

Seguridad Informática



Por: Luis J. Buezo Bueno

Gerente de la Práctica de Seguridad de HP Consulting Iberia.

César Franco Ramos

Arquitecto de Soluciones de HP Consulting Iberia.

VISIÓN GENERAL

Actualmente están claros y argumentados los beneficios que los sistemas de información pueden aportar a cualquier organización o negocio. Pero no podemos olvidarnos de que los usuarios, como destinatarios finales, necesitan percibir un determinado nivel de confianza, en cuanto a los posibles riesgos que pueden estar incurriendo, para utilizar adecuadamente los sistemas de información disponibles. Un ejemplo claro, es el nivel de confianza que tiene que percibir un individuo para poder comprar un determinado artículo o servicio a través de Internet utilizando una tarjeta de crédito convencional.

La seguridad debe ser considerada como un habilitador de servicios de información debido a que dichos servicios no tendrán utilidad si no van acompañados con un nivel de seguridad adecuado que permita a un individuo poder confiar en la utilización del mismo.

Por lo tanto, la Gestión de la Seguridad, ha pasado de considerarse como un área de IT que ponía limitaciones y barreras a un aspecto crítico relacionado con el negocio que acompaña a cada servicio proporcionado por las nuevas tecnologías y que hace factible poder implantar nuevos servicios de manera adecuada.

Al igual que en la sociedad tradicional, dentro de los sistemas de información existen amenazas que afectan a activos críticos y por lo tanto existe un determinado nivel de riesgo. El poder lograr un nivel de riesgo cero es absolutamente imposible, no sólo porque el coste económico sería inabordable, sino también porque afectaría directamente a la adecuación de los servicios a las necesidades de negocio ó de los individuos.

Por lo tanto, la misión ahora es gestionar el adecuado nivel de riesgo, que una vez asumido y controlado, haga factible la implantación correcta de los diferentes servicios dentro de una organización o un negocio.

CONTEXTO ACTUAL

Basándonos en los datos de la encuesta del CSI/FBI del año 2004, el 92% de las empresas encuestadas reportaron incidentes de segu-

ridad en los últimos 12 meses. Los incidentes más típicos fueron por Virus, abusos internos de la infraestructura de comunicaciones, accesos internos no autorizados, y denegaciones de servicio. También se concluye que la gestión de la seguridad es de carácter reactivo, principalmente frente a incidentes, como constata el dato de que el 93% de de las actividades de "Patch Management" fueron a posteriori de una intrusión detectada. En el año 2003 se estimaron unas pérdidas ponderadas de 600.000 por encuestado debido a los incidentes de seguridad detectados.

En empresas analizadas no conocen formalmente el nivel de riesgo asumido dentro de la operativa de sus negocios y existe una sensación de que las inversiones de seguridad realizadas no mitigan los riesgos sobre los activos de la organización. Los empleados no "creen" en la seguridad ya que sin un plan de concienciación es prácticamente inviable implantar un programa de seguridad dentro de la organización. Se sigue trabajando en seguridad de forma reactiva; es

decir, se reacciona frente a un determinado incidente; es necesario que la seguridad sea un proceso continuo proactivo hacia la adaptación al nivel de riesgo deseado por parte del negocio.

Un aspecto muy peligroso, es que en muchos casos se delega la seguridad en el sentido común de los propios empleados. Está ampliamente demostrado que el sentido común no tiene porque estar alineado con la protección de los activos críticos de la compañía. Se ha detectado ausencia de homogeneización y estandarización en cuanto a tecnologías y procesos de seguridad que facilitarían una inversión eficiente y eficaz en seguridad.

Por último, a nivel organizativo, en muchos puestos de responsabilidad se es al mismo tiempo Juez y Parte para procesos críticos de la compañía. Es necesario implantar dentro del organigrama de roles y responsabilidades el principio de "Separación de Responsabilidades" incluso en el propio departamento de Seguridad Corporativo, ya que quien define las políticas y procesos de seguridad en la organización, no debe ser el mismo que las implante, las administre y las opere.

La seguridad necesita no sólo ser demostrada internamente, sino también externamente, ya que sobre ella se basa la confianza en el mundo de la empresa, afectando a todos sus activos.

La seguridad requiere tanto una metodología como una atención constante: es un proceso, no un producto. Necesita:

- Un presupuesto y unas contramedidas basadas en el coste de las pérdidas potenciales.
- Un objetivo claro, una política que permita conseguirlo, y una comunicación de los mismos a todos los niveles de la empresa.
- Un sistema de protección sencillo en su aplicación y predecible en sus resultados.
- Una filosofía que permita agregar nuevos elementos.
- Una evaluación continúa de los activos y los riesgos de la empresa.



La mayoría de los riesgos de seguridad no son técnicos, sino humanos: malos procesos, malentendidos, políticas de seguridad incorrectas (o inexistentes), mala gestión, desconocimiento y gente con malas intenciones.

Del lado de la técnica, los principales agujeros de seguridad suelen venir de la mano de malas implementaciones de los productos, de sistemas o software diseñados sin tener en cuenta la seguridad, o de productos que o bien no funcionan como se espera, o que sólo solucionan parte del problema. Los proveedores no suelen ayudar vendiendo continuamente "productos mágicos" para solucionar el "problema de la seguridad". Cada situación es diferente, y si existiera un producto o solución perfecta para el problema, ya habría sido adoptado por todo el mundo.

En estos casos, lo único que cuenta es la predictibilidad en el comportamiento de los sistemas y las personas, y esto suele (aunque no siempre), venir de la mano de la sencillez.

PRINCIPALES ERRORES DE SEGURIDAD

Por parte de los usuarios:

- Abrir archivos adjuntos en los correos electrónicos sin verificar su fuente y comprobar antes su contenido.
- No instalar los parches de seguridad correspondientes, principalmente en el caso de Microsoft Windows, Explorer y Office.
- Instalar salvapantallas, juegos o programas de fuentes desconocidas (generalmente descargados de Internet). ➔

- No realizar ni probar las copias de seguridad.
- No disponer de software antivirus y firewalls personales, o tenerlos desactualizados.
- Utilizar un modem u otro dispositivo para conectarse a un sistema externo mientras que se sigue conectado a la red de la empresa.

Por parte de los directivos:

- Asignar a gente sin preparación específica para gestionar la seguridad, y no proporcionarles ni la formación ni el tiempo necesario para que aprendan.
- No comprender la relación entre la seguridad de la información y el negocio – a diferencia con la seguridad física, no se prevén las consecuencias de una mala seguridad de la información.
- No tratar con los aspectos operacionales de la seguridad y así asegurar que los potenciales problemas no lleguen a ocurrir.
- Basar la seguridad únicamente en un firewall u otro componente singular similar.
- No darse cuenta del valor real de su información y de la reputación de su organización.
- Autorizando soluciones reactivas, a corto plazo.
- Pretendiendo que el problema desaparecerá si lo ignoran.

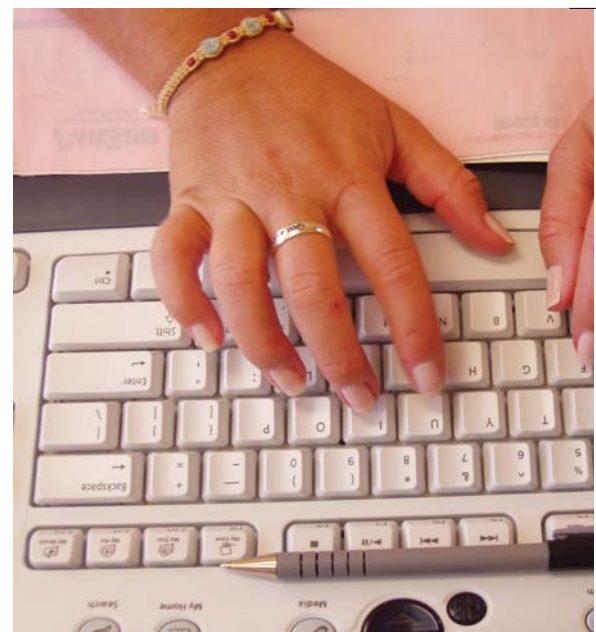
Por parte del personal de Tecnologías de la Información:

- Conectar sistemas a Internet antes de reforzar la seguridad de los mismos.
- Conectar sistemas de prueba a Internet con cuentas de usuario y claves por defecto.
- No actualizar los sistemas cuando se descubren agujeros de seguridad.
- Utilizar telnet y otros protocolos no encriptados para gestionar sistemas, routers, firewalls...
- Dar claves de usuario sin autenticar al solicitante.
- No realizar, mantener o validar las copias de seguridad.
- Mantener en funcionamiento servicios innecesarios, que pueden ser peligrosos.
- Implementar reglas en los firewall que no evitan el tráfico malicioso o peligroso en la entrada o en la salida.
- No implementar o actualizar el software antivirus.
- No educar a los usuarios en qué deben buscar y que hacer cuando vean un potencial problema de seguridad.

Muchos de estos problemas ocurren porque la seguridad se ve exclusivamente como un problema tecnológico, porque el personal técnico no tiene el presupuesto, o porque no existe un responsable global de seguridad que supervise los aspectos relacionados con IT, recursos humanos, edificios, etc. a la misma persona.

LA PROTECCIÓN DE LOS ACTIVOS DE LA EMPRESA

Se entiende por activo de información a cualquier dato creado, utilizado o almacenado, así como el software y el hardware utilizados



SE ENTIENDE POR ACTIVO DE INFORMACIÓN A CUALQUIER DATO CREADO, UTILIZADO O ALMACENADO, ASÍ COMO EL SOFTWARE Y EL HARDWARE UTILIZADOS PARA MANIPULARLOS.

para manipularlos. La protección de los activos de la empresa abarca las siguientes áreas: disponibilidad, confidencialidad, integridad, utilidad y posesión, y no repudio.

Los activos de información deberán evaluarse en base al valor de los activos para las operaciones del negocio, los costes de reposición (hardware, software, datos, pérdida de uso, administración) y el coste de los daños directos e indirectos debidos a la pérdida de información. Así, deberemos tener en cuenta, por ejemplo, cual es el coste de perder la producción por una avería, o qué ocurrirá si la información del servidor no es válida.

Una vez valorados los activos, será necesario evaluar los riesgos, de dónde provienen, y qué probabilidad tienen de ocurrir. La provisión anual de pérdidas deberá calcularse



para todos los activos como el valor de dicho activo por la probabilidad (anual) de que ocurra el riesgo. El presupuesto de seguridad (parte del cual es seguridad IT) deberá ser la suma de todas las provisiones de pérdidas.

La seguridad de la empresa requiere una aproximación holística y consistente en las siguientes áreas: proceso de gestión de la seguridad, seguridad física, seguridad de las operaciones, continuidad de negocio y planificación de recuperación de desastres, sistemas de control de acceso y metodología, criptografía, telecomunicaciones y seguridad de redes, metodología de desarrollo de sistemas y apli-

caciones, implicaciones legales...

Algunos de los aspectos a tener en cuenta en el proceso de conseguir una empresa segura son:

- Estrategia de negocio.
- Continuidad de negocio y recuperación de desastres.
- Estrategia de seguridad.
- Formación para la concienciación en seguridad.
- Políticas de seguridad.
- Planificación de la seguridad.
- Valoración de activos.
- Evaluación del riesgo.
- Evaluación de las amenazas.
- Contramedidas.
- Arquitectura de seguridad.
- Diseño de las aplicaciones.
- Arquitectura de los sistemas de información.
- Políticas y diseño de procesos.
- Servicios de puesta en marcha.
- Servicios de interoperabilidad.
- Auditoría de seguridad.
- Gestión de la seguridad.
- Detección de intrusos.
- Gestión de incidencias.
- Pruebas de continuidad de negocio.
- Actualización de las políticas.
- Gestión de la configuración.

Pueden existir muchos otros, pero estos bastan para ilustrar que no se trata únicamente de una pieza de hardware, o un software determinado. La pregunta a hacerse es: ¿se está haciendo esto en mi empresa y por quién?, y, si no es así, ¿por qué?

LA POLÍTICA DE SEGURIDAD

La política de seguridad debe mostrar quién es el propietario de un activo, quién lo vigila y quién tiene acceso a él, y en qué condiciones. La política también debe definir unos principios generales, procesos y métricas.

El responsable de seguridad y su equipo serán los encargados de la seguridad de los sistemas de información, la seguridad física, las telecomunicaciones y los procedimientos de seguridad.

La política de seguridad necesita ser específica y basada en definiciones de seguridad básicas, así como debe ser comunicada, con el objetivo de actuar como estándar para la regulación de la seguridad. Una vez dispuesta la política, las conductas y acciones pueden ser medidas contra dicha Política ya que es de obligado cumplimiento para todos los empleados y colaboradores de una organización. La Política no debe incluir dependencias con la tecnología, sistemas específicos, términos técnicos, o aspectos organizacionales, porque estos cambian constantemente y obligaría a estar modificándola de manera continua. La recomendación es realizar una revisión anual, siempre dependiendo del tipo de organización y de los cambios que afecten a ésta.

Tanto la ausencia de política de seguridad, como una política mal entendida o mal comunicada, o simplemente no comunicada, implican ausencia de seguridad en la empresa. ➡

LA POLÍTICA DE
SEGURIDAD DEBE MOSTRAR
QUIÉN ES EL PROPIETARIO
DE UN ACTIVO, QUIÉN LO
VIGILA Y QUIÉN TIENE
ACCESO A ÉL, Y EN
QUÉ CONDICIONES.

En el apartado de seguridad en las operaciones, hay que tener en cuenta la protección de ficheros de claves, software (sistemas operativos, utilidades y aplicaciones, código fuente, librerías...), hardware (redes y comunicaciones, ordenadores ...), utilidades del sistema, registros de auditoría – incluyendo informes de violación de acceso a sistemas – copias de seguridad, y formularios e impresiones que contengan información sensible.

En la operación de los sistemas, todo necesita información. Pueden llegar a producirse problemas si los operadores (con altos privilegios de acceso), pueden modificar la información de entrada o de salida, decidir cuando ejecutar las aplicaciones, en qué máquinas, alterar o mover copias de seguridad, robar, modificar o destruir registros, modificar o acceder a las claves de los usuarios... Por todo ello es necesario asumir que toda operación debe estar documentada. Este es un requisito básico tanto para la seguridad como para las auditorías internas y externas.

Teniendo en cuenta todos los aspectos anteriores, será necesario:

- **Definir el proceso de seguridad:** para ello, comenzaremos definiendo y asegurando un primer perímetro que nos ayude a limitar los daños en caso de un problema de seguridad. Partiremos de una base que muestre el estado actual de todos los elementos de la arquitectura – tanto su comportamiento exacto como los procedimientos. Implementaremos un sistema riguroso de control del cambio, y tendremos en cuenta no la funcionalidad sino la predictibilidad de los sistemas involucrados.

- **Implementar la seguridad:** Compararemos la base actual con la política definida. Si no existe la política de seguridad, utilizaremos la arquitectura base y una revisión de la seguridad para comenzar a definir dicha política. La revisión de la seguridad deberá categorizar los cambios en urgentes, no urgentes y opcionales. A continuación pasaremos a solucionar los aspectos urgentes, teniendo en cuenta las necesidades futuras para no tener que rehacer los cambios. Por norma general, la complejidad y la funcionalidad son enemigas de la seguridad.

- **Comunicar y validar:** Asegúrese de que todos los empleados conocen, comprenden y están de acuerdo con la política y la arquitectura de seguridad. Valídela utilizando tanto escenarios como herramientas.

SEGURIDAD ES EL CONCEPTO DE LA PROTECCIÓN DE LOS ACTIVOS DE MANERA ADECUADA A LAS NECESIDADES DE NEGOCIO, LEGISLACIÓN, REGULACIONES, CÓDIGOS DE CONDUCTA Y ESTÁNDARES DE SEGURIDAD



- **Permanecer seguros:** para ello es necesario implementar un conjunto de medidas, empezando por el compromiso de la dirección con la seguridad, un riguroso control de cambios, una revisión periódica del estado actual de la arquitectura, la política y los procedimientos, revisiones periódicas de los activos y los riesgos, comunicación interna, pruebas periódicas del comportamiento y la predictibilidad de los sistemas, buscar siempre lo inesperado, y ser escéptico.

Por lo tanto, seguridad es el concepto de la protección de los activos de manera adecuada a las necesidades de negocio, legislación, regulaciones, códigos de conducta y estándares de seguridad; donde se incluyen aspectos como:

Estrategia de Seguridad desde la dirección.

- Controles de Seguridad Corporativos.
- Políticas de Seguridad
- Procesos de Seguridad
- Roles de Seguridad
- Evaluación y Gestión del Riesgo.
- Sistema de Gestión de la Seguridad de la Información.
- Estándares y Procedimientos de Seguridad.

- Marketing, Comunicación, Concienciación, y Formación.
- Auditoría y Control.

El siguiente esquema resume la jerarquía de componentes que deben estar presentes en una solución de gestión y gobierno de la seguridad:

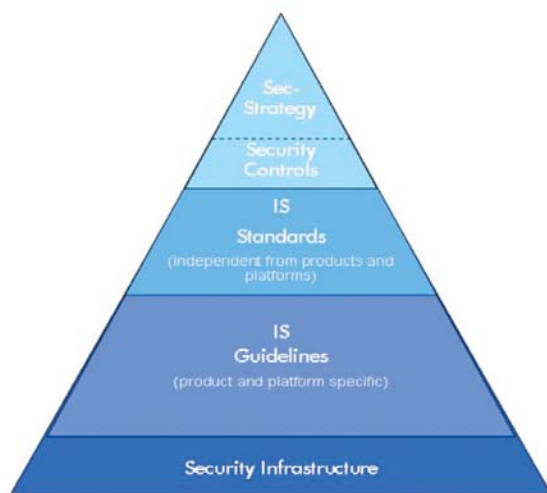
Estrategia de Seguridad: Comienzo formal de la Gestión y Gobierno de la seguridad, donde se definen los Objetivos Estratégicos de Seguridad de la organización por parte de la dirección de ésta.

Controles de Seguridad: Definición de Políticas, roles, responsabilidades y procesos de seguridad dentro de la organización necesarios para cumplir la estrategia definida.

Estándares de Seguridad: Regulación de Controles de Seguridad a aplicar independientes de productos o plataformas específicas y acordes con los controles y estrategia definidos.

Procedimientos de Seguridad: Especificaciones paso a paso de los controles de seguridad ya ligados a productos y plataformas específicas que resuelven los requerimientos antes identificados.

Posterior a todo lo indicado se realizaría la implementación, integración y operación de las tecnologías y plataformas involucradas (HW, SW, Redes, etc) que constituirán lo que se denomina Infraestructura de Seguridad.



METODOLOGÍAS, HERRAMIENTAS Y NORMAS

El marco de referencia utilizado por HP en los proyectos de Gestión y Gobierno de la Seguridad es la normativa ISO/IEC 17799:2005 que define controles de seguridad basados en las mejores prácticas de seguridad que ayudan a realizar la gestión de la seguridad adecuada al nivel de riesgo de la organización.

La norma UNE 71502:2004 ayuda a la implantación de un Sistema de Gestión de Seguridad de la Información SGSI (Sistema de Gestión de la Seguridad de la Información) donde se definen varios pasos o fases en el establecimiento del marco de un SGSI, así como todo lo necesario para emprender el proceso de certificación de dicho SGSI.

También se utilizan las técnicas para la gestión de la seguridad UNE 71501-3:2001 que constituyen un conjunto de guías para ayudar en la definición e implantación de la seguridad.

HP siguiendo el estándar ITIL ha desarrollado el modelo de

Procesos ITSM de tal forma que el proceso de Gestión de la Seguridad incluido en dicho modelo se ha integrado con los procesos de seguridad indicados en la normativa UNE ISO/IEC 17799:2002.

BENEFICIOS

Los principales beneficios de abordar la Gestión y el Gobierno de la Seguridad a nivel organizativo se pueden resumir en los siguientes puntos:

- Permite definir prioridades y realizar la inversión apropiada en seguridad.
- Comenzar a FORMALIZAR la seguridad.
- Aporta una Visión externa independiente.
- Alineamiento entre necesidades del negocio e implantaciones tecnológicas.
- Conocimiento real del RIESGO de la organización.
- FORMALIZACIÓN efectiva de la seguridad.
- Planificación detallada de las inversiones en seguridad.
- Ayuda a la eficiencia económica de la organización.
- Seguimiento de estándares consolidados.
- Demuestra la debida diligencia en seguridad.
- Ayuda a mantener una visión homogénea y uniforme de seguridad entre diferentes estamentos y departamentos.
- Mejora de la confianza y satisfacción de todo el personal relacionado con los sistemas de información.
- Refuerzo del cumplimiento de políticas y requerimientos de seguridad.
- Facilita la mejora continua.
- Gestiona y reduce el impacto en incidentes de seguridad.❖