



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 Uso institucional de redes sociales

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 3.0 | **Categoría** | Política |
| **Última actualización** | 24/05/2022 | **Estado** |  |

# Objetivo

## Gestionar de manera segura los perfiles de redes sociales utilizados por la organización.

# Alcance

## Todos los perfiles de carácter institucional utilizados por la organización en las redes sociales.

# Responsabilidades

**La Dirección** es responsable por difundir la presente política a todo el

personal, independientemente del cargo que desempeñe o de su relación contractual.

**Responsable de Seguridad de la Información** debe velar por el cumplimiento de la presente política. Deberá identificar y promover los controles de seguridad de la información para habilitar el acceso a un proveedor a los activos de información.

Responsable de las comunicaciones debe velar por el contenido de lo que se publica en redes sociales.

# Políticas relacionadas

Política de Seguridad de la Información

Política de Uso aceptable de los activos

Política de Uso de Internet

Política de Finalización o cambio en la relación laboral

# Descripción

La organización puede crear su perfil oficial en las redes sociales (por ejemplo: Instagram, Facebook, Twitter, YouTube) para dar a conocer sus programas, actividades y otros temas de interés, y para tener un contacto directo con la ciudadanía o clientes, y de esta manera poder conocer sus necesidades y requerimientos. No obstante, se debe cumplir con los lineamientos expresados a continuación.

1. La organización no se hace responsable de los sitios web no propios a los que se puede acceder mediante vínculos (links) desde nuestros perfiles o de cualquier contenido puesto a su disposición por terceros, que incluyan fotos, documentos, vídeos y otros contenidos.
2. Si se detecta un contenido potencialmente inseguro, se debe reportar al Responsable de seguridad de la información, y eliminar si corresponde.
3. Se debe tener claramente identificadas las personas (y sus correspondientes usuarios) con acceso a los perfiles en redes sociales, debiendo estos corresponder con cuentas institucionales y no personales.
4. Las cuentas utilizadas para recuperación de los datos de acceso deben ser institucionales.
5. Se deberá seguir las pautas y procedimientos definidos por la organización, para el traspaso de usuarios en casos de cambio o desvinculación de los administradores de los perfiles.
6. Siempre que la red social lo permita, se debe verificar la cuenta, de manera de garantizar a los ciudadanos o clientes que es la cuenta oficial de la organización.
7. La contraseña utilizada en cada cuenta de red social debe ser diferente; la misma deberá ser una contraseña segura conforme a las pautas establecidas en las políticas vigentes.

# Cumplimiento

Se destaca que 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** |
|  |  |  |

