intiza

Seguridad en Dispositivos Móviles

Versión: 1.1

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

NORMA DE SEGURIDAD EN DISPOSITIVOS MÓVILES	intiza Clasificación: Restringida
Tipo: Norma	Fecha vigencia: 02/05/2025
Código: NO-SI-26 Seguridad en Dispositivos Móviles	Versión: 1.1

Contenido

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

1. Objetivo

Definir los lineamientos básicos de seguridad que deben cumplirse en los dispositivos móviles estableciendo los controles necesarios orientados a proteger la información que se gestiona en las computadoras portátiles asignadas a los usuarios de INTIZA.

2. Alcance

Los destinatarios de este documento son todos los colaboradores de INTIZA, ya sean empleados directos o bajo cualquier otro vínculo, incluso los empleados de las distintas contratistas que hagan uso de dispositivos móviles otorgados por la Compañía y/o dispositivos personales (BYOD) que se conecten a los recursos de INTIZA.

3. Responsabilidades

Todos los Colaboradores tienen la responsabilidad de preservar la información y los activos asignados, utilizándolos estrictamente para el cumplimiento de sus funciones y cumpliendo con las políticas y normativas de seguridad vigentes.

Seguridad de la Información es responsable del monitoreo y control de la seguridad de los dispositivos móviles a fin de que los mismos cumplan con los requisitos mínimos de seguridad para proteger y preservar la información corporativa. Como así también, debe asegurar el cumplimiento de esta norma de seguridad para todos los dispositivos móviles que utilizan los colaboradores.

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

4. Desarrollo

4.1. Generalidades

Los dispositivos móviles asignados por INTIZA son herramientas de trabajo, por lo tanto deben usarse sólo con fines laborales.

4.2. Seguridad física de los dispositivos

El usuario es el responsable por el cuidado del dispositivo móvil asignado, deberá garantizar la aplicación de las recomendaciones y herramientas provistas por la Organización. A continuación, se detallan algunos requisitos esenciales:

- Evitar dejar el dispositivo desatendido, sobre todo en lugares públicos, como en oficinas, restaurantes, bares, confiterías, oficinas de proveedores/clientes, centros de estudios, entre otros.
- Aplicar la norma de Escritorio y Pantallas limpias y sus recomendaciones sobre el buen uso de los equipos dispuestas por la compañía, con el objetivo de evitar accidentes que puedan dañar el equipamiento asignado.

Los controles de seguridad podrían variar en base al grado de responsabilidad que tenga la organización sobre el lugar en el cual se utilizan. De todas formas, los controles detallados con antelación deben ser considerados como básicos.

4.3. Configuración de Seguridad

- Por política general, el equipo se bloqueará requiriendo ingresar su contraseña.
- La misma deberá contar con la cantidad de caracteres y complejidad requerida. Durante un tiempo de inactividad de 10 minutos el equipo se bloqueará automáticamente y para reactivar la sesión se deberá ingresar la contraseña.

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

- Se cifrará la información en los dispositivos móviles teniendo en cuenta los requerimientos para con la información clasificada, mediante las herramientas de gestión de cifrado homologada por INTIZA.
- Todos los dispositivos móviles deben tener instalada una herramienta de antivirus y cumplir con la normativa vigente del mismo.
- Establecer la desconexión automática de sesiones para tecnologías de acceso remoto después de un periodo específico de inactividad.

4.4. Instalación de Aplicaciones

- Se debe revisar la correcta configuración de seguridad del dispositivo.
- Gestionar las aplicaciones del dispositivo móvil para evitar generar vulnerabilidades de seguridad.
- Los usuarios solo tendrán los privilegios necesarios para cumplir con sus tareas.

4.5. Borrado remoto

- Se debe contar con la posibilidad de borrar remotamente toda la información almacenada en caso de ser necesario.
- El dispositivo será remotamente formateado en las siguientes situaciones:
    - Robo, hurto o extravío del dispositivo.
    - Desvinculación del colaborador.
    - Se detecta un incumplimiento de la política.
    - Se registra una fuga de información corporativa.
    - Los dispositivos cuya última detección sea por un tiempo prolongado se tomará alguna acción por parte de los administradores de TI, siendo una de las alternativas el borrado completo del dispositivo, incluyendo la desvinculación con las aplicaciones corporativas.

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

4.6. Restricciones

- No están permitidos los cambios de configuración de fábrica.
- No están permitidas aquellas aplicaciones de uso no laboral que perjudiquen el funcionamiento del equipo y/o servicio brindado por la empresa. En caso que se detecte esta situación, TI puede eliminar dichas aplicaciones de forma remota.
- Evitar el uso de redes inalámbricas públicas, o de dudosa procedencia.
- Evitar el uso de servicios como transacciones bancarias, compras y otras operaciones donde se requiera información personal sensible.

4.7. Excepciones

- Toda aquella excepción, conflicto, interpretación o discrepancia de la presente, deberá ser formalmente evaluada, autorizada y aprobada según corresponda por el Comité de Seguridad, debiendo la misma tener una validez acotada en el tiempo de presentarse excepciones y mientras dure la misma se generarán medidas contingentes o controles compensatorios para la protección de los activos de información.

4.8. Dispositivos personales (BYOD)

- Los dispositivos que serán permitidos para acceder a los activos de información de INTIZA deben cumplir con los lineamientos y estándares de seguridad establecidos.
- Todos los dispositivos móviles personales deben ser autorizados por Tecnología y por Seguridad de la Información, previo a acceder a la información corporativa. Sin dicho consentimiento, no estará permitida la conexión de los mismos.
- Se deberá tener identificados e inventariados todos los dispositivos móviles personales (BYOD) y aplicar controles y monitoreo de seguridad sobre los mismos.

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

- INTIZA se reserva el derecho de inhabilitar o desconectar alguno o todos los servicios sin previa notificación, siempre que el dispositivo o línea incurran en un riesgo de seguridad para la compañía.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Política	Seguridad de la Información	PO-SI-01
Norma	Escritorio y Pantallas limpias	NO-SI-06
Norma	Software Malicioso	NO-TI-03

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

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.

	se disemina o por cuál es su fin. Usualmente se divide en: virus, gusanos (worms), troyanos, spyware (software espía).
BYOD	Las siglas en inglés BYOD -Bring your own device- significan Trae tu propio dispositivo. Es un modelo empresarial donde los empleados llevan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la compañía.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	11/08/2022	Creación de la Norma de Seguridad en Dispositivos Móviles.
1.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06 Minuta de Comité de Dirección N° 6
1.1	22/01/2025	Se revisó el documento y se modificaron algunas definiciones.
1.1	02/05/2025	Aprobado por Comité.

Este documento es propiedad exclusiva de INTIZA y su reproducción total o parcial está totalmente prohibida. El uso, copia, reproducción o venta de esta publicación, sólo podrá realizarse con autorización expresa y por escrito del propietario de la publicación. La versión impresa de este documento pierde automáticamente su vigencia.