Política de Organización de la Seguridad de la Información

Fecha: 20/03/2022
Versión: 1.1

Control de versiones

Fecha	Versión	Descripción	Autor
10/12/2022	1.0	Creación del Documento	Comité de Seguridad de la Información
20/03/2023	1.1	Revisión del Documento	Comité de Seguridad de la Información

Contenido

1 Objetivo

Definir un marco de referencia de gestión de la implementación y operación de la seguridad de la información, para la distribución de funciones y responsabilidades.

En la presente política se definen las responsabilidades para los distintos roles que tienen que ver con la seguridad y como ISA Paraguay los implementa.

1.1 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.

1.2 Responsabilidades

- Comité de Seguridad de la Información
- Referentes de Seguridad
- Infraestructura / Operaciones

2 Descripción

Comité de Seguridad de la Información

Es responsabilidad del Comité de Seguridad de la Información la definición de evaluaciones periódicas de la Seguridad de la información.

Dichas evaluaciones se llevarán a cabo en conjunto con el equipo de operaciones y los referentes en seguridad de cada área.

Establecer los mecanismos para notificar la Política de Seguridad de la Información y sus modificaciones a todos los usuarios de ISA Paraguay. Actuar como coordinador en temas de seguridad de la información entre las áreas.

Referentes de Seguridad

Implementar los estándares, normas y procedimientos de control necesarios para asegurar el cumplimiento de las políticas de seguridad de la información definidas.

Infraestructura / Operaciones

Monitorear e inspeccionar todo uso de sus recursos de tecnología de información y ante situaciones irregulares iniciar investigaciones administrativas.

Ante la detección de una conducta por parte de un usuario que interfiera con la normal operación de los sistemas de información o no cumpla con las presentes Políticas de Seguridad, el equipo de operaciones tiene la potestad de bloquear preventivamente los permisos de acceso de este.

Propietarios de los activos de información

En ISA Paraguay el rol propietario de los activos de información recae en los gerentes de cada una de las áreas que componen la empresa los que son responsables de:

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de esta para el negocio, así como documentar y mantener actualizada la clasificación efectuada. Definir cuando corresponda un referente de su gerencia para integrar el Comité de Seguridad de la Información.
- Proponer el contenido de cambios y nuevas políticas de seguridad de la información al Comité de seguridad de la información.
- Autorizar la asignación de permisos de acceso a la información a los usuarios de acuerdo con sus funciones y competencias.
- Colaborar con la Gerencia de Operaciones en la implementación de los controles para el almacenamiento, procesamiento, distribución y uso de la información.
- Colaborar con el área Operaciones en la implementación de los controles de seguridad física necesarios para proteger los activos de información.

Todo el Personal

- Cumplir la normativa aplicable en la materia, en particular con lo establecido por las Leyes 1682/2001 y 1969/2002.
- Cumplir con las políticas de seguridad de la información, así como con los procedimientos que se desprendan de estas, independientemente del cargo que desempeñe y de la naturaleza del vínculo con ISA Paraguay.
- Reportar los eventos o incidentes de seguridad de la información que detecte a su jefatura directa o a la mesa de ayuda de Infraestructura/Operaciones.
- Proteger y resguardar toda la información confidencial, reservada o restringida para el negocio, sean estos informes, datos, proyecciones, métodos, estrategias u otros en el cumplimiento de los objetivos estratégicos.
- Participar de las actividades de capacitación y concientización en seguridad de la información que ISA determine.

- Comprender que el uso de cualquier recurso tecnológico brindado por ISA Paraguay es un medio para el correcto desempeño de sus labores.
- Entender que las cuentas de acceso a los sistemas de ISA Paraguay son de uso exclusivamente personal. Se debe proteger las contraseñas y/o cuentas, no permitiendo a otras personas usar las mismas bajo ningún concepto.
- Devolver todo activo que le haya sido confiado para el desarrollo de sus tareas, al finalizar el vínculo con la empresa y/o cambiar su relación laboral o área de trabajo.

Coordinación de la seguridad

Las actividades vinculadas con la seguridad de la información son coordinadas por el Comité de Seguridad de la información y por cada uno de los Gerentes de Servicios que lo componen.

Contactos con autoridades y grupos de Seguridad

ISA procurará mantenerse en contacto con autoridades nacionales e internacionales vinculadas con la seguridad de la información para de esta manera, recibir advertencias, identificar las mejores prácticas utilizadas, compartir e intercambiar información sobre seguridad y buscar siempre mejorar los controles y prácticas implementadas.

Seguridad de la información en la gestión de proyectos

Se integrará la seguridad de información en la gestión de proyectos para minimizar los riesgos de seguridad que puedan surgir en la gestión y ejecución de estos.

Dispositivos Móviles

Asignación de dispositivos móviles y acuerdo de uso.

La asignación de un dispositivo móvil a cualquier usuario debe ser formalmente establecida por el área de Infraestructura / Operaciones.

Seguridad de los dispositivos

Los dispositivos móviles que contienen información confidencial, reservada y/o secreta deben ser asegurados por medio de contraseñas de inicio del sistema.

Los usuarios deben cuidar los equipos de la empresa de acuerdo con lo establecido en el Acuerdo de Uso de dispositivos móviles.

Requisitos de seguridad

La Gerencia de Infraestructura /Operaciones debe mantener el control administrativo del sistema en todos los dispositivos móviles de funcionarios.

Todos los dispositivos conectados a la red de ISA Paraguay deben usar software antivirus/antimalware/firewall y contar con las últimas actualizaciones.

Debiendo a su vez mantener el software del sistema operativo con las últimas actualizaciones de seguridad.

Todo incidente o evento de seguridad asociado a los dispositivos móviles debe ser debidamente reportado a la Gerencia correspondiente y al Comité de Seguridad de la Información.

Trabajo Remoto

Autorización y uso adecuado

El acceso remoto mediante VPN (Virtual Private Network) u otros mecanismos autorizados se suministran exclusivamente para fines laborales. El mismo debe ser ejecutado desde ambientes seguros que no expongan la información a terceros no autorizados.

El comité de seguridad de la organización es el responsable de definir y autorizar los mecanismos para el acceso remoto.

Los activos documentales y de software también son regidos por la presente política y es responsabilidad del Comité de Seguridad reglamentar el uso y custodia de estos.

Requisitos de Seguridad

- La conexión a la red de ISA Paraguay mediante VPN (virtual private network) debe ser cifrada y controlada al menos mediante una autenticación de usuario y contraseña robusta.
- Cualquier tercero que reciba acceso mediante VPN por razones de servicio debe firmar un acuerdo de uso, comprometiéndose a mantener en secreto sus credenciales de seguridad individuales, y a no compartirlas con otros terceros en ninguna circunstancia.

LEONARDO NOACH