Política de Control de Acceso

Fecha: 29/11/2024
Versión: 1.0

Control de versiones

Fecha	Versión	Descripción	Autor
18/11/2024	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

Contenido

1 Objetivo

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

2 Alcance

El alcance abarca a todos los colaboradores de ISA Uruguay, incluyendo a la plantilla permanente, contratados y proveedores. Además, se aplica a todos los componentes de la infraestructura de ISA Uruguay, así como a todas sus áreas, garantizando que el personal mencionado y los recursos de terceros sigan los lineamientos establecidos para la seguridad de la información.

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

CISO - Es responsable de definir y supervisar la política de control de acceso en toda la organización. Esto incluye desarrollar esta política, establecer lineamientos de protección de datos, y garantizar que se aplique el principio de mínimos privilegios mediante auditorías periódicas. Lidera la gestión de incidentes críticos, asegurando una respuesta adecuada y tomando acciones preventivas para evitar futuras ocurrencias. Coordinar la capacitación en prácticas de seguridad de la información para todo el personal y establecer políticas específicas para el acceso remoto seguro, como el uso de VPN y autenticación multifactor. El CISO colabora con las áreas para definir perfiles de acceso y gestiona herramientas para un control adecuado.

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.

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.

Propietarios de la 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 los colaboradores tengan 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 infraestructura 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

Colaboradores:

Uso de Contraseña

- Los Colaboradores no compartirán sus contraseñas con nadie y evitarán mantener un registro electrónico o en papel de estas, a menos que dichos registros puedan ser almacenados con seguridad.
- Los Colaboradores deberán cambiar sus contraseñas periódicamente o cuando por razones justificadas se le solicite, siempre que el sistema lo permita.
- Los Colaboradores no deberán utilizar la contraseña actual cuando se les exija cambiar la misma. En otras palabras, deben elegir una contraseña diferente cada vez que se les solicite cambiarla.
- Los Colaboradores evitarán utilizar contraseñas que puedan ser adivinadas fácilmente. Estos son algunos ejemplos de contraseñas a ser evitadas:
    - Sus nombres, el de su cónyuge o hijos, o nombres de mascotas.
    - Número de matrícula, de teléfono o de cédula.
    - La marca de su automóvil, el nombre de la calle en la que viven, etc.
    - Fechas de nacimiento, especiales, propias, de su cónyuge o hijos

Todo usuario de una estación de trabajo debe:

- En caso de alejarse o desatender su estación de trabajo, incluso por unos pocos minutos, bloquear el acceso a la misma.
- Cerrar todas las sesiones activas una vez terminada la tarea.
- Siempre que sea posible, cerrar la sesión y apagar la computadora cuando la misma no esté en uso.

Otros requisitos:

Los funcionarios deben tomar todas las medidas necesarias para prevenir el acceso no autorizado a través de su estación de trabajo.

5 Descripción

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.

Control de Acceso a la Red

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 autorizado mediante un proceso establecido. Esto incluye tanto el acceso a la red interna de ISA Uruguay como el acceso a redes externas a través de la red interna.
- Todo dispositivo o usuario solo tendrá acceso después de la solicitud, aprobación por el gerente del área y el CISO, seguido de la configuración por TI y registro para auditoría.
- Toda conexión con redes externas debe cumplir con los siguientes requisitos: configuración de firewall y control de acceso, autenticación multifactor, cifrado de comunicaciones, monitoreo y registro, aprobación del CISO e Infraestructura, pruebas de seguridad previas y cumplimiento normativo.
- En caso de ser necesario implementar excepciones por limitaciones técnicas, cada caso será planteado y debidamente documentado ante el Comité de Seguridad y el mismo deberá ser aprobado explícitamente.

Separación en redes

- Todos los servicios publicados en la red de ISA Uruguay 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 Colaboradores 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.
- Regularmente se deberá realizar una revisión de los derechos de acceso (al menos una vez al año).

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 Colaboradores 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.

Gestión de Contraseñas del Usuario

- El acceso lógico a los sistemas sólo debe ser posible utilizando un proceso de conexión segura:
- Todo acceso a datos de los sistemas de información que no son públicos debe requerir autenticación. La información será accesible una vez que el proceso de conexión (autenticación) haya sido completado.
- Se deberán proteger las estaciones de trabajo bloqueando la sesión luego de un período de inactividad a determinar solicitando al usuario ingrese su identificación nuevamente.
- Asimismo, el sistema de gestión de contraseñas debe:
    - Permitir que un usuario pueda cambiar su contraseña y forzarlo a cambiarla de conformidad con las reglas predefinidas.
    - Enmascarar la contraseña mientras se está ingresando

Control de Acceso al Sistema Operativo

- La identificación de usuarios en todos los sistemas operativos se realiza por medio de usuario de identificación único y personal.
- No se deberán usar cuentas de usuarios genéricas o grupales, salvo en casos excepcionales debidamente justificados.
- Todos los sistemas operativos locales o de red utilizados deben contar, en caso de que sea soportado, con un sistema de gestión de contraseñas que fuerce el cumplimiento de las directivas establecidas.
- Se debe gestionar los siguientes elementos:
    - Largo mínimo de contraseñas.
    - Complejidad de contraseñas.
    - Cambio de contraseñas periódica
    - Diccionario de contraseñas anteriores.
    - Bloqueo de cuentas.

- Registro de eventos.

Control del acceso a las aplicaciones y a la información

- Los sistemas de control de acceso a las aplicaciones e información deben seguir los mismos criterios y exigencias establecidos previamente para los sistemas operativos.
- El acceso a la información y funcionalidades de los sistemas de aplicación deben ser formalmente asignados en base al acceso mínimo necesario.
- La asignación de permisos debe ser formalmente solicitada por el supervisor del colaborador y aprobadas por el propietario del activo de información
- Se deben establecer perfiles de usuarios y roles a nivel de los sistemas de aplicación, a los efectos de la adecuada asignación y restricción de permisos de acceso.

Trabajo Remoto

- El acceso remoto mediante VPN 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.
- En virtud de los riesgos asociados, los privilegios de los usuarios y la sensibilidad de la información, se deberán incorporar medidas de autenticación más robustas a las utilizadas para la conexión incorporando autenticación en base a dos factores distintos siempre que accedan a los sistemas centrales ISA Uruguay.
- Cualquier tercero que reciba acceso remoto por razones de servicio debe firmar un acuerdo de uso, comprometiéndose entre otros aspectos a mantener en secreto y proteger sus credenciales de seguridad individuales, y a no compartirlas con otros terceros en ninguna circunstancia

LEONARDO NOACH