

POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN



Maicao, La Guajira

Código:	PO-860-02	POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	
Versión:	2.0-20-01-25		
Página:	2 de 9		

CONTENIDO

1. INTRODUCCIÓN.....	3
2. GLOSARIO	4
3. OBJETIVO	4
4. ALCANCE.....	4
5. GENERALIDADES	5
5.1 PROCESO DE RESGUARDO DE LA INFORMACIÓN	5
5.2 RESGUARDO DE LA INFORMACIÓN DE LOS SERVIDORES	6
5.3 PROCESO DE RESTAURACIÓN DE LA INFORMACIÓN DESPUÉS DEL INCIDENTE	7
6. CONTROL DE CAMBIOS.....	9

Elabora:	Revisa:	Aprueba:
Jefe de Tecnología y Comunicaciones	Director de Aseguramiento y Tecnología	Gerencia

Código:	PO-860-02	POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	
Versión:	2.0-20-01-25		
Página:	3 de 9		

1. INTRODUCCIÓN

La gestión de la Seguridad, protección y respaldo de la información en la EPS Indígena Anas Wayuu se fundamenta en las directrices establecidas en este documento. Además, la entidad adopta buenas prácticas y herramientas informáticas para respaldar este proceso. Reconociendo que la información se ha transformado en un activo de gran valor, la implementación de políticas eficaces de respaldo, custodia y recuperación se convierte en una necesidad esencial para la entidad.

La EPSI Anas Wayuu cuenta con un plan de respaldo de la información a través de servicios en la nube contratado con la empresa Google la cual nos permite a través de la adquisición de cuentas empresariales el resguardo de la información vital para la operación de la entidad. Esta contratación nos asegura la accesibilidad a la información en cualquier momento y lugar con acceso a internet.

El área de tecnología y comunicaciones vela por la correcta ejecución de las copias de respaldo y restauración de la información en caso de presentarse la necesidad. Para estos respaldos se adquirió 220 cuentas discriminadas de la siguiente manera:

Licenciamiento	Cantidad Licencias
Business Starter 30GB	130
Business Standard 2TB	85
Business Plus 5TB - Vault	5

En las cuentas Business Plus con capacidad de 5 Tera Byte cada una se realiza el proceso de resguardo de la información; es responsabilidad de cada empleado garantizar que la información que sea necesaria para mantener la operabilidad de la entidad quede alojada en estas cuentas dispuestas por el área de tecnología y comunicaciones.

Elabora:	Revisa:	Aprueba:
Jefe de Tecnología y Comunicaciones	Director de Aseguramiento y Tecnología	Gerencia

Código:	PO-860-02	POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	
Versión:	2.0-20-01-25		
Página:	4 de 9		

2. GLOSARIO

- **Copia de Seguridad:** En tecnología una copia de seguridad es una réplica de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de pérdida.
- **ISO 27001:** Es una norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Fue publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).
- **Recuperación:** Se refiere a las estrategias utilizadas para restablecer la información (archivos) a partir de una copia de seguridad almacenada en un medio externo. Este proceso se implementa en situaciones en las que los archivos se han extraviado o eliminado debido a diversas razones, como daño físico del dispositivo o eliminación accidental.
- **Seguridad de la Información:** Garantiza la salvaguarda de los activos de información mediante la implementación de medidas preventivas, con el objetivo de preservar la continuidad del negocio y prevenir la concreción de riesgos.
- **Seguridad Informática:** Asegura la integridad de la infraestructura tecnológica mediante el uso de herramientas o dispositivos físicos, con el fin de prevenir la materialización de amenazas que se propagan a través de la red.

3. OBJETIVO

El objetivo de este documento es garantizar, disponibilidad y confidencialidad de la información de la EPS Indígena Anas Wayuu.

4. ALCANCE

Esta política aplica a los sistemas de información y dispositivos de almacenamiento de datos de la entidad.

Elabora:	Revisa:	Aprueba:
Jefe de Tecnología y Comunicaciones	Director de Aseguramiento y Tecnología	Gerencia

Código:	PO-860-02	POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	
Versión:	2.0-20-01-25		
Página:	5 de 9		

Se tendrá en cuenta para esta política específica de la norma ISO 27001 de 2013.
A.12.3.1 - Controles de copia de seguridad, A.15.1.1 - Procedimientos y responsabilidades de gestión de la seguridad de la información.

5. GENERALIDADES

5.1 PROCESO DE RESGUARDO DE LA INFORMACIÓN

El proceso de almacenamiento en la nube con Google implica utilizar el servicio de Google Drive el cual nos permitirá compartir con cada colaborador la información almacenada en estas.

- Primeramente, en cada cuenta Business plus se crea la carpeta donde se dispondrá toda la información a resguardar, dentro de esta se crea las carpetas dependiendo la organización que nos brinda gestión documental (Direcciones, Jefaturas, Sedes)
- Dentro de cada carpeta se dispondrá de otras carpetas ya discriminando la nomenclatura asignada a cada equipo de la entidad donde se halla que resguardar información
- Luego nos dirigimos al equipo donde se encuentre la información a resguardar y se instala la aplicación de escritorio de Google Drive; esta creara en el explorador de archivos del equipo una unidad nueva; y en esta se inicia sesión con la cuenta Business Plus donde se creó la carpeta correspondiente a ese equipo.
- Se accede a Google Drive (de la cuenta Business Plus) a través de un navegador web y se suben los archivos desde tu dispositivo a Google Drive; los archivos subidos se sincronizan automáticamente con la aplicación de Drive en el escritorio.
- Luego que termine de cargar y sincronizar toda la información subida procedemos a compartir esa carpeta con el colaborador dueño de esta para que solo este tenga acceso a esta.
- Se desconecta del equipo la cuenta Business Plus para evitar el acceso a la información de los demás equipos alojadas en esta. En caso de ser necesario se puede compartir archivos o carpetas de otros equipos, permitiendo que editen o vean los archivos, dependiendo de los permisos que se le otorguen.

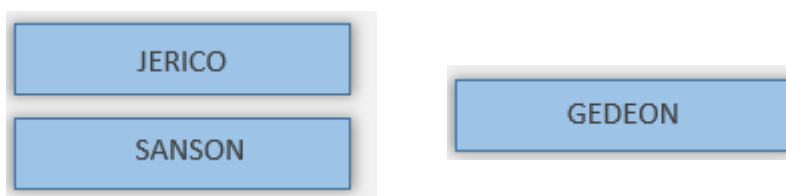
Elabora:	Revisa:	Aprueba:
Jefe de Tecnología y Comunicaciones	Director de Aseguramiento y Tecnología	Gerencia

Código:	PO-860-02	POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	
Versión:	2.0-20-01-25		
Página:	6 de 9		

- Se inicia sesión en el equipo (en la aplicación de escritorio de Google Drive) con la cuenta del colaborador asignado donde ya encontrará la carpeta compartida anteriormente con este desde la cuenta Plus, donde ya tendrá el acceso a toda la información alojada desde la nube.
- Nos dirigimos al explorador de archivos del equipo, a la unidad organizativa creada al momento de instalar la aplicación de Google Drive, donde después de terminada la sincronización podremos observar la carpeta compartida con este colaborador y desde ahí se gestionará toda la información alojada.
- Google nos ofrece desde la consola de administración opciones para controlar quién puede ver, editar o comentar los archivos como también la implementación de medidas de seguridad que ayudan a la protección de esta.

Con esto todos los equipos asociados a la entidad, incluyendo las sedes ubicadas en otros municipios, se encuentran alojando la información de la entidad en las cuentas Business Plus; en caso de presentarse alguna novedad con alguno de los equipos solo sería asignar un equipo nuevo al empleado y abrir la aplicación de Drive con el correo donde tenga alojada su información. Los archivos almacenados en Google Drive están respaldados, lo que puede ayudar en la recuperación en caso de pérdida de datos. Esta también nos permite guardar versiones anteriores de los archivos, lo que puede ser útil si necesitas retroceder a una versión anterior.

5.2 RESGUARDO DE LA INFORMACIÓN DE LOS SERVIDORES



En los servidores **JERICO**, **SANSON Y GEDEON** se encuentran las bases de datos de los Sistemas de Información y los subsistemas de la empresa alojados en los servidores de bases de datos uno en SQL server y el otro en MySQL los cuales están distribuíos en estos dos servidores, los cuales se tomaron medidas contingentes de realizarle una copia de seguridad en la nube de manera diario a ambos servidores asociados

Elabora:	Revisa:	Aprueba:
Jefe de Tecnología y Comunicaciones	Director de Aseguramiento y Tecnología	Gerencia

Código:	PO-860-02	POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	
Versión:	2.0-20-01-25		
Página:	7 de 9		

a una cuenta de Google con suficiente espacio para guardar en la nube la información de estos servidores, por tanto el código fuente de estos subsistemas están alojados

en una cuenta de GitHub por lo cual están en la nube y en los servidores dispuesto por la **EPSI Anas Wayuu**.

En el servidor **Gedeon** tiene un tratamiento especial ya que este funciona con una copia de seguridad que tiene el proveedor y nosotros recibimos la copia del espejo que se actualiza a diario en el servidor 192.168.0.245.

5.3 PROCESO DE RESTAURACIÓN DE LA INFORMACIÓN DESPUÉS DEL INCIDENTE

Paso 1: Preparación antes del desastre

- Monitorear periódicamente la actualización de las imágenes ISO del pen drive.
- Control de versiones de las imágenes ISO.

✓ Creación de una imagen de respaldo

Crear una imagen ISO con Hiren's BootCD: esta imagen se almacena en un dispositivo de almacenamiento externo (como un disco duro externo) y asegurándose de tener varias copias en diferentes ubicaciones seguras.

✓ Se Descarga la última versión de Hiren's BootCD desde su sitio web oficial

Se procederá a grabar la imagen ISO en un disco o crea un dispositivo de arranque USB con la imagen usando herramientas como Rufus o BalenaEtcher.

Pruebas regulares:

Se realizará pruebas periódicas de tus procedimientos de respaldo y restauración para asegurarte de que las imágenes de respaldo sean válidas y se puedan restaurar correctamente.

Paso 2: Respuesta al desastre

- Se procede a salvar el material que sea reutilizable de los servidores, luego

Elabora:	Revisa:	Aprueba:
Jefe de Tecnología y Comunicaciones	Director de Aseguramiento y Tecnología	Gerencia

Código:	PO-860-02	POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	
Versión:	2.0-20-01-25		
Página:	8 de 9		

realizamos las conexiones respetivas de los mismo para restaurar la red local y la red externa, una vez restaurados o en su defecto comprar nuevamente los servidores se procede a ejecutar la copia de seguridad del pen drive de respaldo.

Acceso al medio de arranque:

En caso de un desastre, utiliza el dispositivo USB o CD creado con Hiren's BootCD para arrancar desde el nuevo servidor.

✓ **Montaje de la imagen de respaldo**

Se utilizarán las herramientas de gestión de discos o las funciones proporcionadas por Hiren's BootCD para montar la imagen de respaldo almacenada en el dispositivo externo.

✓ **Restauración de la imagen**

Las opciones proporcionadas por Hiren's BootCD o cualquier otra herramienta de respaldo que servirán para restaurar la imagen del sistema en los servidores.

✓ **Verificación post-restauración**

Se realizarán pruebas para asegurarse de que los servidores restaurados funcionen correctamente.

Verificación para todos los datos importantes estén intactos y que las configuraciones de red y seguridad sean las adecuadas.

Paso 3: Mejoras y Actualizaciones

✓ **Aplicar actualizaciones**

Se Actualiza el sistema operativo y todas las aplicaciones a las últimas versiones para corregir posibles vulnerabilidades.

✓ **Revisar la estrategia de respaldo**

Después de la restauración, revisar y ajustar la estrategia de respaldo según sea necesario. Asegurándose de que esté alineada con los cambios en tu infraestructura y requisitos comerciales.

Elabora:	Revisa:	Aprueba:
Jefe de Tecnología y Comunicaciones	Director de Aseguramiento y Tecnología	Gerencia

Código:	PO-860-02	POLÍTICA DE RESPALDOS, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	
Versión:	2.0-20-01-25		
Página:	9 de 9		

✓ Documentación

Mantener documentación detallada de el plan de recuperación ante desastres, incluyendo información sobre la ubicación de las imágenes de respaldo, las contraseñas necesarias y los procedimientos de restauración.

✓ Almacenamiento seguro

Guardar las copias de seguridad en lugares geográficamente separados para protegerlas contra desastres naturales que puedan afectar una región específica.

6. CONTROL DE CAMBIOS

VERSIÓN	PAGINAS	FECHA DE INICIO	FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN DE CAMBIOS
1.0	Nueve (9)	21/06/2023	No Aplica	Creación
2.0	Nueve (9)	21/06/2023	20/01/2025	Se actualiza en el documento logo de la Supersalud según lo dispuesto por la Circular Externa 2024151000000013-5 de 2024 y cambio en la denominación de cargos.

Elabora:	Revisa:	Aprueba:
Jefe de Tecnología y Comunicaciones	Director de Aseguramiento y Tecnología	Gerencia