



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 Control de acceso físico a áreas seguras.

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

# Objetivo

Establecer los lineamientos generales para controlar el acceso físico a las áreas seguras de la organización, con el objetivo de minimizar el riesgo de accesos no autorizados.

# Alcance

Esta política aplica a todo el personal, proveedores, visitantes, etc. que necesiten acceso a áreas seguras y tengan la autorización correspondiente.

# Responsabilidades

**Responsable de seguridad de la información** es responsable de gestionar la presente política y velar por su cumplimiento.

**Responsable de accesos** es responsable degestionar el control de acceso al área segura y comunicar las asignaciones de los roles entre todas las partes.

**Responsable de la infraestructura** es responsable deasignar los accesos permanentes y temporales al centro de datos.

**Personal con acceso a áreas seguras** es responsable de controlar los accesos a áreas seguras, realizar el acompañamiento de los visitantes y controlar las actividades que se llevan a cabo en dichas áreas.

**Personal de tecnología de la información / infraestructura / administración de red / portería** es responsable por el registro y acompañamiento de los visitantes y revisión de las actividades que realizan en el centro de datos.

# Descripción

Se debe contar con un procedimiento formal para gestionar y revisar periódicamente, los accesos a las áreas seguras. El acceso a áreas seguras se deberá conceder únicamente por motivos específicos y autorizados.

**Gestión de accesos**

Los accesos de tipo permanente deben ser asignados por el responsable de accesos, a aquel personal que así lo requiera en base a requisitos basados en su función en la organización.

Los accesos de tipo temporal, por ejemplo, para el caso de proveedores externos y contratistas, deben ser solicitados al responsable de accesos y autorizados por el responsable de seguridad de la información y se debe proveer al menos la siguiente información: nombre, apellido, cédula de identidad, empresa, fecha de inicio de acceso temporal, fecha fin de acceso temporal, motivo. Los visitantes temporales que requieran acceso a áreas seguras o centros de datos deberán permanecer acompañados de personal con permisos de acceso y portar una identificación visible.

En el caso del centro de datos, se debe registrar la visita en una bitácora de ingresos que deberá contener al menos la siguiente información: fecha, nombre, apellido, cédula de identidad, empresa, hora de entrada, hora de salida, nombre y apellido del funcionario que lo acompaña.

En relación al acceso al centro de datos, se deberá cumplir con lo establecido a continuación.

**Sistema de control de acceso**

1. El acceso al centro de datos deberá realizarse mediante un sistema de autónomo de control de acceso, por ejemplo, con lectores de tarjetas magnéticas, identificación por radiofrecuencia (RFID) o sistemas biométricos
2. El sistema de control de acceso puede ser administrado remotamente y debe mantener información histórica de accesos al centro de datos
3. Se debe contar con un sistema cerrado de TV

**Revisión de accesos al centro de datos**

1. Se debe establecer un procedimiento formal de revisión periódica de los accesos al centro de datos que contemple la información del sistema de control de acceso, el registro de ingresos al centro de datos, el personal con acceso permanente y con acceso temporal.

**Medidas de seguridad interna**

1. Se prohíbe el ingreso al centro de datos con material combustible, líquidos, productos volátiles, y todo producto o sustancia que pudiera ocasionar una reacción química perjudicial para la infraestructura del centro de datos
2. Los pasillos de circulación interna deben mantenerse despejados de todo objeto.

# 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** |
|  |  |  |

