Empresa Pública Metropolitana de Hábitat y Vivienda

Quito Alcaldía Metropolitana

POLÍTICA PARA LA GESTIÓN SEGURA Y ASIGNACIÓN DE PERMISOS EN EL "NAS" INSTITUCIONAL (Network Attached Storage / Almacenamiento Conectado a la Red)

Unidad de Tecnologías de la Información y Comunicación

Mayo, 2025

VERSIÓN 1.0

REGISTRO DE APROBACIÓN DEL DOCUMENTO		
RESPONSABILIDADES	NOMBRE / CARGO	FIRMA
APROBADO POR:	María Gabriela Morales Escobar DIRECTORA DE PLANIFICACIÓN	Firmado electrónicamente por: MARIA GABRIELA MORALES ESCOBAR Validar únicamente con FirmaEC
REVISADO POR:	Alcides Neptalí Rivera Posso ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN 3	Firmado electrónicamente por: ALCIDES NEPTALI RIVERA POSSO Validar únicamente con FirmaEC
ELABORADO POR:	Juan Sebastián Ríos Carrión ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN 3	Firmado electrónicamente por: JUAN SEBASTIAN RIOS CARRION Validar únicamente con FirmaEC

ASESORÍA METODOLÓGICA DE PROCESOS.

REVISIÓN	FIRMA
Nombre: Richard Rubio Puesto: Analista de Planificación y Seguimiento 3 (Responsable de Procesos)	Firmado electrónicamente por: RICHARD EDUARDO RUBIO SALAZAR Validar únicamente con FirmaEC

CÓDIGO	FECHA DE VIGENCIA	VERSIÓN
PO-DP-TIC-01	27-05-2025	1.0

REGISTRO DEL CONTROL DE CAMBIOS DEL DOCUMENTO			
VERSIÓN	CAMBIO	ELABORADO	FECHA
1.0	Creación de la política	Juan Sebastián Ríos Carrión ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN 3	27-05-2025

Contenido

1 SIGLAS Y ABREVIATURAS

ABREVIATURA	SIGNIFICADO
NAS	Network Attached Storage (almacenamiento conectado a la red)
SMB	Server Message Block
2FA	Autenticación de doble factor
EPMHV	Empresa Pública Metropolitana de Hábitat y Vivienda
TICS	Tecnologías de la Información y Comunicación

2 GLOSARIO DE TÉRMINOS

TÉRMINO	DEFINICIÓN
NAS	Un NAS, o almacenamiento conectado a la red, es un dispositivo que proporciona un repositorio centralizado para almacenar, organizar y compartir archivos dentro de una red informática. Funciona como un servidor de archivos especializado y permite que múltiples usuarios autorizados accedan a los mismos documentos y carpetas desde distintos equipos dentro de la red institucional. En el contexto de la EPMHV, el NAS actúa como la principal herramienta para almacenar documentos institucionales, garantizando la disponibilidad de los mismos para las áreas y direcciones autorizadas. Gracias a sus funcionalidades, permite aplicar políticas de acceso controlado, respaldos automáticos y asegurar la integridad de los archivos mediante herramientas de protección como carpetas inmutables (WriteOnce).
SMB (Server Message Block)	El protocolo SMB es una tecnología utilizada para compartir archivos, carpetas, impresoras y otros recursos en una red. Es ampliamente usado en entornos Windows, pero también es compatible con otros sistemas operativos como Linux o macOS. Antes de la implementación actual del NAS en la EPMHV, muchas de las carpetas compartidas funcionaban bajo este protocolo. Cada dirección tenía una carpeta compartida disponible en red, la cual se accedía directamente a través de este mecanismo. Aunque sigue estando presente, su uso está ahora encapsulado dentro del entorno de seguridad y autenticación del NAS.
2FA (Doble Factor de Autenticación)	La autenticación de doble factor es una medida de seguridad que requiere dos métodos distintos de verificación antes de conceder acceso a un sistema. En general, se utiliza algo que el usuario sabe (una contraseña) y algo que el usuario tiene (por ejemplo, un código generado en su celular). Este sistema fortalece considerablemente la seguridad del NAS institucional, ya que, aunque una contraseña sea comprometida, el acceso no será posible sin el segundo factor. En la EPMHV, esta funcionalidad se aplica obligatoriamente tanto para acceso interno como remoto.
Secure SignIn	Secure SignIn es la aplicación oficial desarrollada por Synology para habilitar el segundo factor de autenticación (2FA). Esta herramienta permite que los

TÉRMINO	DEFINICIÓN
	usuarios registren su dispositivo móvil, donde se generarán los códigos temporales que deberán introducir cada vez que ingresen al sistema NAS. Su uso es obligatorio en el acceso a servicios sensibles del NAS de la EPMHV. La Unidad de TICS ha desarrollado un manual interno que guía paso a paso su instalación, vinculación con el NAS y buenas prácticas para su uso seguro.
WriteOnce (carpetas inmutables)	WriteOnce es una característica avanzada de Synology que permite configurar carpetas como inmutables, es decir, que los archivos almacenados en ellas no pueden ser modificados ni eliminados por ningún usuario (ni siquiera administradores) durante un período preestablecido. Esta configuración es especialmente útil para preservar la integridad y validez de documentos institucionales finales, como resoluciones, actas, informes aprobados, contratos y más. El tiempo de inmutabilidad se define por solicitud expresa de la dirección o gerencia interesada, conforme a sus normativas de archivo. Una vez habilitada, la carpeta WriteOnce actúa como una caja fuerte digital, impidiendo cualquier alteración accidental o malintencionada. Es una de las herramientas más efectivas para garantizar la trazabilidad y permanencia de documentos clave dentro de una institución pública.
Permisos de lectura y escritura	El NAS permite gestionar el acceso a carpetas y archivos mediante diferentes niveles de permisos. Los dos más comunes son: • Lectura: permite a un usuario visualizar y descargar los archivos almacenados, pero sin poder modificarlos ni eliminarlos. • Escritura: otorga al usuario la capacidad de crear, modificar y borrar archivos dentro de una carpeta. Los permisos se asignan de manera individual o por grupos, según lo defina cada dirección de la EPMHV. Para mantener la seguridad y la organización documental, se recomienda que solo personal autorizado tenga permisos de escritura en las subcarpetas sensibles.
Sincronización con Synology Drive	Synology Drive es una aplicación que permite mantener sincronizados los archivos entre el NAS y los equipos de los usuarios. De esta forma, los documentos que un usuario guarda en su carpeta local se replican automáticamente en el NAS, y viceversa. En la EPMHV se contempla su uso exclusivo para equipos institucionales, como método de respaldo y continuidad de trabajo. Esta funcionalidad aún está en evaluación, por lo que su implementación se realizará progresivamente una vez que se definan sus condiciones técnicas y de uso.

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	Gestión de infraestructura y bases de datos tecnológica
Nombre de la política	POLÍTICA PARA LA GESTIÓN SEGURA Y ASIGNACIÓN DE PERMISOS EN EL "NAS" INSTITUCIONAL
Código de la política	PO-DP-TIC-01-1.0

Responsable de la política:	Unidad de Tecnologías de la Información y Comunicación, Dirección de Planificación

4 OBJETIVO DEL DOCUMENTO

Establecer directrices técnicas y administrativas para el uso del sistema NAS institucional de la Empresa Pública Metropolitana de Hábitat y Vivienda (EPMHV), con el propósito de promover una gestión segura y responsable de los archivos y accesos, garantizar la integridad de la información institucional y reducir el riesgo de alteraciones o eliminaciones no autorizadas.

Adicionalmente, se busca asegurar la trazabilidad de las acciones realizadas por los usuarios en el sistema, y definir los criterios técnicos y organizacionales para la implementación de mecanismos como carpetas de solo escritura (WriteOnce) y la autenticación multifactor.

5 ALCANCE DEL DOCUMENTO

Esta política se aplica a todas las direcciones, gerencias, unidades y áreas operativas de la EPMHV que tengan acceso al sistema NAS institucional y cualquiera que a futuro requiera acceso, incluyendo, pero no limitándose a las siguientes carpetas que actualmente se encuentran disponibles o habilitadas en el sistema, las mismas que se describen a continuación:

CARPETAS ACTUALES QUE CONSTAN EN EL NAS Y SU RESPECTIVA UNIDAD "DUEÑA DE LA INFORMACIÓN"

Área / Dirección	Carpeta correspondiente en el NAS
Dirección Administrativa	DIR_ADM
Dirección de Comunicación	DIR_COMUNICACION
Dirección de Gestión Técnica	DIR_DGT
Dirección de Estudio y Gestión de Suelos	DIR_EGS
Dirección de Ejecución de Proyectos	DIR_EJECUCION
Dirección de Control, Supervisión y Evaluación	DIR_EVALUACION
Dirección Financiera	DIR_FINANCIERA
Dirección de Asesoría Jurídica y de Patrocinio	DIR_JURIDICO
Dirección de Negocios	DIR_NEGOCIOS
Dirección de Planificación	DIR_PLANIFICACION
Dirección de Gestión Social	DIR_SOCIAL
Dirección de Talento Humano	DIR_TH
Gerencia General	GERENCIA_GENERAL
Gerencia de Operación Urbana	GERENCIA_OU
Gestión de Bienes	GESTION_BIENES
Gestión Documental	GESTION_DOCUMENTAL

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.
Ley Orgánica del Sistema Nacional de Archivos	Art. 20: Establece la responsabilidad de las entidades públicas de organizar, conservar y facilitar el acceso a los documentos, independientemente de su soporte. La información digital debe gestionarse con criterios archivísticos y de seguridad.
Normativa del Archivo General del Estado - Acuerdo 008-NAGE-2013	Art. 11: Las instituciones públicas deben garantizar la autenticidad, integridad, conservación y acceso de los documentos electrónicos. Se recomienda el uso de mecanismos que impidan su alteración.
Código Orgánico Integral Penal (COIP)	Art. 234: Establece sanciones por acceso no autorizado, destrucción o alteración de sistemas informáticos o documentos electrónicos institucionales.
Norma Técnica de Gestión Documental para el Sector Público (Emitida por el Archivo Nacional del Ecuador)	Numeral 6.3.2: Dispone la implementación de medidas técnicas y administrativas que aseguren la protección, acceso controlado, trazabilidad y preservación de documentos electrónicos en los sistemas de archivo digital.
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.
ISO 15489 – Gestión de documentos	Sección 5.3.2: Requiere que las organizaciones públicas gestionen adecuadamente los documentos a lo largo de su ciclo de vida, incluyendo su clasificación, conservación, y acceso a largo plazo en plataformas electrónicas seguras y auditables.

7 OBLIGACIONES Y RESPONSABILIDADES ESPECÍFICAS DE LA POLÍTICA

El/la Jefe/a o Analistas de la Unidad de Tecnologías de la Información y Comunicación (TICS) tiene(n) la responsabilidad de administrar este documento y de velar por su cumplimiento y actualización, así como de evaluar y mejorar la Política de Gestión de Acceso y Conservación de Información Digital en el sistema NAS institucional.

Las obligaciones y responsabilidades específicas por cada rol, se detallan a continuación:

Unidad de TICS

- Administrar técnicamente el sistema NAS, incluyendo la gestión de usuarios, permisos y respaldos.
- Implementar y mantener los mecanismos de autenticación y trazabilidad.

- Verificar el cumplimiento de los lineamientos definidos en esta política.
- Proponer mejoras técnicas y operativas relacionadas con la seguridad del NAS.
- Coordinar con las distintas áreas institucionales la implementación de carpetas WriteOnce, acceso remoto y sincronización de archivos.

Gerentes, Directores/as y Jefes/as de Área

- Solicitar formalmente la creación de carpetas y subcarpetas conforme a sus atribuciones, nivel jerárquico y las necesidades funcionales de sus respectivas áreas.
- Determinar los niveles de acceso requeridos para cada usuario bajo su responsabilidad.
- Definir los periodos de retención de documentos en carpetas inmutables (WriteOnce).
- Garantizar que los usuarios bajo su cargo conozcan y respeten las disposiciones de esta política.

Usuarios/as del sistema NAS

- 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 al NAS.
- Cumplir con las normativas de confidencialidad y protección de la información institucional.

8 POLÍTICA

Reglas y Restricciones de Uso

Acceso y autenticación:

- El acceso al NAS se realizará desde equipos institucionales. En caso de que se requiera acceso externo, el jefe inmediato (gerente o director) deberá solicitar a la UTIC el acceso para el personal a su cargo mediante correo electrónico.
- Todo acceso debe estar autenticado mediante doble factor de autenticación (2FA) con la aplicación móvil Synology Secure SignIn. (Manual de acceso al NASS)
- Queda prohibido el uso de gestores de contraseñas del navegador y el registro de dispositivos como "de confianza" en los navegadores o aplicaciones.

Gestión de carpetas compartidas:

- Cada dirección o gerencia cuenta con una carpeta raíz, y podrá solicitar la creación de subcarpetas con permisos diferenciados por perfil.

Carpetas WriteOnce:

- Son carpetas configuradas en modo inmutable: los archivos que se almacenen en ellas no podrán ser modificados ni eliminados durante un período determinado.
- Están destinadas a conservar documentación institucional definitiva (por ejemplo, resoluciones, estados financieros, actas).
- El período de retención deberá ser solicitado por los directores de área, con base en su normativa interna.

Copias y duplicación de archivos:

- El contenido del NAS no debe ser duplicado en medios externos ni en plataformas en la nube.
- Se desactivarán complementos del NAS que permitan la exportación automatizada de archivos a terceros.
- Se encuentra en evaluación el uso del servicio Synology Drive para permitir sincronización únicamente con equipos de la EPMHV.

Enlaces compartidos:

- Los enlaces públicos preexistentes generados antes de esta política se mantienen operativos.
- La creación de nuevos enlaces deberá ser de carácter institucional.

Consecuencias del Incumplimiento

El incumplimiento de esta política conllevará llamados de atención según los protocolos internos de Talento Humano. Éstos podrán derivar en sanciones administrativas proporcionales a la gravedad del incidente, previa verificación de los hechos por una comisión integrada por representantes de la Unidad de TICS, Talento Humano, el área responsable y un delegado de la máxima autoridad institucional.

Actualizaciones y Revisiones

Esta política será objeto de revisiones periódicas impulsadas por la Unidad de TICS, con el objeto de mejorar o actualizar su contenido.

9 REFERENCIAS BIBLIOGRÁFICAS

- Autenticación de 2 factores (2FA): https://kb.synology.com/es-mx/DSM/help/DSM/SecureSignIn/2factor_authentication?version=7
- Synology WriteOnce (WORM) White Paper: https://kb.synology.com/en-global/WP/WriteOnce_White_Paper/1
- Synology Drive Server: https://kb.synology.com/es-mx/DSM/help/SynologyDrive/drive_desc?version=7
- Manual interno de acceso al NAS elaborado por la Unidad de TICS (versión institucional)