



POLÍTICA SOBRE DISPOSITIVOS MÓVILES Y TELE-TRABAJO

Versión 1.0

7. Apoyo

Código:	POL-07/009/V1.0_Política sobre dispositivos móviles y tele-trabajo
Versión:	1.0
Fecha de emisión:	2025
Creador por:	Depto. Seguridad de la Información
Responsable:	Coordinación del SGSI
Revisión	Anual o ante cambios regulatorios
Nivel de Confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
28-may-25	1.0	Coordinación del SGSI	Creación de documento

Tabla de contenido

1. Objetivo, alcance y usuarios	3
2. Documentos de referencia	3
3. Computación móvil.....	3
3.1. Introducción	3
3.2. Reglas básicas	3
4. Tele-trabajo	4
5. Gestión de registros guardados con base en este documento	5
6. Validez y gestión de documentos	6
.....	6

1. Objetivo, alcance y usuarios

El objetivo del presente documento es evitar el acceso no autorizado a dispositivos ubicados tanto dentro como fuera de las instalaciones de la organización.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todas las personas, datos y equipos incluidos en el alcance del SGSI.

Los usuarios de este documento son todos los empleados de EthicsGlobal.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.6.2 y A.11.2.6
- Política de seguridad de la información
- Política de Clasificación de la Información
- Política de Uso aceptable

3. Computación móvil

3.1. Introducción

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

El equipamiento mencionado precedentemente puede ser llevado fuera de las instalaciones solamente con autorización, de acuerdo a lo establecido en la Política de uso aceptable.

3.2. Reglas básicas

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos (incluyendo automóviles), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Las actualizaciones de parches y demás configuraciones del sistema son realizadas por el departamento de TI de EthicsGlobal utilizando el mecanismo provisto por el desarrollador del Sistema Operativo 1 vez cada 6 meses o cuando exista una alerta de seguridad difundida por el proveedor por sus medios oficiales.
- La protección contra códigos maliciosos se instala y actualiza conforme a las especificaciones del proveedor, en este momento se utiliza Avast Antivirus, pero es susceptible a cambio.
- La persona que utiliza equipamiento de computación móvil fuera de las instalaciones es responsable de realizar periódicamente copias de seguridad de datos mediante el uso de la nube de colaboración (en este momento OneDrive), este proceso se realiza de manera automática dado que cada OS cuenta con una herramienta de respaldo automático.
- La conexión a redes de comunicación y el intercambio de datos debe reflejar la sensibilidad de los datos y se realiza de manera automática de manera local, en conexiones fuera de la ubicación de EthicsGlobal se debe realizar mediante el uso del hotspot móvil que provee el teléfono móvil del usuario, queda prohibido en la medida de lo posible utilizar cualquier red incluso si se encuentra dentro de la red de un cliente.
- La protección de datos sensibles debe ser implementada de acuerdo con la Política de Clasificación de Información.
- En el caso que el equipamiento de computación móvil sea desatendido, se deben aplicar las reglas para equipamiento de usuario desatendido, de acuerdo a la Política de uso aceptable.

El Coordinador del SGSI es el responsable de la capacitación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.

4. Tele-trabajo

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización. El tele-trabajo no incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.

El tele-trabajo debe ser autorizado por el Coordinador del SGSI y gestionado por la gerencia de TI mediante el llenado del registro destinado para este fin.

El Coordinador del SGSI es el responsable de preparar planes y procedimientos para garantizar lo siguiente:

- Protección del equipamiento de computación móvil, de acuerdo a lo indicado en la sección anterior.
- Evitar el acceso no autorizado de personas que viven o trabajan en la ubicación donde se realiza la actividad de tele-trabajo.
- Configuración adecuada de la red local utilizada para conectarse a la Internet.
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Proceso de devolución de datos y equipamiento en caso de finalización del empleo.
- Nivel mínimo de configuración de la instalación donde se realizarán las actividades de teletrabajo.
- Tipos de actividades permitidas y prohibidas.

5. Gestión de registros guardados con base en este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Autorización para tele-trabajo	Carpeta compartida.	Gerente de administración	Controles para resguardo de registros físicos.	Los registros son almacenados por el plazo de 3 años.
Planes y procedimientos para tele-trabajo	Repositorio GIT: ISO 27001 y carpeta compartida	Coordinador del SGSI	Solamente el Coordinador del SGSI puede publicar y editar normas internas	3 años

Solamente el Coordinador del SGSI puede permitir a otros empleados el acceso a cualquiera de los documentos mencionados precedentemente.

6. Validez y gestión de documentos

Esta política será revisada anualmente por el Comité de Seguridad de la Información o, cuando ocurra un cambio significativo en los roles organizacionales.

El propietario de este documento es el Coordinador del SGSI, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con llevar equipamiento de computación móvil fuera de las instalaciones de la organización sin autorización.
- Cantidad de incidentes relacionados con el acceso no autorizado a equipamiento de computación móvil fuera de las instalaciones de la organización.

Representante de la Dirección General
Liuva Anahí Figueroa Gracián


