Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente



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 Seguridad del equipamiento

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

# Objetivo

El equipamiento debe protegerse contra amenazas, tanto físicas como ambientales. Para esto se debe reducir el riesgo de accesos no autorizados, así como también prevenir pérdidas, daños, hurtos o comprometer los activos y/o la interrupción de las actividades del organismo. Se pretende garantizar la continuidad de las operaciones y reducir los efectos causados por errores humanos (accidentales o intencionales) o desastres naturales a través de la implementación de controles físicos y ambientales en los centros de datos y áreas relacionadas (por ejemplo, recinto donde se almacenan los respaldos).

# Alcance

Afecta a toda la infraestructura tecnológica de la organización, en especial a los centros de datos y áreas relacionadas.

# Responsabilidades

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

**Dirección** es responsable de disponer de los recursos necesarios para la implementación de la presente política.

**Personal** es responsable por cumplir con los procedimientos y políticas que estén orientados a la protección y aseguramiento del equipamiento en su poder.

# Políticas relacionadas

Política de destrucción de información

Política de acceso físico a áreas seguras

Política de intercambio de información

Decreto 92/014

# Descripción

Los equipos que conforman la infraestructura tecnológica de la organización tales como, servidores, equipos de comunicaciones, centrales telefónicas, estaciones de trabajo, dispositivos de almacenamiento, etc. que procesen información, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado, adoptando los controles necesarios para mantener estos equipos alejados de sitios que puedan tener riesgo de amenazas físicas y/o ambientales. Las medidas tomadas deberán ser proporcionales a los riesgos identificados.

La gerencia de Tecnología monitoreará, mediante mecanismos adecuados, las condiciones ambientales de las zonas donde se encuentre el equipamiento.

En caso de pérdida o robo de un equipo, se deberá comunicar a la gerencia de Tecnología para que esta pueda informar inmediatamente a la autoridad correspondiente y denunciar ante la autoridad competente, y al Responsable de Seguridad de la Información para que lo registre como incidente de seguridad de la información y realice el tratamiento que corresponda.

Se debe tener en cuenta el cumplimiento con lo establecido en el Decreto 92/014.

**Retiro del equipamiento fuera de las instalaciones**

Todos quienes trabajan en la organización son responsables de velar por la seguridad de los equipos propiedad de la organización, que se encuentren fuera de las instalaciones de esta, siguiendo las siguientes directrices:

1. No dejar los equipos de cómputo desatendidos en lugares públicos o a la vista.
2. Los equipos de infraestructura deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.
3. Los equipos portátiles siempre deben ser llevados como equipaje de mano.
4. El retiro de equipamiento, propiedad de la organización, fuera de las instalaciones del mismo debe seguir los procedimientos establecidos, contemplando cláusulas de confidencialidad e integridad de la información sensible que esté contenida en dicho equipamiento.

**Eliminación o reutilización segura de equipos y medios**

El Organismo debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura, alineados a la política de destrucción de información.

Cuando un equipo sea reasignado o dado de baja, se deberá asegurar la información para luego eliminarla, con el fin de evitar pérdida y/o recuperación no autorizada de la misma.

# 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** |
|  |  |  |

