



SEGURIDAD DE LA

INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento, así como hacer obras derivadas, siempre y cuando tenga en cuenta citar la obra de forma específica.

Política de Control de acceso lógico

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 2.0 | **Categoría** | Política |
| **Última actualización** | 11/075/2022 | **Estado** |  |

# Objetivo

Establecer los lineamientos generales para controlar el acceso lógico a los activos de información.

# Alcance

Todo el personal o proveedores que presten servicios a la organización que requieran acceso lógico a la red, recursos de red y/o cualquier sistema de información de la organización.

# Responsabilidades

**Responsable de seguridad de la información** debe velar por el cumplimiento de la presente política.

**Propietarios de los activos** son responsables por definir y autorizar los derechos y restricciones de acceso a los activos de información, considerando la política de clasificación de la información.

**Gestión humana** es responsable por comunicar a las gerencias de área y a los propietarios de activos, en tiempo y forma las altas, bajas y modificaciones que sean necesarias en relación al personal para que se gestionen los accesos lógicos en tiempo y forma.

**Responsable de tecnología de la información** es responsable de la asignación técnica de los accesos a la red, recursos de red y/o cualquier sistema de información de la organización luego de recibida la autorización correspondiente por parte de los propietarios de los activos.

# Políticas relacionadas

Política de Gestión de usuarios y contraseñas

Política de Finalización o cambio de relación laboral

# Descripción

La organización debe:

1. Determinar los mecanismos de autorización de acceso a los activos de información
2. Contar al menos con un procedimiento formalmente definido para gestionar y controlar los accesos lógicos en la organización que contemple al menos la solicitud, aprobación, revocación y notificación de las solicitudes de autorización de acceso.
3. Contar con un procedimiento formalmente definido para la revisión de los derechos de acceso lógicos. El resultado de la revisión debe ser documentado e informado al responsable de seguridad de la información, a las gerencias y a los propietarios de los activos.
4. Definir la periodicidad de las revisiones de acceso lógico.

Las autorizaciones de acceso deben habilitar el acceso a la información mínima necesaria para el cumplimiento de las tareas asignadas.

La autorización de acceso a activos de información para proveedores u organizaciones externas requiere de acuerdos específicos aprobados por la Dirección o por quien ésta designe.

En relación al acceso de los usuarios privilegiados se deberá mantener un registro de los privilegios asignados en cada sistema o red.

No se podrá otorgar derechos de acceso sin haberse completado el proceso de autorización.

Queda prohibido el uso de códigos de usuarios o contraseñas embebidas, o cualquier otro mecanismo que permita el acceso salteando las reglas de seguridad establecidas por la organización.

# Cumplimiento

Se destaca que el incumplimiento de la presente política aumenta la exposición de la información y el riesgo de tener un incidente de seguridad de la información. Ante la verificación de un incumplimiento la Dirección podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

# Historial de revisiones

|  |  |  |
| --- | --- | --- |
| **Fecha de revisión** | **Responsable** | **Resumen de cambios** |
|  |  |  |

