



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 Intercambio de información

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

# Objetivo

Establecer los criterios sobre la protección de la información cuando la misma es objeto de traslado o intercambio por medios físicos como papel, medios magnéticos de almacenamiento o cualquier otro medio tangible conocido o por conocer, que oficie de contenedor de dicha información; así como la información contenida en medio lógicos; debiendo velar en todo momento por la cadena de custodia.

# Alcance

Toda la información más allá de su clasificación, que en el accionar de la organización, sea objeto de manipulación, traslado o intercambio por medios físicos.

# Responsabilidades

**Responsable de seguridad de la información** debe velar por el cumplimiento de la presente política.

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

# Políticas relacionadas

Política de Cifrado

# Descripción

La organización debe:

1. Definir controles y procedimientos para asegurar la protección de la información durante su intercambio. En particular, se deberá establecer un procedimiento formal que describa las actividades necesarias para el traslado físico de información; el mismo deberá comprender todas las dependencias y locaciones de la organización.
2. Establecer acuerdos de no divulgación con el personal, clientes y proveedores externos que por diversas razones requieran conocer o intercambiar información restringida o confidencial de la organización
3. Establecer acuerdos de intercambio de información (incluyendo la trazabilidad, el no repudio, etiquetado, cadena de custodia, control de acceso) para intercambiar información entre las diferentes áreas del organismo y fuera de éste
4. La información transmitida por correo electrónico desde y hacia direcciones pertenecientes la organización debe estar protegida

El medio en el cual traslade la información, física o lógica, debe garantizar su integridad durante todo el tiempo que insuma el traslado de la información siempre en la medida razonable en relación al carácter de la información contenida y su clasificación.

Si así lo requiere la información contenida, el medio debe garantizar la reserva o confidencialidad de ésta, incluso ante la o las personas que efectúen el traslado o manipulación.

Atento al carácter de la información, de acuerdo a su clasificación, el medio debe resguardar el acceso a la misma durante el traslado o manipulación. El medio debe proporcionar información básica suficiente que haga inequívoca la identificación de lo que contiene y el asunto o tema que involucra el contenido.

En lo que refiere a información en soporte físico, se deberá detallar de forma clara y comprensible, el remitente y destinatario, sean estas personas físicas o jurídicas, así como fecha completa de envío y hora si corresponde, por ejemplo, a efectos de requerimientos jurídicos.

# 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** |
|  |  |  |

