Capítulo XIV

Seguridad de la Información

Seguridad de la información

Tabla de contenido

Seguridad de la información

1.- ¿En qué consiste la administración de seguridad de la información?

La administración de seguridad de la información tiene como propósito alinear la seguridad de TI con la seguridad de la empresa y velar para que la seguridad de la información se maneje adecuadamente en todos los servicios de TI.

Una adecuada administración de la seguridad de la información permitirá asegurar que la información que se almacena y maneja con la infraestructura de TI:

- Está debidamente protegida de su uso por parte de personas no autorizadas –confidencialidad-.
- Está debidamente protegida de cambios que intenten hacer personas no autorizadas –integridad-.

Podemos decir que los principales objetivos de la administración de seguridad son:

- Diseñar una política de seguridad alineada con las políticas de seguridad y necesidades de la empresa.
- Asegurar el cumplimiento de las políticas de seguridad acordadas.
- Mitigar los riesgos de seguridad que puedan amenazar la continuidad del servicio o la confidencialidad e integridad de la información.

Será fundamental comprender que la administración de la seguridad no es únicamente responsabilidad de los técnicos de seguridad de TI, sino que es una responsabilidad de toda la empresa. Siempre se cita, como ejemplo, el caso de aquellas empresas en las que todos los servicios de TI están rodeados de las más rigurosas normas de seguridad, mientras que los reportes que imprimen los usuarios, circulan libremente o descansan sobre los escritorios sin que nadie vele por su confidencialidad. Por esto, no dejamos de enfatizar que la seguridad de la información que maneja y

procesa TI y la seguridad de la empresa deben estar perfectamente alineadas.

Es importante mantener en perspectiva que la seguridad también debe establecerse en función de las necesidades del negocio. Si se cae en el error de establecer la seguridad como una prioridad por sí misma, se limitarán las oportunidades que ofrecen las capacidades de computación y telecomunicaciones para realizar un intercambios de información con los diferentes asociados de negocio, con los que se comparten procesos, como son los clientes -a los que se les da acceso vía Web para realizar transacciones- y los proveedores –con los que se comparten procesos para ordenar bienes o servicios y para cancelar cuentas por pagar-.

La administración de la seguridad debe tomar en cuenta las características del negocio y los servicios que presta la organización TI, para establecer normas, procedimientos y protocolos de seguridad, que aseguren que la información esté debidamente resguardada, pero accesible cuando se necesita, para aquellos usuarios debidamente autorizados.

Una vez establecidos los requerimientos de seguridad del negocio, la administración de la seguridad en TI debe supervisar que tales requerimientos estén contemplados dentro de cualquier acuerdo de servicio que se establezca con los usuarios y, además, debe garantizar su cumplimiento.

La administración de la seguridad debe asimismo, identificar los riesgos a los que está expuesta la infraestructura TI, con el fin de proponer medidas que los mitiguen o eliminen. Esto es, será también importante para la administración de seguridad de información, que esta sea proactiva y evalúe permanentemente los riesgos de seguridad que pueden ir surgiendo a medida que los sistemas y la infraestructura tecnológica vayan evolucionando.

1.1.- Ventajas

Entre las principales ventajas que aporta una adecuada implantación de la disciplina de administración de seguridad de la información, pueden citarse los siguientes:

- Se preserva la integridad de los datos.
- Se preserva la confidencialidad de los datos y la privacidad de clientes y usuarios.
- Se cumple la normativa de la empresa relacionada con la seguridad de información.

- Se evitan interrupciones del servicio causadas por virus, ataques de hackers, etc.
- Mejora la percepción y confianza de los usuarios y clientes en cuanto a la calidad del servicio.

1.2.- Barreras

La implementación de la disciplina de seguridad de la información tropieza con barreras como las siguientes:

- No existen políticas de seguridad en el nivel de la empresa.
- No existe el suficiente compromiso de todos los miembros de la organización TI con la seguridad.
- No se dispone de las herramientas necesarias para monitorizar y garantizar la seguridad del servicio –como software de seguridad, antivirus, hardware de seguridad como firewalls, etc.-
- Se establecen políticas de seguridad excesivamente restrictivas que afectan la buena marcha de las operaciones.
- El personal no recibe una formación adecuada para aplicar correctamente los procedimientos de la disciplina.
- No se realiza una minuciosa identificación y evaluación de riesgos.

2.- La seguridad en el nivel de la empresa

Señalábamos en párrafos anteriores que la administración de seguridad de la información no es sólo un problema de TI, sino que la disciplina debe formar parte de la estrategia y normativa que se hayan establecido en el nivel de la empresa.

En tal sentido, como mínimo, en el nivel de la empresa se deben haber establecido:

1. Categorías

Cada empresa, de acuerdo con las características de sus operaciones, establece diferentes categorías en la confidencialidad de su información; a título de ejemplo podemos citar los siguientes niveles:

- Estrictamente confidencial
- Confidencial
- Sólo para uso interno
- Público

2. Criterios de categorización

Los criterios de categorización, permiten establecer cuando un documento, reporte, memorando, plano, registro de base de datos, etc. es estrictamente confidencial, confidencial, sólo para uso interno o público.

Las empresas acostumbran a identificar en forma visible la categoría de seguridad de cada documento. Así, por ejemplo, veremos memorandos en los que aparecen claramente visibles las palabras "confidencial" o "sólo uso interno"; análogamente, las aplicaciones hacen una indicación similar en los reportes que imprimen.

3. Procedimientos

Los procedimientos establecen qué normas deben cumplirse para proteger la información, de acuerdo con su categoría. Así mismo, establecen qué funcionarios, de acuerdo con su nivel, pueden tener acceso a información clasificada como estrictamente confidencial o confidencial.

Adicionalmente, los procedimientos también establecen las responsabilidades que cada funcionario tiene sobre la información a la que accede y los pasos que deberán darse para cumplir con la normativa al utilizar la información

4. Funcionarios de seguridad por área funcional

Una vez que en el nivel de la empresa se establecen normas y procedimientos de seguridad, normalmente, se establecen las funciones del coordinador de seguridad de cada área del negocio, quien será responsable de velar por la adecuada clasificación de los documentos e información del área, de verificar que los procedimientos de seguridad son viables para su área y de velar por su cumplimiento.

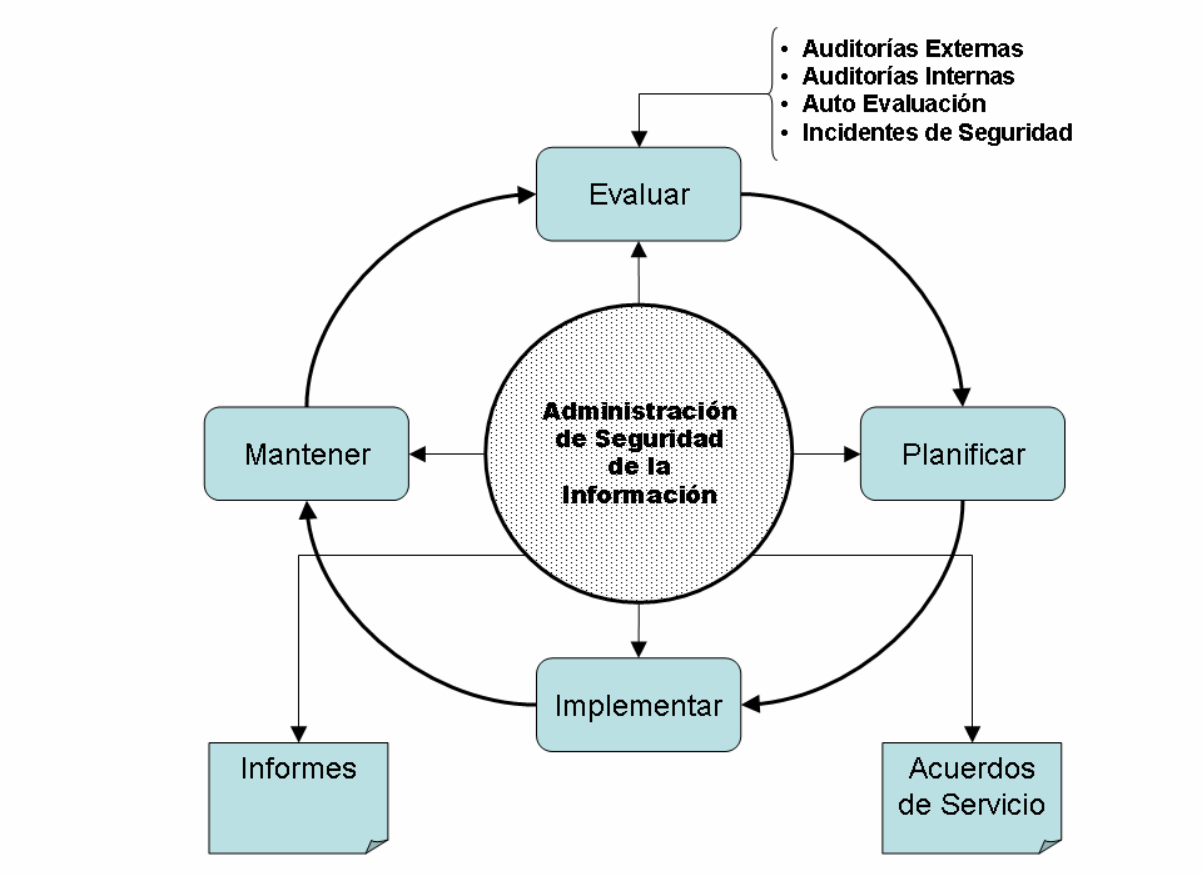
Es costumbre que este rol opere en estrecho contacto con el administrador de seguridad en TI, ya que tendrá como responsabilidad autorizar o revocar los niveles de acceso que se otorguen a los funcionarios de su área, con el fin de poder tener acceso a servicios y aplicaciones, de acuerdo con sus responsabilidades.

3.- Actividades

La administración de la seguridad esta estrechamente relacionada con todas las disciplinas de administración y todos los procesos de TI, por lo que para resultar exitosa requiere el concurso y la colaboración de toda la organización.

Para que esa colaboración sea eficaz es necesario que la administración de la seguridad:

- Establezca una clara y definida política de seguridad que sirva de guía a todos los otros procesos.
- Elabore un plan de seguridad que incluya los niveles de seguridad adecuados tanto en los servicios prestados a los clientes como en los acuerdos de servicio firmados con proveedores internos y externos.
- Implemente el plan de seguridad.
- Monitorice y evalúe el cumplimiento de dicho plan.
- Supervise proactivamente los niveles de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.



4.- Políticas de seguridad

Es imprescindible disponer de un marco general que establezca los criterios para todas las disciplinas y procesos de TI. En especial, la política de seguridad debe establecer:

- La relación con las políticas y normas de seguridad de la empresa.
- La coordinación con las otras disciplinas de administración de servicios de TI.
- La coordinación con los funcionarios responsables de la seguridad de información en las áreas funcionales.
- La estructura organizativa y los responsables del proceso de administración de la seguridad.
- Los recursos necesarios: software, hardware y personal.
- Los programas de divulgación y formación.
- Los procedimientos de análisis de riesgos.
- El nivel de monitorización de la seguridad.
- Los informes que deben ser generados periódicamente.
- Las auditorías externas e internas de seguridad.

5.- El plan de seguridad

El objetivo del plan de seguridad es fijar los niveles de seguridad que deben ser incluidos como parte de los acuerdos de servicio que se establecen con los usuarios y en el nivel operacional.

El plan debe ser desarrollado conjuntamente con la administración de niveles de servicio, responsable en última instancia de la calidad del servicio prestado a los clientes, así como también de la calidad de los servicios que recibe la organización TI de los proveedores externos.

El plan de seguridad debe diseñarse para ofrecer un servicio a los usuarios mejor y más seguro, nunca como un obstáculo para el desenvolvimiento de las actividades del negocio:

- Debe ser coherente

  Los procedimientos de seguridad deben ser coherentes en todas las fases del servicio de TI y para todos los niveles de la organización. Deben tomar en cuenta que "una cadena es tan resistente como el más débil de sus eslabones", por lo que carece de sentido, por ejemplo, establecer estrictas normas de acceso si en las aplicaciones se mantienen vulnerabilidades por un uso

inadecuado de las facilidades de seguridad que ofrecen los manejadores de bases de datos utilizados en la empresa.

- Indicadores Clave

  Siempre que sea posible deben definirse métricas e indicadores clave que permitan evaluar los niveles de seguridad y el cumplimiento de las normas.

6.- Cumplimiento de la normativa de seguridad

La administración de seguridad de la información es responsable de motorizar y coordinar la implementación de los procedimientos y las medidas de seguridad establecidas en el plan de seguridad.

El administrador de la seguridad debe velar por que:

- El personal conozca y acepte las normas de seguridad establecidas y sus responsabilidades.
- Exista una aceptación formal, asegurando que los empleados firmen acuerdos de confidencialidad acordes con su cargo y responsabilidades.
- Se está impartiendo al personal una formación adecuada.
- Se está comunicando adecuadamente la normativa y las consecuencias de las infracciones.

Al establecerse la disciplina de administración de la seguridad de la información, se deben:

- Asignar los recursos necesarios.
- Instalar y mantener las herramientas de hardware y software necesarias para garantizar la seguridad.
- Documentar adecuadamente toda la normativa, los procedimientos e instructivos.
- Establecer las políticas y procedimientos de acceso a la información.
- Establecer acuerdos con el centro de atención en relación con el manejo de incidentes relacionados con la seguridad.
- Establecer acuerdos con la administración de cambios y de versiones, con el fin de asegurar que no se introduzcan vulnerabilidades en las aplicaciones que pasan al ambiente de producción.

- Establecer acuerdos con la administración de la continuidad de los servicios, para asegurar que, bajo ninguna circunstancia, peligra la integridad o la confidencialidad de los datos.
- Establecer procedimientos e implementar herramientas que permitan monitorizar las redes y los servicios para detectar intrusiones y ataques.

Es necesario que tanto la gerencia de TI, como todos los niveles ejecutivos de la empresa otorguen suficiente autoridad a los administradores y se establezcan medidas disciplinarias que deben ser aplicadas cuando los empleados o cualquier otro personal relacionado con los servicios de TI no cumpla con la normativa de seguridad.

7.- Evaluación y mantenimiento

Normalmente las empresas practican evaluaciones en forma continua mediante auditorías de seguridad externas e internas, realizadas por personal independiente de la administración de la seguridad.

El propósito de estas evaluaciones y auditorias deben calificar el nivel de seguridad y proponer mejoras que permitan perfeccionar los procedimientos y las normas de seguridad.

Además de las evaluaciones periódicas, cada incidente relacionado con seguridad deberá investigarse, con el propósito de tomar las medidas correctivas necesarias para evitar su repetición.

La administración de la seguridad debe concebirse como un proceso en continuo perfeccionamiento, por lo que tanto la normativa, como el plan de seguridad deben actualizarse constantemente, al igual que debe renovarse y mejorarse, en forma continua, el conjunto de herramientas de hardware y software implementadas. No existe nada tan vulnerable como una seguridad basada en medidas obsoletas.

Será fundamental que la administración de la seguridad maneje información actualizada sobre nuevos riesgos frente a virus, software espía, malware y ataques de hackers, con el fin de adoptar las medidas necesarias para actualizar hardware y software, sin dejar a un lado los aspectos de comunicación y formación.

8.- Evaluación de la disciplina

Al igual que para todas las disciplinas de administración de servicios de TI, para la administración de la seguridad debe realizarse un riguroso control que asegure el cumplimiento de sus objetivos:

- Acceso eficiente a la información por el personal autorizado.
- Disminución del número de incidentes relacionados con seguridad.
- Identificación proactiva de vulnerabilidades, antes de que estas puedan provocar un incidente de seguridad.

La producción periódica de informes permitirá que la gerencia de TI evalúe el desempeño de la administración de la seguridad de la información y aportará información valiosa a otras áreas de TI. Entre los reportes más importantes a producir, podemos citar:

Entre la documentación generada cabría destacar:

- Relación de incidentes relacionados con seguridad clasificados por su impacto sobre la calidad de los servicios.
- Relación del cumplimiento de los programas de formación y evaluación de sus resultados.
- Identificación de nuevos riesgos y vulnerabilidades que enfrenta la infraestructura TI.
- Resultados de auditorías de seguridad.
- Informes sobre el grado de implementación y cumplimiento de los planes de seguridad establecidos.
- Informes sobre el cumplimiento de los acuerdos de servicio y acuerdos operacionales, en lo relacionado a la seguridad de la información.