

***Secretaría Técnica Ecuador Crece Sin
Desnutrición Infantil***

Política de Dispositivos Móviles

***GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
Y COMUNICACIÓN***

Versión. 1.0

Agosto 2022

		<h1>Política de Dispositivos Móviles</h1>
Fecha: 16/08/2022	Página: 2 de 11	
ÁREA		Unidad de Gestión de Tecnologías

Firmas de Responsabilidad

		NOMBRE	CARGO	FECHA	FIRMA
APROBADO POR	COMITÉ DE SEGURIDA DE LA INFORMACIÓN	Juan Carlos Palacios	Presidente del Comité de Seguridad de la Información	Agosto 2022	
REVISADO POR:	OFICIAL DE SEGURIDA DE LA INFORMACIÓN	José Luis Alcarraz	Oficial de Seguridad de la Información	Agosto 2022	
ELABORADO POR:	Técnico	Erick Andrade	Analista de Tecnología de la Información y Comunicación 2	Agosto 2022	

		<h1>Política de Dispositivos Móviles</h1>
Fecha:	Página:	
16/08/2022	3 de 11	
ÁREA		Unidad de Gestión de Tecnologías

Control de Cambios

Versión	Fecha	Descripción del cambio	Elaborado por:	Solicitado por:
1.0	-	-	-	-
1.1	-	-	-	-
2.0	-	-	-	-
3.0	-	-	-	-

		<h1>Política de Dispositivos Móviles</h1>
Fecha:	Página:	
16/08/2022	4 de 11	
ÁREA		Unidad de Gestión de Tecnologías

Tabla de contenido

1. ANTECEDENTES	5
2. OBJETIVO.....	5
3. MARCO LEGAL.....	5
4. RESPONSABILIDADES	7
5. GLOSARIO DE TÉRMINOS	8
6. POLÍTICA.....	9
7. ÁMBITO DE APLICACIÓN.....	11

		<h1>Política de Dispositivos Móviles</h1>
Fecha: 16/08/2022	Página: 5 de 11	
ÁREA		Unidad de Gestión de Tecnologías

1. ANTECEDENTES

Que, mediante Edición Especial No. 228 de 10 de enero de 2020 fue publicado en el Registro Oficial el Acuerdo Ministerial No. 025-2019 que contiene en su Anexo el Esquema Gubernamental de Seguridad de la Información (EGSI versión 2.0), el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva (APCID).

Que, mediante Acuerdo No. 25 - 2019, el Ministerio de Telecomunicaciones y de la Sociedad de la Información dispone, en su Art.1, la implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el Esquema Gubernamental de Seguridad de la Información – EGSI.

Que, mediante Acuerdo No. 25 - 2019, el Ministerio de Telecomunicaciones y de la Sociedad de la Información recomienda, en su Art.3, utilicen como guía las Normas Técnicas Ecuatorianas NTE INEN –ISO/IEC 27000 para la Gestión de Seguridad de la Información.

En virtud de lo expuesto, y, en función de las competencias y atribuciones de la Unidad de Tecnología de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil, se elabora el documento “Política de Dispositivos Móviles”, a fin de ponerlo a consideración del Comité de Seguridad de la Información para su análisis y posterior aprobación por parte de la máxima autoridad o su delegado.

2. OBJETIVO

Establecer y proporcionar las políticas, normas y responsabilidades asociadas al acceso y uso de equipos móviles dentro de la red de comunicaciones de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil, con el propósito de minimizar riesgos en la seguridad de la información.

3. MARCO LEGAL

Código Orgánico Integral Penal - COIP. - artículos 178, 230, 234.

Artículo 178.- Violación a la Intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, accede, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio (...).

		<h1>Política de Dispositivos Móviles</h1>
Fecha: 16/08/2022	Página: 6 de 11	
ÁREA		Unidad de Gestión de Tecnologías

Artículo 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (...).

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

Guía para la implementación de controles de seguridad de la información (NTEINEN ISO/IEC 27002:2017) perteneciente al Esquema Gubernamental de Seguridad de la Información EGSi V2, emitido en Acuerdo Ministerial No. 25 - 2019 con Registro Oficial Edición Especial 228 de 10 - ene - 2020.

EL ESQUEMA GUBERNAMENTAL DE DISPOSITIVOS MÓVILES EGSi señala:

2.2 DISPOSITIVOS MÓVILES

2.2.1 Políticas de Dispositivos Móviles

Control

Elaborar, implementar y socializar una política formal, adoptar medidas de seguridad adecuadas para la protección y gestión de los riesgos generados por el uso de dispositivos móviles.

Recomendaciones para la implementación:

- 2.2.1.1 Registro de dispositivos móviles, debidamente autorizados;
- 2.2.1.2 Requisitos para la protección física;
- 2.2.1.3 Restricciones de Instalación de software;
- 2.2.1.4 Requisitos para las versiones de software de dispositivos móviles y la aplicación de Parches;
- 2.2.1.5 Restricciones de conexión a sistemas de gestión de la información;
- 2.2.1.6 Controles de Acceso;
- 2.2.1.7 Técnicas Criptográficas;
- 2.2.1.8 Protección contra virus;
- 2.2.1.9 Inhabilitación, borrado y bloqueos remotos;

		<h1>Política de Dispositivos Móviles</h1>
Fecha: 16/08/2022	Página: 7 de 11	
ÁREA		Unidad de Gestión de Tecnologías

2.2.1.10 Copias de respaldo;

2.2.1.11 Control sobre la utilización de servicios y aplicaciones web.

Cuando la política de dispositivos móviles permita el uso de dispositivos móviles personales o privados, la política y las medidas de seguridad relacionadas deberían considerar también:

2.2.1.12 La separación del uso de los dispositivos con fines privados respecto a los de la institución, incluyendo el uso de software de soporte para permitir dicha separación y proteger los datos de la institución en un dispositivo privado;

2.2.1.13 Determinar los protocolos de seguridad inalámbrica su madurez y debilidades;

2.2.1.14 Considerar que no se haga un acopia de respaldo, de la información almacenada en los equipos móviles, por ancho de banda o conexión a la red el momento de ejecutar el respaldo.

4. RESPONSABILIDADES

Para cumplir con los objetivos de la Política de Seguridad de la Información de la STECSDI se establecen los siguientes roles y responsabilidades:

La/El Secretario /a Técnico/a (Máxima autoridad o su delegado/a)

- Responsable de revisar, aprobar y suscribir en general todos los documentos relacionados con las políticas de seguridad de la información.

El comité de Seguridad de la Información tendrá como principales responsabilidades:

- a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.
- b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos.
- d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.
- e) Promover la difusión de la seguridad de la información dentro de la institución.

		<h1>Política de Dispositivos Móviles</h1>
Fecha:	Página:	
16/08/2022	8 de 11	
ÁREA		Unidad de Gestión de Tecnologías

f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.

g) El comité deberá convocarse bimensualmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.

h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

Unidades de Tecnologías de la Información

Implementa las directrices de seguridad definidas para el manejo de la información.

Funcionarios (as) de la Secretaría Técnica Ecuador Crece Sin Desnutrición Infantil

Son los servidores públicos que administran los activos de información, son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Dispositivos Móviles vigente y además, tienen la obligación de reportar los eventos que ponen en riesgo la seguridad de la información.

5. GLOSARIO DE TÉRMINOS

Dispositivos Móviles: Es todo equipo que posee características relacionadas con tamaño reducido, movilidad, capacidad de comunicación inalámbrica y capacidad de interconexión con otras personas o sistemas, los cuales permiten procesar, recibir y enviar información.

Información: Conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado.

Seguridad de los Activos de Información: Asegurar la disponibilidad, confidencialidad e Integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operacional de la STECSDI.

Red inalámbrica: Es aquella que permite conectar diversos nodos sin utilizar una conexión física, sino estableciendo la comunicación mediante ondas electromagnéticas. La transmisión y la recepción de los datos requieren de dispositivos que actúan como puertos. Las redes inalámbricas permiten.

		<h1>Política de Dispositivos Móviles</h1>
Fecha: 16/08/2022	Página: 9 de 11	
ÁREA		Unidad de Gestión de Tecnologías

Seguridad de la Información: Conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad.

6. POLÍTICA

1. La Unidad de Gestión de Tecnologías de la STECSDI define a los siguientes equipos como dispositivos móviles: computadoras portátiles, teléfonos inteligentes, tabletas y relojes inteligentes tanto institucionales como personales y proveerá las condiciones para el manejo de los dispositivos móviles institucionales; así mismo velará por que los funcionarios de la STECSDI usen de manera responsable y correcta los dispositivos y los servicios proporcionados por la STECSDI.
2. La Unidad de Gestión de Tecnología de la STECSDI, no será responsable del soporte técnico de los dispositivos móviles personales como actualización de software, respaldo de información, mantenimiento preventivo y correctivo, análisis de virus, ni proveerá de accesorios adicionales como cables o cargadores.
3. La Unidad de Gestión de Tecnología determinará los mecanismos de seguridad para los dispositivos móviles como: registros de nuevos dispositivos (mac-address).
4. La Unidad de Gestión de Tecnología controlará el acceso de los dispositivos móviles en la red institucional y de equipos portátiles en tránsito; es decir equipos de terceros o visitantes que por algún motivo requieran el acceso a la red inalámbrica, podrán conectarse a la red **“Infancia-móviles”**, red definida por parte de la Unidad de Tecnología para este fin.
5. Todo computador portátil de propiedad de la STECSDI debe ser incorporado al dominio de la red institucional, con todas las configuraciones y políticas definidas de acuerdo a los procedimientos de la Unidad de Gestión de Tecnologías.
6. Es responsabilidad del funcionario de la STECSDI mantener la configuración establecida por las Unidad de Gestión de Tecnologías en los computadores portátiles de propiedad de la institución.
7. Se establecerá las siguientes recomendaciones y medidas de seguridad para los funcionarios de la STECSDI en virtud que las computadoras portátiles de propiedad de la institución pueden ser utilizadas por los funcionarios fuera de las instalaciones por cumplimiento de aspectos laborales o por motivos de teletrabajo:

		<h1>Política de Dispositivos Móviles</h1>
Fecha:	Página:	
16/08/2022	10 de 11	
ÁREA		Unidad de Gestión de Tecnologías

- a) Se recomienda a los funcionarios de la STECSDI no conectarse a redes públicas inseguras para envío de información sensibles, la Unidad de tecnología difundirá campañas de seguridad de acceso a redes seguras.
 - b) Se analizará toda unidad de almacenamiento externo cuando sea conectada al dispositivo móvil, a través de la herramienta de antivirus instalada en el equipo.
 - c) Se recomienda al funcionario a cargo del dispositivo móvil precautelar la integridad física del equipo, de ninguna manera el equipo será desatendido en lugares públicos o a la vista en el caso de que este siendo transportado, la Unidad de Gestión de Tecnologías difundirá campañas de seguridad para el cuidado de los dispositivos.
 - d) Se recomienda a los funcionarios No compartir, ni entregar el usuario y contraseña del equipo portátil de la STECSDI a personas ajenas a la institución ya se corre el riesgo de que la información institucional pueda ser alterada, eliminada o robada; el equipo será de uso exclusivo para desempeñar las actividades laborales. La Unidad de Tecnología difundirá campañas de seguridad.
8. Todo computador portátil de propiedad de los funcionarios o de la STECSDI que ingresen o salgan deberán ser registrados conforme los procedimientos dispuestos por la Dirección Administrativa.
 9. Se recomienda que si los funcionarios usan una red externa a la STECSDI Es responsabilidad del funcionario de la STECSDI evitar conectarse a redes públicas que sean de fácil acceso (sin contraseña), que puedan comprometer la información institucional almacenada en el computador portátil.
 10. La Unidad de Gestión de Tecnologías vigilará que los equipos portátiles se encuentren actualizados el antivirus institucional de manera mensual.
 11. Es responsabilidad de la gestión interna de soporte de la STECSDI, realizar las configuraciones iniciales en los dispositivos móviles institucionales, mantener el estándar de aplicaciones instalados de acuerdo con las directrices de la Unidad de Gestión de Tecnologías.
 12. Los funcionarios a cargo del computador portátil de la STECSDI, no podrán instalar aplicaciones en los equipos sin la previa autorización y solicitud al responsable de la Unidad de Gestión de tecnologías al correo electrónico soporte.tecnología@infancia.gob.ec, canal oficial de la mesa de servicio.

		<h1>Política de Dispositivos Móviles</h1>
Fecha: 16/08/2022	Página: 11 de 11	
ÁREA		Unidad de Gestión de Tecnologías

13. La Unidad de Gestión de Tecnología de la STECSDI deberá controlar el registro de nuevos dispositivos y la cancelación de dispositivos móviles no autorizados que se detecten en la red institucional; dicha actividad lo deberá realizar de manera mensual.

14. La Unidad de Gestión de Tecnología de la STECSDI deberá monitorear las redes inalámbricas y controlar el acceso de dispositivos móviles.

7. ÁMBITO DE APLICACIÓN

Esta política es de cumplimiento obligatorio para todos los funcionarios de la STECSDI y se aplicará a todos los dispositivos móviles de propiedad, así como también a dispositivos móviles personales de los funcionarios y dispositivos móviles externos.