Política de Seguridad de las Operaciones

Fecha: 20/02/2023
Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
10/11/2022	1.0	Creación del Documento	Comité de Seguridad de la Información

Contenido

1 Revisiones

Fecha	Versión	Descripción	Autor
10/11/2022	1.0	Creación del Documento	Comité de Seguridad de la Información

2 Objetivo

Asegurar la operación correcta y segura de los equipos que procesan información de ISA, así como de sus clientes en los servicios previstos por ella.

3 Alcance

Todos los sistemas de información y activos de Información de ISA ya sea en los equipos administrados por ISA como en los administrados por terceros.

4 Vigencia

La presente norma entra en vigor a partir de su aprobación y publicación por parte del Directorio de la empresa.

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

5 Responsabilidades

- Infraestructura / Operaciones
- Comité de Seguridad

6 Desarrollo

El Área de Infraestructura / Operaciones es responsable de asegurar la correcta gestión de los centros de procesamiento de información que estén bajo su responsabilidad

El Comité de Seguridad es el responsable a través de los Referentes de cada área de velar por la correcta aplicación de la presente política así como de formalizar los procedimientos necesarios para la concientización de los usuarios en los distintos aspectos de seguridad.

Asegurar la correcta operación en las instalaciones de procesamiento de información

- Los procedimientos de operación deben documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
- La formalización y el establecimiento de un procedimiento que permita el adecuado control de los cambios en los sistemas e instalaciones de procesamiento de información.
- Supervisar y adaptar el uso de recursos, así como formular proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido de los sistemas.
- La separación de los recursos para desarrollo, prueba y producción, con el propósito de reducir los riesgos de acceso no autorizado o los cambios al sistema operacional.

Protección ante software malicioso

- La implementación de controles de detección, prevención y recuperación para protegerse contra códigos maliciosos.
- La formalización de procedimientos adecuados para concientizar a los usuarios

Respaldo

Realizar copias de respaldo de la información y del software de acuerdo con los requisitos del negocio y la legislación pertinente y probarse regularmente acorde con los requisitos de respaldo formalmente aceptados.

Control de software en producción

Establecer procedimientos para supervisar la instalación de software en los sistemas operativos y revisarse con regularidad los resultados de las actividades de supervisión.

Gestión de vulnerabilidades técnicas

Se debe obtener regularmente información oportuna acerca de las vulnerabilidades técnicas de los sistemas existentes o en nuevos desarrollos. Así mismo debe evaluarse la exposición de ISA a tales vulnerabilidades, y se debe tomar medidas adecuadas para el tratamiento del riesgo asociado.

El equipo de Infraestructura / Operaciones es el responsable de verificar alertas sobre nuevas vulnerabilidades tanto en software como en hardware.

FIRMADO DIGITALMENTE tuid CERTIFICACIÓN DIGITAL AVANZADA
LEONARDO NOACH