



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 Registro y auditoria de eventos de sistemas de información

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 2.0 | **Categoría** | Política |
| **Última actualización** | 11/07/2022 | **Estado** |  |

# Objetivo

Monitorear y registrar los eventos de dispositivos de red y sistemas informáticos para detectar posibles fallas o situaciones inesperadas, generar evidencia y actuar con la mayor premura posible.

# Alcance

Todos los sistemas informáticos y dispositivos de red de la organización.

# Responsabilidades

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

**Responsable de tecnología de la información** es responsable por la gestión del monitoreo de los elementos que componen la red, recursos de red y/o cualquier sistema informático de la organización, así como de la revisión periódica de los registros.

# Políticas relacionadas

Política de Gestión de cambios

Política de Gestión de incidentes de seguridad de la información

# Descripción

La organización debe:

1. Contar con procedimientos formales que soporten la gestión del monitoreo de los elementos de red y sistemas informáticos
2. Registrar los eventos y definir el tiempo de retención de éstos
3. Definir la periodicidad de las revisiones de los registros
4. Revisar periódicamente los registros de eventos

Se debe registrar, al menos:

1. Fechas y horarios
2. Origen
3. Destino
4. Conexiones
5. Acciones
6. Inicio de sesión fallidos
7. Cambios en las configuraciones de los sistemas

La hora de los sistemas informáticos debe estar sincronizada con una sola fuente de referencia de tiempo.

Los registros deben estar protegidos contra posibles alteraciones o accesos no autorizados.

# 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** |
|  |  |  |

