



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 Gestión de usuarios y contraseñas

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 2.0 | **Categoría** | Política |
| **Última actualización** | 11/07/2022 | **Estado** |  |

# Objetivo

Establecer los lineamientos para la adecuada asignación y uso de las cuentas de usuarios y contraseñas.

# Alcance

Todas las cuentas de usuarios y contraseñas utilizadas en los sistemas y aplicaciones existentes.

# Responsabilidades

**Responsable de seguridad de la información** debe velar por el cumplimiento de la presente política y realizar las revisiones oportunas.

**Responsable de tecnología de la información** es responsable por la implementación técnica de esta política.

**Personal** es responsable por cumplir con lo establecido en la presente política. En particular, las personas con usuario privilegiado deberán responder directamente por las operaciones y transacciones que se ejecuten con las cuentas de usuario asignadas bajo su responsabilidad.

# Políticas relacionadas

Política de control de acceso lógico

Política de Finalización o cambio de relación laboral

Política de controles criptográficos

# Descripción

La organización debe contar con procedimientos formalmente definidos que cubran los siguientes puntos:

1. Altas, bajas y modificaciones de usuarios y derechos de acceso lógico
2. Altas, bajas y modificaciones de usuarios con acceso privilegiado
3. Autorizaciones de acceso lógico
4. Revisión de los derechos de acceso lógico

Los usuarios y contraseñas a recursos de la organización son personales e intransferibles.

No se permite utilizar usuarios genéricos, salvo excepciones debidamente analizadas y autorizadas por el responsable de seguridad de la información.

Toda cuenta de usuario debe tener asignada una contraseña.

Toda persona es responsable de la actividad asociada a su usuario. La organización debe registrar la actividad de los usuarios, para su posterior control en caso de ocurrencia de incidentes.

Las contraseñas deben requerir cierto nivel de complejidad mínimo y no pueden estar asociadas a datos personales que permitan su deducción como, por ejemplo: nombres propios, nombre de usuario, números de documento, dirección, teléfono, etc.

Las contraseñas deben cumplir, al menos, con los siguientes requerimientos:

1. Longitud mínima de 8 caracteres,
2. Estar formada por al menos 3 características de las siguientes:
3. Caracteres alfabéticos mayúsculas
4. Caracteres alfabéticos minúsculas
5. Caracteres numéricos
6. Caracteres especiales o extendidos

Deberá establecerse la validez de las contraseñas; el plazo dependerá de la criticidad del sistema de información al cual se accede.

Se debe:

1. Forzar al usuario a cambiar su contraseña en su primer uso y/o luego de ser asignada por un administrador de sistema.
2. Realizar el bloqueo de la cuenta luego de reiterados intentos fallidos de inicio de sesión.
3. Garantizar que el almacenamiento y la transmisión de las contraseñas de usuario se realizan de forma segura, de manera tal que los administradores de sistemas o todo aquel que cuente con usuario privilegiado, no tenga acceso a las mismas.

## Usuarios con acceso privilegiado

La solicitud de una cuenta de usuario privilegiado debe ser realizada por el Jerarca autorizado, con la justificación de necesidad de uso y dirigida al Responsable de Tecnología de la Información, quien cumplirá con la solicitud de acuerdo a lo establecido en el procedimiento definido.

Las cuentas de usuario privilegiado sólo deben ser otorgadas al personal de nivel técnico apropiado y únicamente para el cumplimiento de sus funciones.

Los accesos realizados con cuentas de usuario privilegiados deben ser registrados y controlados periódicamente.

Una cuenta de usuario privilegiado sólo podrá ser utilizada en la actividad de administración o configuración del sistema para la cual se requieren dichos privilegios. No podrá ser utilizada en actividades rutinarias para la que exista un perfil de menores privilegios que lo permita.

No se podrán utilizar las cuentas de usuario privilegiado definidas por defecto en sistemas y componentes, ADMIN, ROOT o similares. Siempre que sea posible las mismas deben ser eliminadas o deshabilitadas, además de modificadas sus contraseñas por omisión. Se debe contar con un mecanismo de recuperación de acceso privilegiado, dicho mecanismo debe mantener las garantías de reserva.

El acceso privilegiado debe realizarse desde dispositivos debidamente fortalecidos para tal fin.

# 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** |
|  |  |  |

