intiza

Software Malicioso

Versión: 2.1

Confeccionó	Revisó	Aprobó
BDO **Consultoría Externa**	 **Carla Leiva - CISO**	 **Francisco Canale - Director**

NORMA DE SOFTWARE MALICIOSO	intiza Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 02/05/2025
Código: NO-TI-03- Norma de Software Malicioso	Versión: 2.1

Contenido

1. Objetivo

Definir los lineamientos generales y establecer los requerimientos para una adecuada protección contra código malicioso dentro de los sistemas de información de INTIZA.

2. Alcance

Todos los sistemas informáticos que soportan los procesos de negocio de la organización y toda persona con acceso autorizado a los servicios de red de la compañía.

3. Responsabilidades

Seguridad de la información es responsable de monitorear los eventos de códigos maliciosos e informar la presencia de los mismos a Tecnología quien tomará las medidas pertinentes. Deberá además estar informada sobre la aparición de vulnerabilidades en los sistemas y/o nuevas amenazas de código malicioso. Asimismo, debe investigar y proponer las correcciones inmediatas a través de parches y actualizaciones.

Tecnología es responsable de que el software de detección esté instalado, configurado de acuerdo a los lineamientos establecidos y funcionando con las definiciones de virus y/o afines actualizadas.

4. Desarrollo

4.1. Consideraciones Generales

El código malicioso es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de

seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

Todos los medios removibles recibidos de fuentes sospechosas deben ser analizados previos a su utilización.

4.2. Software para la Detección de Código Malicioso

Se debe instalar en las computadoras de la compañía (servidores y estaciones de trabajo, un software de detección de código malicioso. El mismo debe ser homologado por INTIZA y configurado de acuerdo con los lineamientos establecidos en el presente documento. De no ser esto posible, la conexión debe tener accesos y permisos limitados para reducir los riesgos de propagar código malicioso.

Se debe contar con una (o más) consolas de Administración Centralizada que sean capaces de monitorear todas las unidades de trabajo y actualizar aquellas que no tengan el software al día, también debe permitir elaborar reportes y estadísticas sobre actualizaciones e infecciones.

Adicionalmente se debe realizar una revisión periódica mediante métodos alternativos, para chequear la integridad de la información y la no existencia de código malicioso en los sistemas de la Compañía (ej. penetration test, escaneos con herramientas específicas, etc.). Si en alguna ocasión el software antivirus falla o el archivo no pasa el testeo del antivirus, el usuario debe contactar inmediatamente con Tecnología. Lo mismo aplica a cualquier medida de protección que se considere desactualizada, que no esté funcionando correctamente o cuando se detecte algún comportamiento sospechoso de los sistemas.

Los dispositivos de terceros que sean autorizados a ingresar en la red de la Compañía deben ser chequeados en cuanto al software de código malicioso que tengan instalado. Éste debe incluir características similares a las establecidas corporativamente y debe estar actualizado a la fecha.

4.3. Requerimientos Mínimos para el Software de Detección de Código Malicioso

El software de detección de código malicioso debe ser capaz de:

- Detectar con la mayor precisión posible, un amplio rango de virus.
- Detectar virus y/o afines ocultos dentro de archivos comprimidos.
- Escanear cualquier dispositivo móvil que sea conectado a los equipos
- Analizar todas las unidades de almacenamientos removibles.
- Proveer una opción para determinar si las definiciones de virus se encuentran desactualizadas.
- Recibir y actualizar las definiciones de virus sin ningún tipo de intervención por parte de los usuarios.
- Proveer una referencia a las descripciones de los virus conocidos.
- Proveer a los usuarios información sobre la versión actual y la fecha de la última actualización de la definición de virus.
- Proveer a los usuarios la capacidad de iniciar la actualización de la definición de virus.
- Soportar una infraestructura que brinde administración centralizada sobre las opciones de configuración.

4.4. Requisitos mínimos de configuración del Software de Detección de Código Malicioso

El software de detección de código malicioso debe estar configurado para:

- Permanecer siempre activo cada vez que el sistema esté operando, por ejemplo, proveer la protección en tiempo real.
- Analizar todas las operaciones de entrada y salida de datos.
- Analizar periódicamente todos los datos contenidos en el sistema.

- Enviar alertas cuando se han detectado virus.
- Informar la ruta de destino completa (path) donde fue detectado el código malicioso.
- Limpiar, borrar o poner en cuarentena los archivos infectados.
- Evitar que los usuarios modifiquen los parámetros de análisis.

4.5. Requerimientos para el Registro de Eventos

Los registros de los análisis efectuados por los programas de detección de código malicioso deben, como mínimo, contener:

- Versión del programa de detección
- Fecha y hora del análisis
- Detalles de los parámetros relevantes de análisis
- Resultados de análisis
- Resultados de las actividades de remoción de virus y/o afines y archivos u objetos que no pudieron ser analizados

Se deben registrar todas las actualizaciones de los programas de detección de código malicioso.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Política	Seguridad de la Información	PO-SI-01

5.2. Definiciones

Término	Descripción
Código Malicioso (Malware)	Es un término que engloba cualquier programa, documento o mensaje susceptibles de causar perjuicios a los usuarios de los sistemas informáticos. Una característica común entre las diferentes clases de código malicioso es que ingresan y funcionan en los equipos de los usuarios sin el conocimiento de estos. El código malicioso puede ser clasificado por cómo se ejecuta, como se disemina o por cuál es su fin. Usualmente se divide en: virus, gusanos (worms), troyanos, spyware (software espía).
Virus	Es un programa de computadora, tal y como podría ser un procesador de textos, una hoja de cálculo o un juego, que causa eventos inesperados y, usualmente, indeseados; como el formateo del disco duro, borrado de archivos, mensajes, entre otros. Un verdadero virus no puede diseminarse a otra computadora sin la intervención humana.
Gusanos (Worms)	Los gusanos no causan necesariamente daño al software o hardware, pero si viajan en secreto reproduciéndose a través de la red.
Troyanos	Los Troyanos aparentan ser programas útiles o inofensivos, pero pueden contener escondidos otro código malicioso como virus o gusanos.

Spyware (Software Espía)	Este software registra la actividad del usuario (sobre todo en la Web) para obtener datos de este y por ejemplo dirigirle publicidad personalizada. Además, el accionar de estos códigos de software es poco ético, porque invaden la privacidad de los usuarios y son potencialmente peligrosos, ya que este software suele actualizarse en forma automática, abriendo un hueco en el sistema por el que podría entrar un código malicioso y ser aprovechado por hackers para penetrar.
Software no malicioso.	Son programas que generalmente son molestos para el usuario ya que causa daño moral, incluyendo pérdidas de tiempo, molestias al personal de soporte, entre otros. Estos programas se pueden clasificar en: **Jokes:** Son aplicaciones inofensivas que simulan ser virus informáticos. **Hoaxes:** También son programas de broma como define el nombre.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	01/12/2021	Creación de la Norma de Software Malicioso.
1.0	02/05/2022	Aprobado por Comité de Dirección: MI-DI-03- Minuta de Comité de

		Dirección N° 3
2.0	31/08/2022	Se agrega responsabilidades de Tecnología y se cambia la disposición del texto.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06 Minuta de Comité de Dirección N°6.
2.1	30/04/2025	Se revisó el documento y se confirmó su vigencia.
2.1	02/05/2025	Aprobado por Comité.