DigiPro, S.A. de C.V.

Hoja de revisión.

Este documento fue creado conforme a los requerimientos institucionales, revisado por el área de Control y Cumplimiento y aprobado por la Dirección de Tecnologías de Información.

Estamos de acuerdo con su contenido e implementación, en caso de haber cualquier modificación o adición a este documento, es responsabilidad del área emisora indicar la modificación o adición, previa aprobación de las áreas involucradas para evitar errores, incrementar el control interno y/o mejorar la productividad de los departamentos involucrados.

Control de Cambios		
Versión	**Cambios realizados**	**Fecha**
01	Documento de nueva creación	13/01/2025

Tabla de contenido

1 Política de Dispositivos Móviles.

Cualquier equipo móvil que contenga información de la organización debe cumplir con las siguientes medidas de seguridad. Y dicha información no debe vivir en dispositivos personales o en equipos que no estén específicamente autorizados por el área de Seguridad Informática.

Laptops o tabletas electrónicas:

- Registrar la información del equipo móvil en el inventario de activos.
- Activar el bloqueo del equipo y el acceso mediante contraseña.
- Contar con un antivirus actualizado.
- No instalar software que permita la explotación de riesgos que comprometan la seguridad de la información o el incumplimiento de leyes o regulaciones.
- Implementar controles adicionales para proteger la información personal o clasificada como crítica/sensible en el equipo, por ejemplo, cifrado del disco duro de equipo, proteger el acceso al documento mediante contraseñas entre otros.
- Realizar respaldo de la información de la organización cada 3 meses.
- No utilizar funciones que permitan el “recordar contraseña o conexiones de red”.
- No descuidar el equipo especialmente si no se cuenta con cable de seguridad.
- No dejar el equipo en lugares que puedan ser susceptibles a robo (en lugares visibles dentro del auto, en lugares públicos, cafeterías, eventos, conferencias, etc.).
- Bloquear el equipo cuando no permanezca cerca del mismo.
- No exponer el equipo a cambios de temperatura drásticos.
- Evitar la conexión mediante WiFi en lugares públicos y de aquellas conexiones sin control de acceso.
- Informar de inmediato al Área de Seguridad Informática la pérdida o hurto del dispositivo, quién retirará los accesos a los servicios de red y sistemas.
- Notificar el robo o pérdida del equipo al personal de infraestructura tecnológica.
- Permitir la verificación del cumplimiento de estas políticas por las áreas de Seguridad Informática e Infraestructura que realizan la verificación.
- Firmar una responsiva sobre el buen uso y cuidado del equipo (aplica a equipo propiedad de la empresa).

Equipo Móvil:

- Registrar la información del equipo móvil en el inventario de activos, especialmente el número IMEI.
- Acceder al equipo mediante un número, una secuencia de movimientos (Bloqueo de equipo).
- Únicamente se permite el uso de correo electrónico de la organización, el acceso a la red interna o sistemas de la organización está prohibido por este medio.

- Mantener el software del dispositivo actualizado, estas actualizaciones deben descargarse de sitio de confianza.
- No utilizar el equipo móvil como medio de almacenamiento de información de la empresa.
- No utilizar funciones que permitan el “recordar contraseña o conexiones de red”.
- No exponer el equipo a cambios de temperatura drásticos.
- Notificar el robo o pérdida del equipo al personal de infraestructura tecnológica.
- No utilizar el equipo propiedad de DigiPro para temas personales.
- Permitir la verificación del cumplimiento de estas políticas por las áreas de seguridad de la Información e Infraestructura.
- Firmar una responsiva sobre el buen uso y cuidado del equipo (aplica a equipo propiedad de la empresa).

Medios removibles:

- No almacenar la información confidencial en cualquier medio removible.
- No utilizar los medios removibles como medios de almacenamiento permanentes.
- Registrar la información del medio removible en el inventario de activos.
- Contar con una carta responsiva del medio autorizado.
- Analizar el dispositivo antes de uso para verificar que no cuente con virus o código malicioso.
- No exponer el equipo a cambios de temperatura drásticos.
- Permitir la verificación del cumplimiento de estas políticas por las áreas de Seguridad Informática e Infraestructura.
- Eliminar la información del dispositivo cuando ya no sea requerida.
- Notificar el robo o pérdida del medio al personal de Seguridad Informática y/o Infraestructura.
- Firmar una responsiva sobre el buen uso y cuidado del medio.
- Transportar el medio removible en un maletín o medio que lo proteja de amenazas ambientales, separado del equipo portátil, de ser posible implementar un mecanismo de control de acceso lógico.

2 Cumplimiento.

- ISO/IEC 27001:2022 / Apéndice A / A.5 Controles Organizacionales / A. 5.1 Políticas de seguridad de la información
- ISO/IEC 27001: 2022 / Apéndice A / A.8 Controles Tecnológicos / A. 8.1 Dispositivos de punto final de usuario
- ISO/IEC 27001:2022 / Apéndice A / A.5 Controles Organizacionales / A.5.10 Uso aceptable de la información y otros activos asociados

- ISO/IEC 27001:2022 / Apéndice A / A.7 Controles Físicos / A. 7.10 Medios de almacenamiento