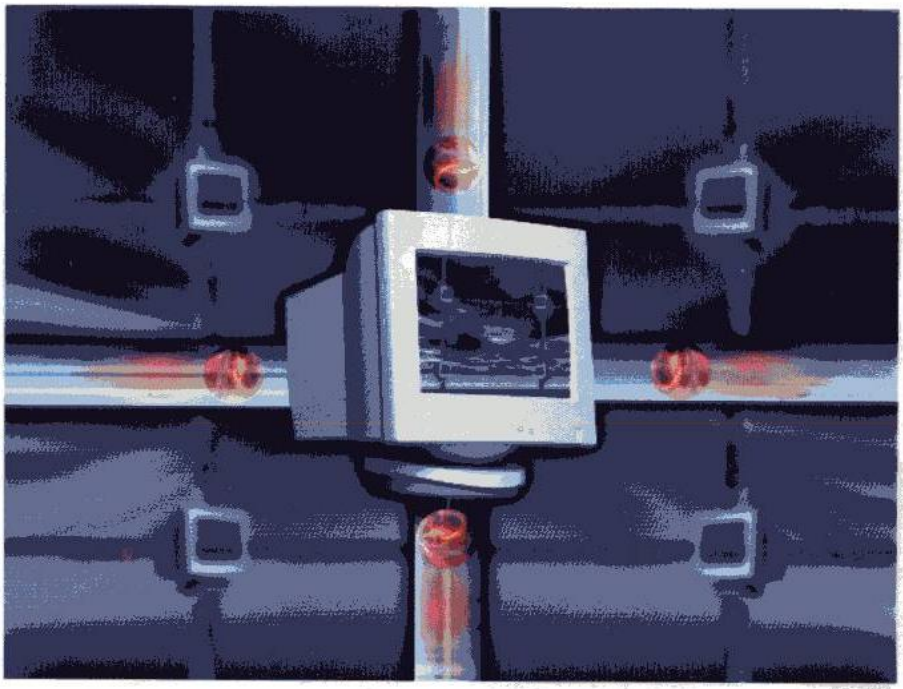
LA SEGURIDAD DE LA INFORMACIÓN EN NUESTRO PAÍS

La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios.

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información esta expuesta a un mayor rango de amenazas y vulnerabilidades.

Una gestión de Seguridad de la Información no sólo es la compra de un Antivirus, Firewall, Linux o Software libre o sistemas de backup sino es todo un proceso. Seguridad de la Información implica un sistema de IT-Security Management siendo ésta parte de Risk Management de la organización. IT- Security Management tiene que garantizar la Integridad, Confidencialidad, Disponibilidad e Irrefutabilidad de la información.



¿Qué tareas tiene la Gerencia en una Gestión de Seguridad de la Información?

Uno de los componentes primordiales en la implantación exitosa de una Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que una Gestión de Seguridad de la Información afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar una Gestión de Seguridad de la Información una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

¿Cómo asegurar su información?

Fon Perú dá las siguientes recomendaciones para asegurar la información dentro de la empresa:

1.- Concepto de activos

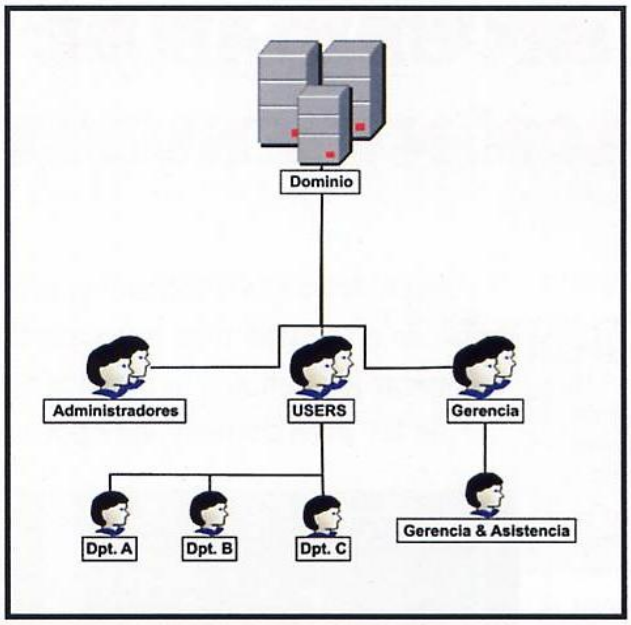
Identificar los valores en riesgo de la empresa, entidad u organización, el valor del proceso de negociación con sus clientes y/o el valor de su producción. Debemos revisar, evaluar y hacer un listado de los activos actuales del sistema y la gerencia debe sensibilizarse con la importancia de la seguridad de su información.

2.- Política de Seguridad

La política de seguridad es sumamente importante para la empresa, entidad u organización, involucra a todo el personal. La gerencia debe aprobar, publicar y comunicar con un documento »la política de seguridad» a todos los empleados en forma apropiada, entendible y accesible, los procedimientos específicos y detallarlos para el uso de su sistema y reglas de seguridad que los usuarios deben cumplir.

Otro punto es definir las configuraciones y aplicaciones de sus equipos (computadores y servidores) para el buen uso. Por ejemplo: No permitir el uso del chat, no bajar ningún tipo de archivos (fotos y música), siendo este un medio de trasmisión de virus, spams, etc. o infiltrados en red.

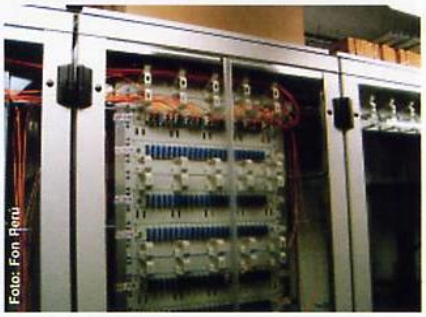
Si fuera necesario la gerencia debería tomar los servicios de consultores externos especializados en seguridad de información (FON PERU) para mantenerse al día con las tendencias de la industria, evolución de las Normas ISO y métodos de evaluación.



3.- Control y Revisión

Dependiendo del tamaño de la empresa, entidad u organización, el control de la política de seguridad puede ser manejado por un asesor y/o consultor especialista ya sea interno o externo, revisando y coordinando los resultados.

Mantener la alta protección al acceso de distribución de cables, los servidores y componentes de redes como switches y routers



Alta protección contra influencia ambiental

No podemos olvidar los requerimientos de confidencialidad o acuerdos de no divulgación de necesidades de la empresa para la protección de la información, éstas deben estar debidamente identificadas y revisadas regularmente, haciendo backups si es posible a diario.

Revisar la continuidad del negocio, las condiciones legales, los cambios en el ambiente técnico y las consecuencias de las violaciones de la política de seguridad para el éxito de la empresa.

4.- Productos y programas (hardware y software)

Antes de comprar un producto como antivirus, firewall u otros productos de seguridad, debemos tener en cuenta un concepto global de las necesidades propias de la empresa, entidad u organización; para así implementar, aplicar y configurar correctamente los hardware y software bajo las necesidades y bajo la política de seguridad aprobada por la Gerencia.

5.Capacitación

Capacitar a los empleados y/o usuarios a que estén preparados para sostener la política de seguridad de la empresa en el curso normal de su trabajo y así reducir el riesgo de error humano. Un buen nivel de conocimiento de procedimientos de seguridad a todo el personal minimizan los posibles riesgos.

La capacitación debe incluir requisitos de seguridad, responsabilidades legales y controles del negocio, así como prácticas en el uso correcto de procedimientos de concesión (log-on), uso de paquetes de software, etc. Tener personal motivado (feliz) es tener personal mas confiable y pueden causar menores incidentes en la seguridad de información de la empresa.

Por: Ing. Christopher Hafer
Gerente General
FON PERÚ S.A.C.