



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 riesgos de seguridad de la información

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

# Objetivo

Fijar los criterios básicos necesarios para la gestión del riesgo de seguridad de la información en la organización.

# Alcance

Todos los activos de información del organismo, incluso aquellos gestionados mediante contratos con terceros.

# Responsabilidades

**Dirección** es responsable por generar las condiciones adecuadas para la ejecución y comunicación de la presente política, así como de establecer el alcance para su aplicación. Además será quien defina el nivel aceptable de riesgos y validará los planes de tratamiento.

**Propietarios de los activos de información** tendrán que dar aplicación a la presente política e identificar, estimar y valorar los riesgos identificados. Es responsable, en conjunto con el responsable de seguridad de la información, por la definición de las acciones de tratamiento de los riesgos de seguridad de la información.

**Equipo responsable de gestión de riesgos o Responsable de seguridad de la información** debe velar por el cumplimiento de la presente política y brindar asesoramiento en la identificación de las amenazas que pueden afectar a los activos de información y las vulnerabilidades que propician las mismas e informar al Comité de Seguridad de la Información y/o la Dirección sobre los resultados de la evaluación de los riesgos. Además, debe velar por el cumplimiento de la presente política. Es responsable, en conjunto con los propietarios de los activos de información, por la definición de las acciones de tratamiento de los riesgos de seguridad de la información.

# Políticas relacionadas

Política de Continuidad de las operaciones

# Descripción

La Dirección del organismo reconoce la importancia de preservar los activos de información, por lo que asigna alta prioridad a la gestión de riesgos a través de la identificación, evaluación y tratamiento de los riesgos relativos a la seguridad de la información.

El organismo debe:

1. Establecer, formalizar y poner en práctica una metodología para la gestión de riesgos.
2. Definir y establecer en forma explícita el nivel de aceptación del riesgo por parte de la Dirección.
3. Realizar evaluaciones periódicas de riesgo en seguridad de la información; contemplando las etapas de identificación, análisis, y valoración del riesgo.
4. Contar con la aprobación explícita de los planes de tratamiento del riesgo residual.
5. Mantener informadas a las partes involucradas sobre el estado del riesgo.

# 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** |
|  |  |  |

