La gestión de activos y la seguridad de la información

Responsabilidad por los activos

Objetivo: Identificar los activos de la organización y definir las responsabilidades para la apropiada protección.

Inventario de activos

Los activos asociados con la información y los recursos de procesamiento de la información deberían ser identificados y se debería elaborar y mantener un inventario de estos activos.

Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir la creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. La documentación debería mantenerse en inventarios dedicados o existentes según corresponda.

El inventario de activos debería ser exacto, actualizado, coherente y alineado con otros inventarios.

Para cada uno de los activos identificados, debería asignarse un propietario y debería identificarse la clasificación.

Los inventarios de activos ayudan a asegurarse de que se logre la protección efectiva, pero también pueden ser requeridos para otros propósitos, como por ejemplo por razones de salud y seguridad, de seguros o financieras (gestión de activos).

Propiedad de los activos

Los activos registrados en el inventario deberían tener un propietario.

Las personas, así como otras entidades que tengan aprobada la responsabilidad de gestión del ciclo de vida de los activos, califican para ser asignadas como propietarias de activos.

Usualmente se implementa un proceso para asegurarse de la asignación oportuna de la propiedad de los activos. La propiedad debería asignarse cuando los activos son creados o cuando son transferidos a la organización. El propietario del activo debería ser responsable de la gestión apropiada de un activo durante todo el ciclo de vida del activo.

El propietario del activo debería:

a) asegurarse de que los activos sean inventariados;
b) asegurarse de que los activos sean clasificados y protegidos adecuadamente;
c) definir y revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, tomando en cuenta las políticas aplicables de control de acceso;
d) asegurarse del manejo adecuado cuando el activo es eliminado o destruido.

El propietario identificado puede ser una persona o una entidad que tiene aprobada la responsabilidad de gestión para el control de todo el ciclo de vida de un activo. El propietario identificado no necesariamente tiene algún derecho de propiedad sobre el activo.

Las tareas rutinarias pueden ser delegadas, por ejemplo, a un custodio que esté al cuidado diariamente de los activos, pero la responsabilidad continúa siendo del propietario.

La gestión de activos y la seguridad de la información

En sistemas de información complejos puede resultar útil designar grupos de activos que actúan en forma conjunta para proveer un servicio particular. En este caso, el propietario del servicio es quién rinde cuentas por la entrega del servicio, incluyendo la operación de sus activos.

Uso aceptable de los activos
Se deberían identificar, documentar e implementar las reglas para el uso aceptable de la información, de los activos asociados con la información y de los recursos para el procesamiento de la información.

Los empleados y los usuarios de partes externas que utilizan o tienen acceso a los activos de la organización deberían ser conscientes de los requisitos de seguridad de la información de la información de la organización, otros activos asociados con información y recursos e instalaciones de procesamiento de la información.

Devolución de activos
Todos los empleados y usuarios de partes externas deberían devolver los activos de la organización que estén en su poder, al finalizar su relación laboral, contrato o acuerdo.

El proceso de finalización debería ser formalizado para incluir la devolución de todos los activos físicos y electrónicos previamente proporcionados pertenecientes o confiados a la organización.

En los casos en que un empleado o usuario de parte externa compre el equipo de la organización o utilice su equipo personal, deberían seguirse procedimientos para asegurarse de que toda información pertinente sea transferida a la organización y borrada de forma segura del equipo.

En los casos en que un empleado o usuario de parte externa tenga conocimiento que sea importante para las operaciones en curso, esa información debería ser documentada y transferida a la organización.

Durante el período de aviso de la finalización, la organización debería controlar la copia no autorizada de información pertinente (por ejemplo, propiedad intelectual) por los empleados y contratistas en proceso de finalización.

Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel de protección apropiado, de acuerdo con su importancia para la organización.

Clasificación de la información
La información debería ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.

La clasificación y los controles de protección asociados a la información deberían tener en cuenta las necesidades del negocio de compartir o restringir información, así como los requisitos legales. Otros activos aparte de la información, también pueden ser clasificados de conformidad con la clasificación de información que es almacenada, procesada, manipulada o protegida por el activo.

La gestión de activos y la seguridad de la información

Los propietarios de los activos de información deberían rendir cuentas por su clasificación. El esquema de clasificación debería incluir las convenciones para la clasificación y los criterios para la revisión de la clasificación en el tiempo. El nivel de protección en el esquema debería ser evaluado mediante el análisis de la confidencialidad, integridad, disponibilidad y cualquier otro requisito para la información considerada. El esquema debería estar alineado con la política de control de acceso.

Cada nivel debería tener un nombre que tenga sentido en el contexto de la aplicación del esquema de clasificación.

El esquema debería ser coherente en toda la organización para que todos clasifiquen de la misma forma la información y los activos relacionados, tengan un entendimiento común de los requisitos de protección y la apliquen adecuadamente.

La clasificación debería ser incluida en los procesos de la organización, debería ser compatible y coherente en toda la organización. Los resultados de la clasificación deberían indicar el valor de los activos en función de su sensibilidad y criticidad para la organización, por ejemplo, en términos de confidencialidad, integridad y disponibilidad. Los resultados de la clasificación deberían ser actualizados de acuerdo con los cambios de su valor, sensibilidad y criticidad durante su ciclo de vida.

La clasificación les ofrece a las personas que tratan con información, una indicación concisa de cómo manejarla y protegerla. La creación de grupos de información con necesidades de protección similares y la especificación de los procedimientos de seguridad de la información que se aplican a toda la información en cada grupo, facilitan esto. Este enfoque reduce la necesidad de una evaluación de riesgos caso por caso y el diseño personalizado de los controles.

La información puede dejar de ser sensible o crítica después de cierto periodo de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deberían ser tomados en cuenta, puesto que una sobre-clasificación conllevaría a la implementación de controles innecesarios que resultan en gastos adicionales o, por el contrario, en una baja clasificación, que puede poner en peligro el logro de los objetivos del negocio.

Un ejemplo de un esquema de clasificación de confidencialidad de la información se podría basar en cuatro niveles, de la siguiente manera:

a) la divulgación no causa ningún daño;
b) la divulgación causa incomodidad menor o inconveniencia operativa menor;
c) la divulgación tiene un impacto significativo a corto plazo en las operaciones o los objetivos tácticos;
d) la divulgación tiene un grave impacto en los objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la organización.

Etiquetado de la información

Se debería desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación adoptado por la organización.

Los procedimientos para el etiquetado de la información necesitan cubrir la información y sus activos relacionados en formato físico y electrónico. El etiquetado debería reflejar el

esquema de clasificación. Las etiquetas deberían reconocerse fácilmente. Los procedimientos deberían proporcionar orientación sobre dónde y cómo se adjuntan las etiquetas, considerando cómo la información es accedida o cómo se manipulan los activos dependiendo de los tipos de medios. Los procedimientos pueden definir casos en los que se omite el etiquetado, por ejemplo, el etiquetado de información no confidencial, para reducir las cargas de trabajo. Los empleados y los contratistas deberían ser conscientes de los procedimientos de etiquetado.

La salida de los sistemas que contienen información clasificada como sensible o crítica debería llevar una etiqueta de clasificación adecuada.

El etiquetado de la información clasificada es un requisito clave para acuerdos que impliquen compartir información. Las etiquetas físicas y los metadatos son una forma común de etiquetado.

El etiquetado de la información y sus activos relacionados, puede a veces tener efectos negativos. Los activos clasificados son más fáciles de identificar y por consiguiente robar por parte de los atacantes internos o externos.

Manejo de los activos
Se deberían desarrollar e implementar procedimientos para el manejo de los activos de acuerdo con el esquema de clasificación de la información adoptado por la organización.

Deberían elaborarse procedimientos para el manejo, procesamiento, almacenamiento y comunicación de la información coherentes con su clasificación.

Deberían considerarse los siguientes elementos:

a) las restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación;
b) el mantenimiento de un registro formal de los receptores autorizados de los activos;
c) la protección de las copias temporales o permanentes de información a un nivel coherente con la protección de la información original;
d) el almacenamiento de los activos de TI en concordancia con las especificaciones del fabricante;
e) un rotulado claro de todas las copias de los medios para la atención del receptor autorizado.

El esquema de clasificación utilizado en la organización puede no ser equivalente a los esquemas utilizados por otras organizaciones, incluso si los nombres de los niveles son similares; además, la información que se mueve entre organizaciones puede variar en la clasificación dependiendo de su contexto en cada organización, incluso si los esquemas de clasificación son idénticos.

Los acuerdos con otras organizaciones que incluyen el intercambio de información deberían incluir procedimientos para identificar la clasificación de la información y para interpretar las etiquetas de clasificación de otras organizaciones.

La gestión de activos y la seguridad de la información

Manejo de los medios

Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de la información almacenada en los medios.

Gestión de medios removibles

Se deberían implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.

Se deberían considerar las siguientes directrices para la gestión de medios removibles:

a) si ya no es necesario, el contenido de cualquier medio reutilizable que ha de ser removido de la organización debería hacerse irrecuperable;
b) cuando sea necesario y práctico, debería requerirse autorización para los medios a retirar de la organización y se debería mantener un registro de dicha remoción, a fin de mantener una pista de auditoría;
c) todos los medios se deberían almacenar en un ambiente a salvo y seguro, de acuerdo con las especificaciones del fabricante;
d) si la confidencialidad o la integridad de los datos son consideraciones importantes, se deberían utilizar técnicas criptográficas para proteger los datos en los medios removibles;
e) para mitigar el riesgo de degradación de los medios mientras los datos almacenados se sigan necesitando, los datos deberían transferirse a medios nuevos antes de convertirse en ilegibles;
f) se deberían almacenar copias múltiples de los datos valiosos en medios independientes para reducir aún más el riesgo del daño o pérdida casual de los datos;
g) se debería considerar el registro de los medios removibles para limitar la oportunidad de pérdida de datos;
h) las unidades de medios removibles sólo se deberían habilitar si existe una razón del negocio para hacerlo;
i) cuando existe la necesidad de utilizar medios removibles, se le debería dar seguimiento a la transferencia de información a tales medios.

Se deberían documentar los procedimientos y los niveles de autorización.

Eliminación de medios

Los medios se deberían eliminar de manera segura, cuando ya no se necesiten, utilizando procedimientos formales.

Se deberían establecer procedimientos formales para la eliminación segura de los medios, para minimizar el riesgo de fuga de información confidencial a personas no autorizadas.

Los procedimientos para la eliminación segura de los medios que contienen información confidencial, deberían ser acordes con la sensibilidad de esa información. Se deberían considerar los siguientes ítems:

a) los medios que contengan información confidencial se deberían almacenar y eliminar de forma segura, por ejemplo, mediante incineración o trituración, o el borrando sus datos para su uso por otra aplicación dentro de la organización;
b) se deberían establecer procedimientos para identificar los elementos que puedan requerir la eliminación segura;

c) puede ser más fácil organizar que todos los elementos de los medios sean recolectados y eliminados de forma segura, en lugar de tratar de separar los elementos sensibles;
d) muchas organizaciones ofrecen servicios de recolección y eliminación de los medios; se debería tener cuidado en la selección de una parte externa apropiada con los controles y experiencia adecuados;
e) la eliminación de los elementos sensibles se debería registrar a fin de mantener una pista de auditoría.

Cuando se acumulen medios para la eliminación, se debería tomar en cuenta el efecto de combinación, el cual puede causar que una gran cantidad de información no sensible se convierta en sensible.

Los dispositivos dañados que contienen datos sensibles pueden requerir una evaluación de riesgos, para determinar si los elementos deberían ser destruidos físicamente, en lugar de ser enviados para su reparación o desecho.

Traslado de medios físicos
Los medios que contienen información se deberían proteger contra el acceso no autorizado, mal uso o corrupción durante su transporte.

Se deberían considerar las siguientes directrices para proteger a los medios que contienen información que es transportada:
a) se deberían utilizar transportistas o mensajeros confiables;
b) se debería acordar con la alta dirección una lista de mensajeros autorizados;
c) se deberían desarrollar procedimientos para verificar la identificación de los mensajeros;
d) el embalaje debería ser suficiente para proteger el contenido de cualquier daño físico que pueda producirse durante el tránsito y de acuerdo con las especificaciones del fabricante, por ejemplo, la protección contra cualquier factor ambiental que puede reducir la eficacia de restauración de los medios, tales como la exposición al calor, la humedad o los campos electromagnéticos;
e) se deberían mantener registros identificando el contenido de los medios, la protección aplicada, así como el registro de la hora de transferencia a los custodios durante el tránsito y de la recepción en el destino.

La información puede ser vulnerable al acceso no autorizado, mal uso o corrupción durante el transporte físico, por ejemplo, cuando se envían los medios a través del servicio postal o por mensajería. En este control, los medios incluyen los documentos en papel.

Cuando la información confidencial en los medios no se encuentra cifrada, se debería considerar la protección física adicional de los medios.