SUPERINTENDENCIA DE COMPETENCIA ECONÓMICA

POLÍTICA INSTITUCIONAL PARA LA RESTRICCIÓN DEL USO DE DISPOSITIVOS ELECTRÓNICOS PERSONALES

Junio 2026

Quito – Ecuador

Av. de los Shyris N44-93 y Río Coca, Edificio Ocaña
Quito - Ecuador
PBX: 593-2 395-6010

1. BASE LEGAL

La presente política para la *"Restricción del Uso de Dispositivos Electrónicos Personales"* se fundamenta en las disposiciones legales, reglamentarias y técnicas que se detallan a continuación; cuya observancia resulta directamente vinculante para la gestión segura de la información institucional, así como para el control, regulación y supervisión del uso de dispositivos móviles personales en el ámbito institucional:

1.1. Constitución de la República del Ecuador:

Artículo 66, números 19, 20,21
Artículo 76, número 7, letra d
Artículo 82
Artículo 226
Artículo 227

1.2. Ley Orgánica de Regulación y Control del Poder de Mercado (LORCPM)

Artículo 38
Artículo 47
Artículo 48
Artículo 56
Artículo 56.1

1.3. Ley Orgánica de Regulación Contra la Competencia Desleal

Artículo 9, letras: l, m, o, q
Artículo 11

1.4. Ley Orgánica de Protección de Datos Personales

Artículo 10

1.5. Norma Técnica Ecuatoriana NTE INEN ISO/IEC 27001:2022

5.- LIDERAZGO
6.- PLANIFICACIÓN
7.- SOPORTE, 7.3 Concienciación

1.6. Esquema Gubernamental de Seguridad de la Información (EGSI v.3.0)

Anexo C.- GUÍA PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, 4.- Controles tecnológicos; 4.1. Dispositivos de usuario final; 4.2. Derechos de acceso privilegiado; 4.3. Restricción de acceso a la información; 4.12. Prevención de fuga de datos.

1. OBJETO

El objeto de esta política es reducir el riesgo de fuga, captura o transmisión no autorizada de información institucional mediante la aplicación de reglas que limiten el uso de dispositivos electrónicos personales en áreas restringidas.

Esta política constituye un instrumento normativo específico que forma parte integrante del Sistema de Gestión de Seguridad de la Información de la Superintendencia de Competencia Económica, expedido en el marco del Esquema Gubernamental de Seguridad de la Información Versión 3 (EGSI v.3.0).

2. DEFINICIONES

a) **Dispositivo Electrónico Personal (DEP):** equipo de uso personal con capacidad de capturar, almacenar, reproducir o transmitir información, tales como: teléfono celular, tablet, laptop personal, reloj inteligente/wearable, cámara, grabadora, entre otros de similares características.
b) **Medio de Almacenamiento Extraíble (MAE):** USB, disco externo, tarjeta SD u otro medio portátil de almacenamiento.
c) **Área restringida:** espacio físico donde se procesa, almacena o discute información reservada y/o confidencial de la SCE (por ejemplo: archivos/repositorios, salas de reuniones confidenciales, oficinas donde se sustancien procedimientos, u otros definidos por el OSI en función del riesgo).
d) **Autorización excepcional:** permiso temporal otorgado por el OSI mediante formulario (Anexo 1), con condiciones, alcance y vigencia definidos; la DNATH interviene cuando la excepción corresponda a supuestos administrativos (p. ej., salud/condición laboral u otros definidos por la SCE).
e) **Autoresguardo:** condición mediante la cual el propietario mantiene bajo su custodia el DEP y el MAE; cumpliendo las reglas de esta política.

3. PRINCIPIOS DE APLICACIÓN

a) **Seguridad de la información:** Se implementarán mecanismos que permitan preservar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.
b) **Proporcionalidad:** Se aplicarán medidas idóneas, necesarias y no excesivas según el nivel de riesgo.
c) **Respeto de derechos:** Las medidas implementadas evitarán la afectación a los derechos de intimidad, privacidad y propiedad de las personas relacionadas a esta política, y; sus procedimientos se sujetarán al debido proceso.
d) **No intrusión:** Los procedimientos implementados excluyen la revisión de contenido de los dispositivos y los controles físicos invasivos.
e) **Viabilidad operativa:** Los controles efectuados son simples y ejecutables, sin necesidad de implementación de infraestructura costosa, o la aplicación de monitoreo permanente.

4. REGLA GENERAL

4.1. Prohibición de uso en áreas restringidas

En áreas restringidas se prohíbe el uso de DEP y el ingreso/uso de MAE, salvo autorización excepcional. En particular, en estos espacios se prohíbe:

a) Capturar imágenes, audio o video;
b) Realizar llamadas o videollamadas;
c) Conectar MAE a equipos institucionales;
d) Activar o utilizar mecanismos de conectividad no autorizados (hotspot/Bluetooth u otros); y,
e) Almacenar o transmitir información institucional no autorizada en DEP y MAE.

4.2. Controles físicos razonables

Las áreas restringidas contarán con controles físicos razonables y proporcionales a su nivel de riesgo, priorizando medidas organizativas y de bajo costo (señalización, reglas de no uso, autoresguardo, y autorizaciones), sin que ello implique instalación obligatoria de infraestructura adicional.

4.3. Protección de derechos en el control

Se prohíbe expresamente:

a) Revisar, acceder, visualizar o analizar contenido del DEP y MAE; y,
b) Aplicar controles físicos invasivos (registros corporales, inspecciones personales directas).

Los controles se limitan a mecanismos objetivos, externos y no intrusivos, como:

a) Señalización visible de *"Área restringida – no uso de DEP y MAE"*;
b) Verificación visual externa (no invasiva) y/o declaración voluntaria de portación;
c) Requerir que el DEP y el MAE permanezcan sin uso y bajo autoresguardo conforme la sección 6.

5. MEDIDAS OPERATIVAS SIMPLES

5.1. Autoresguardo obligatorio

Para el ingreso y permanencia en áreas restringidas, toda persona deberá cumplir obligatoriamente con las siguientes disposiciones:

a) Los DEPs y MAEs deberán ser numerados y con nombre de cada servidor y deberán permanecer almacenados en los casilleros individuales, habilitados por la Dirección Nacional Administrativa, ubicados en cada área restringida. Cada casillero permanecerá asegurado bajo llave, cuya custodia y responsabilidad

corresponderá exclusivamente al servidor o usuario asignado durante el tiempo de permanencia en el área restringida.

b) Los DEPs y MAEs deberán mantenerse resguardados dentro del casillero durante toda la permanencia en el área restringida.

5.2. Determinación y señalización de áreas restringidas

El OSI identificará y comunicará las áreas que se consideran como restringidas, conforme el análisis de riesgo, y coordinará con la Dirección Nacional Administrativa la señalización (impresión y colocación) y la definición de zonas habilitadas para el uso normal de DEPs y MAEs fuera de dichas áreas.

Serán consideradas como áreas restringidas los espacios donde se procese, almacene o discuta información reservada y/o confidencial perteneciente a los procedimientos administrativos derivados de los procesos agregadores de valor de la SCE, tales como:

a) Archivos físicos y repositorios documentales;
b) Salas de reuniones donde se traten asuntos confidenciales;
c) Oficinas donde se sustancien procedimientos administrativos; y,
d) Cualquier otro espacio definido en función del análisis de riesgos.

El OSI será responsable de identificar, clasificar, actualizar y comunicar dichas áreas conforme al EGSI v.3.0.

6. AUTORIZACIONES EXCEPCIONALES

6.1. Autorización

Solo se otorgarán autorizaciones excepcionales cuando: i) exista una necesidad institucional debidamente justificada vinculada al cumplimiento de funciones, actividades o requerimientos operativos, ii) no exista una alternativa viable de menor impacto o restricción, y; iii) se establezcan condiciones verificables (alcance, vigencia, área, dispositivo identificado).

6.2. Autoridad y ruta

a) OSI: Autoriza excepcionalmente el uso de DEPs y MAEs mediante el Anexo 1, y registra la misma.
b) DNATH: Interviene cuando la excepción se fundamente en supuestos administrativos (p. ej., salud/condición laboral, emergencias médicas o familiares, u otros definidos por la SCE), o cuando corresponda por gestión disciplinaria.

6.3. Condiciones mínimas obligatorias en toda autorización

Toda autorización debe indicar, como mínimo:

a) Beneficiario;
b) Área restringida específica;
c) Tiempo (inicio/fin o condición);
d) Identificación del dispositivo (tipo, marca/modelo, IMEI/serie);
e) Condiciones de uso (qué está prohibido y qué excepcionalmente se habilita);
f) Obligación de reporte inmediato de incidentes al OSI.

6.4. Revocatoria

El OSI podrá revocar la autorización de forma inmediata por incumplimiento, incidente y/o variación del riesgo. La revocatoria quedará registrada.

7. INCUMPLIMIENTOS Y MEDIDAS INMEDIATAS

7.1. Incumplimientos

a) Usar DEPs Y MAEs en áreas restringidas sin autorización;
b) Intentar evadir los controles establecidos;
c) Capturar/grabar/transmitir información institucional en áreas restringidas sin autorización;
d) Incumplir las condiciones de una autorización.

7.2. Medidas inmediatas de control

a) Retiro del dispositivo del área restringida (salir del área);
b) Suspensión o revocatoria de la autorización;
c) Restricción de acceso a las áreas restringidas, cuando corresponda;
d) Registro del hecho y notificación al OSI y a la DNATH.

8. GESTIÓN DE INCIDENTES

Los hechos que comprometan confidencialidad, generen fuga de información o afecten el debido proceso se gestionarán conforme el procedimiento institucional de incidentes.

El OSI comunicará de estas situaciones a la DNATH y al CSI, y; a la máxima autoridad, únicamente en incidentes críticos acorde el procedimiento institucional.

9. RESPONSABILIDADES

a) **Comité de Seguridad de la Información (CSI):** Aprueba la política y revisa su actualización cuando corresponda.
b) **Dirección Nacional Administrativa de Talento Humano (DNATH):** Gestiona acciones administrativas/disciplinarias, y atiende casos administrativos de excepción cuando corresponda.
c) **Oficial de Seguridad de la Información (OSI):** Autoriza las excepciones, mantiene el registro (Anexo 3), asesora la implementación de la señalización básica y canaliza los incidentes suscitados.

d) **Todos los usuarios:** Cumplen la regla de no uso, auto resguardo y reporte de incidentes.

10. CONTROL Y REVISIÓN

La política será sujeta de revisión cuando existan variaciones relevantes de riesgo o de normativa.

El OSI presentará al CSI un reporte anual, identificando:

a) Número de autorizaciones emitidas, y
b) Número de incidentes reportados, vinculados a esta política.

11. VIGENCIA

La presente política entrará en vigencia a partir de su aprobación y difusión institucional; y formará parte integrante del EGSI v.3.0 de la Superintendencia de Competencia Económica.

Elaborado y aprobado por Comité de Seguridad de la Información (CSI):

Revisado y aprobado por:	Mgs María Gabriela Vinocunga Batallas **Presidenta Comité de Seguridad de la Información**	Validar únicamente en FirmaEC. Firmado electrónicamente por: MARIA GABRIELA VINOCUNGA BATALLAS
	Dr. Patricio Hernán Rubio Román **Miembro CSI**	Firmado electrónicamente por: PATRICIO HERNAN RUBIO ROMAN
	Tnlg. Cristóbal Rubén Conrado Armas **Delegado CSI**	Validar únicamente en FirmaEC. Firmado electrónicamente por: CRISTOBAL RUBEN CONRADO ARMAS
	Ing. Henry Omar Carrera Hidalgo **Miembro CSI**	Validar únicamente en FirmaEC. Firmado electrónicamente por: HENRY OMAR CARRERA HIDALGO
	Ing. María Fernanda Melendres Robalino **Miembro CSI**	Validar únicamente en FirmaEC. Firmado electrónicamente por: MARIA FERNANDA MELENDRES ROBALINO
	Sra. Andrea Pamela Acevedo Minchala **Delegado CSI**	Validar únicamente en FirmaEC. Firmado electrónicamente por: ANDREA PAMELA ACEVEDO MINCHALA

	Abg. Jorge Marcelo Rojas Salazar **Miembro CSI**	Validar únicamente en FirmaEC. Firmado electrónicamente por: JORGE MARCELO ROJAS SALAZAR
Elaborado por:	Mgs. Carlos Eduardo Muñoz Montesdeoca **Oficial de Seguridad de la Información de la SCE**	Validar únicamente en FirmaEC. Firmado electrónicamente por: CARLOS EDUARDO MUNOZ MONTESDEOCA

ANEXO 1

Formulario de Solicitud de Autorización Excepcional

A) Datos generales de la solicitud

Solicitante (nombre/cargo):			
Unidad:			
Área restringida específica:			
Fecha de solicitud:			
Tipo de caso:	Operativo:	Administrativo (DNATH):	Detalle de solicitud para casos Administrativos:

B) Tipo de autorización solicitada

Justificación de la solicitud:			
Vigencia solicitada	desde[dd-mm-aaaa]	Hasta [dd-mm-aaaa]	Cumplimiento de condición:

C) Identificación del dispositivo tecnológico personal

Tipo (MAE / DEP)	Marca	Modelo	Color	Identificador (IMEI/Serie)	Descripción adicional

D) Controles propuestos y condiciones solicitadas

Se autoriza	Si	No
Capturar imágenes, video o audio		
Realizar llamadas o videollamadas		
Conectar medios extraíbles a equipos institucionales Si se autoriza MAE: Equipo institucional destino (código/inventario): _____ Responsable de supervisión: _____ Propósito: _____		
Activar o utilizar mecanismos de conectividad no autorizada (hotspot, Bluetooth, etc.)		

E) MEDIDA DE AUTORESGUARDO:

( ) Regla base (sin uso / silencio / pantalla apagada)

( ) Casilleros (cuando aplique)

F) VENTANA HORARIA (SI APLICA):

Desde ____ : ____ Hasta ____ : ____

Firmas

Firma titular del área restringida: _____ Nombre: Cargo:	Firma OSI: _____ Nombre: Cargo:
DNATH (si aplica): _____ Nombre: Cargo:	Firma servidor público requirente: _____ Nombre: Cargo:

ANEXO 2

Registro de Incidencias

Fecha	Hora	Área	Descripción breve	Medida inmediata aplicada	Notificación			Responsable que reporta
					OSI	DNATH	CSI	

ANEXO 3

Registro OSI de Autorizaciones

Fecha y hora autorización del formulario	Área restringida	Cargo	Propietario	Tipo (MAE / DEP)	Marca	Modelo	Color	Identificador (IMEI/Serie)	Descripción adicional	Fecha de revocatoria de la autorización	Motivo de la revocatoria