En definitiva, las amenazas hechas realidad pueden llegar a afectar los datos, en las personas, en los programas, en los equipos, en la red y algunas veces, simultáneamente en varios de ellos, como puede ser un incendio.

Podríamos hacernos una pregunta realmente difícil: ¿qué es lo más crítico que debería protegerse? La respuesta de la mayoría, probablemente, sería que las personas resultan el punto más crítico y el valor de una vida humana no se puede comparar con las computadoras, las aplicaciones o los datos de cualquier entidad. Ahora bien, por otra parte, podemos determinar que los datos son aún más críticos si nos centramos en la continuidad de la entidad.

Como consecuencia de cualquier incidencia, se pueden producir unas pérdidas que pueden ser no sólo directas (comúnmente que son cubiertas por los seguros) más fácilmente, sino también indirectas, como la no recuperación de deudas al perder los datos, o no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información.

Sabemos que se producen casos similares en gran parte de entidades, pero en general no conocemos a cuáles han afectado (o lo sabemos pero no podemos difundirlo), porque por imagen estos no se hacen públicos y el hecho de que se conozcan muchos más referidos a Estados Unidos y a otros puntos lejanos que respecto de nuestros países no significa que estemos a salvo, sino que nuestro pudor es mayor y los ocultamos siempre que podemos.

NIVELES DE TRABAJO

- Confidencialidad
- Integridad
- Autenticidad
- No Repudio
- Disponibilidad de los recursos y de la información
- Consistencia
- Control de Acceso
- Auditoría

Confidencialidad

Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

Integridad

Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:

· Causadas por errores de hardware y/o software.

· Causadas de forma intencional.

· Causadas de forma accidental

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

Autenticidad

En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

No – repudio

Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

Disponibilidad de los recursos y de la información

De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

Consistencia

Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

Control de acceso a los recursos

Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

Auditoría

Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

En cuanto a los dos últimos puntos resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre "espiar" y "monitorear" a los mismos. La ética es algo que todo buen administrador debe conocer y poseer.

Finalmente, todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios. De esta manera, es posible sentar de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios conozcan sus derechos y obligaciones (es decir, las políticas), de tal forma que no se sientan agredidos por los procedimientos organizacionales.

Algoritmo

Cuando se piensa establecer una estrategia de seguridad, la pregunta que se realiza, en primera instancia, es: ¿en qué baso mi estrategia?. La respuesta a esta pregunta es bien simple. El algoritmo Productor/Consumidor.

En este algoritmo, hay dos grandes entidades: una que es la encargada de producir la información; la otra entidad es el consumidor de esta información y otra, llamada precisamente "otros". Entre el productor y el consumidor, se define una relación que tiene como objetivo una transferencia de "algo" entre ambos, sin otra cosa que intervenga en el proceso. Si esto se logra llevar a cabo y se mantiene a lo largo del tiempo, se estará en presencia de un sistema seguro.

LEER

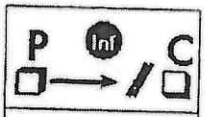
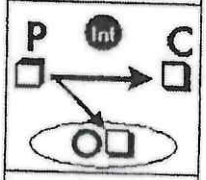
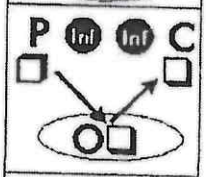
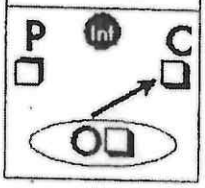
En la realidad, existen entidades y/o eventos que provocan alteraciones a este modelo. ***El estudio de la seguridad, en pocas palabras, se basa en la determinación, análisis y soluciones de las alteraciones a este modelo.***

En una observación y planteo del modelo, determinamos que sólo existen cuatro tipos de alteraciones en la relación producción-consumidor (ver el gráfico del algoritmo)

Antes de pasar a explicar estos casos, habrá que definir el concepto de "recurso".

Algoritmo del Productor - Consumidor de Información

Metas de Seguridad

1 - Interrupción	Disponibilidad	
2 - Intercepción	Privacidad	
3 - Modificación	Integridad	
4 - Producción	Integridad	

Recurso, está definido en el diccionario Espasa Calpe como "bienes, medios de subsistencia".

Esta es una definición muy general. De todas maneras, resulta conveniente para nuestra tarea. Podemos mencionar como recurso a cualquier cosa, ya sean bienes específicos o que permitan la subsistencia de la organización como tal.

Debido a ello, es que podemos diferenciar claramente tres tipos de recursos:

· Físicos

· Lógicos

· Servicios.

Los recursos físicos son, por ejemplo, las impresoras, los servidores de archivos, los routers, etc.

Los recursos lógicos son, por ejemplo, las bases de datos de las cuales sacamos la información que permite trabajar en la organización.

Los servicios son, por ejemplo, el servicio de correo electrónico, de página WEB, etc.

Todas las acciones correctivas que se lleven a cabo con el fin de respetar el modelo estarán orientadas a atacar uno de los cuatro casos. Explicaremos y daremos ejemplos de cada uno de ellos.

El caso número uno es el de **Interrupción**. Este caso afecta la disponibilidad del recurso (tener en cuenta la definición de recurso: físico, lógico y servicio).

Por ejemplo:

Recurso afectado	Nombre	Causa	Efecto
Servicio	Correo electrónico	Alguien dio de baja el servidor (por algún método)	No poder enviar mail
Físico	Impresora	Falta de alimentación eléctrica.	No imprime

El segundo caso es el de **Intercepción**, en el cual se pone en riesgo la privacidad de los datos.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Datos sobre cuentas en el banco	Se ha puesto un dispositivo que permite monitorear los paquetes en la red y sacar información de ellos	Conseguir datos privados sobre montos de cuentas corrientes
Servicio	Correo electrónico	Se ha implantado un programa que duplica los mensajes (mails) que salen de una sección y los envía a una dirección.	Leer información

El tercer caso, **Modificación** afecta directamente la integridad de los datos que le llegan al consumidor.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Base de datos de pagos en cuentas corrientes	Se ha implantado un programa que redondea en menos los pagos y carga éstos redondeos a una cuenta corriente	Incrementar el crédito de una cuenta corriente en base al redondeo realizado en los pagos
Servicio	Servidor de página WEB	Alguien logró ingresar como WEBMASTER y ha cambiado los contenidos de la página	Los datos mostrados en la página no son los reales

El cuarto y último caso es el de la **producción impropia de información**. En éste, la información que recibe el consumidor es directamente falaz.

Recurso afectado	Nombre	Causa	Efecto
Lógico	Datos de deudores	Se ha generado una base de datos falsa, la que ante el pedido de informes, responde ella con sus datos	Hacer pasar a los deudores como que no lo son
Servicio	Servidor WEB	Alguien se ha apropiado del password del WEBMASTER y, modificando el direccionamiento, logra que se cargue otra página WEB	Redireccionar la página WEB hacia otro sitio

Una vez que estamos enterados de que hay sólo cuatro posibles casos de causas posibles de problemas, ¿qué se hace?. Hay que identificar los recursos dentro de la organización.

¿Cómo establecer los niveles de riesgo de los recursos involucrados?

Al crear una política de seguridad de red, es importante entender que la razón para crear tal política es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son costeables. Esto significa que se debe entender cuáles recursos de la red vale la pena proteger y que algunos recursos son más importantes que otros. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. A pesar de la cantidad de publicidad sobre intrusos en una red, varias encuestas indican que para la mayoría de las organizaciones, la pérdida real que proviene de los "miembros internos" es mucho mayor (tal cual se ha explicado anteriormente).

El análisis de riesgos implica determinar lo siguiente:

- Qué se necesita proteger
- De quién protegerlo

· Cómo protegerlo

Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

En el análisis de los riesgos, es necesario determinar los siguientes factores:

· Estimación del riesgo de pérdida del recurso (lo llamaremos **Ri**)

· Estimación de la importancia del recurso (lo llamaremos **Wi**)

Como un paso hacia la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico. Por ejemplo, al riesgo (**Ri**) de perder un recurso, se le asigna un valor de cero a diez, donde cero, significa que no hay riesgo y diez es el riesgo más alto. De manera similar, a la importancia de un recurso (**Wi**) también se le puede asignar un valor de cero a diez, donde cero significa que no tiene importancia y diez es la importancia más alta. La evaluación general del riesgo será entonces el producto del valor del riesgo y su importancia (también llamado el peso). Esto puede escribirse como:

WRi = Ri *Wi

Dónde:

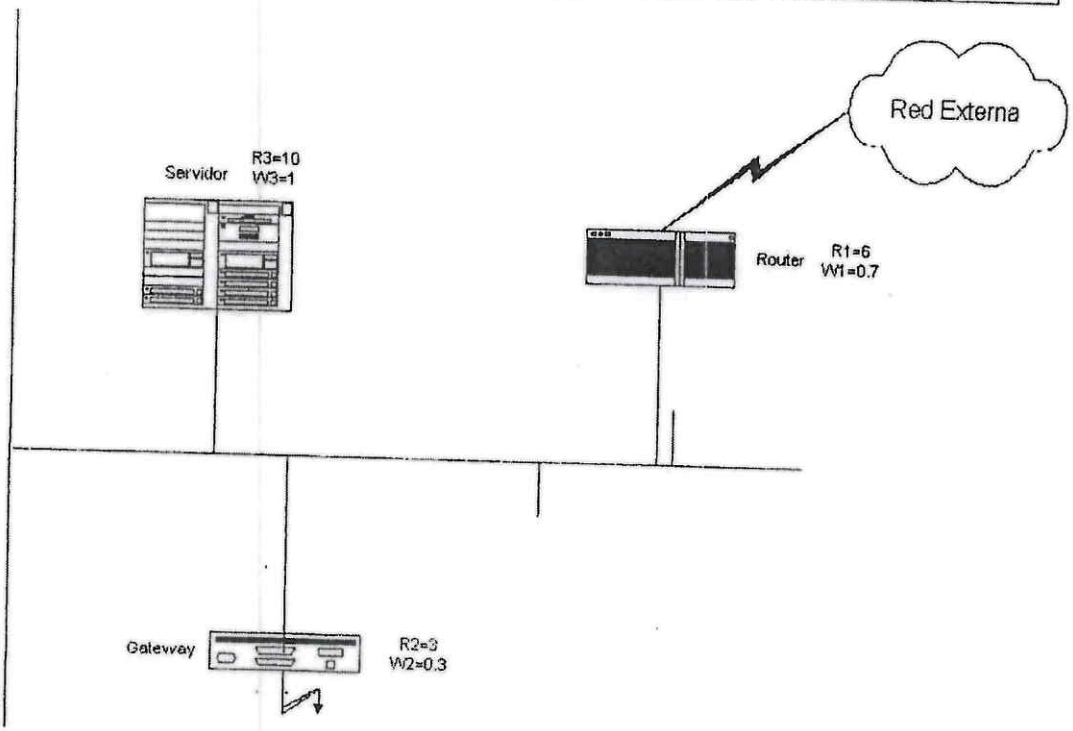
WRi: es el peso del riesgo del recurso "i" (también lo podemos llamar ponderación)

Ri: es el riesgo del recurso "i"

Wi: es la importancia del recurso "i"

Ejemplo práctico

Supongamos una red simplificada con un router, un servidor y un bridge.



Los administradores de la red y de sistemas han producido las estimaciones siguientes para el riesgo y la importancia de cada uno de los dispositivos que forman nuestra red:

Como se ve, a cada uno de los componentes del sistema, se le ha asignado un cierto riesgo y una cierta importancia. Hay que destacar que estos valores son totalmente subjetivos, dependen exclusivamente de quien o quienes están realizando la evaluación.

Tenemos, entonces:

Router:

R1 = 6
W1 = 7

Bridge:

R2 = 6
W2 = 3

Servidor:

R3 = 10
W3 = 10
El cálculo de los riesgos evaluados, será, para cada dispositivo:

Router:

WR1 = **R1** * **W1** = 6 * 7 = 42

Bridge:

WR2 = **R2** * **W2** = 6 * 3 = 1.8

Servidor:

WR3 = **R3** * **W3** = 10 * 10 = 100

La tabla que sigue a continuación, nos muestra cómo podríamos llevar a cabo esta tarea de una manera ordenada y los valores que contiene son los que hemos tratado:

Recurso del sistema		Riesgo (Ri)	Importancia (Wi)	Riesgo Evaluado (Ri * Wi)
Número	Nombre			
1	Router	6	7	42
2	Bridge	6	3	18
3	Servidor	10	10	100

Vemos que, en este caso, el recurso que debemos proteger más es el Servidor ya que su riesgo ponderado es muy alto. Por tanto, comenzaremos por buscar las probables causas que pueden provocar problemas con los servicios brindados por él.

Hay que tener muy en cuenta que, al realizar el análisis de riesgo, se deben identificar **todos** los recursos (por más triviales que parezcan) cuya seguridad está en riesgo de ser quebrantada.

Ahora bien, ¿cuáles son los recursos?

Los recursos que deben ser considerados al estimar las amenazas a la seguridad son solamente seis:

Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.

Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Datos: durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, en tránsito sobre medios de comunicación.

Gente: usuarios, personas para operar los sistemas.

Documentación: sobre programas, hardware, sistemas, procedimientos administrativos locales.

Accesorios: papel, formularios, cintas, información grabada.

La pregunta que cabe formular, luego de haber hecho el trabajo anterior, es cómo protegemos ahora nuestros recursos. Tal vez, ésta sea la pregunta más difícil de responder, pues, según el recurso del que se trate, será el modo de protegerlo.

Primero, deberemos tener en cuenta qué es lo queremos proteger. Si se trata de los problemas ocasionados por el personal propio o de intromisiones clandestinas que puedan afectar la operatoria de la organización.

Hay que tener en cuenta, que todos los estudios realizados demuestran que el **80%** de los problemas proceden de los llamados "clientes internos" de la organización (los empleados o elementos que se desempeñan en la organización), y sólo el **20 %** restante, proviene de elementos externos a la organización.

Una aproximación acerca de cómo proteger los recursos de los problemas originados por el cliente interno consiste en la identificación del uso correcto de los mismos por parte de éstos.

Pero primero, deberemos saber quiénes son los que van a hacer uso de los recursos. Es decir se debe contar, previamente, con un conocimiento cabal de todos los usuarios que tenemos en el sistema. Esta lista no es obligatoriamente individual, sino que puede ser, en efecto, una lista por grupos de usuarios y sus necesidades en el sistema. Esta es, con seguridad, la práctica más extendida pues, definida la necesidad de un grupo de usuarios, lo más efectivo es englobarlos a todos en un mismo grupo.

Una vez identificados los usuarios (o grupos de usuarios), se puede realizar la determinación de los recursos de que harán uso y de los permisos que tendrán.

Esto es sencillo de realizar con una tabla como la siguiente:

Recurso del sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	Nombre			
1	Base Datos Cuentas Corrientes	Grupo de auditores	Local	Lectura
2	Router 2500	Grupo de mantenimiento de comunicaciones	Local y remoto	Lectura y escritura

Este modelo, nos permitirá disponer para cada usuario (o grupos de usuarios), la información de qué se les está permitido hacer y qué no.

El otro problema que nos presentamos, es el de las intromisiones clandestinas.

Aquí, es preciso tener en cuenta el tipo de recurso a proteger. En base a ello, estará dada la política de seguridad.

Daremos, a continuación, algunos ejemplos acerca de a qué nos estamos enfrentando:

· ¿Cómo aseguramos que no están ingresando a nuestro sistema por un puerto desprotegido o mal configurado?

· ¿Cómo nos aseguramos de que no se estén usando programas propios del sistema operativo o aplicaciones para ingresar al sistema en forma clandestina?

· ¿Cómo aseguramos de que, ante un corte de energía eléctrica, el sistema seguirá funcionando?

· ¿Cómo nos aseguramos de que los medios de transmisión de información no son susceptibles de ser monitoreados?

· ¿Cómo actúa la organización frente al alejamiento de uno de sus integrantes?

La respuesta a estos interrogantes reside en la posibilidad de conseguir dicha seguridad por medio de herramientas de control y seguimiento de accesos, utilizando check-lists para comprobar puntos importantes en la configuración y/o

funcionamiento de los sistemas y por medio de procedimientos que hacen frente a las distintas situaciones.

Es muy aconsejable que se disponga de una agenda con las tareas que se deben llevar a cabo regularmente, a fin de que el seguimiento de los datos obtenidos sea efectivo y se puedan realizar comparaciones válidas al contar con datos secuenciales.

Esta agenda, podría ser en sí misma un procedimiento.

Damos, a continuación, un ejemplo de procedimiento de chequeo de eventos en el sistema:

Diariamente:

· Extraer un logístico sobre el volumen de correo transportado. Extraer un logístico sobre las conexiones de red levantadas en las últimas 24 horas.

Semanalmente:

· Extraer un logístico sobre los ingresos desde el exterior a la red interna.

· Extraer un logístico con las conexiones externas realizadas desde nuestra red.

· Obtener un logístico sobre los downloads de archivos realizados y quién los realizó.

· Obtener gráficos sobre tráfico en la red.

· Obtener logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino).

Mensualmente:

· Realizar un seguimiento de todos los archivos logísticos a fin de detectar cambios (realizados con los archivos de back-up del mes anterior).

Cabría resaltar que, en gran parte, este procedimiento puede ser automatizado por medio de programas que realicen las tareas y sólo informen de las desviaciones con respecto a las reglas dadas.

ACERCA DE LOS PROCEDIMIENTOS

Si se piensa certificar ISO, es indispensable tener un manual de procedimientos escrito y llevarlo a cabo al pie de la letra. De esta manera, cabría pensar que un manual de procedimientos es un paso adelante para poder llegar a la certificación ISO.

Procedimiento de alta de cuenta de usuario

Cuando un elemento de la organización requiere una cuenta de operación en el sistema, debe llenar un formulario que contenga, al menos los siguientes datos:

· Nombre y Apellido

· Puesto de trabajo

· Jefe inmediato superior que avale el pedido

· Descripción de los trabajos que debe realizar en el sistema

· Consentimiento de que sus actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las normas de "buen uso de los recursos" (para lo cual, se le debe dar una copia de tales normas).

· Explicaciones breves, pero claras de cómo elegir su password.

Asimismo, este formulario debe tener otros elementos que conciernen a la parte de ejecución del área encargada de dar de alta la cuenta, datos como:

· Tipo de cuenta

· Fecha de caducidad

· Fecha de expiración

· Datos referentes a los permisos de acceso (por ejemplo, tipos de permisos a los diferentes directorios y/o archivos)

Si tiene o no restricciones horarias para el uso de algunos recursos y/o para el ingreso al sistema.

Procedimiento de baja de cuenta de usuario

Este procedimiento es el que se lleva a cabo cuando se aleja un elemento de la organización o cuando alguien deja de trabajar por un determinado tiempo (licencia sin goce de sueldo, vacaciones, viajes prolongados, etc.). En base a la explicación anterior hay, entonces, dos tipos de alejamientos: permanente y parcial.

Aquí, es necesario definir un circuito administrativo a seguir, y que como todos los componentes de la política de seguridad, debe estar fuertemente apoyado por la parte gerencial de la organización.

Un ejemplo de este circuito, podría ser: ante el alejamiento de un elemento de la organización, la gerencia de personal (o la sección encargada de la administración de los RRHH), debe informar en un formulario de "Alejamiento de personal", todos los datos del individuo que ha dejado la organización, así como de la posición que éste ocupaba y el tipo de alejamiento (permanente o no).Una vez llegada la información al departamento encargado de la administración de sistemas, se utiliza para dar de baja o inhabilitar la cuenta del usuario.

La definición de si se da de baja o se inhabilita es algo importante pues, si se da de baja, se deberían guardar y eliminar los archivos y directorios del usuario, mientras que si sólo se inhabilita, no pasa de esa acción. Si el alejamiento del individuo no era permanente, al volver a la organización, la sección que había informado anteriormente de la ausencia, debe comunicar su regreso, por medio de un formulario dando cuenta de tal hecho para volver a habilitar la cuenta al individuo.

Procedimiento para determinar las buenas passwords

Aunque no lo parezca, la verificación de palabras claves efectivas no es algo frecuente en casi ninguna organización. El procedimiento debe explicar las normas para elegir una password:

Se debe explicitar

· La cantidad de caracteres mínimo que debe tener,

· No tiene que tener relación directa con las características del usuario.

· Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.

· Determinar, si es posible, el seguimiento de las palabras claves (llevar registros de las palabras claves anteriores elegidas por el usuario).

Una vez que el usuario ha elegido su password, se le debe correr un "programa crackeador" para tener idea de cuán segura es, en base al tiempo que tarda en romper la palabra.

Procedimientos de verificación de accesos

Debe explicar la forma de realizar las auditorías de los archivos logísticos de ingresos a fin de detectar actividades anómalas. También debe detectar el tiempo entre la auditoría y cómo actuar en caso de detectar desviaciones.

Normalmente, este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar. Escanean archivos de "log" con diferentes fechas tomando en cuenta las reglas que se le han dado. Ante la detección de un desvío, generan reportes informando el mismo.

En el procedimiento debe quedar perfectamente indicado quién es el responsable del mantenimiento de estos programas y cómo se actúa cuando se generan alarmas.

Procedimiento para el chequeo del tráfico de la red

Permite conocer el comportamiento del tráfico en la red, al detectar variaciones que pueden ser síntoma de mal uso de la misma.

El procedimiento debe indicar el/los programas que se ejecuten, con qué intervalos, con qué reglas de trabajo, quién se encarga de procesar y/o monitorear los datos generados por ellos y cómo se actúa en consecuencia.

Procedimiento para el monitoreo de los volúmenes de correo

Este procedimiento permite conocer los volúmenes del tráfico de correo o la cantidad de "mails" en tránsito. Dicho procedimiento se encuentra realizado por programas que llevan las estadísticas, generando reportes con la información pedida. El conocimiento de esta información permite conocer, entre otras cosas, el uso de los medios de comunicación, y si el servidor está siendo objeto de un **"spam"**.

Como en los casos anteriores, en el procedimiento debe estar explicitado quién es el encargado del mantenimiento y del análisis de los datos generados, y qué hacer cuando se detectan variaciones.

Procedimientos para el monitoreo de conexiones activas

Este procedimiento se efectúa con el objeto de prevenir que algún usuario deje su terminal abierta y sea posible que alguien use su cuenta. El procedimiento es ejecutado por medio de programas que monitorean la actividad de las conexiones de usuarios.

Cuando detecta que una terminal tiene cierto tiempo inactiva, cierra la conexión y genera un log con el acontecimiento.

Procedimiento de modificación de archivos

Este procedimiento sirve para detectar la modificación no autorizada y la integridad de los archivos y, en muchos casos, permite la traza de las modificaciones realizadas. Al igual que en los casos anteriores, debe estar bien determinada la responsabilidad de quién es el encargado del seguimiento y de actuar en caso de alarmas.

Procedimientos para el resguardo de copias de seguridad

Este procedimiento debe indicar claramente dónde se deben guardar las copias de seguridad y los pasos a seguir en caso de problemas. Para lograr esto, deben estar identificados los roles de las personas que interactúan con el área, a fin de que cada uno sepa qué hacer ante la aparición de problemas.

Procedimientos para la verificación de las máquinas de los usuarios

Este procedimiento permitirá encontrar programas que no deberían estar en las máquinas de los usuarios y que, por su carácter, pueden traer problemas de licencias y fuente potencial de virus. El procedimiento debe explicitar los métodos que se van a utilizar para la verificación, las acciones ante los desvíos y quién/quiénes lo llevarán a cabo.

Procedimientos para el monitoreo de los puertos en la red

Este procedimiento permite saber qué puertos están habilitados en la red, y, en algunos casos, chequear la seguridad de los mismos. El procedimiento deberá describir qué programas se deben ejecutar, con qué reglas, quién estará a cargo de llevarlo a cabo y qué hacer ante las desviaciones detectadas.

Procedimientos de cómo dar a publicidad las nuevas normas de seguridad

Este tipo de procedimiento no siempre es tenido en cuenta. Sin embargo, en una organización es muy importante conocer las últimas modificaciones realizadas a

los procedimientos, de tal manera que nadie pueda poner cómo excusa "que no conocía las modificaciones". En él, debe describirse la forma de realizar la publicidad de las modificaciones: puede ser mediante un mailing, por exposición en transparencias, por notificación expresa, etc.; quién estará a cargo de la tarea y las atribuciones que tiene.

Es fundamental tener en cuenta este último punto ya que un porcentaje de los problemas de seguridad, según está demostrado en estudios de mercado, proviene del desconocimiento de las normas y/o modificaciones a ellas por parte de los usuarios.

Procedimientos para la determinación de identificación de usuario y grupo de pertenencia por defecto

Este procedimiento determina la forma de establecer las identificaciones y los grupos a los que pertenecerán los usuarios por defecto en el momento de darlos de alta. En él deben explicarse, concisamente, los pasos a seguir para cambiar los derechos y las identificaciones de los usuarios dados de alta y la manera de documentar los mismos, así también como quién será responsable de la tarea.

Procedimientos para recuperar información

Este procedimiento sirve para reconstruir todo el sistema o parte de él, a partir de las copias de seguridad. En él, deben explicarse todos los pasos a seguir para rearmar el sistema a partir de los back-up existentes, así como cada cuánto tiempo habría que llevarlos a cabo y quiénes son los responsables de dicha tarea.

Check-Lists

Las check-lists, como su nombre lo indica, son listas con un conjunto de ítems referentes a lo que habría que chequear en el funcionamiento del sistema.

Algunos ejemplos de check-lists:

· Asegurar el entorno. ¿Qué es necesario proteger? ¿Cuáles son los riesgos?

· Determinar prioridades para la seguridad y el uso de los recursos.

· Crear planes avanzados sobre qué hacer en una emergencia.

· Trabajar para educar a los usuarios del sistema sobre las necesidades y las ventajas de la buena seguridad

· Estar atentos a los incidentes inusuales y comportamientos extraños.

· Asegurarse de que cada persona utilice su propia cuenta.

· ¿Están las copias de seguridad bien resguardadas?

· No almacenar las copias de seguridad en el mismo sitio donde se las realiza

· ¿Los permisos básicos son de sólo lectura?

· Si se realizan copias de seguridad de directorios/archivos críticos, usar chequeo de comparación para detectar modificaciones no autorizadas.

· Periódicamente rever todo los archivos de "booteo de los sistemas y los archivos de configuración para detectar modificaciones y/o cambios en ellos.

· Tener sensores de humo y fuego en el cuarto de computadoras.

· Tener medios de extinción de fuego adecuados en el cuarto de computadoras.

· Entrenar a los usuarios sobre qué hacer cuando se disparan las alarmas.

· Instalar y limpiar regularmente filtros de aire en el cuarto de computadoras.

· Instalar UPS, filtros de línea, protectores gaseosos al menos en el cuarto de computadoras.

· Tener planes de recuperación de desastres.

· Considerar usar fibras ópticas como medio de transporte de información en la red.

· Nunca usar teclas de función programables en una terminal para almacenar información de login o password.

· Considerar realizar autolog de cuentas de usuario.

· Concientizar a los usuarios de pulsar la tecla ESCAPE antes de ingresar su login y su password, a fin de prevenir los "Caballos de Troya".

· Considerar la generación automática de password.

· Asegurarse de que cada cuenta tenga un password.

· No crear cuentas por defecto o "guest" para alguien que está temporariamente en la organización.

· No permitir que una sola cuenta esté compartida por un grupo de gente.

· Deshabilitar las cuentas de personas que se encuentren fuera de la organización por largo tiempo.

· Deshabilitar las cuentas "dormidas" por mucho tiempo.

· Deshabilitar o resguardar físicamente las bocas de conexión de red no usadas.

· Limitar el acceso físico a cables de red, routers, bocas, repetidores y terminadores.

· Los usuarios deben tener diferentes passwords sobre diferentes segmentos de la red.

· Monitorear regularmente la actividad sobre los gateways.