SEPRO TECH
Security Process and Technology

EBook

La gestión de Activos de información

By Seprotech team

Hoy en dia los ciberataques están siendo cada vez más agresivos, y con consecuencias que han afectado a organizaciones pertenecientes tanto al sector público como al sector privado, dejando en muchos casos graves consecuencias como el daño reputacional, patrimonial y violación a la privacidad de datos.

Los errores que vuelven a un sistema vulnerable ante ataques, son cada dia un desafío para los profesionales de TI, quienes deben invertir importantes esfuerzos en materia de prevención de incidentes. Por otro lado, el Global Risks Report 2022, indica que las empresas deben operar en un mundo en que el 95% de los problemas de ciberseguridad pueden atribuirse a un error humano, y donde amenazas internas (intencionales o accidentales) representan el 43% de todas las infracciones.

Debido a lo anterior, es necesario establecer mecanismos de protección de los activos de información de las organizaciones, de forma que el SGSI (Sistema de gestión de seguridad de la información) pueda brindar a la Alta Dirección una gestión adecuada, que considere los mecanismos de control y protección, designación de responsabilidades e inventarios de activos actualizados.

> 95%
>
> de los problemas de ciberseguridad pueden atribuirse a un error humano.
>
> WEF- The Global Risk Report 2022.

Una adecuada gestión de activos de información permite mitigar de forma efectiva riesgos de incidentes de seguridad, elaborar controles preventivos, focalizar los recursos técnicos y humanos en la respuesta ante incidentes de seguridad.

A través de metodologías es posible estructurar los inventarios de activos, de una forma que facilite su clasificación y el tratamiento de los activos de información. Así también es posible el establecimiento de responsabilidades que les cabe a los dueños y custodios de activos de información, cuya labor es fundamental para asegurar a la alta dirección, la existencia de controles adecuados y alineados con la estrategia empresarial.

Un buen diseño y una adecuada implementación de controles, permite mejorar el perfil de riesgo de los activos de información, ya que proporcionan un nivel importante de mitigación para las amenazas o vectores de ataques. Es riesgo residual (riesgo después de aplicado un control), es un resultado que determinará si se deben aplicar controles adicionales, o simplemente verificar si el resultado residual se encuentra dentro de los parámetros del riesgo aceptado por la Organización.

Es por ello que presentamos la metodología para comenzar la iniciación de un proceso de Gestión de activos de Información, paso a paso y explicando los detalles para conseguir los objetivos del Gobierno de la Seguridad.

Identificación

Todas las organizaciones necesitan elementos claves para el funcionamiento del negocio, por lo que es relevante saber detectar estos elementos de valor o activos de información.
Los activos de información son aquellos elementos que permiten la transmisión, almacenamiento y procesamientos de información, y que tienen un valor para la organización. Efectivamente podríamos encontrar muchos de ellos al interior de la organización, ya que de acuerdo con la definición podríamos tener entre ellos, por ejemplo, redes de transmisión de datos, bases de datos, servidores, computadores, aplicaciones, carpetas, bóvedas.
Podríamos continuar enumerando los distintos elementos que en definitiva se encuadran en la definición, pero es necesario aplicar el criterio de la importancia para la organización.
De acuerdo con la naturaleza e importancia para el negocio, algunos de los activos comenzarán a tener una importancia relativa, es por ello que se hace necesario determinar una o más variables que permitirán determinar un "peso específico" de importancia en la organización.

Una forma sencilla sería determinar el costo de adquisición del activo, sin embargo, este tipo de criterio no es fácilmente aplicable a los activos intangibles como la información.
Es por ello que un criterio enfocado en el negocio, nos permite establecer el valor relativo a la importancia para los procesos claves de la organización.
A través de un inventario actualizado de activos, y la información documentada de los procesos claves del negocio, es posible armonizar la gestión de los activos de información con el negocio.
Para inventariar los activos de infraestructura tecnológicas es clásicamente realizable de forma automática, a través de sistemas basados en agentes, que mantienen actualizado el inventario.

Los activos intangibles tienen directa relación con la naturaleza del negocio, ya que reflejan usualmente reflejan el resultado de un proceso, información de entrada para un proceso productivo, información clave para la venta, o para las decisiones estratégicas del negocio. Los activos intangibles también son inventariables.

Propiedad

Cuando ya hemos logrado tener una base importante de los activos de la Organización, es fundamental comenzar la búsqueda de los "Dueños" y "Custodios" de los activos de información, quienes serán dos actores claves para gestionar debidamente los activos de información.
El dueño de activos es quien asume la responsabilidad (Acountable) del activo de forma integral. Vale decir, es el encargado de definir las reglas de acceso y uso del activo de información, alineado con los con la estrategia empresarial. Es también el encargado de definir el ciclo de vida del activo, lo que permite por ejemplo, determinar la fecha de recambio de una activos físicos, o el cambio de clasificación de un activo primario (información).

Generalmente los Dueños de activos son aquellos colaboradores que lideran procesos dentro de una organización, principalmente en aquellos procesos que hacen parte de la cadena productiva, o de procesos que aportan valor directo al producto o servicio final.
Por otro lado, los custodios son los responsables de adoptar las reglas o disposiciones de los Dueños de activos, y habilitar controles que permitan el cumplimiento de las reglas de uso y acceso a los activos de información.
A través de los custodios, se customizan los sistemas para proveer, sistemas de control de acceso, elementos de monitoreo, herramientas de registros de auditoría, y todos aquellos procedimientos que contribuyan al cumplimiento de las reglas definidas.

Clasificación

La clasificación de los activos tiene por objetivo estructurar los activos basado en el criterio del costo monetario y de la necesidad del saber.
La norma ISO/IEC 27005 define fundamentalmente activos primarios y activos de soporte. Los *activos primarios* son aquellos naturalmente intangibles, correspondiente a información para el funcionamiento de un negocio. Son ejemplo de aquellos tales como:

- Información de Datos personales (PII)
- Información de inteligencia de negocio
- Prospecciones
- Invenciones
- Códigos fuentes

De acuerdo con la naturaleza del negocio, algunos de los activos podrían clasificarse como Esenciales (clave o core del negocio), y Generales correspondiente a información utilizada como apoyo para la gestión.
Para los activos primarios podremos aplicar el criterio de la "necesidad del saber", esto significa que los activos primarios de acuerdo a su nivel de confidencialidad los podemos clasificar en tres niveles: Pública, Uso interno, Restringida.

La información Pública, es aquel tipo de información cuya fuente es abierta, vale decir, se encuentra accesible por cualquier individuo.
La información de Uso Interno, es aquella que su uso está restringido sólo a los colaboradores internos de la organización, o grupos de interés específicos y que su difusión no autorizada, podría generar impacto para la organización.
La información Restringida, es aquella con el nivel más alto de confidencialidad, que representa la esencia del negocio, y que su difusión no autorizada, podría generar fuertes impactos para el negocio, como también generar daño reputacional o pérdida de confianza en el mercado.

Como se puede observar, la clasificación permite una estructura claramente enfocada en el negocio, lo que facilita una serie de decisiones estratégicas para la seguridad de la información.

Los *activos de soporte* son aquellos elementos que contienen o brindan soporte a los activos primarios, y que son necesarios para realizar el tratamiento definido por la Organización. Son ejemplos de ellos tales como:

- Servidores
- bases de datos
- Bóvedas
- Redes de comunicaciones
- Servicios Cloud
- Personas o Colaboradores

Asimismo, los activos pasan a ser parte de las temáticas tratadas en instancias como comités de seguridad, comités de riesgo, y otras instancias en donde se toman decisiones que buscan la protección de los activos de información.
En síntesis, los activos primarios se clasifican en niveles de confidencialidad y los activos de soporte se valorizan.

Tratamiento

Como ya tenemos el inventario de activos debidamente clasificados y valorizados, debemos aplicar el tratamiento adecuado para proporcionar las capas de control según la clasificación.

Con la ayuda de los dueños (Owner) de los activos de información, se deben determinar las reglas de uso de los distintos activos de información, tales como: permisos de acceso a la información, accesos a aplicaciones o bases de datos, ingresos a centros de datos, acceso a reportes de gestión , etc.

Generalmente las políticas de accesos a los activos, están definidas en políticas internas de la organización, las cuales son debidamente aprobadas por la Alta dirección.

Los niveles de clasificación de la información permiten definir el/los controles que mitigan riesgos para cada activo de información. Esto significa que mientras mayor sea el nivel de confidencialidad, mayor será la cantidad de controles aplicables al activo. Por ejemple una activo que tenga una clasificación como "Restringida", deberá contar con infraestructura que brinde alta disponibilidad, controles que realizan verificación de integridad, control de accesos avanzado y mecanismos de cifrado en tránsito y en reposo de los datos.

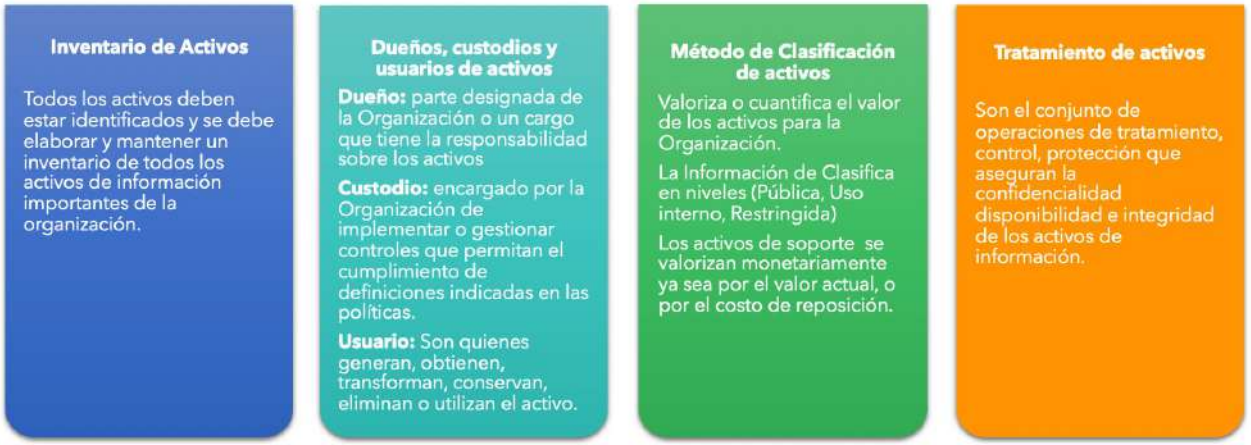
Por otro lado la información clasificada como pública, solamente necesita estar disponible para para organización.

Claramente los activos con un nivel de confidencialidad elevado exigirán controles más estrictos, es por ello que existe una proporcionalidad entre la cantidad y endurecimiento de controles, y la clasificación de la información.

La labor del custodio, es esencial para implementar las disposiciones y políticas indicadas por los dueños de activos. Los custodios deben verificar que los mecanismos de control, tales como: Servidores de acceso, Firewall, IPS, IDS, DLP hagan cumplir las definiciones detalladas en las políticas internas de la compañía. Así también deben reportar la efectividad de lo controles, de tal forma de evaluar de forma continua el riesgo residual para cada uno de los activos de información.

Los activos de información poseen un riesgo inherente, lo que puede ser mitigado a través de controles y definiciones según lo indicado por los dueños. Así con la ayuda de los custodios, es posible implementar las directivas de seguridad, o políticas indicadas por el gobierno de la seguridad y los dueños de activos de información.

En resumen, la gestión de los activos permite mitigar riesgos inherentes, como también los riesgos que pueden emanar de la naturaleza del negocio en relación a los activos. A través de una metodología adecuada, es posible orientar los esfuerzos en seguridad, y de esta forma reducir el riesgo a un nivel aceptado por la organización.



(By Seprotech team)

Gestionamos la seguridad de la Información, aplicando las mejores prácticas y estándares. Realizamos análisis de riesgos para la protección de los activos de información, diseñamos controles orientados al cumplimiento de los objetivos de mitigación de riesgos y auditorías de infraestructura tecnológica.

http://seprotech.la