



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 Cumplimiento

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 2.0 | **Categoría** | Política |
| **Última actualización** | 27/06/2022 | **Estado** |  |

# Objetivo

Lograr que todas las obligaciones legales, reglamentarias y contractuales que afectan a la organización estén debidamente identificadas, documentadas y actualizadas.}

# Alcance

Todas las operaciones de la organización.

# Responsabilidades

**Dirección** es responsable por identificar toda la normativa aplicable con el fin de cumplir con los requisitos de acuerdo al contexto en el que cumple sus funciones, teniendo en cuenta aspectos legales y regulatorios, contratos, etc.

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

# Descripción

La organización debe tener identificada toda la normativa vigente relacionada a sus operaciones.

A continuación, se lista de forma no taxativa, la normativa en materia de seguridad de la información que podría aplicar:

1. Ley 18.331: Protección de datos personales y acción de habeas data
2. Ley 18.381: Acceso a la información pública
3. Decreto 451/009: Centro Nacional de Respuesta a Incidentes de Seguridad Informática
4. Decreto 452/009: Política de seguridad de la información
5. Decreto 92/014: Ciberseguridad
6. Leyes que declaren secreta información (secreto tributario, secreto estadístico, secreto bancario, etc.)

Si la organización, como parte de sus procesos operativos, debe relacionarse con otros países, la Dirección deberá considerar el cumplimiento en toda la normativa extranjera que sea pertinente.

Se debe hacer uso legal de los productos de software e información y mantener control de las licencias de software.

Se deben realizar revisiones independientes de seguridad de la información para asegurar la adecuación del sistema de gestión de seguridad de la información, y su cumplimiento con la normativa vigente y el Marco de Ciberseguridad. Estas revisiones podrán constar de hackeos éticos, pruebas de penetración, evaluación de vulnerabilidades y auditorías de seguridad de la información, y deben ser realizadas por personal (interno o externo) independiente del área donde se encuentran los servicios bajo revisión. Los resultados de las revisiones independientes son informados a las Gerencias, al Responsable de Seguridad de la Información, el Comité de Seguridad de la Información y a la Dirección.

# 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** |
|  |  |  |

