

Introducción de la Seguridad Informática a la Empresa

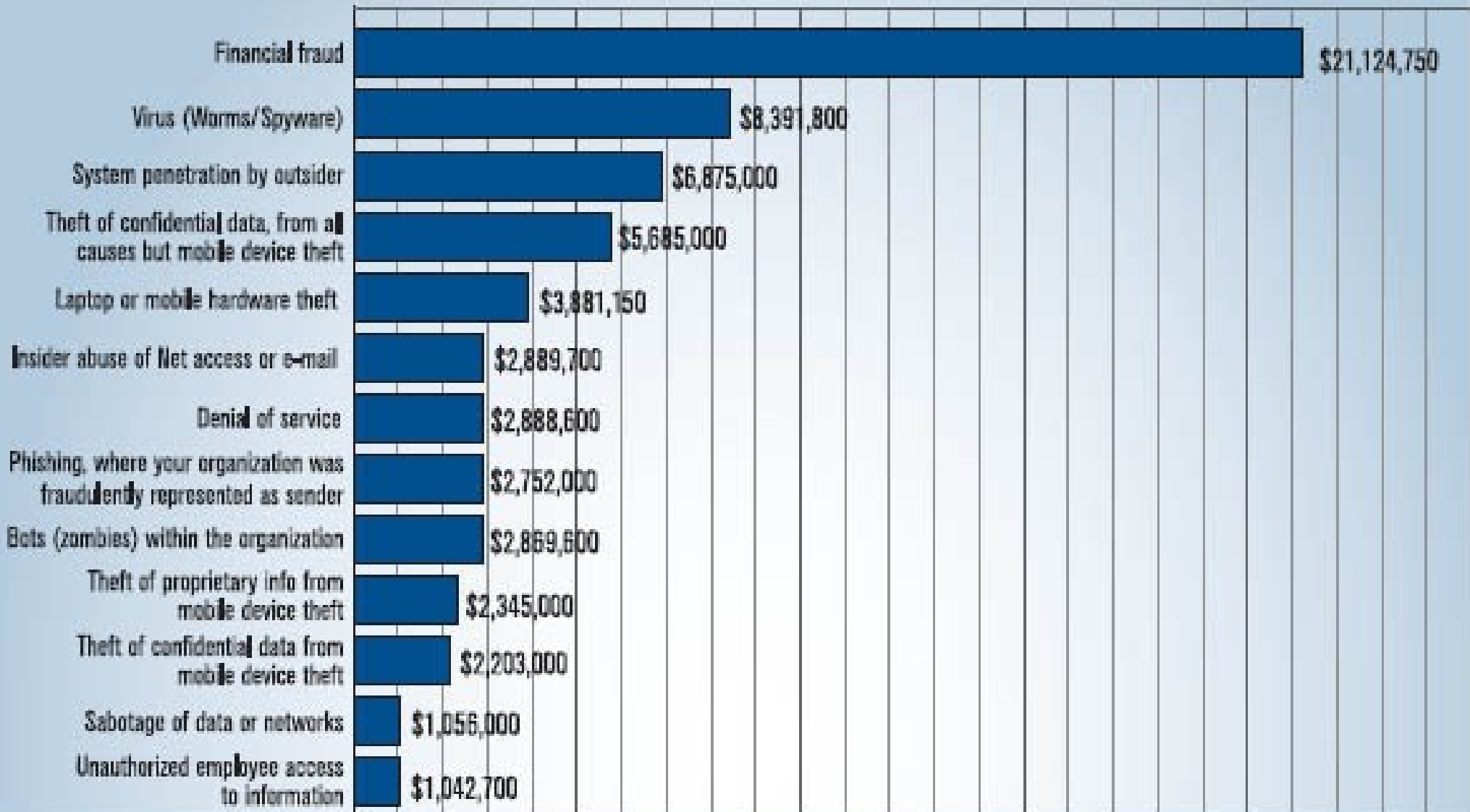


GREX Tecnologías de Información

MC. Helios Mier

helios.mier [en] grex.com.mx

Creative Commons 2.0: Atribución
Algunos derechos reservados, México 2008



CSI 2007 Computer Crime and Security Survey

2007: 194 Respondents

Source: Computer Security Institute

Aprender a valorar la información

- Los resultados que presenta un sistema de trabajo y de información resumen todo el esfuerzo e inversión para obtenerla.
- La información se valúa por la suma de todo el esfuerzo que costo producirla, más los beneficios que trae en forma de ventajas para el negocio.
- Hay que aprender a distinguir entre lo que es material y lo que es invaluable.

Datos e información

- Datos: valores que se han obtenido por un proceso de recolección.
 - Reportes, mediciones, bitácoras, etc...
- Información: los datos que han sido procesados y que ahora se les ha encontrado un sentido.
 - Estadísticas, tendencias, gráficas, etc...
- Sistema de información: todo el proceso, herramientas y personal que se ve involucrado.

Partes del sistema de información

- Recolección de datos
- Almacenamiento de datos
- Introducción al sistema
- El sistema y procesamiento de datos
- Almacenamiento de información resultante
- Presentación de información y resultados
- Comunicación de la información

Desastre informático

- Pérdida de la información:
 - los medios de almacenaje se han destruido y todo lo que había en ellos. No hay forma de recuperarlo mas que volverlo a hacer todo.
- Robo de información:
 - Una persona no autorizada tiene conocimiento de un secreto de la empresa y lo puede usar en su beneficio.
- Alteración de la información:
 - Los datos y la información no son fidedignos, se tomarán decisiones en base a información irreal.

Identificación de activos

- Toda la empresa cuenta con varios tipos de información de muchos usos y formas.
- La información es intangible, siempre esta contenida dentro de algún medio de almacenaje.
- El valor de la información puede cambiar con el paso del tiempo.
- El medio de almacenaje siempre tiende a degradarse con el paso del tiempo.

Enumeración de los activos

- En base a los componentes:
 - Activos de Información
 - Activos de Software
 - Activos de físicos
 - Servicios
- Primero se realizará una lista de todos ellos.
- Puede haber elementos que se compongan de otros mas simples.

- Activos de información:
 - Bases de datos:
 - Concentración de registros (clientes, proveedores, productos, personal, etc...)
 - Archivos de datos:
 - Detalles de transacciones de cada actividad (ventas, compras, pagos, inventarios, bitácoras, etc..)
 - Procedimientos operacionales y de soporte
 - La documentación de como funcionan y se hacen las cosas dentro de la empresa.
 - Archivos de información:
 - Datos e información que no está en uso pero tiene que conservarse por diversas razones.
 - Planes de contingencia:
 - La preparación de la empresa para actuar en tiempos de crisis.

- Activos de software

- Software de sistema:

- Funciones y servicios esenciales (sistema operativo, administradores de bases de datos, servicios de red, etc..)

- Software de aplicación comerciales:

- Herramientas que se adquieren en forma de cajas con cualquiera vendedor (procesador de palabras, hoja de cálculo, etc...)

- Software ad-hoc (desarrollo personalizado)

- Programas que fueron creados para uso exclusivo de la empresa de acuerdo a sus propios procedimientos.
 - Desarrollados internamente
 - Desarrollados externamente

- Activos físicos

- Equipo de cómputo

- PC de escritorio, laptops, servidores

- Equipo móvil

- Celulares, cámaras, agendas, MP3, etc..

- Equipo de comunicaciones

- Modems, routers, fax, PBXs, etc..

- Medios de almacenamiento

- Cintas, discos duros, discos compactos, discos flexibles, USBs, memory cards.

- Equipo técnico

- Reguladores, nobreaks, aire acondicionado.

- Mobiliario y equipo

- Escritorios, racks, etc..

- Servicios
 - Aquellos que la empresa haya subcontratado
 - Ej. un despacho de contabilidad., Auditores
 - Aquellos que la comunican hacia el exterior
 - Teléfono, Redes de área extensa (WANs), proveedores de Internet
 - Aquellos externos que la empresa requiere
 - Energía eléctrica, suministros de consumibles, mensajería y paquetería.
 - Soporte general
 - Vigilancia, limpieza, mantenimiento, etc...

Actividad 1

- Elaborar una lista de activos.
- En base a su experiencia, en un departamento típico de cualquier empresa (inventarios, compras, etc...) realizará una lista de activos.
- Identifique elementos de acuerdo a la clasificación de activos que se ha presentado.
- Entre más detallada se realice la lista se podrá tener un mejor control de ellos.
- Duración 15 minutos.
- Realize la lista en forma de columnas, se usará.

Registrabilidad de activos

- De cada uno de los activos enumerados, se determinan roles y responsabilidades:
 - Propietario
 - Determina el valor del activo y decide sobre su destino.
 - Guardián o custodio
 - Almacena y controla el acceso al activo. Tiene la responsabilidad de mantener la integridad del activo.
 - Operador
 - Trabaja con el activo. No puede tomar otra acción más que las encomendadas.
- Se ponen nombres o puestos a los roles.
- Nadie fuera de esta lista tiene que ver con el activo.

Ejercicio 2

- En su empresa existen personas con diferente nivel de autoridad y funciones.
- Cada uno de los activos listados previamente, deben de tener asignados personas o puestos en los 3 roles: propietario, guardian y operador.
- No use los nombres reales de sus compañeros.
- Al finalizar analice su esquema, escoja a una persona de su lista, ¿que pasaría si esa persona de su empresa se convierte en una amenaza.?
- Duración 10 minutos, 10 minutos discusión.

Clasificación de los activos

- Evaluar cada activo desde diferentes puntos de vista:
 - Confidencialidad
 - Si puede ser compartido libremente con cualquiera
 - Si sus beneficios dependen de su secrecidad y ante quienes.
 - Valuación
 - Que tanto es estimado el activo, alto, medio, bajo.
 - Costoso de conseguir/reparar.
 - Esencial para otro activo.
 - No necesariamente siempre en valores materiales.

- Tiempo de vida
 - Si su beneficio o necesidad aumenta en determinados tiempos o se perderá después de un tiempo o condiciones.
- Derechos de acceso
 - Si personas o grupos pueden usarlo, quién es el que decide esos derechos. Normalmente el rol de propietario.
- Destrucción:
 - La forma en que se debe desechar cuando ya no sea útil.
 - Nunca se debe tirar un papel o un disco así nomás a la basura.
 - Afecta particularmente a medios de almacenamiento, electrónicos o materiales.
- **NOTA:** Para determinar esta clasificación hay que analizar desde tres perspectivas: Jefes, administradores y empleados.

Ejercicio 3

- Seleccione 5 elementos de su lista de activos
- Por cada uno de esos 5, elabore una descripción que explique el nivel de necesidad en cuanto a las propiedades de Confidencialidad, Valuación, Tiempo de vida, Control de acceso y Destrucción.
- Aquí empieza la parte laboriosa de la identificación de activos informáticos porque sale a relucir que tan bien se conocen las funciones de la empresa.
- Si no se puede realizar la explicación, merece ser estudiado con mayor detalle. Ya es una mejora.
- Duración 15 minutos, 10 minutos discusión.

Riesgo

- Se define como la probabilidad de perdida.
 - $\text{Riesgo} = \text{daño o perdida} * \text{probabilidad de que suceda}$
- En seguridad la formula es más compleja
 - Una amenaza (natural o humana, accidental o incidental) aumenta la probabilidad de que suceda un daño.
 - Una vulnerabilidad aumenta la probabilidad de éxito de una amenaza.
 - Un ataque puede afectar varios activos, aumentando el posible daño o pérdida.

Conceptos de seguridad

- Amenaza
 - Factores que pueden impactar negativamente al activo
- Vulnerabilidad
 - Punto débil en el activo, aumenta la probabilidad de éxito de un ataque.
- Ataque
 - La acción directa o indirecta por dañar un activo.
- Mecanismo de protección
 - La medida establecida para eliminar una vulnerabilidad, contener una amenaza o impedir un ataque.

Administración de riesgos

- Identificar los activos, determinar su importancia e identificar la amenazas contra ellos así como la magnitud del posible daño.
- La profundidad con la que se realizó el análisis de amenazas ayudará a establecer los mecanismos más precisos.
- No se puede llegar al 100% de seguridad, pero se puede lograr el establecimiento de las protecciones más efectivas en relación con la inversión adecuada.

Mecanismos protección

- Establecer herramientas, procesos y capacitación para anular, aminorar o transferir riesgos.
- El principal objetivo es evitar un desastre.
 - Se estudiarán y atenderán anticipadamente las posibles causas.
- El segundo objetivo es facilitar la recuperación en caso de que un desastre se presente y reducir su impacto.
 - Por si alguna causa no contemplada o excepcional se presenta.

Los perfiles de los mecanismos



La lista de chequeo

- Es una de las principales técnicas de control de la seguridad.
- Se elabora una lista por cada activo o grupo de activos.
- Una lista de actividades a realizar o requisitos a cumplir en un sistema.
- La revisión periódica de la lista de chequeo por cada computadora es lo que añadirá resistencia a desastres.

Contenido de la lista

- Alcance de la revisión: Activo o grupo de activos
- Nombre o identificador.
- Fecha de revisión.
- Lista de actividades y su estado:
 - Satisfactorio: la revisión se realizó
 - no satisfactorio.: no se realizó la revisión o el resultado no fue el mejor esperado.
- Observaciones encontradas.
- Consideraciones a tomar en la próxima revisión.

Alcance de la lista de revisión

- Las amenazas de seguridad pueden afectar a múltiples escalas y tratarse de forma conjunta:
 - A nivel de empresa en general
 - A nivel de instalación en particular
 - A nivel de sistema específico (conjunto de activos)
 - A nivel de un activo individual

Amenazas desde el exterior

- Son causas de desastre ajenas al funcionamiento del sistema.
- Presentaremos una lista de causas muy probables conocidas.
 - A veces un problema crónico tiene una causa tan simple que no anticipamos.
- Aunque parezcan obvias, en la seguridad hay que comenzar a revisar por lo trivial primero.

Amenazas desde el exterior

- Todas aquellas que salen de la cobertura de la empresa pero que pueden afectar negativamente:
 - Origen ambiental
 - Proviene del lugar y circunstancias donde se encuentra el sistema.
 - Origen tecnológico
 - Proviene de las características de los sistemas que usamos
 - Origen humano
 - Causadas por diversos motivos de las personas.

Amenazas de origen ambiental

- De origen natural
 - Clima
 - El calor y la humedad con los principales enemigos de la electrónica.
 - Los sistemas mas importantes deben de tener protección adecuada.

Añadir a la lista de chequeo revisiones para:

- Ventilación y control del calor para cada computadora (ej. Retirar de la pared)
- Ventilación adecuada para la oficina
- Exposición de la computadora a luz directa del sol (no debe de pegar de frente).
- Localización de tuberías y tomas de agua, drenaje cercanas a las computadoras.
- Revisar periodicamente por indicios de filtraciones de agua.

- Exposición a inundaciones e incendios naturales
 - La correcta preparación del lugar para resistir clima extremo.
 - Los antecedentes climáticos de la zona brindarán la información necesaria para ver si este tipo de eventos son un factor importante.
 - Además del daño a las instalaciones, se analiza el daño a los servicios: energía eléctrica, comunicaciones de teléfono e internet.

Añadir a la lista de chequeo revisiones para:

- Cumplimiento de las instalaciones con el reglamento de protección civil local.
- Establecimiento de planes de emergencia en caso de desastre.
- Resistencia de las instalaciones o necesidad de construir instalaciones especialmente diseñadas para centros de cómputo.
- Necesidad de establecer protecciones físicas adicionales para los servicios
- Necesidad de instalar fuentes de generación de energía locales.
- Analizar la necesidad de sistemas de comunicaciones inalámbricos.
- Redundancia: tener un duplicado de las instalaciones en otro lugar.

- Polvo y desechos volátiles

- Degradan con el paso del tiempo los aparatos mecánicos de la computadora:
 - Los discos duros son principalmente mecánicos.
- El polvo puede obstruir los conectores de la computadora y provocar un corto circuito.
- Limpieza interna y externa periódica de partes móviles.
- El polvo puede atraer otros bichos.
- Evitar el derrame accidental de líquidos.

Añadir a la lista de chequeo revisiones para:

- Limpieza y engrasado de impresoras.
- Limpieza de ventiladores y ductos de aire de la oficina.
- Limpieza de los ventiladores de la computadora (fuente, procesador, video)
- Publicar anuncios para el cuidado de desechos cerca de la computadora:
 - No comer, fumar ni beber cerca.
- Enseñar y recordar al personal de limpieza los cuidados cerca de una computadora.

- Fauna

- Roedores

- Tienen una predilección por el ambiente de una red:
 - Establecen nidos debido al calor de las computadoras.
 - Muerden cualquier cosa:
 - Cables de energía y causan cortos.
 - Cables de red y causan desconexiones.
 - A veces cuesta mucho trabajo reparar un cable.

- Insectos

- Se introducen en los equipos y causan cortos electricos.
 - Las secreciones deterioran los materiales.

Añadir a la lista de chequeo revisiones para:

- Fumigación y control de plagas de forma periódica, no importa que no se vean.
- Limpieza integral profunda de forma periodica, cada rincón y cada hueco.
- Necesidad de proteger de la interperie los cableados.

- Animales grandes

- Control de el acceso de organismos grandes a las zonas de procesamiento de datos.
- Daño físico a los equipos por golpes o secreciones.
- Desorganización del lugar. Ejemplo tirar papeles accidentalmente.

- Microscopicos

- Lugares con mucha humedad favorecen el crecimiento de hongos.
- Los archivos de papeles se degradan expuestos al ambiente.
- Los discos de computadoras mal archivados suelen crecer hongos (sobre todo si son de baja calidad)

Añadir a la lista de chequeo revisiones para:

- Necesidad de instalar barreras delimitadoras de zonas.
- Establecimiento de puntos de control y revisión de ingreso y egreso de personas.
- Duplicidad de archivos, tener dos o mas copias correctamente almacenadas.
- Evaluar la posibilidad de digitalizar archivos (escanear todo).
- Periodicamente rehacer el archivo (volver a fotocopiar, volver a grabar discos)

• De origen circunstancial

– Incendios

- Siempre son un riesgo presente, de manera que hay que tener medidas preparadas para en caso de uno.
- Cada tipo de industria tiene ciertas necesidades de seguridad industrial. Hay que revisar el reglamento de protección civil local.
- Invitar a los vecinos a participar en sus revisiones de seguridad industrial. Una zona preparada es mejor que un local.
- Y cuidar que la computadora no sea la causa de uno. Como todo aparato eléctrico, hay que tomar medidas.

Añadir a la lista de chequeo revisiones para:

- Revisar el manual de procedimientos para el manejo de materiales peligrosos.
- Contar con el tipo y cantidad de extintores necesarios.
- Revisar periódicamente el estado y carga de extintores.
- Realizar capacitación para el personal en caso de emergencias.
- Realizar simulacros con el personal de la empresa y los de alrededor.

• Robos

- La seguridad física siempre es necesaria.
- La oportunidad hace al ladrón, pero se mantendrá alejado cuando se da cuenta que el lugar es vigilado.
- Más que cuidar la computadora físicamente, cuidamos la información que contienen.

Añadir a la lista de chequeo revisiones para:

- Instalación y mantenimiento de barreras y candados
- Cambiar periódicamente llaves y combinaciones.
- Recordar periódicamente al personal de no dejar laptops, agendas o celulares en el carro
- Evaluar la necesidad de crear una zona de alta seguridad en la empresa.
- Definir los puntos donde es necesario la instalación de vigilancia y monitoreo.
- Evaluar el desempeño de los vigilantes.
- Realizar estudios de antecedentes del personal que conforma la vigilancia.
- Establecer una regla de separación de responsabilidades.
- Establecer un procedimiento de “confirmación por pares”.
- Establecer una estricta política del tipo de información que se prohíbe salga de la oficina.

Amenazas de origen tecnológico

- Origen de Hardware
 - Particularmente las fallas eléctricas son las que causan daños.
 - La mayor parte del hardware es desechable.
 - En la seguridad se cuida que cuando falle, no se pierda lo que contiene la computadora.

Añadir a la lista de chequeo revisiones para:

- Revisar la carga de aparatos en contactos eléctricos.
- Revisar la instalación de tierra física.
- Establecer mantenimiento periódico a los centros de carga
- Poner barreras y candados a centros de carga, paneles de pastillas y fusibles.
- Uso de reguladores de voltaje en cada sistema.
- Uso de No-breaks en las computadoras importantes.
- Revisar la capacidad de los no-breaks y la carga conectada.
- Revisar el tiempo de vida útil de los no-breaks.

De origen de software

- En el producto

- Los programas que usamos son propensos a fallas.
- Siempre se están descubriendo nuevas vulnerabilidades pero también aparecen “parches”.
- El Hacking de los sistemas particularmente consiste en encontrar los agujeros.
- Todos los productos comerciales periodicamente publican parches.
- Parche: actualización para corregir un error de software

- **Es una de las reglas obligatorias el buscar y aplicar parches periódicamente.**
 - El uso de software “viejo” es casi una garantía de problemas crónicos, por ejemplo los virus.
 - Algunos parches se distribuyen automáticamente, pero la mayoría no lo hace.
 - En una computadora hay muchos productos diferentes, la protección se dará por mantenerlos todos ellos con los parches al día.
- **OJO:** la mayoría de los productos de software niegan las actualizaciones para productos pirateados.
- **Nota:** Si un producto no se puede actualizar, lo puedes cambiar.

- Ejemplo: productos de Microsoft
 - Establecen una fecha fija para publicar parches para todos sus productos.
 - Segundo martes de cada mes.
 - Se tiene que revisar que cada computadora haya recibido su parche.
 - No todas tienen activada la opción de actualizaciones automáticas.
 - Opción de activarlo
 - Opción de instalarlo de forma manual.

- Control de software

- En una computadora hay muchos productos diferentes.
- Cada uno maneja diferentes versiones.
- Todos manejan un ciclo de vida por el fabricante: entre 5 y 7 años y termina su soporte oficial. (no más parches)
- Cada programa le añade carga a la computadora, a veces están funcionando partes de él aunque no se haya ejecutado manualmente.
- Dos opciones: quitar productos o aumentar capacidad.

Añadir a la lista de chequeo revisiones para:

- Levantar un inventario de software que la empresa necesita
- Levantar un inventario de lo que cada computadora tiene instalado
- Periódicamente revisar que cada computadora no tenga otros programas y desinstalarlos.
- Revisar el estado de la licencia de cada software.
- Revisar que cada programa se encuentre en sus versiones más recientes.
- De acuerdo a la lista de software, revisar cada uno con el fabricante y buscar sus parches.
- Periódicamente buscar los nuevos parches, al menos cada mes.

- En el uso y configuración de un producto:
 - Casi todos los programas vienen de fabrica con todas sus características y opciones preparadas que sea fácil instalar.
 - Muchas de las opciones de seguridad vienen apagadas.
 - Se volverá una regla que cada ocasión que se instale una computadora, habrá que configurarla.

Añadir a la lista de chequeo revisiones para:

- Establecer una guía de instalación y configuración para todas las computadoras.
- Quitar a los sistemas herramientas que no se necesitan.
- Hacer un inventario de hardware de cada computadora
- Reunir en un solo lugar copias de los discos de instalación, controladores, números de serie y copias de las licencias.

Para windows:

- Establecer cuentas de usuario
- Activar actualizaciones automáticas
- Eliminar programas de autoinicio

- Comunicaciones (Red local)

- La red local (cableada) tiene que tener una configuración que cubra las necesidades de todos los usuarios y los programas que se usan.
- La velocidad de la red debe ser la óptima, la más común y barata es una “red switchheada de 100mbps”. (5-25 usuarios que usan internet, comparten carpetas e impresoras, y accesan a base de datos)
- Entre más usuarios hay que crecer la red (gigabit y ruteo) cuando es grande la red se debe de manejar un concepto de cableado estructurado.

Añadir a la lista de chequeo revisiones para:

- Establecer direccionamiento de red estáticos
- Establecimiento formal de nombramiento y dominios de red
- Configuración de cuentas de usuario en el dominio de red.
- Revisar las capacidades del equipo activo de red.
- Crear diagramas conceptuales de la red
- Establecer etiquetado de los cables de red.

- Comunicaciones (Red inalámbrica)
 - Las redes inalámbricas son cómodas y funcionales, pero no es una regla que tenga que haber una siempre.
 - Si se va a introducir una a la empresa, hay que considerar sus implicaciones.
 - El principal cuidado de una red inalámbrica es su acceso y alcance (50 mts en interiores , 100mts o más en exteriores).
 - Es obligatorio usar una clave de acceso para la red.

Añadir a la lista de chequeo revisiones para:

- Establecer una clave de acceso a la red de tipo WPA/WPA2. Si es necesario, hay que usar otro punto de acceso.
- Si no se va a utilizar la red inalámbrica, hay que apagar el servicio.
- Configurar manualmente las computadoras que se conectarán a la red inalámbrica.
- Establecer direcciones estáticas a la red inalámbrica y deshabilitar el DHCP.
- Cambiar la clave de acceso a la administración de la red inalámbrica.

- Comunicaciones (Acceso a internet)
 - Internet = conectividad para todos, en ambos sentidos.
 - Tiene que haber una segmentación entre la red local y el internet. Que los usuarios puedan salir, pero que nadie pueda entrar desde el exterior.
 - Se estudia cuando el internet es una necesidad para el negocio y cuando se vuelve un medio de entretenimiento/ocio.

Añadir a la lista de chequeo revisiones para:

- Presencia y configuración del router de internet.
- Activación y endurecimiento del firewall de red.
- Cambiar la clave de acceso del router de internet.
- Evaluar la necesidad de otros programas de control de acceso a sitios en internet.
- Crear un reglamento de uso de internet para la empresa.
- Revisar periódicamente la presencia de programas que degraden la calidad de la conexión de internet: (P2P, toolbars, etc...)

De origen humano

- Virus y gusanos
 - Código Malicioso: software programado para una acción hostil. Existen para todo tipo de sistemas.
 - Existen miles de gusanos, desde los muy peligrosos hasta los muy molestos. Siempre habrá uno nuevo cada día.
 - Son el problema crónico, que aumenta de probabilidad de impacto conforme el usuario usa internet.

Añadir a la lista de chequeo revisiones para:

- Revisar que cada computadora tenga un antivirus con suscripción. No piratas.
- Verificación de que el antivirus se encuentra con acceso a actualizaciones automatizadas.
- Ver si la empresa requiere un antivirus simple o una suite de protección.
- Programas revisiones completas del sistema de forma semanal.
- Establecer un procedimiento de recolección de reportes del antivirus y analizarlos.
- Establecer una política de revisar discos que provengan una red externa.
- En las políticas de seguridad de la empresa, el alcance puede incluir las computadoras caseras de cada persona.
- Definir que computadoras importantes tengan prohibido sean usadas de forma personal

- Los códigos maliciosos se combaten conociendo los tipos que hay:
 - *Virus*: con un programa antivirus.
 - *Gusanos*: con parches de software al día y oportunamente.
 - *Spyware y addware*: con un antispyware o cambiando los programas de acceso a internet (navegador y correo)
 - *Caballos de troya*: Cambiando la cuenta de usuario a una cuenta sin privilegios de administrador.
 - *Puertas traseras*: con un firewall.
 - *Programas de hacking*: educar a las personas que no jueguen al hacker en la red, consulten a un experto.
- Formatear una computadora no es una garantía de que el virus se elimine.
- Se puede quitar un virus sin necesidad de formatear.

- El hacker en internet

- Existen siempre personas buscando objetivos de oportunidad.
- Se aprovecharan de un error nuestro al cubrir los puntos esenciales (siempre los encuentran):
 - Parches de software, firewall de la red, errores de configuración.
- La detección y reacción con prontitud ante la emergencia reducirá el impacto y el daño.

Añadir a la lista de chequeo revisiones para:

- Enseñar a los usuarios a establecer contraseñas resistentes
Mala contraseña: secreto Buena contraseña: S3cr3t0
- Establecer la costumbre en los usuarios para cambiar la contraseña cada 2 o 4 semanas
- Hacer un listado de cuentas de correo, bancos, sistemas que usa la empresa.
- Hacer un reglamento de uso de cuentas: Quién. Cuándo y dónde se usan.
- Establecer un procedimiento de vigilancia y reporte de actividades en cuentas.
- Realizar una lista de puntos de contacto, telefonos y procedimientos en caso de emergencia con un banco así como de autoridades y policía.
- Establecer un proceso de manejo de emergencia, no entrar en pánico.

- El criminal cibernético
 - Van en aumento y cada vez son más ingeniosos y agresivos.
 - Su principal herramienta es el engaño y la decepción:
 - Para lograr que descargues y ejecutes un programa.
 - Para llevarte a que escribas información en una página.
 - No siempre es dinero lo que buscan.
 - Un poco de saludable desconfianza es la mejor consejera. Nadie es lo que dice ser en internet.

Añadir a la lista de chequeo revisiones para:

- Crear cuentas de correo personales y otras para uso de la empresa.
- Enseñar a el usuario a nunca abrir archivos adjuntos en un correo, aunque provengan de un amigo.
- El establecimiento de un sistema de correo propio de la empresa elimina riesgos al usar servicios de cuentas de correo gratuitos.
- Acostumbrar a los usuarios a usar la computadora con una cuenta de usuario que sin privilegios de administrador.

Añadir a la lista de chequeo revisiones para:

- Verificar y analizar en conjunto cualquier acción que se pida hacer desde una aparente empresa o autoridad externa, no importando que tan urgente se oiga.
- Enseñar a los usuarios a NO participar en reenvíos de cadenas de correos.
- Diseñar y Publicar un reglamento de uso de las computadoras.
- Establecer un programa periódico de capacitación y concientización sobre el uso de internet.
- Pláticas y mesas redondas para comentar acontecimientos o temas.
- Enseñar al personal a reconocer los tipos de fraudes que existen y como los realizan.
- Invitar al personal a participar en foros de seguridad y atender eventos.
- Establecer en la empresa un proceso para el manejo de desechos:
 - En papeles revisar que tipo de información contienen antes de tirar.
 - En discos, que no se arrojen a la basura sin antes haberlos destruido
 - En computadoras, no deshacerse de ellas hasta que se limpien los discos.
- Evaluar la necesidad de que una computadora portátil requiera protección adicional de la información en caso de extravío.

El uso del dinero electrónico

- Las tarjetas y movimientos por internet son el principal objetivo de muchos de los criminales cibernéticos.
- En el uso de las tarjetas en cajeros: Revisar si el cajero tiene algún daño de cualquier tipo, y no aceptar ayuda de extraños, por mas convincentes.
- Movimientos de dinero en internet: hacerlo desde una computadora confiable. Si no se puede proteger toda la empresa, invertir en construir una computadora “tanque” de alta resistencia.

El phishing

- Engañar al usuario para visitar un sitio falso e introduzca sus claves como si lo realizara en el sitio real.
- Usan complejos mecanismos para ocultar lo que sucede realmente.
- Una protección simple: recordar que nadie es lo que dice ser en internet.
- No confiar el programas y archivos que nos manden, incluso si provienen de un conocido.

BancaNet se renueva constantemente incluyendo nuevas funcionalidades y servicios, modernizando la operación en su conjunto. A tal efecto y para continuar teniendo acceso a toda la gama de servicios que te ofrecemos, es necesario que aceptes el nuevo Clausulado del Contrato de Prestación de Servicios.

Recuerda que BancaNet te permite administrar tus finanzas personales de forma fácil, rápida y segura en cualquier momento y sin importar donde te encuentres..

Actualmente, disfrutas este conjunto de beneficios pagando comisiones por algunas transacciones. A partir de Mayo de 2006, buscando mejores opciones de pago para tus necesidades, Banamex pone a tu disposición dos esquemas alternativos de pago por el servicio, de los cuales debes elegir uno. Por lo tanto le pedimos que ingrese a su cuenta seleccionando la que a usted le corresponda haciendo click en uno de los siguientes links. Una vez en su cuenta seleccione el metodo de pago que mas le acomode.

BancaNet**BancaNet**
Empresarial**BancaNet**
Corresponsales

Banamex pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la ultima tecnología en protección y encriptación de datos.
Una vez mas Banamex líder en el ramo.

Le recordamos que últimamente se envían e-mails de falsa procedencia con fines fraudulentos y lucrativos. Por favor nunca ponga los datos de su tarjeta bancaria en un mail y siempre compruebe que la procedencia del mail es de @banamex.com

**Justificación y
Sentido de urgencia**

**Instrucciones
para usar el
sitio falso**

**Enlaces a sitios falsos,
ocultan el verdadero
destino del enlace**

**Mensajes para convencer
que el correo es serio**

**Teléfonos y correos
del defraudador, para
en caso de que la víctima
trate de verificar el correo,**

Amenazas en el Interior

- Las más peligrosas y dañinas.
- Siempre tienen una gran probabilidad de presentarse.
- El atacante tiene una ventaja única, normalmente nadie lo esperaba.
- Dos tipos
 - Accidentales
 - Intencionales

Accidentes internos

- Situaciones triviales o excepcionales que pueden tener grandes consecuencias.
- El proceso de copias de respaldo es la última opción para no perder información.

Añadir a la lista de chequeo revisiones para:

- El proceso de respaldo de información tiene que estar documentado
- Acostumbrar a todos los operadores y guardianes de información a crear copias
- Programar que las copias se realicen periódicamente, con mayor frecuencia los sistemas de mayor uso e importancia.
- Establecer un servidor remoto de almacenamiento de información.
- Evaluar la necesidad de establecer un servicio de almacenamiento de información fuera de sitio.

Seguridad física

- Casi todas los mecanismos de protección contra ataques cibernéticos son inefectivos cuando un intruso tiene acceso directo a la computadora.
- A este nivel solo la criptografía puede brindar la protección suficiente para asegurar la confidencialidad.

Añadir a la lista de chequeo revisiones para:

- Consideraciones de seguridad física: puertas, barreras, trampas, candados.
- Vigilancia presencial o de circuito cerrado de televisión.
- Mecanismos de control de acceso: tarjetas, huellas digitales, biometricos, etc..
- Evaluar si una computadora o servidor se le pueden extraer unidades de disco o desactivar interfaces USB, ratón y teclado si no se va a usar directamente.

Amenazas intencionales

- La ingeniería social
 - Usar artimañas para convencer a la persona para realizar una actividad que el atacante requiere.
 - El ataque más sutil es el “por favor” y por la puerta de enfrente. Los hacks más famosos han sido de esta manera.
 - Definir claramente cuál es la información de la empresa y personal que nunca debe de comunicarse bajo cualquier motivo. Enseñar a las personas a desconfiar de la gente.

Añadir a la lista de chequeo revisiones para:

- Definir tareas que requieran un proceso de “autorización por pares”, que otra persona confirme, revise, autorize una operación.
- Establecer procesos de levantamiento de registros de actividad, de acceso, de uso, etc.
- Recopilar y analizar las bitácoras periódicamente.
- Establecer sistemas de credencialización y control de acceso a áreas de la empresa.

Los empleados descontentos

- Amenaza latente y de gran potencial dañino.
 - Sabotaje interno por diversos motivos personales.
 - Espionaje corporativo por algún soborno.
 - Acoso entre empleados
 - Robos y fraudes de oportunidad.
- Todos se mantendrán a raya si saben que son vigilados.

Añadir a la lista de chequeo revisiones para:

- Definir la política de vigilancia y monitoreo de personas, accesos, internet, etc..
- Es ilegal invadir la privacidad de la persona aún dentro del trabajo, a menos que previamente se le haya informado sobre la existencia de medidas de vigilancia, su funcionamiento de acuerdo a un reglamento y obtenido el consentimiento.
- La empresa adquiere la responsabilidad de no difundir la información que recolecte sobre las personas que tienen contacto con ella.

Definición de funciones

- Principio de separación de responsabilidades
 - Que una función importante no quede a cargo de una sola persona o que no tenga todas las llaves necesarias
- Principio del menor privilegio posible
 - Dar a cada persona solo lo necesario para cumplir con su labor
- Principio de rotación de personal
 - Procurar rotar periódicamente al personal de funciones, sobre todo en las de recursos valiables.
 - No necesariamente tiene que ser personal nuevo.

Recursos humanos

- Al contratar personal
 - Análisis de antecedentes
 - Firmas de cartas de no divulgación y confidencialidad.
 - Acuerdo de apego a reglamentos internos.
- Al cesar personal
 - No informar su baja hasta que se hayan obtenido claves de acceso a sistemas y cambiado/eliminado
 - Retirar completamente sus credenciales de acceso.
 - Auditar el sistema que usaba por cualquier anomalía.
 - Reiterar sus compromisos de confidencialidad.

Ejercicio 4

- Para cada uno de los 5 activos que se han trabajado se le hará una lista de las amenazas que tienen probabilidad de impacto.
- Se mencionarán todas las posibles amenazas, y después se describe cuales son las que tienen una probabilidad alta, media o baja.
- No se debe descartar ninguna por más trivial que parezca.

¿Y ahora que sigue?

- La elaboración de una lista de activos brindará una mejor comprensión de lo que hay que proteger.
- La elaboración de la lista de amenazas presentará el nivel de riesgo de cada activo.
- Se puede ya a comenzar a establecer mecanismos de protección para los activos más importantes, empezando por sus amenazas más probables.

¿Porqué tanto trabajo?

- La seguridad es un proceso de calidad.
- La documentación de las cosas es para establecer control y métricas. No se puede mejorar lo que no se puede medir.
- Que no te digan y no te cuenten que es lo que se hace en tu empresa.
- Si se deja que la seguridad se quede en la parte exclusivamente técnica, no se podrán atacar los problemas de raíz.
- No necesitas ser un técnico experimentado para crear un buen proceso de seguridad.

¿Preguntas?

GREX Tecnologías de Información

MC. Helios Mier

helios.mier [en] grex.com.mx

Creative Commons 2.0: Atribución
Algunos derechos reservados, México 2008