Empresa Pública Metropolitana de Hábitat y Vivienda

Quito Alcaldía Metropolitana

POLÍTICA PARA LA GESTIÓN SEGURA PARA SISTEMAS EN CLOUD

Unidad de Tecnologías de la información y Comunicación

Octubre, 2025

VERSIÓN 1.0

A. REGISTRO DE APROBACIÓN DEL DOCUMENTO		
RESPONSABILIDADES	**NOMBRE / CARGO**	**FIRMA**
APROBADO POR:	María Gabriela Morales Escobar **COORDINADORA DE PLANIFICACIÓN**	Firmado electrónicamente por: MARIA GABRIELA MORALES ESCOBAR Validar únicamente con FirmaEC
REVISADO POR:	Juan Sebastian Rios Carrión **ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN 3**	Firmado electrónicamente por: JUAN SEBASTIAN RIOS CARRION Validar únicamente con FirmaEC
ELABORADO POR:	Fernanda Iguamba Farinango **ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN 3**	Firmado electrónicamente por: FERNANDA DE LOS ANGELES IGUAMBA FARINANGO Validar únicamente con FirmaEC

CÓDIGO	**FECHA DE VIGENCIA**	VERSIÓN
PO-DP-TIC-03	02-10-2025	1.0

A. REGISTRO DEL CONTROL DE CAMBIOS DEL DOCUMENTO			
VERSIÓN	**CAMBIO**	**ELABORADO**	**FECHA**
1.0	Creación de la política	Fernanda Iguamba Farinango **ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN 3**	02-10-2025

Contenido

1 SIGLAS Y ABREVIATURAS

ABREVIATURA	SIGNIFICADO
MFA	Autenticación multifactor.
DRP	Plan de Recuperación ante Desastres.
RTO	Tiempo Objetivo de Recuperación.
LOPDP	Ley Orgánica de Protección de Datos Personales.
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission.
NIST	National Institute of Standards and Technology.
CSA	Cloud Security Alliance.
VPC	Virtual Private Cloud.
2FA	Doble Factor de Autenticación.
RPO	Punto Objetivo de Recuperación, indica el tiempo maximo que una organización puede tolerar de pérdida de datos en caso de un desastre o fallo de un sistema

2 GLOSARIO DE TÉRMINOS

TÉRMINO	DEFINICIÓN
Sistema institucional en la nube	Conjunto de aplicaciones, servicios y datos de la EPMHV que se encuentran alojados en infraestructura cloud pública, privada o híbrida.
Proveedor Cloud	Entidad que provee servicios de infraestructura, plataforma o software como servicio bajo contrato con la EPMHV.

3 IDENTIFICACIÓN DE LA POLÍTICA Y PROCESO INSTITUCIONAL

Nombre del Proceso al que pertenece la política	Gestión de las Tecnologías de la Información y Comunicación
Nombre del Subproceso al que pertenece	Seguridad de la Información y Continuidad de Servicios.
Nombre de la política	POLÍTICA DE SEGURIDAD PARA SISTEMAS INSTITUCIONALES EN CLOUD.
Código de la política	PO-DP-TIC-03-1.0
Responsable de la política:	Unidad de Tecnologías de la Información y Comunicación, Dirección de Planificación

4 OBJETIVO DEL DOCUMENTO

Garantizar la seguridad de los sistemas institucionales desplegados en la nube mediante la aplicación de estándares de confidencialidad, integridad, disponibilidad, legalidad y trazabilidad, en cumplimiento de la normativa ecuatoriana y estándares internacionales.

5 ALCANCE DEL DOCUMENTO

Esta política se aplica a todas las direcciones, gerencias, unidades y áreas operativas de la EPMHV que tengan acceso a sistemas institucionales en cloud y cualquiera que a futuro requiera acceso.

6 BASE LEGAL ESPECÍFICA

LEY/NORMA/ RESOLUCIÓN	ARTICULADO PRINCIPAL
Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)	**Art. 7**: Las instituciones del Estado deben garantizar el acceso a la información pública, debiendo conservar los documentos en medios accesibles y seguros para su consulta, incluyendo archivos digitales.
ISO/IEC 27001 – Gestión de Seguridad de la Información	**Cláusula A.9** - Control de acceso: Se debe limitar el acceso a la información y sistemas a las personas autorizadas. Incluye autenticación y asignación de privilegios según el rol.

7 OBLIGACIONES Y RESPONSABILIDADES ESPECÍFICAS DE LA POLÍTICA

El personal de la Unidad De Tecnologías De La Información Y Comunicación (TICS) tiene la responsabilidad de administrar este documento y de velar por su cumplimiento y actualización, así como de evaluar y mejorar la política para la gestión segura para sistema en cloud.

Las obligaciones y responsabilidades específicas se detallan a continuación:

Unidad de TICS

- Los sistemas deben contar con controles de seguridad MFA.
- Monitorear incidentes y coordinar auditorías.
- Aprobar revisiones y gestionar incidentes críticos.

Directores/as y Gerentes

- Solicitar formalmente la creación de necesidades de acceso de su personal.

- Determinar los niveles de acceso requeridos para cada usuario bajo su responsabilidad.
- Garantizar que los usuarios bajo su cargo conozcan y respeten las disposiciones de esta política.

Usuarios/as del sistema

- Hacer uso adecuado y seguro de los recursos asignados.
- No compartir credenciales ni utilizar mecanismos inseguros de acceso.
- Evitar el uso de dispositivos no autorizados para conectarse a los sistemas.
- Custodiar credenciales y reportar incidentes.
- Cumplir con las normativas de confidencialidad y protección de la información institucional.

8 POLÍTICA

Reglas y Restricciones de Uso

Gestión de identidad y accesos:

- El acceso a los sistemas se realizará preferentemente desde equipos institucionales.
- En casos excepcionales y justificados, los responsables de área podrán solicitar acceso remoto.
- Todo acceso debe estar autenticado mediante doble factor de autenticación (2FA).
- Queda prohibido el uso de gestores de contraseñas del navegador y el registro de dispositivos como “de confianza” en los navegadores o aplicaciones.
- Deshabilitación de cuentas activas de manera inmediata cuando Talento Humano notifique la desvinculación del funcionario mediante correo electrónico.
- Revisión semestral de privilegios.

Protección de datos

- Cifrado SSL en reposo y en tránsito.
- Eliminación segura según LOPDP.

Periodicidad de respaldos

- Respaldo mensual de código fuente de conservación almacenado en medio estándar del NAS.

Custodia y acceso

- Las copias de seguridad estarán bajo la custodia exclusiva de la Unidad de TICS.
- El acceso estará restringido a personal autorizado con MFA obligatorio.

Pruebas y restauración

- Se realizarán pruebas de restauración al menos 1 veces por año para verificar la integridad y usabilidad de las copias.

Monitoreo y registros

- Recolección de datos: logs de los sistemas levantados en el servidor cloud**.**
- Retención mínima de logs: 12 meses.

Consecuencias del Incumplimiento

El incumplimiento de esta política conllevará llamados de atención según los protocolos internos de Talento Humano. Estos podrán derivar en sanciones proporcionales a la gravedad del incidente, previa verificación de los hechos por la Unidad de TICS y el área responsable.

Actualizaciones y Revisiones

Esta política no es un documento definitivo. Será objeto de revisiones periódicas impulsadas por la Unidad de TICS, con la posibilidad de incorporar sugerencias provenientes de cualquier área de la EPMHV interesada en mejorar o actualizar su contenido.

REFERENCIAS

- Autenticación de 2 factores (2FA): https://kb.synology.com/es-mx/DSM/help/DSM/SecureSignIn/2factor_authentication?version=7
- ISO/IEC 27001 – Gestión de Seguridad de la Información.