Política de Control de Acceso Lógico

Fecha: 20/02/2022
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 Objetivo

Establecer los requisitos mínimos para el acceso lógico a la información de ISA por medio de sus redes, sistemas y aplicaciones.

2 Alcance

Todo el personal de ISA, refiriendo al personal de la plantilla permanente, contratados y proveedores.

3 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.

4 Responsabilidades

- Referentes de Seguridad
- Gerencia de Recursos Humanos
- Infraestructura/Operaciones

5 Desarrollo

5.1 Referentes de Seguridad

Los Referentes de Seguridad de cada una de las áreas de la empresa son los responsables de velar por el cumplimiento de la presente política

5.2 Gerencia de Recursos Humanos

Es responsable de notificar a el área de Infraestructura/Operaciones las modificaciones que sean necesarias respecto al personal para gestionar el acceso lógico.

5.3 Infraestructura/Operaciones

- Asignar técnicamente los accesos a los recursos tecnológicos que administre, luego de recibida la autorización correspondiente por parte de los propietarios de los activos.
- Implementar las medidas técnicas necesarias para dar cumplimiento a la presente política, en los recursos tecnológicos bajo su custodia.

5.4 Propietarios de los activos de información

- Definir y autorizar los derechos y restricciones de acceso a los activos de información, considerando la Política de Clasificación, Etiquetado y Tratamiento de la información.
- Controlar que el personal tenga las autorizaciones necesarias para el cumplimiento de su función basado en el principio de mínimo privilegio para el cumplimiento de su función.
- Informar a los administradores de los sistemas de información de los cambios del personal en sus funciones (altas, bajas o cambio de funciones o roles) que tengan algún impacto en los permisos de acceso a los sistemas.
- Proporcionar la información necesaria a la gerencia de TI o proveedores de sistemas en lo que respecta a definir los requisitos de seguridad necesarios de acuerdo con la clasificación de la información para los nuevos sistemas y aplicaciones que adquiera, desarrolle o mantenga.
- Gestionar las autorizaciones internas en los sistemas de información.
- Gestionar la implementación de las medidas técnicas necesarias para dar cumplimiento a la presente política en los recursos tecnológicos bajo su custodia.

5.5 Requisitos de negocio del control de acceso

Requisitos de control de acceso lógico

Establecer lineamientos de control de acceso lógico en los recursos tecnológicos en base a los requisitos de negocio y seguridad de la información.

Acceso a las redes y a los servicios de red

- Todo acceso a la red y a los servicios de la Administración debe ser controlado y será objeto de un proceso de autorización establecido. Esto incluye el acceso a la red interna de ISA y el acceso a redes externas a través de la misma red interna.
- Todo dispositivo o usuario tendrá acceso únicamente luego de obtener una aprobación expresa a través del proceso de autorización adecuado.
- Cualquier interconexión de la red corporativa hacia redes externas debe contar con una aprobación expresa, así como debe cumplir con todos los requisitos estipulados previamente a dicha interconexión.
- En caso de ser necesario implementar excepciones por limitaciones técnicas, cada caso será planteado ante el Comité de Seguridad y el mismo deberá ser aprobado explícitamente.

Separación en redes

- Todos los servicios publicados en la red de ISA Paraguay deberán estar autenticados como mínimo mediante usuario y contraseña.
- El perímetro de la red debe ser controlado mediante filtros (por ej: firewalls) en tiempo real con reglas que cuenten con autorización previa para proteger adicionalmente a la red y los servicios de accesos no autorizados.

Gestión de acceso del usuario

Cuentas de usuarios

En el manejo de cuentas y sistemas que conciernen a la aplicación o derechos de acceso a la red se deben respetar las siguientes reglas:

- Los usuarios deben tener cuentas de usuarios que los identifique en forma personal única. No se deberán usar cuentas genéricas/ grupales, salvo en casos excepcionales debidamente justificados o por períodos temporales.
- Para asignar derechos de acceso a un usuario se deberá requerir el acuerdo formal de su superior y del propietario de los sistemas.
- Las cuentas con autorizaciones especiales como ser los administradores de sistemas operativos/dispositivos de red/bases de datos, etc. deberán tener un mecanismo de autenticación robusta.
- Las cuentas de administrador no deben ser utilizadas para tareas diarias que no las requieren, se deberá tratar de minimizar la cantidad de cuentas de usuarios administradores existentes.
- Se debe seguir un procedimiento formal y debe llevarse un registro inalterable cuando se atribuyen privilegios o derechos de acceso de administrador.

Control de acceso al sistema y a las aplicaciones

Gestión de permisos de acceso a los sistemas

- La asignación de acceso a los sistemas debe ser estrictamente monitoreada y asignada exclusivamente por una necesidad de conocer y/o hacer.
- Las solicitudes de altas/bajas o modificaciones de autorizaciones debe realizarse de acuerdo con los procedimientos establecidos.
- La asignación de permisos debe ser formalmente solicitada por el propietario de los activos, según los procedimientos establecidos.
- Como mínimo anualmente, los propietarios de los activos deben realizar una revisión de los derechos de acceso otorgado a todos los usuarios y determinar su validez.

- Se debe establecer perfiles de usuarios y roles en los sistemas de aplicación a los efectos de la adecuada asignación y restricción de permisos de acceso.
- Los sistemas considerados críticos o sensibles deben contar con controles adicionales y deberán estar aislados de sistemas con niveles de sensibilidad y accesos diferentes.

FIRMADO DIGITALMENTE tuid CERTIFICACIÓN DIGITAL AVANZADA

LEONARDO NOACH