CONTENIDO

1. INTRODUCCIÓN

El siguiente documento hace parte de la **POLITICA GENERAL DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION Y COMUNICACIONES** de la entidad

El instituto municipal de recreación y deporte IMRD de chía, basará la administración de la Seguridad de protección y respaldo de la información, en las políticas contenidas en este documento;

2. GLOSARIO DE LOS TERMINOS

- **Acuerdo de Confidencialidad:** Contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.
- **BACKUP / Copia de Seguridad:** En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.
- **Cintoteca:** Almacén donde se depositan las cintas magnéticas que no se encuentran en uso en tareas de respaldo o en custodia externa.
- **Copia de seguridad Completa (full):** Una copia de seguridad que incluye la totalidad de archivos previamente seleccionados de un sistema informático.
- **Copia de seguridad incremental:** Una copia de seguridad que respalda los archivos creados o modificados desde la última copia de seguridad completa. La restauración de los datos debe realizarse con la última copia de seguridad completa y las copias de seguridad incrementales posteriores.
- **Custodia de Medios:** Corresponde al almacenamiento seguro de los medios magnéticos fuera de la entidad, a cargo de un proveedor externo.
- **Encargado de Seguridad:** Persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información a la UAEMRV y supervisar el cumplimiento de la presente Política.
- **Firewall:** Dispositivo tecnológico que tiene como función proteger la red interna de una compañía de accesos no autorizados del exterior vía Internet.
- **GSIT**: Gestión de Servicios e Infraestructura tecnológica.
- **Librería de Cintas / LTO (Library):** Sistema de Backup robotizado que utiliza como medio de almacenamiento cintas magnéticas. Es el puente de conexión entre la red de datos y las cintas de respaldo.
- **LTO (Linear Tape-Open):** Tecnología de cinta magnética de almacenamiento de datos, desarrollada originalmente a finales de 1990 como alternativa de estándares abiertos a los formatos de cinta magnética patentada que estaban disponibles en ese momento.
- **Recuperación:** Hace referencia a las técnicas empleadas para recuperar la información (archivos) a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers
- **NAS (Network Attached Storage):** Almacenamiento conectado en red es el nombre dado a una tecnología de almacenamiento dedicada a compartir la

capacidad de almacenamiento de un computador (servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo.

- **Seguridad de la Información:** Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.
- **Seguridad Informática:** Se encarga del aseguramiento de la infraestructura tecnológica mediante herramientas o elementos físicos, para evitar que se materialización las amenazas que se propagan por la red.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Sistemas de Información:** Medios de almacenamiento y procesamiento de los datos de la entidad y que ofrecen algún servicio informático especifico.
- **Tareas de respaldo:** Programación de las copias de seguridad que incluyen: la fuente, el destino y la periodicidad.
- **Tercero(s):** Cualquier persona natural o jurídica en calidad de proveedor, outsourcing o consultor.
- **TIC:** Tecnologías de la información y comunicaciones.
- **USB:** El Universal Serial Bus (USB) (bus universal en serie BUS) es un estándar industrial desarrollado en los años 1990 que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre ordenadores y periféricos y dispositivos electrónicos.
- **Usuario:** Este concepto cobija a todos los clientes internos, servidores públicos y contratistas que utilicen la red de la entidad.
- **VPN:** Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Prívate Network, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
- **WAN:** Wide área network o red de área amplia, es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales (LAN).

3. OBJETIVOS GENERAL

Definir los lineamientos generales aplicables a los sistemas de información y a la infraestructura critica de la entidad, para garantizar las copias de seguridad, así como la custodia o protección de la misma.

3.1 OBJETIVOS ESPECIFICOS

- Identificar la información crítica o sensible que se debe proteger.
- Garantizar que la información reciba un nivel apropiado de protección de acuerdo con la importancia y criticidad para la entidad.
- Definir el proceso de respaldo, custodia y recuperación de la información.

4. ALCANCE

Esta política aplica a todos los sistemas de información y dispositivos de almacenamiento de datos de información catalogados como información crítica e importante, para la prestación de los servicios internos y externos de la Unidad.

El o los responsables de administrar la infraestructura tecnológica o que tengan interacción con la misma deberán cumplir esta política.

Se tendrán en cuenta para esta política específica los controles A.12.3 Copias de respaldo, tomado de la norma ISO 27001:2013.

5. DECLARACION

En este documento se encuentran los lineamientos que aseguran una actuación adecuada para alcanzar un alto nivel en cuanto a seguridad de la información en el IMRD CHIA. La información es un activo importante para la entidad, tiene un alto valor para la misma, por esto mismo la unidad ha definido las directrices de seguridad para la protección y respaldo de la información por medio de las cuales se deben orientar todas las acciones a seguir. Estas directrices hacen parte del marco de POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE INFORMACIÓN Y COMUNICACIONES y están basadas en las buenas prácticas, leyes y normas relacionadas con la seguridad de la información:

- Ley 1273 de 2009 – De La Protección de la Información y de los datos.
- ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información (SGSI), ISO/IEC 27002:2005 – Código para la Práctica de la Gestión de la Seguridad de la Información.
- ISO 22301:2012 – Seguridad de la Sociedad: Sistemas de Continuidad del Negocio y la Norma Técnica Colombiana NTC- ISO: 9001.

Por lo anterior, se busca minimizar riesgos en la perdida de información, asegurar la continuidad en la operación de los servicios de infraestructura del IMRD CHIA y ayudar en el cumplimiento de los objetivos misionales.

Acuerdo de confidencialidad:

Todos los Usuarios que administran, leen, modifican o generen información en el IMRD CHIA deben firmar un acuerdo de confidencialidad o de no divulgación como parte de sus términos y condiciones iníciales de empleo. Esta directriz también incluye a personal en provisionalidad, de carrera, ops y los usuarios externos no contemplados en un contrato formalizado.

6. GENERALIDADES.

7. Respaldos:

8. De acuerdo con la identificación previa de los activos de información, se debe catalogar cada activo de información que requiera respaldo, de acuerdo con la importancia o criticidad de esta para ser incluidas en los procedimientos de respaldo y protección, (BD, correo electrónico, información almacenada en "google drive" copia de seguridad de equipos de cómputo, copia de seguridad de la información de los servidores entre otros).

9. El proceso de GSIT debe definir el procedimiento para el respaldo y protección de la información catalogada como critica o de alta importancia para la entidad, definiendo la periodicidad, medios de almacenamiento, procedimiento para recuperación, responsable de la generación.

10. Es responsabilidad de los líderes de procesos y jefes de dependencias garantizar que la información institucional identificada y catalogada como critica "aquella necesaria para mantener operativos los procesos de la entidad", sea almacenada en los servidores (nube o en sitio) de la entidad, para que a su vez sea almacenada en la NAS o SAM.

11. Para la gestión de archivos compartidos de los usuarios, se deben crear carpetas compartidas para cada una de las dependencias de la entidad en el servidor de archivos, siguiendo una nomenclatura de tablas de retención documental generadas el área de gestión documental.

12. No se permite almacenar en servidores ni equipos de cómputo de la entidad, información personal, música, videos, documentos transitorios, documentos confidenciales, backups de equipos de escritorio, backups de correo electrónico y demás que no sea relevante en el cumplimiento de los objetivos de la Entidad.

13. Es responsabilidad de los líderes de proceso y jefes de dependencias identificar claramente la información crítica a su cargo, identificar los riesgos y generar el plan de continuidad en el cual debe estar incluido la solicitud de respaldo al administrador de copias de seguridad.

14. Los líderes de proceso y jefes de dependencias son los únicos autorizados para solicitar el respaldo y/o recuperación de información mediante un formato dispuesto para tal fin, indicando los datos del solicitante, datos de la aplicación, datos de los archivos (tipo y ubicación), datos de la BD (ubicación, motor y versión), accesos, periodicidad del respaldo y tipo de respaldo. Siempre que exista alguna modificación o adición en la fuente de la información, se debe generar el formato descrito y entregarlo al administrador de copias de seguridad.

15. Se debe contar con el procedimiento de respaldo de información tan pronto un funcionario se desvincule del IMRD CHIA.

16. Se deben establecer los tipos de respaldo generado, (completo, incremental), la frecuencia de estos y el tiempo de retención en los medios internos y externos.

17. El software o aplicativo de respaldo y restauración de información debe estar instalado en los servidores para los cuales se haya hecho solicitud de copias de seguridad. Si es un software de pago, se debe contar con las licencias necesarias que garanticen el cumplimiento de dicha solicitud.

18. Es recomendable la custodia y almacenamiento de los medios magnéticos (cintas) con una empresa externa especializada en el tema.

19. El encargado de la administración de copias de seguridad deberá realizar pruebas aleatorias de la integridad de los respaldos y hacer pruebas de restauración sobre ambientes de pruebas controlados para validar la efectividad de los respaldos.

20. Las copias de respaldo deben ser debidamente rotuladas con nombre, contenido y fecha según el procedimiento predeterminado para este fin.

21. Restauración:

22. Los líderes de proceso y jefes de dependencias son los únicos autorizados para solicitar la recuperación de información ante una pérdida total, parcial o para realizar pruebas controladas.

23. Se debe diligenciar en su totalidad el formato respaldo y recuperación de Información y ser entregado al administrador de copias.

24. Es responsabilidad del administrador de copias informar la disponibilidad de los respaldos, realizar el trámite para obtener los medios magnéticos, ejecutar el procedimiento de recuperación e informar los resultados.

REVISIÓN Y APROBACIÓN:

Elaborado y/o Actualizado por Sistemas imrd chia, I Proceso:	Validado por RESPONSABLE DIRECTIVO SIG del Proceso:	Aprobado por:
Contratista / Proceso GSIT	Firma: ALDOVER ALEXANDER COLORADO CASTAÑO	Firma: FABIAN EDUARDO ROMERO OVIEDO
Acompañamiento EQUIPO TÉCNICO SIG:		