



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 Protección contra software malicioso

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

# Objetivo

Asegurar que la información y los sistemas informáticos que la procesan se encuentren protegidos contra software malicioso (por ejemplo: virus, gusanos, troyanos, spyware, adware intrusivo, crimeware, entre otros).

# Alcance

Todos los sistemas informáticos que soportan los procesos de negocio del organismo.

# Responsabilidades

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

**Responsable de tecnología de la información** es responsable por la gestión técnica relacionada a la presente política.

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

# Descripción

Se debe utilizar una solución antivirus corporativo que cumpla con:

1. Estar posicionada entre las de mejor desempeño por parte de al menos un análisis periódico, independiente e internacionalmente reconocido en las últimas dos revisiones
2. De preferencia incluir dispositivos móviles como parte de la solución
3. De preferencia implementar seguridad de navegación y correo

La organización debe:

1. Definir procedimientos y responsabilidades de gestión para la protección de los sistemas ante software malicioso.
2. Brindar capacitación al personal afectado en la operación y uso de la solución antivirus, así como cualquier otro mecanismo utilizado para la detección de software malicioso.
3. Concientizar a los usuarios finales sobre las formas en las que se puede adquirir el software malicioso, los riesgos y problemas que acarrea, así como sobre el procedimiento que se debe seguir en caso de sospechar o constatar estar afectado (tanto en los equipos informáticos a los cuales accede regularmente como otros en los que haya detectado su presencia). Este procedimiento debe estar formalizado y difundido a nivel de todo el organismo.
4. Contar con controles que prevengan y detecten el uso de software no autorizado (por ejemplo, lista blanca de aplicaciones), ya que estos pueden abrir la puerta a software malicioso.
5. Contar con controles que eviten el acceso a sitios web maliciosos y/o no autorizados (por ejemplo, listas negras).
6. Analizar periódicamente los sistemas informáticos en búsqueda de software malicioso.
7. Analizar periódicamente los logs de los sistemas en búsqueda de actividades inusuales.

Todo equipo informático, tanto de escritorio, portátil, servidores y demás, debe estar protegido por una solución técnica residente en el equipo contra software malicioso, gestionado de forma centralizada. Esta solución técnica, así como la base de datos y registro de las amenazas a detectar, deben estar actualizadas y acompañarse de un procedimiento que explicite un comportamiento preventivo de los usuarios y personal especializado de TI.

# 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** |
|  |  |  |

