Política de Gestión de Activos de Información

Fecha: 11/12/2024
Versión: 1.1

Control de versiones

Fecha	Versión	Descripción	Autor
15/11/2024	0.1	Creación del Documento	Comité de Seguridad de la Información
29/11/2024	1.0	Revisión del Documento	Comité de Seguridad de la Información
11/12/2024	1.1	Actualización con EOL	Comité de Seguridad de la Información

Contenido

1 Objetivo

Asegurar que todos los activos de información se gestionen y protejan adecuadamente de acuerdo con su valor para la organización, estableciendo responsabilidades claras para su uso, protección y clasificación.

2 Alcance

Aplica a todos los activos de información y medios asociados, así como a todo el personal y áreas de la organización. Esto incluye proteger los activos contra accesos, alteraciones, pérdidas o destrucciones no autorizadas, siguiendo los principios de confidencialidad, integridad y disponibilidad.

3 Vigencia

La presente norma entra en vigor a partir de su aprobación y publicación por parte del Comité de Seguridad.

Esta política será revisada en un período no mayor a tres años, o ante cambios que así lo ameriten.

4 Definiciones

Activos de Información - son todos los recursos de información, incluyendo datos, sistemas, infraestructuras, servicios y conocimientos, que la organización utiliza para operar y alcanzar los objetivos definidos por el comité ejecutivo. Estos activos son esenciales para el cumplimiento de las metas estratégicas y requieren una gestión adecuada para garantizar su protección y disponibilidad.

5 Responsabilidades

Comité de Seguridad/CISO – Debe velar por el cumplimiento y revisión periódica de la presente política, así como la definición del procedimiento para la clasificación de la información.

Propietarios de los activos:

- Identificar correctamente sus activos de información.
- Clasificar estos activos según criterios de sensibilidad previamente definidos.
- Cumplir con los requisitos de los niveles de clasificación, etiquetado y tratamiento de la información.

- Asegurar que los procedimientos implementados sean adecuados y suficientes para la protección, almacenamiento y mantenimiento de la información.

Colaboradores: son responsables de asegurar la integridad, disponibilidad y confidencialidad de la información que controlan o a la cual tienen acceso, cumpliendo con todas las políticas y procedimientos establecidos dentro del Sistema de Gestión de la Seguridad de la Información.

6 Desarrollo

Se pautarán los lineamientos de uso de activos tales como: correo electrónico, aplicaciones, equipos, recursos de comunicación, Internet, redes sociales, entre otros y establecer los controles que realizará y las responsabilidades de los usuarios.

6.1 Inventario de Activos

Los activos de información y las instalaciones de procesamiento de información deben ser debidamente identificados e inventariados.

6.2 Gestión de Cambios en Activos

Cualquier cambio en los activos de información, incluyendo su adición, eliminación o transferencia de propiedad, debe ser aprobado y documentado conforme a los procedimientos establecidos por el Comité de Seguridad.

6.3 Propietarios de los activos

Los activos inventariados deben tener asignado un propietario. En caso de equipos informáticos de uso personal, el usuario asignado será su propietario. En caso de documentos, tanto digitales como impresos, los mismos serán responsabilidad del Gerente del área considerado, o a quien este delegue.

6.4 Uso Aceptable

Establecer prácticas de uso responsable para todos los activos de información de la organización, garantizando que su empleo sea seguro, conforme a las normas y alineado con los objetivos de la empresa.

Acceso y Autenticación

El acceso a los activos de información se limitará a usuarios autorizados y debe realizarse mediante credenciales seguras y mecanismos de autenticación aprobados por ISA Uruguay. Los usuarios no deben compartir sus credenciales de acceso ni permitir el uso de sus cuentas por otras personas.

Uso Ético y Seguro

Los activos de información deben ser utilizados exclusivamente para fines laborales y en concordancia con los objetivos de la empresa. Está prohibido el uso de estos activos para actividades personales, ilegales, o que puedan comprometer la seguridad de la organización.

Protección de la Información

Todo colaborador es responsable de garantizar la confidencialidad, integridad y disponibilidad de la información que maneja. Esto incluye evitar compartir información confidencial fuera de la empresa y proteger los datos frente a accesos no autorizados o manipulaciones indebidas.

Almacenamiento y Manejo de la Información

La información debe almacenarse en medios autorizados y bajo las condiciones de seguridad definidas. No se permite el uso de dispositivos no autorizados (como discos externos o unidades USB personales) para almacenar información de la organización sin la aprobación explícita del CISO.

Retención y Eliminación de Información

Los activos de información que ya no sean necesarios deben ser eliminados de manera segura siguiendo las pautas establecidas y en conformidad con las normativas legales y reglamentarias aplicables.

Responsabilidad en el Uso de Equipos

Todo equipo (hardware o software) proporcionado por la organización debe utilizarse exclusivamente para fines laborales. Se prohíbe la instalación de software no autorizado y el acceso a sitios web que no estén relacionados con las actividades de la empresa.

Reportes de Incidentes

Todos los colaboradores deben reportar de inmediato cualquier incidente de seguridad o actividad sospechosa que pueda comprometer los activos de información. Los reportes deben realizarse siguiendo el procedimiento establecido por el Comité de Seguridad.

6.5 Control de Acceso

El acceso a los activos de información será concedido bajo un esquema de autorización basado en roles. Los accesos deben ser revisados periódicamente para asegurar que solo el personal autorizado tiene acceso a la información según los principios de necesidad y mínimo privilegio.

6.6 Clasificación de la información

La información debe ser debidamente clasificada por sus propietarios.

La clasificación debe ser realizada en base a los criterios y niveles establecidos en la *Política de Clasificación, Etiquetado y Tratamiento de la Información*.

6.7 Uso de Software Obsoleto

El uso de software obsoleto en la organización está estrictamente regulado para garantizar la protección de los activos de información y la continuidad operativa. Todo software que haya alcanzado su fin de soporte o que represente un riesgo significativo debe ser identificado, evaluado y reemplazado de acuerdo con los procedimientos establecidos por el Comité de Seguridad.

Cualquier excepción debe ser documentada, justificada técnicamente y aprobada por el CISO, asegurando la implementación de medidas de mitigación adecuadas.

LEONARDO NOACH