencias devastadoras para su empresa. Proteger todos los gateways y vulnerabilidades podría parecer ser una tarea de grandes proporciones para aquellas empresas que tienen muchas sucursales para proteger con un soporte de TI insuficiente.

CAPÍTULO 4

PROPUESTA DE UNA METODOLOGÍA DE FORMULACIÓN DE POLÍTICAS EN SEGURIDAD INFORMÁTICA

CAPÍTULO 4

PROPUESTA DE UNA METODOLOGÍA DE FORMULACIÓN DE POLÍTICAS EN SEGURIDAD INFORMÁTICA

Es importante anotar que la política de seguridad de la información de una organización es un simple documento que articula la filosofía, los requerimientos reglamentarios y las creencias que la organización tiene en relación con la protección a los recursos de la información. Esta política explica con documentos el enfoque del entorno, del personal y de los procesos en donde la aplica, así como las consecuencias de su incumplimiento. La Política de Seguridad de la Información es parte de un conjunto de políticas que generalmente cumplen las organizaciones. Otras políticas solucionan áreas críticas como los recursos humanos, las instalaciones y las finanzas. Estas políticas deben ser complementadas y respaldadas con la Política de Seguridad de la Información.

Características principales de una Política de Seguridad de la Información:[50]

- "Debe estar escrita en lenguaje simple, pero jurídicamente viable
- Debe basarse en las razones que tiene la empresa para proteger la información
- Debe ser consistente con las demás políticas organizacionales
- Debe hacerse cumplir. Se exige y mide el cumplimiento

[50] Manual de seguridad en sistemas de información, SISCO México, 2002, p. 56

- Debe tener en cuenta los aportes hechos por las personas afectadas por la política
- Debe definir el papel y responsabilidades de las personas, departamentos y organizaciones para los que aplica la política
- No debe violar las políticas locales, estatales o federales
- Debe definir las consecuencias en caso de incumplimiento de la política
- Debe estar respaldada por documentos "palpables", como los estándares y procedimientos para la seguridad de la información, que se adapten a los cambios en las operaciones de las empresas, las necesidades, los requerimientos jurídicos y los cambios tecnológicos."

Redactar una política para la seguridad de la información puede ser sencillo comparado con su implementación y viabilidad. La política organizacional y las presiones por lo general aseguran que habrá dificultad y consumo de tiempo para crear y adoptar una Política de Seguridad de la Información, a menos que un autentico líder dirija el programa de políticas. Esta persona generalmente es una persona influyente, un facilitador y sobretodo una persona que sepa escuchar y convencer, para que pueda articular y aclarar las inquietudes y temores de las personas respecto a la introducción de una nueva política.

La creación de una Política de Seguridad de la Información es responsabilidad de la empresa y requiere mucha interacción humana para garantizar que el resultado final satisface las necesidades de la empresa y es aceptada como parte normal de las operaciones de la compañía por parte de las personas para quienes aplica la política. Lo más importante es que la introducción de una política efectiva de seguridad de la información debe contar con el respaldo y más alto compromiso de la gerencia ejecutiva de la organización.

METODOLOGÍA DE POLÍTICAS EN SEGURIDAD INFORMÁTICA

OBJETIVO

La función de este documento es la selección de los controles necesarios para poder asegurar un nivel aceptable en la seguridad de la información dentro de las áreas de una organización.

Según la metodología BS7799 es necesario:

- Analizar las amenazas
- Analizar las vulnerabilidades
- Analizar los riesgos
- Determinar controles aplicables y
- Proponer un enunciado de aplicabilidad (Política)

Para efectos prácticos, lo anterior se determina a través de:

a) ***Describir la actividad*** que se va a llevar a cabo para ubicar la situación de la organización, esto con la finalidad de detectar la situación particular que guarda el área o el proceso.

b) Ubicar ***el hallazgo*** o la anomalía que ejemplifica el estado en que se encuentra la organización o el área referente a ese tema.

c) Por último ***las recomendaciones*** que se sugieren seguir en cada desviación o anomalía, para efecto de apegarse a las políticas que salvaguarden la información de la empresa o institución.

Se sugiere la metodología BS7799, ya que tiene diversas cualidades para efecto de mantener los sistemas vigilados y seguros, enumeraremos sus propiedades:

- Es la que tiene mayor demanda en instituciones públicas y empresas privadas principalmente en Europa, por estar respaldadas en el Instituto Británico de Estandarización el cual avala las mejores prácticas de seguridad de la información en Inglaterra.

- Dado su gran uso en las organizaciones y tomando en cuenta sus códigos de compatibilidad con la Organización Internacional de Estandarización (ISO) ha sido tomado como base para mejorar las prácticas en seguridad informática de las empresas que tienen sus diferentes tipos de certificaciones.

A continuación se muestra el ejemplo de un manual en el que se incluyen diversas políticas de seguridad. Se encuentra dividido en dos partes y a su vez la primera en diez apartados, que son los que propone la Metodología BS7799, mencionada con anterioridad:

Primera parte. Código de práctica para sistemas de Administración de Seguridad de la información, contiene diversos controles de seguridad divididos en diez secciones, los cuales se adaptan a las necesidades especificas que empresas de diversos sectores.

1. Políticas de seguridad
2. Organización y control de activos
3. Clasificación y control de activos
4. Seguridad del personal
5. Seguridad física y ambiental
6. Administración de redes y equipo de cómputo.
7. Control de acceso a sistemas.
8. Desarrollo y mantenimiento de sistemas.
9. Planeación para la continuidad del negocio
10. Cumplimiento

Segunda parte. Indica los requerimientos para establecer, implementar y documentar medidas de seguridad de la información. Consta de cuatro fases: evaluación de riesgos, manejo de riesgos, implementación de los dispositivos de seguridad y enunciado de aplicabilidad.

- **Evaluación de riesgos:** es el análisis de lo que puede sucederle la información y el impacto que incide, y que puede tener en los objetivos de la compañía.
- **Manejo de riesgos:** es el plan que la empresa puede utilizar para reducir los riesgos. Los métodos utilizados en el manejo de riesgos no solo comprenden dispositivos de seguridad, como firewalls, sino también seguridad física, procedimientos administrativos, planes de contingencia e iniciativas de los recursos humanos.

- **Dispositivos de seguridad:** son las herramientas actuales y recursos identificados y adoptados por la empresa para minimizar los riesgos.
- **Enunciado de aplicabilidad:** es un plan de seguridad que se requiere para la acreditación BS7799. Este instructivo comprende los controles de seguridad que la empresa ha adoptado y las razones por las cuales se tomaron esas medidas. Además la empresa debe listar los controles que no se han adoptado y de igual forma, indicar la razón[51].

[51] Russell Deborah. Op Cit. p. 58-60

4.1 POLÍTICAS DE SEGURIDAD

Objetivo: Proporcionar dirección y soporte de la administración para la seguridad de la información.

Documento – Política de seguridad de la información

Descripción: Un documento de política deberá ser aprobado por el área correspondiente y según sea apropiado, publicado y comunicado a todos los empleados.

Hallazgo: La política de la empresa se publica en la intranet para que sea consultada por todos los empleados.

Recomendaciones: A cada empleado entregarle una copia en papel del documento de políticas de la empresa y que firmen un documento en el que se indique que la han recibido y leído.

Revisión y Evaluación

Descripción: La política se deberá revisar con regularidad y en el caso de que se realicen cambios, se deberá verificar que siga siendo apropiada.

Hallazgo: No se han realizado actualizaciones a todas las políticas desde hace dos años.

Recomendaciones: Establecer un calendario de revisión para cada rubro que conforma el documento de políticas de la empresa.

4.2 ORGANIZACIÓN DE SEGURIDAD

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

Administración de seguridad de la información

Descripción: Se deberá establecer un comité de administración para asegurarse de que haya una dirección clara y un soporte de administración visible para que las iniciativas de seguridad sean puestas en marcha.

Hallazgo: Actualmente no se cuenta con un comité para la verificación de la seguridad en las áreas de trabajo, así como en las operaciones diarias del negocio.

Recomendaciones: El área encargada de generar y revisar el documento de políticas de la organización deberá organizar un comité con personal de todas las áreas de la empresa.

Coordinación de seguridad de la información

Descripción: En donde sea apropiado para el tamaño de la organización, se deberá utilizar un comité funcional de representantes administrativos que forman parte importante de la organización, con el fin de coordinar la implantación de controles para seguridad de la información.

Hallazgo: Actualmente no se cuenta con un comité de este tipo

Recomendaciones: El área encargada de generar y revisar el documento de políticas de la organización deberá organizar un foro con personal de todas las áreas de la empresa.

Asignaciones de responsabilidades de seguridad de la información

Descripción: Se deberán definir claramente las responsabilidades para la protección de activos individuales y para llevar a cabo los procesos de seguridad específicos.

Hallazgo: No se cuenta con una definición de las responsabilidades de cada empleado del área en cuanto a seguridad de la información.

Recomendaciones: En la descripción de puestos se deben incluir las responsabilidades de seguridad de la información.

Identificación de riesgos en acceso de terceros

Descripción: Deberán evaluarse los riesgos asociados con el acceso a los inmuebles de procesamiento de la información en la organización por terceros.

Hallazgo: Con frecuencia accede personal externo al área, sin embargo no se cuenta con controles estrictos de acceso.

Recomendaciones: Establecer como política que personal externo se registre en al entrada y salida al área de estudio, y siempre se identifique con su gafete de empleado, en caso de serlo, o con el gafete de visitante.

Requerimientos de seguridad en el contrato de terceros

Descripción: Las disposiciones que implican el acceso de terceros a la empresa, deberán estar basados en un contrato formal que contenga todos los requerimientos necesarios para la seguridad.

Hallazgo: En el contrato que se firma con terceros, no se especifican restricciones ni responsabilidades en cuanto a seguridad de la información se refiere.

Recomendaciones: Agregar cláusulas de restricciones y responsabilidades en cuanto a seguridad de la información, al contrato con terceros.

Requerimientos de seguridad en el contrato de terceros

Descripción: Los requerimientos de seguridad de una organización que provee la administración y control de todos o alguno de sus sistemas de la información, redes y/o ambiente de oficina, deberán estar citados en un contrato acordado entre las partes.

Hallazgo: En el área de estudio se cuenta con este tipo de servicio sin embargo no se tienen especificados en un contrato los requerimientos de seguridad con los que deberá cumplir la empresa que esta ofreciendo el outsourcing.

Recomendaciones: Establecer en los contratos de servicio de outosourcing, los requerimientos de seguridad con los que deberá cumplir la empresa y su personalidad durante el ofrecimiento del servicio.

4.3 CLASIFICACIÓN Y CONTROL DE ACTIVOS

Inventario de activos

Descripción: Deberá crearse y mantenerse un inventario de todos los activos importantes.

Hallazgo: No se cuenta específicamente con un inventario de todos los activos, solamente se cuenta con inventarios de equipo de computo y de bienes inmuebles.

Recomendaciones: Complementar los formatos de los Inventarios con los que cuenta el área, Además de implementar un inventario de libros y/o manuales que se tienen en el área. El activo deberá tener adherido de manera visible una etiqueta que indique el número de Inventario asignado. También se sugiere un formato de resguardo, en el que se responsabiliza al empleado por el equipo de cómputo, y mueblería asignado. De acuerdo a la clasificación de activos elaborada para este análisis de riesgo, asignarle el nivel de protección apropiado.

Clasificación de la información

Descripción: Las clasificaciones y controles de protección asociados para la información deben adaptarse a las necesidades del área con el fin de compartir o restringir información y los impactos del negocio asociados con dichas necesidades.

Hallazgo: La información del área no se tiene clasificada de acuerdo a sensibilidad.

Recomendaciones: Mantener actualizada la clasificación de activos.

Etiquetado y manejo de información

Descripción: Se deberá definir un conjunto de procedimientos para etiquetar y manejar la información de acuerdo con el esquema de clasificación adoptado.

Hallazgo: La información del área no se tiene etiquetada de acuerdo a sensibilidad.

Recomendaciones: De acuerdo la clasificación de la información del área registrada en el inventario de activos, esperar la información y restringirla de acuerdo al nivel asignado.

4.4 SEGURIDAD DEL PERSONAL.

Seguridad en la definición de puestos y recursos

Descripción: La forma den que los puestos y responsabilidades de seguridad están incluidos en la política de seguridad de la información de la empresa se deberá documentar en las definiciones del empleo según sea apropiado.

Hallazgo: La descripción de puestos y responsabilidades se hace saber al empleado de manera verbal.

Recomendaciones: Documentar la descripción de puestos incluyendo las responsabilidades para seguridad de la información.

Verificación de la información del personal y políticas

Descripción: Las revisiones de verificación sobre personal permanente deberán llevarse a cabo en el momento que se solicite el empleo

Hallazgo: Actualmente no se realiza ninguna verificación a los antecedentes laborales proporcionados por el empleado

Recomendaciones: Verificar telefónicamente los datos, de al menos el trabajo anterior que el empleado proporcionó.

Acuerdos de confidencialidad

Descripción: Los empelados deberán firmar un contrato de confidencialidad como parte de sus términos y condiciones iniciales de contratación.

Hallazgo: Actualmente no se firma ningún acuerdo de confidencialidad ni se hace referencia la misma en el contrato laboral

Recomendaciones: Incluir en el contrato laboral, cláusulas correspondientes a confidencialidad.

Términos y condiciones de contratación

Descripción: Los términos y condiciones de contratación deben establecer la responsabilidad del empleado en cuanto a la seguridad de la información.

Hallazgo: En el contrato laboral actual no se establecen responsabilidades del empleado sobre seguridad de la información.

Recomendaciones: Incluir en el contrato laboral las responsabilidades del empleado sobre seguridad de la información.

Entrenamiento del usuario

Descripción: Asegurarse de que los usuarios están conscientes de las amenazas y riesgos sobre seguridad de la información y que están equipados para apoyar la política de seguridad de la empresa en el curso de su trabajo. Todos los empleados de la empresa y terceros usuarios, cuando es relevante, deben recibir el entrenamiento y actualización regular apropiados en las políticas y procedimientos de la organización.

Hallazgo: Hasta el momento, no se les ha dado a los empleados de la empresa ningún tipo de entrenamiento sobre las políticas de la empresa o sobre las actualizaciones que se hagan sobre las mismas. Los procedimientos se van dando a conocer a los empleados conforme a sus labores por lo que no conocen todos los procedimientos de la empresa. Actualmente las políticas se publican en la Intranet de la empresa pero no es obligatorio para los empelados que las consulten o lean.

Recomendaciones: Elaborar un plan de entrenamiento para informar a los empelados sobre las políticas y procedimientos de la empresa, además de entregar a cada uno, una copia en papel, del documento de políticas de la empresa, además de que firmen un documento donde se den por enterados de las mismas. Adicionalmente, seguir publicando las políticas en la Intranet pero notificando a los empelados sobre modificaciones las cuales deberán ser entregadas también en papel.

4.5. SEGURIDAD FÍSICA Y AMBIENTAL

Perímetro de seguridad física

Descripción: Las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen inmuebles de procesamiento de información.

Hallazgo: El área de estudio se encuentra dentro del edificio principal de la empresa y no cuenta con medidas exclusivas de seguridad física.

Recomendaciones: Asignación de medidas exclusivas de seguridad física para el área de estudio.

Controles de entrada física

Descripción: Las áreas seguras deberán estar protegidas por controles de entrada apropiados para asegurar que únicamente se permita el acceso al personal autorizado.

Hallazgo: Actualmente se cuenta con algunos controles de entrada tales como personal de vigilancia quienes solicitan registro de entrada y salida de los visitantes y revisan que los empleados porten su gafete en un lugar visible.

Recomendaciones: Instalación de equipo de rayos X para revisión a paquetes que traigan consigo los visitantes y empleados. Asignar gafetes de colores a los visitantes de acuerdo al área a la que vayan. El visitante deberá ser recogido en la recepción y acompañado por personal del área a su destino, de igual forma a su salida deberá ser acompañado a la recepción.

Definición de áreas seguras.

Descripción: Deberán crearse áreas seguras con el fin de proteger oficinas, cuartos e inmuebles con requerimientos especiales de seguridad.

Hallazgo: El área de estudio se considera vulnerable por la información que maneja, sin embargo no cuenta con ningún tipo de protección adicional.

Recomendaciones: Aquellas áreas consideradas sensitivas deberán protegerse con medidas de seguridad adicionales a las que se implanten en toda la empresa.

Trabajo en áreas seguras

Descripción: Los controles y estándares adicionales para trabajar en áreas seguras deberán usarse para mejorar la seguridad provista por los controles físicos que protegen las áreas seguras.

Hallazgo: En el área de estudio no se cuenta con controles físicos.

Recomendaciones: Deberán aplicarse al área de estudio los controles de entrada física.

Localización y protección del equipo

Descripción: El equipo deberá localizarse o protegerse para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades de acceso no autorizado.

Hallazgo: El servidor que se utiliza en el área de estudio, se encuentra en la oficina del gerente al cual no cuenta con la temperatura adecuada. El área de estudio cuenta con aire acondicionado pero actualmente existen dos de cuatro ventilaciones descompuestas por lo que generalmente la temperatura es alta.

Recomendaciones: Ubicar el servidor en un site con las condiciones adecuadas. Solicitar que se arreglen lo antes posible las ventilaciones para contar con temperatura adecuada.

Fuentes de energía

Descripción: El equipo deberá protegerse de fallas de energía y otras anomalías eléctricas.

Hallazgo: De los 10 equipos de cómputo que se encuentran en el área, 7 están conectados a un no-break

Recomendaciones: Solicitar equipos no-break para todos los equipos de cómputo del área.

Seguridad en el cableado

Descripción: El cableado eléctrico y de telecomunicaciones que portan datos o servicios de información de soporte deberán protegerse de interceptación o daño.

Hallazgo: El cableado eléctrico que se encuentra en canaletas ubicadas en el piso falso y aparentemente se encuentra en buenas condiciones; y de acuerdo a los reportes mostrados y al calendario de mantenimiento, este se lleva a cabo dos veces al año. Sin embargo, el cableado no está identificado con etiquetas, las conexiones eléctricas tampoco están señalizadas y por lo tanto cualquier dispositivo puede ser conectado en las conexiones para el equipo de computo o periféricos y provocar una baja de energía.

Recomendaciones: El área responsable de la instalación y mantenimiento del cableado deberá etiquetarlo, además de señalizar y distinguir las conexiones eléctricas para equipo de cómputo y periféricos de aquellas conexiones que se pueden utilizar para otras (cafetera, ventiladores, etc).

Mantenimiento del equipo

Descripción: El equipo deberá mantenerse de acuerdo con las instrucciones del fabricante y/o procedimientos documentados para asegurar su disponibilidad e integridad continua.

Hallazgo: No se tienen todos los manuales de instalación y mantenimiento de los equipos con los que cuenta el área tampoco se cuenta con un plan para mantenimiento preventivo a los equipos de computo o periféricos, en caso de falla se informa al área de soporte técnico de la empresa quienes son los encargados de darle servicio a estos equipos.

Recomendaciones: Registrar los manuales de instalación y mantenimiento para evitar pérdidas en caso de ser prestados a otras áreas. Investigar si otras áreas de la empresa pudieran tener los manuales de instalación y mantenimiento que hacen falta para obtener una copia. Acordar con el área de soporte técnico que se calendaricen mantenimientos frecuentes a los equipos de computo del área.

Seguridad del equipo

Descripción: Los procedimientos y controles de seguridad deberán usarse para asegurar el equipo que se usa afuera de las premisas de la organización.

Hallazgo: Ningún equipo de cómputo o periférico del área cuenta con póliza de seguro

Recomendaciones: Solicitar que se aseguren todos los equipos de computo o periféricos del área.

Retiro o re-uso seguro del equipo

Descripción: La información deberá borrarse del equipo antes de retirarlo o volverlo a usar.

Hallazgo: No es frecuente que se saque equipo del área, sin embargo cuando sucede, no se borra la información.

Recomendaciones: Establecer un procedimiento para borrar la información que pudiera contener el equipo de cómputo que por alguna razón tenga que ser utilizado fuera del área.

Escritorio limpio y la política de borrar la pantalla

Descripción: Las organizaciones tendrán e implantaran una política de escritorio limpio y de borrar la pantalla con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

Hallazgo: Actualmente el control de escritorio limpio no se aplica pero puede ser aplicable. En el esquema existente no se contempla como obligatoria la activación de protección de pantalla.

Recomendaciones: Establecer como política del área mantener la documentación sensitiva fuera del alcance de cualquier persona que transite por el área así como establecer contraseña en el protector de pantalla.

4.6 ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

Controles contra software malicioso

Descripción: Se deberá implantar controles de detección y prevención para la protección contra software malicioso así como procedimientos de concientización apropiados para el usuario.

Hallazgo: Actualmente se cuenta con un procedimiento informal para distribución e instalación de este tipo de software. No se ha capacitado al personal del área sobre los diferentes tipos de virus informativos y su propagación ni sobre los riesgos que implica no tener actualización el software antivirus

Recomendaciones: Establecer como política la actualización de software antivirus en cada equipo de cómputo del área así como capacitación al personal sobre los riesgos mencionados.

Software antivirus

Descripción: Se deberán implantar un software antivirus así como procedimientos de seguimiento apropiados para el usuario

Hallazgo: Actualmente se cuenta con un procedimiento informal para instalación y actualización de software antivirus el cual esta publicado en la intranet de la empresa, sin embargo no se notifica a los empleados sobre las nuevas versiones de antivirus disponibles.

Recomendaciones: Documentar el procedimiento y asignar a un responsable para mantener actualizado el software antivirus en cada equipo de computo del área, controlando esta situación a través del formato recomendado. Solicitar al área responsable de hacer las publicaciones en la intranet, que a

través de correo electrónico se le notifique al responsable del área de estudio, sobre las nuevas versiones disponibles de software antivirus.

Procedimientos para el manejo de incidentes

Descripción: Se deberán tener bien detallados los procedimientos necesarios para el manejo de incidentes de software malicioso

Hallazgo: Actualmente no se cuenta con un procedimiento para reportar incidentes de software malicioso.

Recomendaciones: Definir e implantar un procedimiento para el manejo de incidentes relacionados con software malicioso, deberá estar bien documentado y darlo a conocer a los empleados de la empresa para poder hacer referencia al mismo en caso de cualquier incidente.

Programas de difusión a usuarios

Descripción: se deberá implantar un programa de difusión de las herramientas utilizadas contra el software malicioso.

Hallazgo: Hasta el momento no se ha llevado a cabo una campaña de difusión entre los empelados de la empresa, sobre las herramientas autorizadas y utilizadas en al misma contra software malicioso.

Recomendaciones: Establecer calendarios de capacitación al personal sobre las herramientas utilizadas y autorizadas, su importancia y el buen manejo de este tipo de herramientas.

Información de respaldo

Descripción: Regularmente se deberán realizar copias de respaldo de la información esencial del negocio así como del software.

Hallazgo: Cada empleado tiene un espacio reservado en el servidor para almacenar la información que requiera guardar, si embargo no es obligatorio y tampoco se hace hincapié en que sea la información vital que maneja cada uno. Actualmente se realizan respaldos de la información almacenada en el servidor, pero no se tiene un calendario para realizarlos.

Recomendaciones: Documentar y dar a conocer una política de almacenamiento de información esencial del negocio en el servidor, elaborar un calendario para realizar los respaldos de esta información, que se recomienda sean realizados al menos dos veces por semana y elaborar un formato para administrar los respaldos obtenidos. Se recomienda utilizar como medios de almacenamiento DAT o CD dependiendo de la cantidad de información a respaldar.

Administración de medios de computación removibles

Descripción: Se deberá controlar la administración de medios removibles de computadoras, tales como cintas, discos y casetes.

Hallazgo: El personal del área tiene a su disposición diversos medios de almacenamiento como CD, DAT o disquetes, los cuales deben ser utilizados con fines laborales únicamente. No se cuenta con un registro de las entradas y salidas del área únicamente. No se cuenta con un registro de las entradas y salidas del área de dichos medios de almacenamiento.

Recomendaciones: Dado que para tener un control total de salidas de los medios de almacenamiento mencionados se tendría que asignar de tiempo completo un recurso por el gran movimiento que existe de los mismos dentro y fuera del área, se recomienda tener control solo sobre los respaldos realizados ya que la información se considera confidencial y sensible por lo que se sugiere utilizar para tal efecto el formato conveniente.

Procedimientos de manejo de la información

Descripción: Los procesos para el manejo y almacenamiento de la información deberán establecerse con el fin de proteger dicha información de la divulgación no autorizada o del mal uso de la misma.

Hallazgo: el personal encargado de la información es el responsable de su manejo, almacenamiento y resguardo y del número de copias que se generen

de la misma. Actualmente el control sobre el resguardo depende exclusivamente de los cajones con llave con los que cada empleado cuente.

Recomendaciones: Elaborar una política para manejo y almacenamiento de información en la que se indique, por ejemplo, que no debe estar a la vista información sensitiva. En caso de incumplimiento con esta política indicar también las sanciones.

Seguridad de documentación del sistema

Descripción: Deberá protegerse la documentación del sistema del acceso no autorizado.

Hallazgo: El personal encargado de la información es el responsable del manejo, almacenamiento y resguardo de la misma. Actualmente el control sobre el resguardo depende exclusivamente de los cajones con llave con los que cada empleado cuente.

Recomendaciones: Elaborar una política para manejo y almacenamiento de información en la que se indique, por ejemplo, que no debe estar a la vista información sensitiva. En caso de incumplimiento con esta política indicar también las sanciones.

Seguridad de correo electrónico

Descripción: Se deberá desarrollar una política para el usuario de correo electrónico y se deberán colocar controles apropiados para reducir los riesgos de seguridad creados por el correo electrónico.

Hallazgo: Actualmente el servicio de correo electrónico está encargado de otra área, este servicio es utilizado por todo el personal del área, y cada uno tiene usuario y clave personal, sin embargo la contraseña es igual al usuario y se le recomienda al empleado que la cambie en cuanto acceda a su correo por primera vez, sin embargo esto no se verifica posteriormente.

Recomendaciones: El área responsable deberá generar los usuarios con la característica de que sea obligatorio el cambio de contraseña la primera vez que se acceda a la cuenta.

Política de seguridad de correo electrónico

Descripción: Es importante considerar medidas de protección para el acceso de los buzones de correo por personal no autorizado.

Hallazgo: Generalmente, se evita que personas que no tienen cuenta de acceso utilicen cuentas de otras personas.

Recomendaciones: Establecer como política de seguridad que toda persona que no tenga buzón de correo asignado, no solicite utilizar el buzón de otra personan que e le sea proporcionado, en caso contrario se hará acreedor de la sanción indicada en la política.

Protección contra virus

Descripción: Contar con software antivirus

Hallazgo: Se cuenta con software antivirus, sin embargo en ocasiones no se actualiza con la debida oportunidad dado que dicha actualización la realiza cada empleado.

Recomendaciones: Documentar el procedimiento y asignar a un responsable para mantener actualizado el software antivirus en cada equipo de computo del área, controlando esta situación a través del formato conveniente.

Periodos de retención

Descripción: establecer periodos de retención de los mensajes, depurando aquellos que obtengan la información sensitiva tan pronto como sea posible.

Hallazgo: El área responsable de generar los buzones de correo para los empleados recomienda que en los equipos se creen carpetas personales a fin de que todos los mensajes sen transferidos en forma inmediata y

automática del servidor de correo electrónico al equipo del empleado, sin embargo casi ningún empleado cuenta con esta configuración.

Recomendaciones: Establecer como política de seguridad, la recomendación mencionada, indicando también la ruta en la que deben encontrarse dichas carpetas.

Autenticación de correo

Descripción: Se deben establecer mecanismos de seguridad para el correo electrónico

Hallazgo: No se cuenta con este tipo de mecanismos.

Recomendaciones: Un mecanismo para garantizar la autenticidad de la información en los mensajes de correo electrónico, es el uso de firmas digitales, con esto se puede asegurar que el origen de la información es valido, sin embargo puede ser no aplicable al área de estudio dado que es costoso tener firmas digitales para todos los empleados de la misma.

Seguridad de sistemas de oficina electrónicos

Descripción: Deberán prepararse e implantarse políticas y estándares para controlar los riesgos de negocios y seguridad asociados con los sistemas electrónicos de oficina (Los servicios electrónicos de oficina son las herramientas de software como Microsoft).

Hallazgo: No se cuenta con políticas que indiquen que el software comercial autorizado debe ser el único a instalarse en los equipos de cómputo, en base a las funciones que realiza cada empleado.

Recomendaciones: Elaboración de políticas para controlar esta situación.

Política de seguridad de oficina

Descripción: Establecer políticas de restricción y control de acceso a herramientas, equipos e infraestructura

Hallazgo: No se cuenta con políticas que regulen el software, equipo o herramienta que deberá utilizarse, en base a las funciones de cada empleado.

Recomendaciones: Elaboración de políticas para controlar esta situación.

Acceso restringido

Descripción: Aplicar restricciones de acceso de acuerdo al nivel del personal o ámbito de competencia.

Hallazgo: En algunos de los sistemas utilizados en el área se manejan claves de acceso de acuerdo al nivel del personal pero esto no es un estándar.

Recomendaciones: Establecer como política que se contemplan niveles de acceso para todas las aplicaciones utilizadas en el área de estudio, de acuerdo al nivel del personal o ámbito de competencia.

Seguridad de los respaldos

Descripción: Realizar respaldos de información sensitiva para asegurar su recuperación.

Hallazgo: Se realizan respaldos de la información que se almacena en el servidor pero no se encuentra toda aquella considerada como sensitiva.

Recomendaciones: Establecer como política, de acuerdo a la clasificación de la información del área, que todos los empleados responsables de la misma, la coloquen en su espacio reservado del servidor para que sea respaldada.

Otras formas de intercambio de información

Descripción: Los procedimientos y controles deberán ser apropiados para proteger el intercambio de información a través del uso de medios de comunicación por voz, fax y video.

Hallazgo: No existen restricciones en cuanto a intercambio de información sensitiva por medios de comunicación como fax o teléfono.

Recomendaciones: Establecer como política que no se discuta o intercambie información sensitiva por fax o teléfono.

4.7 CONTROL DE ACCESOS

Política de control de acceso

Descripción: Los requerimientos para el control de acceso deberán definirse y documentarse, al igual que se deberá restringir el acceso a lo que se define en la política del control de acceso.

Hallazgo: Algunas aplicaciones cuentan con restricciones para acceder información sensitiva. En cuanto documentación sensible, no se cuenta con ningún tipo de restricción ni protección mas que las medidas que el propio empelado aplique.

Recomendaciones: Establecer políticas para manejo y restricción del el acceso a información sensible, ya sea por sistema o en papel.

Privilegios mínimos

Descripción: Se debe contar con la premisa de que todo lo que no está restringido está disponible.

Hallazgo: Actualmente no se cuenta con políticas que especifiquen la información que debe ser restringida por ser sensitiva.

Recomendaciones: De manera detallada se debe analizar los equipos y/o aplicaciones que deben tener acceso restringido por la información que contienen, ya que de no ser especificado como tal puede ser utilizado en formas indebidas.

Controles de acceso discrecional

Descripción: Para información particularmente sensible, los usuarios no deben tener la habilidad de permitir el acceso a otros usuarios.

Hallazgo: Actualmente no se tienen controles de restricción sobre información sensible.

Recomendaciones: Se deben establecer los mecanismos de control de acceso apropiados para que los usuarios con acceso a información sensible no tengan la capacidad de otorgar permisos de acceso a otros usuarios.

Registro de usuarios

Descripción: Debe existir un registro formal de usuarios y procedimientos de registro para garantizar el acceso a múltiples sistemas de información y servicios de usuario.

Hallazgo: No se cuenta con un registro actualizado de los usuarios dados de alta en los sistemas utilizados en el área. Actualmente no se cuenta con un procedimiento formal para solicitar claves de usuarios y contraseña, por lo que se deberá generar uno.

Recomendaciones: Generar un formato por empleado, en el que se registren las claves de usuario asignadas a cada uno y su respectiva contraseña. Este formato deberá guardarse en sobre cerrado, ser controlado por personal de la misma área con total responsabilidad y confidencialidad y sólo abierto en caso de contingencia.

Administración de privilegios

Descripción: La distribución de privilegios de los usuarios deberá ser restringida y controlada.

Hallazgo: La administración de privilegios de algunas aplicaciones esta a cargo del área sin embargo se otorgan sin previo análisis.

Recomendaciones: Para las aplicaciones de las cuales el área si puede administrar privilegios, se tendrá que evaluar los privilegios asignados a cada usuario y en su caso restringir aquellos que se consideren inadecuados.

Administración de contraseña de usuarios

Descripción: La distribución de contraseñas será controlada a través de un proceso administrativo formal.

Hallazgo: No se cuenta con un procedimiento formal para solicitud de claves de usuarios y contraseñas para los sistemas utilizados y administrados por el área.

Recomendaciones: Generar un formato para solicitar claves de usuarios de los sistemas o aplicaciones controladas por el área.

Revisión de derechos de acceso de usuarios

Descripción: Se deberá llevar a cabo un proceso formal en inventarios regulares para revisar los derechos d acceso del usuario.

Hallazgo: La administración de privilegios de algunas aplicaciones esta a cargo del área sin embargo se otorgan sin previo análisis.

Recomendaciones: Para las aplicaciones de las cuales el área si puede administrar privilegios, se tendrá que evaluar los privilegios asignados a cada usuario y en su caso restringir aquellos que se consideren inadecuados.

Utilización de la contraseña

Descripción: Se deberá solicitar a los usuarios que sigan las buenas prácticas de seguridad para seleccionar y utilizar sus contraseñas.

Hallazgo: Actualmente las contraseñas asignadas son iguales a la clave de usuario respectiva, y no es obligatorio que se cambie la primera vez que se accede con ella.

Recomendaciones: Establecer como obligatorio que la contraseña asignada sea modificada la primera vez que se accede con ella. Además de establecer como política que las contraseñas son personales e intransferibles.

Identificación del usuario y autenticación.

Descripción: Todos los usuarios tendrán una identificación única (ID del usuario) para su uso personal y único de manera que las actividades pueden servir para rastrear a la persona responsable

Hallazgo: Todos los empleados del área cuentan con usuarios y contraseñas personales, pero dado que no se tiene una relación de estas claves con el personal responsable, no se pueden asociar las actividades rastreadas con un empelado en especifico.

Recomendaciones: Establecer como política que la contraseña sea modificada la primera vez que se accede con la clave de usuario, de esta forma el empleado responsable de dicha clave será el único que conozca la contraseña.

Autenticaciones

Descripción: Se deben establecer los medios apropiados para asegurar que se requiera como mínimo el uso de contraseñas para todos los sistemas y/o aplicaciones a los que se tienen múltiples accesos.

Hallazgo: No se especifica un mínimo de caracteres para componer una contraseña, por lo que algunas se componen de un número, letra o enter.

Recomendaciones: Establecer como política que las contraseñas tengan un mínimo de seis caracteres alfanuméricos.

Sistemas de administración de contraseñas

Descripción: Se deberá instalar un sistema de administración de contraseñas para proveer un medio interactivo y efectivo, el cual asegure la calidad de las contraseñas.

Hallazgo: Las contraseñas son asignadas por el personal responsable de generar las claves de usuario.

Recomendaciones: Instalación de un software generador de contraseñas.

Time-out en las terminales

Descripción: Las terminales iniciativas en lugares de alto riesgo o que sirven a sistemas de alto riesgo deberán apagarse después de un periodo definido de inactividad para evitar el acceso por personas no autorizadas.

Hallazgo: No es obligatorio contar con este tipo de protección en los equipos de cómputo que se utilizan en el área de estudio.

Recomendaciones: Establecer como política que se active esta opción en cada uno de los equipos de cómputo del área, estableciendo un tiempo estándar de inactividad, e indicar las sanciones a las que se harán acreedores quienes no cumplan con dicha política.

Restricción de acceso de información

Descripción: Se deberá restringir el acceso a la información y a las funciones del sistema de aplicaciones de acuerdo con la política de control de acceso.

Hallazgo: Algunas aplicaciones cuentan con restricciones para acceder información sensitiva

Recomendaciones: Establecer políticas para manejo y restricción en el acceso a información sensible contenida en los sistemas y/o aplicaciones que se utilizan en el área de estudio

Aislamiento de sistemas sensibles

Descripción: Los sistemas sensibles deberán tener un ambiente de cómputo dedicado (aislado).

Hallazgo: Los sistemas que manejan información sensible, y son consultados por el área no se encuentran aislados de los demás ni en equipos especiales.

Recomendaciones: Instalar estos sistemas en equipos que no se encuentren a la vista de los empelados y solo en aquellos que sean totalmente necesarios muy autorizados.

Computadoras móviles

Descripción: Deberá existir una política formal y se deberán adoptar controles apropiados para la protección contra el riesgo de trabajo con inmuebles de computo móviles, en particular, en ambientes desprotegidos.

Hallazgo: En el área de estudio no se cuenta con equipo de computo portátil

Recomendaciones: Para toda la institución deberá considerarse la importancia del uso, manejo y resguardo del equipo de cómputo portátil.

4.8 MANTENIMIENTO Y DESARROLLO DE SISTEMAS

Validación de datos de entrada

Descripción: La entrada de datos a los sistemas de aplicación deberán validarse para asegurar que es correcta y apropiada

Hallazgo: En algunos desarrollos se contempla la validación de datos de entrada pero no en todos.

Recomendaciones: Establecer que en el diseño de todos los desarrollos se maneje validación a los campos de captura. Analizar las aplicaciones desarrolladas por el área de estudio y que se encuentran actualmente en producción, de tal forma que se pueda aplicar esta validación sin que afecte la operación ni la continuidad del negocio.

Autenticación del mensaje

Descripción: Se deberá implementar la verificación de mensajes para las aplicaciones en donde existe un requerimiento de seguridad para proteger la integridad del contenido del mensaje.

Hallazgo: Existen aplicaciones desarrolladas por el área en la que se realiza intercambio de información sin ninguna garantía de que se protegía, dado que o se utilizan procedimientos de autenticación.

Recomendaciones: Analizar la viabilidad de implementar mecanismos de autentificación para las aplicaciones que se necesite y que actualmente están en producción. Además de establecer, como requerimiento de seguridad, en el diseño de las aplicaciones este tipo de mecanismos.

Validación de datos de salida

Descripción: La salida de datos de un sistema de aplicación deberá validarse para asegurar que el procesamiento de la información almacenada es correcto y apropiado según las circunstancias

Hallazgo: El cliente es quien realiza esta validación a la información procesada en producción y en caso de existir errores lo reporta al área de desarrollo respectiva para revisión al código.

Recomendaciones: En el proceso de pruebas a las aplicaciones deberá haber una fase para que el usuario cliente pueda llevar a cabo revisiones de validación.

Política en el uso de controles criptográficos

Descripción: Se deberá desarrollar y seguir una política en el uso de controles criptográficos para la protección de a información

Hallazgo: No se utiliza ningún tipo de mecanismos de encripción de información en el área de estudio.

Recomendaciones: Desarrollar una política para establecer los servicios y mecanismos criptográficos de acuerdo la clasificación de los activos de información en grado de confidencialidad.

Encripción

Descripción: Deberá aplicarse la encripción para proteger la confidencialidad de la información sensible o critica

Hallazgo: No se utiliza ningún tipo de mecanismos de encripción de información en el área de estudio

Recomendaciones: Para cada categoría en la clasificación deberán estar indicados los mecanismos de encripción para su implantación inmediata.

Firmas digitales

Descripción: Las firmas digitales deberán aplicarse para proteger la autenticidad e integridad de la información electrónica.

Hallazgo: No se utilizan herramientas para firmas digitales en el área de estudio.

Recomendaciones: Analizar la viabilidad de instalar mecanismos o herramientas de firmas digitales de acuerdo al tipo de información que se maneja en el área.

Administración de claves

Descripción: Se deberá utilizar un sistema de manejo de claves basado en un conjunto de normas, procedimientos y métodos acordados para apoyar el uso de técnicas criptográficas.

Hallazgo: No se cuenta con una herramienta para administración de claves.

Recomendaciones: Analizar la viabilidad de instalar mecanismos generadores de claves para tener un mayor control de las mismas.

Control de software operacional

Descripción: Se deberá aplicar el control de la implantación de software en sistemas operacionales.

Hallazgo: No se cuenta con un registro sobre las versiones de software y sus respectivas actualizaciones, que se tienen instaladas en cada equipo del área

Recomendaciones: Generar e implantar un formato en el que se registren y especifiquen las versiones de las herramientas de software instalada en cada equipo, así como los diferentes parches o actualizaciones en caso de que aplique, de esta forma se puede controlar que se tenga lo mismo en todos los equipos del área. Este formato deberá ser verificado y confirmado al menos cada mes.

Restricciones en los cambios a los paquetes de software

Descripción: Las modificaciones a paquetes de software serán restringidas y se controlaran estrictamente los cambios esenciales.

Hallazgo: No se hacen modificaciones a paquetes de software utilizados en el área, por ejemplo para desarrollo de las aplicaciones, pero lo que se puede controlar son las actualizaciones a éstos paquetes de software que dado que tienen que estar instalados en cada maquina de los programadores, es posible que no todos cuenten con los mismos parches instalados y se tengan diferentes versiones para desarrollo.

Recomendaciones: Generar e implantar un formato en el que se especifiquen las versiones de las herramientas de software instaladas en cada equipo, así como los diferentes parches o actualizaciones en caso de que aplique, de esta forma se pueda controlar que se tenga lo mismo en todos los equipos del área.

4.9 ADMINISTRACIÓN DE CONTINUIDAD DEL NEGOCIO

Proceso de administración de continuidad del negocio

Descripción: Deberá haber un proceso de administración apropiado para desarrollar y mantener la continuidad del negocio a través de la organización.

Hallazgo: No se cuenta con un procedimiento formal para especificar los pasos a seguir con los activos críticos de la empresa, ya sea antes, durante y después de que se presente una contingencia.

Recomendaciones: Elaborar e implantar como política, un procedimiento para asignar responsabilidades, en cuanto a los activos críticos de la empresa se refiere, antes, durante y después de una contingencia.

Continuidad del negocio y análisis de impacto

Descripción: Se debe desarrollar un plan estratégico, basado en la evaluación de riesgos apropiada, para el enfoque global de la continuidad del negocio.

Hallazgo: No se cuenta con un inventario de activos actualizado en el que se indique el grado de confidencialidad que deben de tener asignado.

Recomendaciones: En base a los resultados obtenidos a través del análisis de riesgo aplicado al área de estudio, se especifica la clasificación de los activos, identificados, por lo que se deberá asignar el nivel de protección recomendado en el mismo.

Escritura e implantación del plan de continuidad

Descripción: Se deberán desarrollar planes para mantener o restaurar las operaciones del negocio.

Hallazgo: No se cuenta con un procedimiento formal para especificar los pasos a seguir con los activos críticos de la empresa, durante y después de que se presente una contingencia.

Recomendaciones: Elaborar e implantar como política, un procedimiento para asignar responsabilidades, en cuanto a los activos críticos de la empresa se refiere, antes, durante y después de una contingencia.

Marco de trabajo del plan de continuidad

Descripción: Se deberá mantener un marco de trabajo único de los planes de continuidad del negocio para garantizar que todos los planes concuerden así como identificar prioridades para pruebas y mantenimiento.

Hallazgo: No se cuenta con un procedimiento formal para especificar los pasos a seguir con los activos críticos de la empresa, durante y después de que se presente una contingencia.

Recomendaciones: Asignar un grupo de personas o un área para el desarrollo de los procedimientos y políticas relacionadas con la continuidad del negocio y planes de contingencia.

Pruebas, mantenimiento y re-evaluación del plan de continuidad del negocio

Descripción: Los planes de seguridad del negocio deberán probarse con regularidad y mantenerse mediante revisiones regulares que son actuales y efectivos.

Hallazgo: No se cuenta con un procedimiento formal para especificar los pasos a seguir con los activos críticos de la empresa, durante y después de que se presente una contingencia.

Recomendaciones: Una vez que se desarrollen los planes de contingencia correspondientes, se recomienda que se hagan simulacros para tener referencias de las respuestas que se puedan obtener y verificarlos al menos cada seis meses.

4.10 CUMPLIMIENTO

Salvaguarda de archivos organizacionales

Descripción: Los registros importantes de una organización deberán protegerse de pérdidas, destrucción y falsificación.

Hallazgo: No se cuenta con respaldos de toda la información importante del área, adicionalmente los respaldos que se tienen están almacenados en el mismo lugar que la información.

Recomendaciones: Desarrollar y establecer como política que toda la información considerada como sensible, sea depositada en el servidor del área para su respaldo.

Protección de los datos y privacidad de información personal

Descripción: Se deberán aplicar controles para proteger la información personal de acuerdo con la legislación importante.

Hallazgo: No es requerimiento que los empleados almacenen la información vital en su espacio reservado del servidor.

Recomendaciones: Desarrollar y establecer como política que toda la información considerada como sensible, sea depositada en el servidor del área para su respaldo.

Prevención del mal uso de las instalaciones de procesamiento de información

Descripción: La administración autorizará el uso de inmuebles de procesamiento de la información y se deberán aplicar controles para evitar el mal uso de dichos inmuebles

Hallazgo: No se cuenta con controles o políticas especificas sobre el uso de los inmuebles del área.

Recomendaciones: Desarrollar y establecer como política, el uso para el cual están diseñados los inmuebles de procesamiento de la información del área.

Controles de auditoria del sistema

Descripción: Las auditorias de los sistemas operativos serán planeadas y acordadas de manera que se reduzca al mínimo el riesgo de alteraciones a los procesos del negocio.

Hallazgo: Hasta el momento, no se han realizado auditorias a los sistemas desarrollados o utilizados por el área, tampoco se han realizado a los procedimientos que se utilizan.

Recomendaciones: La empresa deberá designar a un área especializada en realizar auditorias a todos los departamentos de la empresa, para verificar el grado de aplicación y cumplimiento de las políticas establecidas actualmente, y en caso de que se implementen los controles recomendados en este enunciado.

Protección de herramientas de auditoria del sistema

Descripción: Deberá protegerse el acceso a las herramientas de auditoria del sistema para evitar el mal uso o vulnerabilidad posibles.

Hallazgo: Ninguna aplicación desarrollada por el área o utilizada en la misma, cuenta con logs de auditoria.

Recomendaciones: Establecer como política que en el diseño de los nuevos desarrollos sea necesario generar las bitácoras correspondientes y asignarles el nivel adecuado de protección, de tal forma que no cualquier usuario pueda consultarlas. Para las aplicaciones que actualmente están en producción, y que fueron desarrolladas por el área de estudio, se deberá analizar la viabilidad de aplicar esta herramienta.

CONCLUSIONES

CONCLUSIONES

A lo largo de este trabajo, se ha establecido la importancia que tiene definir y mantener el mejor nivel posible en la seguridad informática dentro de las organizaciones.

Para lograrlo se ha postulado la necesidad de establecer las políticas y lineamientos de seguridad informática, de acuerdo a:

- El tipo de organización
- Modelo y madurez de la infraestructura informática
- Cantidad y tipo de empleados, socios y proveedores
- Modelo de operación
- Necesidades específicas de sistemas en la organización

Se establecieron ciertos requerimientos que las organizaciones deberán cubrir, entre los cuales se pueden mencionar:

- La necesidad de que las empresas se encuentren siempre alerta con los intrusos.
- Salvaguardar la información estratégica de la organización.
- Protegerla contra accesos no autorizados, intentos de destrucción o inutilización.
- Protección de la infraestructura informática, tanto de los equipos en si como de la red.
- Protección de los sistemas y bases de datos.
- Salvaguardar la confidencialidad de la información y de los mensajes que viajan en la infraestructura.

Por todo lo anterior es preponderante establecer esquemas de seguridad en los sistemas de almacenamiento de información entre los cuales están los siguientes:

- Mecanismos de control de acceso a la información.
- Respaldo continuo de la información.
- Encriptado, autentificación y firmas digitales.
- Políticas de seguridad claras que le den al empleado los parámetros y estándares para que sepa la forma en cómo resguardar el equipo y la información..
- También es primordial esquemas de seguridad física en el área de sistemas o en los departamentos en los que se tengan equipos de cómputo.

Se revisó también la utilidad de aprovechar diversas metodologías para evaluar los sistemas de seguridad en informática. Conociendo la forma de evaluar cuantitativa y cualitativamente la situación que guarda la empresa con respecto al manejo de sus esquemas de seguridad informática.

Cuando se evalúan los niveles de seguridad en una empresa se están evaluando los siguientes factores: normatividad de la empresa, organización, metodologías, objetivos de control, procedimientos de control, tecnología de seguridad y herramientas de control. En base a todo esto, se puede proponer un primer esquema donde definimos distintos niveles de protección, de acuerdo a la evaluación cualitativa y cuantitativa efectuada, que nos permita proteger a la organización en los aspectos más estratégicos. De esta manera habremos conseguido una situación nueva en la que el nivel de seguridad sea superior al anterior. Es importante mantenerse en este ciclo permanentemente buscando mejorar el nivel de seguridad constantemente, alertas a nuevas amenazas.

En el caso que se presenta se hace uso de la metodología BS7799, ya que permite definir cada uno de los aspectos involucrados para mantener los

sistemas vigilados y seguros. Esta metodología es la más utilizada en empresas europeas por estar respaldadas en el Instituto Británico de Estandarización el cual avala las mejores prácticas de seguridad de la información en Inglaterra, además de que cuenta con códigos de compatibilidad con la Organización Internacional de Estandarización (ISO) y permite a las organizaciones obtener las certificaciones de los diversos sistemas de calidad en las empresas.

Finalmente abordó una manera concreta para elaborar las políticas de seguridad dentro de una organización, así como una metodología que facilita la elaboración, utilizando 3 etapas:

1. La descripción de lo que se debe realizar.
2. El hallazgo de lo que se encuentre en el área analizada.
3. Las recomendaciones y acciones a llevar a cabo.

De esta manera se cumplen los objetivos que se propusieron en la introducción de este trabajo, proponiendo marcos de acción traducidos en políticas, los cuales nos ayudarán a mantener y mejorar los sistemas de seguridad en los sistemas de una organización.

Se estableció que el cumplimiento de estas políticas por parte de los empleados será factor estratégico y fundamental para que no se ponga en riesgo la información y datos de la organización, y así de esta manera se evitarán contingencias desagradables que perjudiquen la operación de la misma, lo que coadyuvará en el aspecto económico a la organización, pues se evitarán gastos adicionales e imprevistos al tener la información protegida y disponible de acuerdo a los perfiles de usuario, para todos los usuarios internos y también hacia fuera, con los proveedores, clientes, etc.

Una organización que tenga la posibilidad de mantener alejados a los intrusos de sus medios informáticos tenderá a salvaguardar su propio negocio, sus intereses, sus clientes y gozará de una imagen de confiabilidad hacia la sociedad que hace uso de sus servicios.

En la actualidad es un requisito saber que las organizaciones con las que tenemos relación a través de sistemas y terminales, son organizaciones responsables, seguras y de buena reputación. Principalmente porque las tendencias en los negocios a nivel nacional e internacional son utilizar las transacciones electrónicas, uso masivo e intensivo del internet, lo cual facilita el intercambio de información, la transmisión de conocimientos, la adquisición de productos o a la contratación de servicios por éste medio.

Si las organizaciones son capaces de asumir esta responsabilidad, destinar los recursos humanos y financieros necesarios para establecer y ejecutar las políticas de seguridad informática adecuadas, revisando periódicamente estas normas, actualizándolas de acuerdo a su natural evolución, podremos pensar que las ventajas que brinda el uso de la tecnología se puedan seguir expandiendo. De otra manera la confianza de los usuarios retardará la penetración de las Tecnologías Informáticas en México.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Ballesteros Inda Nicolás, Fundamentos de informática, Editorial Prentice may, México, 2000.

Basile Dante, Desarrollo de sistemas, Editorial Macchi, Buenos Aires – Argentina, 1998.

Bohlander George y Sherman Arthur. Administración de la Información. México. Ediciones Thomson. 1999.

Braun Unda, M. Apuntes de la materia Ciencias y técnicas de la información, UNAM, ENEP Acatlán, 2000.

Cieland David I., William R. King, Manual para la Administración de Proyectos, Editorial Compañía Editorial Continental, S.A. de C.V., México, 1990

Cobb Stephen, Manual de seguridad para PC y redes locales, MacGrawHill, España, 1994.

Coss Bu Raúl, Análisis y Evaluaciones de Proyectos de Información, Editorial Limusa, México 1999

García Cabeza Camilo, Félix José Pascual Miguel, Julián Chaparro Pelaéz. "Sistemas de información y comunicaciones para la gestión del conocimiento". Universidad Politécnica de Madrid. España 2001.

García Mendoza Alberto, Evaluación de Proyectos en las organizaciones, Editorial Mc Graw Hill, México, 1998

Gido Jck y Clemens James, Administración Exitosa de Proyectos, Editorial Internacional Thomson Editores S.A. de C.V. México, 2001.

Gómez Ceja Guillermo. Planeación y Organización de Empresas. México., Mc Graw Hill. 1994.

H. Davenport Thomas. Ecología de la información. México., OXFORD. 1999.

Klander, Lars, A prueba de Hackers, Editorial Anaya, España, 1998.

Lawrence J. Gitman, Administración de sistemas, Editorial Pearson Educación, México, 2000

Matthews Don Q. Diseño de sistemas de información administrativa., Argentina., El Ateneo. 1977

N. Smith, Joe, Sistemas de control de acceso del Proyecto Salt River, en Phoenix, Arizona, Presidente del Comité Permanente para Seguridad de Empresas de Servicios Públicos, USA, 2002.

Reza Trosino Jesús Carlos, Como Desarrollar y Evaluar Programas en las Organizaciones, Editorial Panorama, México, D.F. 1996

Rodríguez Luis Ángel, Seguridad de la información en sistemas de cómputo, Ediciones Ventura, México 1995.

Rodríguez Valencia Joaquín. Introducción a la Administración con Enfoque de sistemas, 3ª edición, México 1998. editorial., Ecafsa.

Terry, Ph. D. George. Principios de Administración. México., CECSA. 2000.

Vázquez Torres, Norma Angélica, Seguridad en los sistemas informáticos en las empresas, Editorial Trillas, México, 1993.

Wentz Walter, Administración y Métodos, Editorial Trillas, Mexico, 1993

Otras fuentes

Operating and Installation Manual Process Security, Campbell Company, USA, 2000.