



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 Respaldo de información

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

# Objetivo

Preservar la información de la organización o en poder de ésta y poder restaurarla en tiempo y forma en caso de pérdida.

# Alcance

Toda la información que esté soportada en medios de almacenamiento lógicos.

# Responsabilidades

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

**Propietarios de los activos de información** son responsables por establecer la frecuencia de respaldo y el tiempo de retención de éstos.

**Responsable de tecnología de la información** es responsable por proveer los medios técnicos para la realización de los respaldos y el cumplimiento de la presente política.

# Políticas relacionadas

Política de continuidad de las operaciones y recuperación ante desastres

Política de controles criptográficos

# Descripción

La organización debe contar con un plan y un procedimiento formales para la realización de los respaldos, para garantizar que la información pueda ser reconstruida en caso de pérdida u otra necesidad.

Los propietarios del activo determinarán la frecuencia y tiempo de retención del respaldo, teniendo en cuenta el marco normativo aplicable, así como la valoración del activo a fin de minimizar la pérdida o destrucción total o parcial del mismo, su disponibilidad y confidencialidad. Esta información debe reflejarse en el plan y procedimiento de respaldos.

Los respaldos deben ser probados en intervalos regulares a los efectos de garantizar su confiabilidad ante la necesidad de uso en caso de emergencia. Se debe definir un procedimiento de prueba de respaldos, así como la periodicidad de su ejecución.

Se debe tener en consideración la confidencialidad de la información y en caso que sea requerido, los respaldos deberán estar cifrados de conformidad con la política establecida.

El organismo debe disponer de un lugar adecuado para el almacenamiento seguro de los respaldos que sea consistente con las medidas de protección ambiental del sitio principal.

Se debe contar con respaldos fuera del sitio principal (off-site), conservando las condiciones ambientales consistentemente con las del sitio operativo y con controles de seguridad física adecuados. Debe definirse un procedimiento donde se defina la frecuencia y las actividades necesarias para la transferencia de los respaldos fuera del organismo.

# 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** |
|  |  |  |

