POLÍTICA PARA LAS COPIAS

DE SEGURIDAD

2026

Contenido

1. INTRODUCCIÓN

Teniendo en cuenta que la información constituye uno de los activos más importantes para la operación y continuidad de los procesos de Canal Capital. Su pérdida, alteración o indisponibilidad puede generar impactos significativos en la productividad, cumplimiento normativo, reputación institucional, y toma de decisiones estratégicas,

En virtud de lo anterior, y en cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI), se establece la siguiente política para la gestión de copias de seguridad, la cual define los lineamientos, responsabilidades y controles necesarios para garantizar la disponibilidad e integridad de la información crítica a través de mecanismos adecuados de respaldo, restauración y/o recuperación.

2. OBJETIVO

Establecer los lineamientos y controles necesarios para la ejecución, verificación, y restauración de copias de seguridad de la información crítica de Canal Capital, garantizado su disponibilidad e integridad, ante posibles fallos, pérdida, incidentes o desastres, en cumplimento con los controles de seguridad que sugiere la ISO/IEC 27001:2022 (Seguridad de la información en servicios de almacenamiento en la nube y copias de seguridad de la información).

3. ALCANCE

La presente política aplica para todos los activos de información, tales como: bases de datos, sistemas de información, archivos electrónicos, unidades de red, correo electrónico, Google Drive y configuraciones críticas de la infraestructura tecnológica de Canal Capital, tanto en ambientes On-Premise como en la nube.

4. DEFINICIONES[1]

Acceso a la Información: Conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema de bases de datos, bibliotecas, archivos e Internet.

Acción Correctiva: Medida orientada a eliminar la causa de cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.
Acción Preventiva: Medida orientada a prevenir cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.

[1] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Activo de Información: Datos o información que tienen un valor para una Entidad.

Aplicaciones: Es todo software que se utiliza para la gestión o manejo de la información.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona en cualquiera de los sistemas de información de la entidad.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Backup (Copia de seguridad): Proceso mediante el cual se realiza una duplicación de archivos, datos, configuraciones o sistemas, con el fin de ser restaurados en caso de pérdida, daño o incidente.

Backup completo: Tipo de respaldo que copia todos los archivos y datos seleccionados, independientemente si se han cambiado o no desde el último backup realizado.

Backup incremental: Tipo de copia de seguridad que solo guarda los archivos o datos que han cambiado desde el último backup realizado.

Backup diferencial: Tipo de copia de seguridad que incluye todos los cambios realizados desde el último backup completo.

Criptografía: La criptografía es la ciencia y el arte de proteger la información mediante técnicas matemáticas, con el fin de garantizar la confidencialidad, integridad, autenticidad y no repudio de los datos. Utiliza algoritmos y protocolos para cifrar la información y hacerla ilegible para cualquier persona no autorizada. La criptografía es fundamental en la seguridad de las comunicaciones electrónicas, como en el caso de pagos en línea, mensajes privados o autenticación de usuarios.

Cifrado en tránsito: Protección de los datos durante su transmisión a través de redes mediante mecanismos criptográficos.

Cifrado en reposo: Protección de datos almacenados mediante algoritmos de cifrado, para evitar accesos no autorizados.

Confidencialidad: Mantener la información oculta a individuos, entidades o procesos no autorizados.

Control: Procedimiento, procesos, políticas que permiten mantener el riesgo de la seguridad de la información por debajo del riesgo presente.

Disponibilidad: Mantener la información accesible a quien la necesita en el momento que la necesite.

Restauración: Proceso de recuperación de datos desde una copia de seguridad, utilizado para devolver

un sistema, dispositivo o información a su estado operativo previo.

Riesgo: Posibilidad de que ocurra un contratiempo.

RTO (Recovery Time Objetive): Tiempo máximo de tolerancia para restaurar un sistema o servicio tras una interrupción.

Seguridad de la Información: Según ISO 27002 es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática: Encargada de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de gestión de seguridad de la información seguro y confiable.

SGSI Sistema de Gestión de Seguridad de la Información: Es un mecanismo que permite preservar la confidencialidad, integridad y disponibilidad de la información.

Sistema crítico: aplicación, servicio, base de datos o recurso, cuya indisponibilidad puede afectar gravemente la operación de la entidad.

Usuario: Cualquier persona que haga uso de los servicios de red proporcionados por la entidad tales como equipos de cómputo, sistemas de información y redes.

Vulnerabilidad: Condición de un sistema que lo hace susceptible a una amenaza.

5. NORMATIVIDAD

Canal Capital acoge las normas vigentes de seguridad de información, protección de datos personales y directrices de ciberseguridad a nivel nacional y territorial aplicando las prácticas y estándares recomendados para su cumplimiento.

- Ley 1474 de 2011, reglamentada por el Decreto Nacional 734 de 2012 y reglamentada parcialmente por el Decreto Nacional 4632 de 2011, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales.
- Ley 1712 de 2014, reglamentada parcialmente por el Decreto Nacional 103 de 2015, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Conpes 3854 de 2016, que es la Política de Seguridad Digital para Colombia y en la cual se establecen nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la

innovación.

- Decreto 1413 de 2017, Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 612 de 2018, por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 1081 de 2015, Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
- Decreto 767 de 2022, (Actualización de Política de Gobierno Digital) Por el cual se establecen los lineamientos generales de la Política de GobiernoDigital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 02277 de 2025, con la cual se actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI), contenido en el Anexo 1 de la Resolución 500 de 2021, y se derogan disposiciones anteriores que resultaban contrarias a los nuevos estándares internacionales en esta materia. Esta actualización del MSPI fortalece la estrategia de seguridad digital del Estado colombiano, al adoptar los lineamientos de la norma ISO/IEC 27001:2022. Esto permite a las entidades públicas contar con una herramienta moderna, robusta y alineada con las mejores prácticas internacionales para proteger los activos de información, y garantizar la prestación continua de servicios esenciales a la ciudadanía.

6. TIPOS DE COPIAS DE SEGURIDAD

Datos operativos:

- Documentos (unidades de red), que incluye: vídeos, piezas gráficas digitales, Archivos editables: proyectos audiovisuales (Premiere, After Effects, Cap Cut) y de diseño (Illustrator, Photoshop).
- Bases de datos
- Archivos de aplicaciones
- Copias de correo electrónico.

Configuraciones de infraestructura:

- Archivos de configuración de servidores
- Scripts
- Certificados SSL
- Reglas y/o configuraciones del Firewall.
- Configuraciones de Switch de distribución, Switch de borde, Switch Core, controladora WiFi, servidores de transmisión, entre otros.

Backups en nube:

- Snapshot de instancias o servidores.
- Copias o instantáneas de volúmenes.
- Bases de datos.
- Configuraciones de IAM
- Políticas de seguridad de acceso a los diferentes componentes, por ejemplo, políticas de S3.
- Plantillas de IaC (Infraestructura como Código).
- Repositorios de código fuente.
- Configuraciones de WAF.
- VPC
- S3
- Todos los servicios que se implementen en nube

7. FRECUENCIA DE COPIAS DE SEGURIDAD

La frecuencia de las copias de seguridad tiene como objetivo garantizar que la información, los sistemas de información y los dispositivos críticos puedan ser recuperados en el menor tiempo posible y con el mínimo impacto para Canal Capital ante eventos que afecten la operación. En función de ello, se establecen los siguientes lineamientos:

- **Bases de datos:** Copias incrementales diarias y copia completa semanal.
- **Archivos de usuarios en unidades de red:** Copia incremental diaria y copia completa semanal.
- **Servidores de aplicaciones (Snapshot):** Copia incremental diaria y copia completa semanal.
- **Configuraciones de servidores:** copia completa semanal o ante cualquier cambio significativo.
- **Dispositivos de red:** copia completa semanal o ante cualquier cambio significativo.
- **Correo electrónico:** copia completa del buzón de correo electrónico y Google Drive por usuario, 6 meses después de la finalización del vínculo contractual con Canal Capital, antes de eliminar una cuenta de correo o antes de realizar transferencias de propiedad del Drive.
- **Componentes en Cloud:** según la criticidad del recurso, mínimo semanal, y siempre antes de actualizaciones o cambio mayores.

8. ALMACENAMIENTO DE LAS COPIAS DE SEGURIDAD

Las copias de seguridad que se generen deben ser almacenadas de manera cifrada, de acuerdo con su criticidad, estableciendo controles de acceso estrictos, además se deben tener en cuenta los siguientes lineamientos para su almacenamiento:

On-site: Almacenamiento en los dispositivos de respaldo o solución de backup ubicado en el Centro de Datos de Canal Capital en la sede principal.

Off-site: Copia en ubicación física o medios distintos o en servicios de almacenamiento.

Cintas de almacenamiento: Utiliza tecnología de cintas magnéticas LTO-8 para los respaldos de información. Cada cinta tiene una capacidad nativa de 12 TB, lo que permite manejar grandes volúmenes de datos. Esta solución es crucial para establecer una "air gap" o barrera física que protege los datos de amenazas cibernéticas, ya que la información se almacena fuera de la red.

El proceso de respaldo se divide en dos flujos principales. El primero es un respaldo completo y diario para el área misional. En este proceso, se transfieren a las cintas una gran variedad de videos en formato MXF, incluyendo producciones finalizadas, material en bruto, programas con y sin closed caption, y coberturas de eventos. Una vez que el sistema verifica que la integridad de la copia es correcta, el archivo original se elimina del servidor de origen para liberar espacio de almacenamiento. El segundo flujo de trabajo es para las tareas administrativas. Aquí se realizan respaldos incrementales diarios y uno completo semanal de todos los documentos de las diferentes dependencias que se encuentran en las unidades de red.

Para asegurar que todo el sistema funcione correctamente, se hace un respaldo del catálogo de cintas. Este catálogo es un índice de todo el contenido guardado y su respaldo asegura que la información pueda ser localizada y recuperada de manera eficiente si es necesario. Por último, la custodia de las cintas una vez grabadas, se guardan en un lugar seguro con acceso y manejo controlados.

Nube: Copia de seguridad de los diferentes componentes desplegados en dicha plataforma.

9. RESTAURACIÓN COPIAS DE SEGURIDAD

La restauración de las copias de seguridad permitirá confirmar la integridad de los datos, así como validar su efectividad y los tiempos de recuperación (RTO), asegurando que la información sea completamente funcional. Para ello, se establecen los siguientes lineamientos:

- **Documentación de las pruebas:** se debe documentar el proceso de las pruebas de restauración, en la "Bitácora de respaldos de información" (dispuesta en la Intranet), la cual permitirá guardar trazabilidad, en función del éxito de la copia de seguridad o del proceso de restauración.
- **Periodicidad:** se deben realizar pruebas de restauración de las copias de seguridad trimestralmente, con el objetivo de validar la integridad de los datos.
- **Inventario:** se debe mantener un inventario de las copias de seguridad disponibles, junto con sus ubicaciones.

10. TIEMPOS DE RETENCIÓN DE LAS COPIAS DE SEGURIDAD

Datos operativos:

Los tiempos de retención de las copias de seguridad deberán estar alineados con las Tablas de Retención Documental (TRD) de la organización, considerando la naturaleza y el tipo de la información respaldada.

- Para información de funcionarios, contratistas y proveedores, los respaldos deberán conservarse por el periodo definido en las TRD y en cumplimiento con la normativa contractual y de protección de datos vigente.
- Los diferentes tipos de backups (completos, incrementales y diferenciales) deberán conservarse según

su categoría en las TRD.

- Una vez cumplido el periodo de retención, las copias deberán eliminarse de forma segura, utilizando métodos de borrado seguro o destrucción física, garantizando la imposibilidad de recuperación no autorizada.

Configuraciones de infraestructura local y nube:

- Diarios: Retención de 7 días.
- Semanales: Retención de un mes
- Mensuales: Retención de 12 meses

Anuales: Retención de 5 años.

11. ROLES Y RESPONSABILIDADES

- **Líderes técnicos / Coordinadores de área:** ejecución de respaldos, monitoreo, verificación y pruebas de restauración.
- **Oficial de Seguridad de la Información:** supervisión del cumplimiento de la política y gestión de accesos.