



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 de controles criptográficos

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

# Objetivo

Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información digital.

# Alcance

Toda la información digital más allá de su clasificación, que requiera ser protegida para mantener la confidencialidad, autenticidad e integridad.

# Responsabilidades

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

**Responsable de tecnología de la información**, es el responsable de la gestión técnica de los controles criptográficos.

**Personal y proveedores** deben cumplir con lo establecido en la presente política.

# Políticas relacionadas

Política de Intercambio de información

# Descripción

La organización deberá determinar las herramientas criptográficas basadas en algoritmos probados y aceptados por la industria que serán utilizados para proteger la información. Proporcionará también los recursos necesarios para el soporte de hardware adecuado, así como para su protección física y lógica.

Se deben utilizar controles criptográficos en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera del ámbito de la organización.
3. Para el resguardo de información, cuando así surja de la evaluación de riesgos.

La organización debe:

1. Definir procedimientos para la gestión de claves, la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.
2. Asignar los roles del responsable de la gestión de claves.
3. Establecer los algoritmos de cifrado a utilizar para los distintos escenarios, así como la longitud de la clave.

# 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** |
|  |  |  |

