



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 Relacionamiento con proveedores

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 1.0 | **Categoría** | Política |
| **Última actualización** |  | **Estado** |  |

# Objetivo

Mantener la seguridad de los activos de información que deban ser accedidos por proveedores.

# Alcance

Todos los activos de información que deban ser accedidos por proveedores.

# Responsabilidades

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

**Propietario del activo** es responsable por evaluar y, autorizar o negar las solicitudes de acceso a los activos de información que se encuentren bajo su responsabilidad.

**Responsable de tecnología de la información y/o el responsable de seguridad física**, son responsables por la asignación técnica de los permisos de acceso sobre los activos de información que hayan sido previamente autorizados a los proveedores.

# Políticas relacionadas

Política de gestión de acceso lógico

Política de gestión de acceso físico al centro de datos

Política de gestión de acceso físico a áreas seguras

Política de gestión de incidentes de seguridad de la información

# Descripción

La organización debe:

1. identificar todos los proveedores de servicios que requieran el acceso tanto físico como lógico a activos de información. Un manejo inadecuado de la seguridad de la información en el relacionamiento con proveedores puede poner en riesgo la imagen la organización ante la pérdida, robo, acceso no autorizado o divulgación no autorizada de información.
2. contar con un procedimiento formal para la identificaciónde los proveedores, que incluya el tipo de información que deberán acceder y los requisitos de seguridad mínimos para cada tipo de activo de información. La información recabada mediante este procedimiento, servirá de base para el establecimiento de la relación formal con los proveedores, contratos y acuerdos de niveles de servicios que deben existir para cada proveedor. Se debe establecer formalmente en los contratos y acuerdos las obligaciones de ambas partes (organización y proveedor) en relación a la seguridad de la información. Asimismo, se debe establecer la posibilidad de derecho a auditar los procesos y controles de los proveedores de servicios de la organización relacionados con el acuerdo.
3. considerar la gestión de incidentes de seguridad de la información asociada al acceso a activos de información por parte de proveedores. Los incidentes de seguridad de la información deberán ser gestionados según lo acordado en la Política de gestión de incidentes de seguridad de la información.

# 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** |
|  |  |  |

