PROCESO O ÁREA AUDITADA: Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital, PL-TI-02 Versión 04, fecha: 31/01/2022, el cual se encuentra establecido en la secretaría TIC	**FECHA DE ELABORACIÓN:** 13 - diciembre - 2023
DIRECTIVO RESPONSABLE: José Duván Lizarazo Cubillos – Jefe de Oficina de Control Interno de Gestión	**DESTINATARIO:** **HÉCTOR FABIO HINCAPIÉ LOAIZA** Secretario Tecnología de la información y comunicaciones

ASPECTOS GENERALES DEL PROCESO DE AUDITORÍA

OBJETIVO:

Evaluar el seguimiento al Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital, PL-TI-02 Versión 04, fecha: 31/01/2022, estableciendo un marco de gestión de riesgos a través del cual se mitigan las vulnerabilidades y amenazas asociadas a los activos de información de la Entidad Territorial Gobernación del Quindío, con el fin de lograr reducir la probabilidad e impacto en la Entidad.

ALCANCE:

Se realizará la verificación a la implementación Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital, PL-TI-02 Versión 04.

METODOLOGÍA:

La metodología para desarrollar la presente auditoría es la contemplada Guía de Auditoria para Entidades Públicas 2015 de la Función Pública, para lo cual:

1. Se realizará reunión de apertura de la auditoria.
2. Solicitud de información.
3. Determinación de muestra de auditoría.
4. Construcción de papeles de trabajo.
5. Diseño y aplicación de las siguientes pruebas:

- Visitas a todos y cada uno de puesto o cuartos donde se encuentran los RACK
- Visita a la data center de la Entidad territorial
-. Se verificará las políticas y procedimientos relacionados con el Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital.

6. Desarrollo de observaciones.
7. comunicación de resultados preliminares para aclaraciones del informe preliminar.
8.comunicacion Informe Final de Auditoria.

INFORME EJECUTIVO

El seguimiento realizado se abordó desde la revisión de las evidencias presentadas por la secretaría de Tecnologías de la Información y las Comunicaciones, donde la Oficina de control interno de gestión solicita a través de oficio CIG 13.31.01 – 00457 del 19 de octubre de 2023 para dar inicio al Plan de Auditoría y la apertura de la Auditoría Interna a procesos No.012 de 2023, con el fin de realizar Seguimiento al Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital, PL-TI-02.

Una vez obtenida la información requerida y aportadas las evidencias pertinentes el equipo auditor procede a realizar las inspecciones de todos los documentos adoptados y publicados en la página de la gobernación del Quindío, de conformidad con MIPG y relacionados con el objeto de auditoría, rastreando toda aquella información que de una u otra manera tiene trazabilidad con el mismo.

La metodología por desarrollar en la presente auditoría es la contemplada Guía de Auditoría para Entidades Públicas 2015 de la Función Pública

ETAPA DE PLANEACIÓN

En la etapa de planeación el equipo auditor revisó los criterios de auditoría, políticas, procedimientos y guías en razón a procesos auditores desarrollados conforme al Plan de Auditoría vigencia 2023, igualmente se analiza la matriz Mapa de riesgos de seguridad digital MR-TIC-02, versión 01 del 06 de noviembre de 2020, "Mapa de Riesgos de Gestión" y los controles establecidos en el proceso, con el fin de alcanzar los objetivos del proceso auditor, de la siguiente manera:

CRITERIOS DE AUDITORIA

- Decreto 187 del 28 de marzo del 2019, como una más de sus secretarías y creando a su vez dos direcciones que ayudarán a cumplir los objetivos institucionales que la entidad trace a corto, mediano y largo plazo

- Decreto 00629 del 17 de noviembre de 2021 "Por medio del cual se modifica, actualiza y compila el plan estratégico de tecnologías de la información (PETI), la política de seguridad y privacidad de la información, el plan de seguridad y privacidad de la información, el plan de tratamiento de riesgos de seguridad de la información y seguridad digital, la política de tratamiento de datos personales y el plan de capacidad de tecnologías de la información para el departamento del Quindío; se actualiza el RNBD y se adoptan otras disposiciones".

- Decreto 1078 de 2015 "Por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de la Información y las comunicaciones". "Esta versión incorpora las modificaciones introducidas al decreto único reglamentario del sector de tecnologías de la información y las comunicaciones a partir de la fecha de su expedición. última fecha de actualización: 20 de octubre de 2023**".**

- Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018.

- NTC ISO31000, Numeral 2.9

- Normativa ISO 9001, así como de la LOPD (Ley Orgánica de Protección de Datos).

- Ley 1712 de 2014, "Ley de Transparencia y del Derecho de Acceso a la Información Pública" la cual hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley".

- Guía No 21 Gestión de Incidentes de Seguridad de la Información.

- Guía No 3. Procedimientos de seguridad de la información

- Tecnologías de Operación -TO (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

- Norma ISO 27001

-

1. REVISIÓN GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

Para el análisis y revisión al *Plan gestión de riesgos seguridad de seguridad, privacidad de la información y seguridad digital*. PL-TIC-02, el equipo auditor verifica cada uno de los riesgos establecidos en el Plan con los procedimientos que se tienen establecidos para la mitigación de estos.

1.1 Plan gestión de riesgos seguridad de seguridad, privacidad de la información y seguridad digital. PL-TIC-02

Objetivo general

- Plantear y establecer un marco de gestión de riesgos a través del cual se mitiguen las vulnerabilidades y amenazas asociados a los activos de información de la gobernación del Quindío, con el fin de lograr reducir su probabilidad e impacto en la entidad

Objetivos específicos:

- Proteger y conservar los activos informáticos de la gobernación del Quindío contra riesgos, desastres naturales o actos malintencionados.
- Garantizar la operatividad de la red interna de la gobernación del Quindío, cuando se presente alguna eventualidad.
- Evaluar los riesgos de los procedimientos de contingencia requeridos cuando se presenta una interrupción de las operaciones, de forma que sólo se inviertan los recursos necesarios.
- Identificar las amenazas e impactos de seguridad digital asociadas a los procesos de la entidad.
- Gestionar los riesgos identificados con una matriz que ayude a reducir su probabilidad e impacto si se este se llegará a materializar.
- Minimizar la posible pérdida de información en el evento inesperado, previendo procedimientos de recuperación efectivos y eficientes.

1.1.1 Identificación de los riesgos.

1.1.2 Riesgo por incidencia externa

a. Desastres naturales:

"(…)

El edificio de la gobernación cuenta con una estructura sismo resistente, que ayuda a que en caso de terremoto este pueda seguir en pie o, en consecuencia, con muchos menos daños que otros edificios.

Por otra parte, la red interna de la gobernación del Quindío está respaldada con UPS, para evitar que los Switchs se dañen en caso de tormentas eléctricas, con este mismo respaldo cuentan los servidores de la gobernación que se encuentran en el data center.

Análisis:

Para lo expuesto anteriormente la secretaría TIC cuenta con un Plan de mantenimiento preventivo y correctivo PL – TIC – 04, donde se establece **Mantenimiento preventivo,** el cual contiene rutinas de mantenimiento que varían de acuerdo con el tipo de equipo, que para las UPS con que cuenta la Administración departamental establece:

UPS

- ✓ Desarmado.
- ✓ Revisión de Baterías.
- ✓ Revisión de placa electrónica de poder.
- ✓ Pruebas de Mantenimiento.

Observaciones:

- Se evidencia a través de visita al Data center en el primer piso de la Entidad donde se encuentran la UPS que da soporte a los principales servidores (PCT, SEVENET, CONTROLDOC, TELEFONIA, INTERNET), Esta se encuentra en buen estado y los técnicos encargados en la operación de la misma informan del mantenimiento realizado a la UPS y cumple con la función en caso de presentarse fallos de energía, para continuar con el funcionamiento eficiente y eficaz que brinda a la entidad Territorial Gobernación del Quindío.
  De igual forma se anexa reporte por la secretaría TIC, a través de informe remitido en julio 19 de 2023, evidenciando mantenimiento y compra de baterías Anexo 1 evidencias secretaría TIC.

- No obstante, la secretaria TIC cuenta con un cronograma para la realización del mantenimiento dos veces al año para cada secretaria, el cual no evidencia en el cronograma visitas programadas a los lugares donde se encuentran las UPS ubicadas y/o periodicidad de mantenimiento para las mismas. Por otra parte, para el segundo semestre No se evidencia o reporta por la secretaría TIC mantenimiento a los equipos tecnológicos con que cuenta la entidad territorial Gobernación del Quindío, acción fundamental en el cumplimiento de las actividades del día a día de los funcionarios y colaboradores en la Entidad.

b. **Modificaciones a la constitución política**

Leyes, decretos, resoluciones, ordenanzas, etc. Que expida el gobierno nacional a cargo del ministerio de Tecnologías de la información y comunicaciones MinTic, sobre el trato, seguridad y manejo de la información que tienen los entes gubernamentales.

Observación: Conforme al Plan establecido por la secretaría TIC para los decretos, leyes, resoluciones y ordenanzas, el equipo auditor verifica que la Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018, insumo para la construcción y funcionamiento de las políticas y planes de la Administración departamental, presenta una versión desactualizada, que para la fecha la función pública adopta la versión 6 de 2022.

Es importante aclarar que a través de Auditoria N. 4 Política de privacidad de seguridad de la información – privacidad y confidencialidad vigencia 2022 se establecieron varias recomendaciones relacionadas con leyes y decretos los cuales presentaban desactualización que, a la fecha en las políticas, procedimientos NO realizaron las actualizaciones respectivas como lo establece la ley.

1.1.3 Riesgos por incidencia interna

a. Perdida de la Información

La Gobernación del Quindío, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center.

Análisis

La secretaría TIC cuenta con un procedimiento P-TI C-01 cuyas generalidades y controles son:

Generalidades

"(…)

La gobernación del Quindío a través de la secretaria TIC ha identificado los procesos operativos o de misión crítica que se manejan a través de los diferentes aplicativos de la Entidad, los cuales son respaldados con copias de seguridad diaria, la frecuencia de estas copias fue establecidas por la Secretaría TIC".

Controles

"(…)

- Las copias de seguridad de los aplicativos Sevenet, PCT, Siscar, Siscar Web, Estampilla Pro-hospital y pagina web e intranet, se deberán de realizar diariamente y registrasen en las bitácoras correspondientes para cada uno de los aplicativos."
- Los servidores públicos efectuaran copias de seguridad supervisadas por el personal de la Secretaría TIC, cuando los equipos de cómputo sean enviados a mantenimiento preventivo o correctivo, previniendo así la pérdida de información.
- Los Administradores de las bases de datos realizaran pruebas de restauración de los backups con la periodicidad establecida en el plan de copias de seguridad, para garantizar que las copias son leídas y restauradas correctamente

(…)"

Observaciones:

El equipo auditor NO evidencia copias de seguridad para los aplicativos Siscar web y estampilla Pro-hospital y las copias diarias del Full PCT como lo tiene establecido en el plan de contingencia en el aplicativo PCT. *(PL-TIC-07 PLAN DE CONTINGENCIA PCT).*

Recordando que el aplicativo hace parte de gestión financiera y nómina, utilizado para la totalidad de las dependencias de la Entidad Territorial Gobernación del Quindío.

Por otra parte, se evidencia que los planes de contingencia establecidos para sevenet, PCT, Siscar Web, la Secretaría TIC informa que los equipos electrónicos determinados como planes de contingencia deben estar ubicados fuera de las instalaciones de la Administración Departamental, para los cuales se incumple con el control establecido ya que se encuentran ubicados en el data center de la Entidad.

Se recomienda a la secretaría TIC analizar y monitorear los controles que tiene establecidos en el Plan de contingencia PCT y los procedimientos para las copias de seguridad y recuperación de información, para evitar que el riesgo se materialice.

Anexo 2 cd. evidencias secretaría TIC Backups 1de enero a 31 de octubre de 2023.

Años	FECHA	TIPO	Cuenta de TIPO
2023	ene	HUMANO	92
		INTRANET	27
		OBJETOSPCT	10
		PCT	308
		SEVENET	25
		SISCAR	20
	feb	HUMANO	86
		INTRANET	31
		OBJETOSPCT	10
		PCT	285
		SEVENET	24
		SISCAR	10
		OBJETOS	10
	mar	HUMANO	93
		INTRANET	34
		PCT	325
		SEVENET	24
		SISCAR	16
		OBJETOS	20
	abr	HUMANO	81
		INTRANET	15
		PCT	285
		SEVENET	16
		SISCAR	15
		OBJETOS	10
	may	HUMANO	97
		INTRANET	31
		PCT	348
		SEVENET	32
		SISCAR	22
		OBJETOS	11
		SGDA	1
	jun	HUMANO	69
		INTRANET	15
		PCT	246
		SEVENET	25
		SISCAR	9
		SGDA	4
		(en blanco)	
	jul	HUMANO	76
		INTRANET	23
		PCT	267
		SEVENET	28
		SISCAR	14
		OBJETOS	14
		SGDA	5

	ago	HUMANO	36
		INTRANET	7
		PCT	120
		SEVENET	12
		SISCAR	8
		OBJETOS	4
		SGDA	3
	sep	HUMANO	44
		INTRANET	11
		PCT	160
		SEVENET	8
		SISCAR	6
		OBJETOS	12
		SGDA	14
	oct	HUMANO	26
		INTRANET	6
		PCT	122
		SEVENET	10
		SISCAR	5
		OBJETOS	10
		SGDA	7
Total general			**3840**

Fuente: Evidencias secretaría TIC reporte Backups corte 31 de octubre 2023

b. Falla de equipos electrónicos

Para mitigar el riesgo, la gobernación del Quindío a través de la secretaria TIC y con el apoyo de la empresa contratista a cargo de los mantenimientos preventivos y correctivos, viene realizando y ejecutando un plan de mantenimiento preventivo, el cual incluye un cronograma de actividades y que es ejecutado durante todo el año.

Análisis:

El equipo auditor verifica el PLAN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO PL-TIC-04 y EL PROCEDIMIENTO P-TIC-21 IDENTIFICACION Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN encontrando,

- PL- TIC-04: Frecuencia del mantenimiento.

"(…)

La Secretaría TIC de la gobernación del Quindío ha definido que el mantenimiento debe realizarse mínimo dos veces al año, sin embargo, en cualquier momento que surja una eventualidad con el equipo de cómputo se le aplicara el mantenimiento preventivo en forma integral por el equipo de sistemas de la Secretaría TIC ".

- P-TIC-17

"(….)

Controles

- Los Administradores de las bases de datos realizaran pruebas de restauración de los backups con la periodicidad establecida en el plan de copias de seguridad, para garantizar que las copias son leídas y restauradas correctamente.
- La Secretaría TIC conservará las copias de seguridad en un lugar externo a los del origen de la información, el cual debe contar con las medidas protección y seguridad física adecuadas.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PUBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: P-TIC-21 tabla1: criterios de clasificación

- **Observaciones:**
  Si bien se tiene establecido realizar el mantenimiento preventivo y correctivo dos veces al año para el segundo semestre la secretaria TIC NO reporta contrato con la empresa encargada en realizar el mantenimiento y NO se evidencia el desarrollado de la actividad, incumpliendo con lo establecido en el Plan, el cual permite mantener trazabilidad de los equipos pertenecientes a la Administración departamental y análisis para la toma de decisiones (compra de equipos, software) logrando determinar acciones que mejoren la vida útil de los equipos de cómputo.

  Por otra parte en el Procedimiento P-TIC-17 se tiene establecido controles sobre los activos con que cuenta la Entidad Territorial Gobernación del Quindío, los cuales NO se ven reflejados en los controles que se deben establecer como es la protección y adecuación que requiere el sitio instalado en el centro de convenciones donde se tienen ubicados equipos como la NAS y otros equipos (Backups) que se realizan diariamente a procesos y procedimientos desarrollados por todos y cada uno de los funcionarios y colaboradores de la Entidad Territorial Gobernación del Quindío.

  Por último, se evidencia que el cuarto de comunicaciones ubicado en el centro de convenciones no tiene una adecuada instalación física y la protección requerida, la cual No posee una Planta eléctrica, sistema de refrigeración, Seguridad física, dejando ver lo vulnerable que es el sitio.

- **Falla en servidores**
  Los servidores se actualizan constantemente con las últimas actualizaciones de seguridad, además estos cuentan con monitores de confiabilidad y rendimiento que envían alertas al administrador ante cualquier eventualidad.

- **Virus informáticos**
  Contra los virus informáticos, la gobernación del Quindío cuenta con antivirus en todos los equipos de cómputo de esta, que protegen los equipos en tiempo real. Además de lo anterior, cabe destacar que, a través del año, se está ejecutando el mantenimiento preventivo el cual incluye mantenimiento de software y sistema operativo (desinfección).

- **Seguridad o robo**
  Para reducir el riesgo de robo la gobernación del Quindío cuenta con un plan de mantenimiento de las cámaras de seguridad para del edificio, así como un estudio de la viabilidad para aumentar el número de las cámaras con el fin de reforzar la seguridad de este. la gobernación cuenta con vigilantes las 24 horas del día.

- **Calentamiento de la Sala de Cómputo (Data center)**
  Este riesgo tiene una baja probabilidad de ocurrencia, debido a que la gobernación del Quindío ha implementado procedimientos para su mitigación, tales como: La implementación en el centro de cómputo principal (piso 1) de un Sistema de Temperatura autorregulada, provisto de un sistema de aire acondicionado, con sensores ambientales para el control y monitoreo de temperatura.
- **Accesos no autorizados a los sistemas de información**
  "(…)
  Por otra parte, y con el fin de evitar acceso no autorizado a los sistemas de información por parte de personas tanto internas como externan a la gobernación del Quindío; La entidad cuenta con un firewall instalado y con un sistema de **antivirus** licenciado que brindan seguridad a la hora de bloquear intentos de ataques o accesos a sistemas de información de la entidad"

- **Activos de la información desactualizados**

Dentro de los planes y controles que la Secretaría TIC ejecuta, se tiene establecido el catálogo de servicios tecnológicos y la arquitectura de servicios TI, los cuales deben de tener actualizados los activos de la información para su correspondiente actualización anual. Igualmente, la secretaria TIC cuenta con un sistema de información, el cual hace un levantamiento de la información de los equipos de la entidad, su licenciamiento y sus características de hardware

Análisis

Para los riesgos Falla en servidores, virus informáticos, seguridad o robo, calentamiento de la sala de cómputo (Data center), accesos no autorizados a los sistemas de información y Activos de la información desactualizados se analiza los procedimientos implementados por la secretaría TIC en Administración de la Infraestructura tecnológica P-TIC-02 y Protección de Activos Tecnológicos P-TIC-19, encontrando lo siguiente:

Administración de la Infraestructura tecnológica P-TIC-02
Alcance

Este procedimiento aplica para la gestión de los recursos tecnológicos, como son: el antivirus corporativo, los servidores, la plataforma de correos institucionales y la red de datos y el canal de internet, siendo las herramientas vitales para que los demás recursos tecnológicos puedan operar con total normalidad en todas las dependencias de la Administración Central Departamental.

Objetivo

Este procedimiento tiene por objeto:
La administración del antivirus corporativo que permite la gestión de las estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central. A través de la consola de antivirus, se pueden gestionar tareas, aplicar políticas de seguridad, controlar el estado del sistema y responder rápidamente a problemas o amenazas en equipos remotos.
"(…)"

GENERALIDADES

Un plan de seguridad de la información eficaz para cualquier empresa implica la elección de la mejor solución de acuerdo con sus necesidades. El antivirus corporativo contribuye con la protección contra los códigos maliciosos al permitir que los administradores TI puedan responder con facilidad y velocidad frente a diversos ataques informáticos, obtener reportes del funcionamiento de la seguridad en toda la red, actualizar las bases de firmas para todos los equipos y ejecutar las soluciones del antivirus, todo desde una misma locación, sin importar la cantidad de equipos que la conforman o la distribución de esta. " (…)"

Observaciones

Si bien la Secretaría TIC cuenta con un aplicativo llamada OCSinventory1, cuya finalidad es levantar la información de hardware y software de cada equipo de la gobernación del Quindío, y permite establecer una base de datos actualizada de equipos de cómputo. De acuerdo a evidencias reportadas, el software OCSinventory1 presentan inconsistencias ya que el equipo auditor ha tomado evidencia de algunos equipos los cuales no tienen instalado el antivirus, razón por la cual se recomienda analizar y monitorear la administración del antivirus ya que por medio de este aplicativo es donde se obtiene el inventario de los equipos electrónicos con que cuenta la Administración Departamental y mantener en constante supervisión la protección contra los códigos maliciosos y así evitar vulnerabilidades para el funcionamiento de la seguridad en toda la red de la Entidad, y evitar al máximo la disminución de la materialización de riegos asociados a ataques graves a la plataforma informática. Lo anterior también permite controlar el estado del sistema y responder rápidamente a problemas y amenazas en equipos remotos.

Protección de Activos Tecnológicos P-TIC-19 versión 01 fecha: 30/11/202
ALCANCE

Este procedimiento aplica para la gestión de protección de los activos tecnológicos de la gobernación del Quindío, como son: el acceso a las instalaciones de la data center de la entidad, la protección que tiene este contra acceso no autorizados, sobrecargas eléctricas y condiciones ambientales correctas.

OBJETIVO

Este procedimiento tiene por objeto;

- Indicar como se realiza la verificación de acceso a la data center de la entidad.
- Comprobar las condiciones ambientales del cuarto de cómputo.
- Verificar que el flujo de corriente no afecte a los equipos instalados de la data center de la entidad.

GENERALIDADES

"El modelo de seguridad y privacidad de la información (MSPI) el cual adopto la gobernación del Quindío, incluye los procedimientos de seguridad de acuerdo con la guía No 3. (Ministerio de tecnologías de la información y comunicaciones MinTic, 2016), y el cual hace parte del componente de seguridad y privacidad de la información, de la estrategia de gobierno digital. Para el desarrollo del componente de Seguridad y Privacidad de la Información,

se ha diseñado unos documentos de lineamientos "Modelo de Seguridad y Privacidad de la Información" el cual lo largo de los últimos años se ha ido actualizando en función de las modificaciones de la norma técnica que le sirve de sustento: ISO 27001, las mejores prácticas y los cambios normativos que tengan impacto sobre el mismo.
(…)".

Observaciones.

Se evidencia que el Procedimiento protección de Activos Tecnológicos P-TIC-19 versión 01 fecha: 30/11/2020 presenta desactualización en actividades y flujograma. No obstante, se evidencia que en el desarrollo del procedimiento se toma de referencia la Guía No 3. (Ministerio de tecnologías de la información y comunicaciones MinTic, 2016), la cual está vigente para el periodo evaluado, en consecuencia, el equipo auditor verifica y evidencia falencias para algunos procedimientos de ***seguridad y privacidad de la Información*** detallando lo siguiente;

- **Gestión de activos**

Observaciones.

Para el procedimiento en mención la oficina de control interno de gestión realiza observaciones y recomendaciones a través del seguimiento Mapa de Riesgos de Gestión en el riesgo R1 presencia de fallas a hurtos en hardware y software (Base de datos) en custodia de la secretaría TIC, donde se reitera las falencias al consolido realizado en el aplicativo OCSinventory1 al inventario reportado por la secretaria a 31 de agosto de 2023 donde NO se tiene un total exacto del número de equipos con que cuenta la Entidad. También se evidencia duplicidad en direcciones IP y casillas vacías en el archivo que arroja el aplicativo, evidenciando que el total de equipos presenta inconsistencias.

Por otra parte, en el Plan de mantenimiento preventivo y correctivo PL-TIC-04

- Levantamiento de Información
- Mantenimiento preventivo
- Revisión y análisis del informe y formulación de acciones de mejora

El equipo auditor no evidencia hojas de vida de cada uno de los equipos, a la fecha no se encuentran actualizadas y su archivo no se clasifica por equipo como lo manifiesta el Plan, sino en un expediente consolidado de la totalidad de equipos de la Entidad, donde no se distingue cronología y lineamientos archivísticos implementados.

No se ha realizado la baja definitiva de equipos que, de acuerdo con concepto técnico, análisis

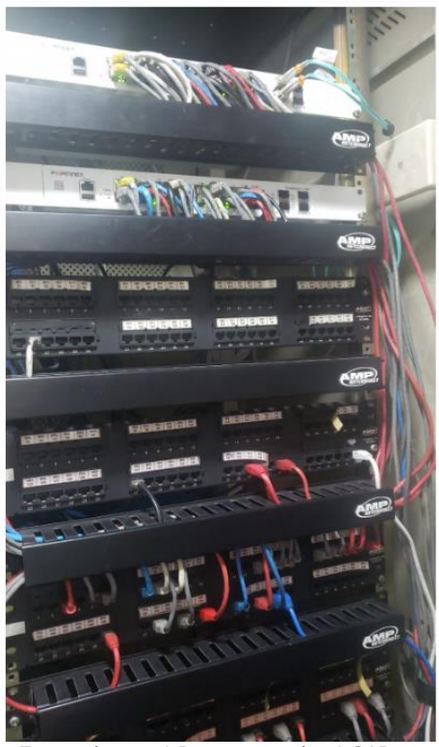
de uso y depreciación requiere de esta gestión tanto a nivel técnico, de recursos físicos y contable. Como se establece en la Política Nacional para la Gestión Integral de los Residuos de Aparatos Eléctricos y Electrónicos.

Se determina que el total de inventario con que cuenta la Entidad es primordial en la toma de decisiones para el presupuesto requerido en cuanto a cobertura, necesidad de infraestructura (activos desactualizados) y sistemas vinculados. Todo lo anterior es insumo para mantener trazabilidad de los errores y soluciones más comunes que se generen en los equipos informáticos.
Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.

- **Seguridad física y del entorno**
  Para el procedimiento se establece que al ingresar a los centros de procesamiento de datos y los centros de cableado tendrán restricción de acceso a personal
  "(…)"
  Observaciones:
  En el recorrido realizado a los cuartos de comunicaciones y cuarto principal Data center, se evidencio cambios significativos como son:
  Data Center.
- El aire acondicionado mejoro notablemente.
- Compra de switches
- Cableado fibra óptica donde se tiene dos canales designados uno como principal y el segundo como Backups. Ver imagen 1
  De igual forma se evidencia objetos que no corresponden y equipos que llevan más de dos (2) años y a la fecha no se les ha dado de baja o puesto en funcionamiento, donde la secretaria TIC a través de S.TIC- 62.217.00 – 0756 del 4 de julio de 2023 Informe de avance a observaciones realizadas a la Auditoria N.01 del 2022 manifiesta que se tiene la posibilidad de que entren en funcionamiento. Los cuales deben realizar verificación y análisis ya que pueden presentar obsolescencia al momento de incurrir en gastos para que entre en funcionamiento. Ver imagen 3.

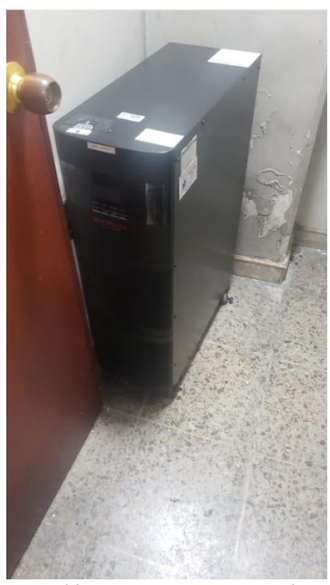
  También se evidencia que el Data center NO cumple con las normas y especificaciones del Cableado Estructurado y No cuenta con las especificaciones mínimas, una de ellas es el piso falso, el cual una vez instalado la Entidad ahorraría gastos en consumo energía, permitiendo mejorar los sistemas de enfriamiento, ya que la conductividad y la distribución se realizaría de forma localizada y mayor aprovechamiento del espacio.

Visita al Data Center piso 1 CAD-



Fuente: imagen1 Data center piso 1 CAD

Fuente: imagen2 Data center piso 1 CAD



Fuente: imagen3 Data center piso 1 CAD objetos que no corresponden

Visita a los cuartos de comunicaciones

En el recorrido se evidencia que para algunos cuartos de comunicaciones como se evidencia imagen 4 correspondiente al piso 7 Secretaría Administrativa, continua con objetos que no corresponde al cuarto se switches, evidenciando que se pueden presentar riesgos para el funcionamiento de los equipos encontrando:

- Poca ventilación hay que recordar lo que puede ocasionar que los equipos no estén debidamente ventilados y refrigerados (calentamiento y bajo rendimiento)
- Recordar que estos cuartos no son bodegas.

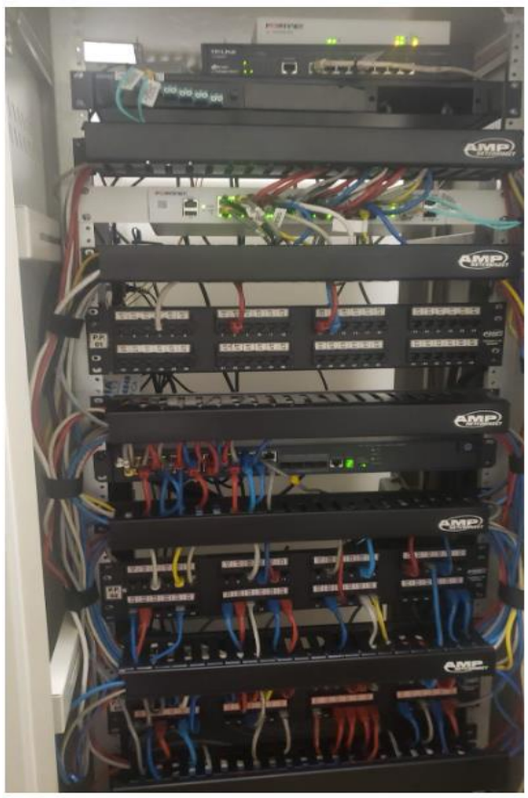
-. Falta de limpieza tanto para los equipos como los cuartos, es de recordar que la acumulación

de polvo en los equipos contribuye al bajo rendimiento de estos.
- En el piso 9 la chapa presenta averías

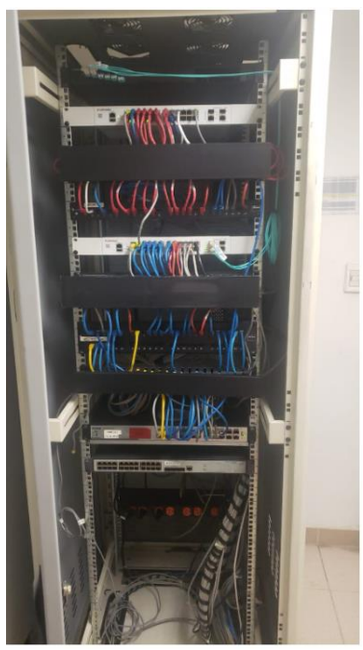
Es de informar que si bien se presenta avance en el mantenimiento y cambio de cableado y equipos electrónicos en la Administración Departamental es vital que se continúe cumpliendo de las políticas, procesos, procedimientos y guías establecidas por la secretaría TIC


Fuente: imgenes 4 piso 7 secretaria Administrativa cuarto de comunicaciones


Fuente: imgenes 5 piso 3 secretarias Hacienda y Salud cuarto de comunicaciones




Fuente: imgenes 6 piso 9 secretarias Educacion y Agricultura cuarto de comunicaciones




Fuente: imgenes 7 piso 3 secretarias Educacion, Turismo y Cultura cuarto de comunicaciones

- **Establecimiento del contesto**

- **Contexto Externo**

A nivel nacional el decreto 1581 del año 2012 “Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales” y el cual hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual “todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
(…)

Observación
La Oficina de control interno de gestión obedeciendo a lo establecido en el formato Plan de gestión de riesgos de seguridad, privacidad de la información y seguridad digital, evidencia que en la vigencia 2022 desarrollo la Auditoria N. 04 en Política de privacidad de seguridad de la información - Privacidad y confidencialidad.
Donde se registraron 3 hallazgos que a la fecha la secretaría TIC, No suscribió y No ejecuto el Plan de Mejora, que de acuerdo con lo estipulado debió registrarse 15 días hábiles después de finalizado.

- **Contexto Interno**

La gobernación del Quindío dentro de su estructura organizacional recientemente modificada adhirió a la secretaría TIC, mediante el decreto 187 del 28 de marzo del 2019, como una más de sus secretarías y creando a su vez dos direcciones que ayudarán a cumplir los objetivos institucionales que la entidad trace a corto, mediano y largo plazo.
Dentro de las funciones de la secretaría TIC están Diseñar y formular los planes, programas y proyectos, así como fortalecer el uso, la innovación y la apropiación de las tecnologías de la información y las comunicaciones y la gestión de la información, con el fin de propiciar la implementación de la TI en el Departamento del Quindío.
(…)

Observación
El equipo auditor verifica a través de la página web de la gobernación del Quindío el Decreto por medio del cual se crea la Secretaría TIC, que a la fecha mantiene un compromiso en la implementación continua en cada uno de las políticas, planes y procedimientos del plan de Gestión de Seguridad, privacidad de la Información, la articulación con otros procesos misionales y las acciones encaminadas al mejoramiento de los procesos, con el objetivo de mejorar la satisfacción de los usuarios en términos de confidencialidad, integridad y disponibilidad de la información.

Fuente: link página web Gobernación del Quindío referente al Decreto 187 del 28 de marzo de 2019 pagina
https://quindio.gov.co/home/docs/items/item_101/GACETA_No._027_DECRETO_187_de_28_Marzo_de_2019.pdf

- **Identificación de activos de seguridad de la Información**

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018.
(…)

Referencia del catálogo de servicios tecnológicos
Fichas de servicios con que cuenta la secretaría TI:

- **Servicio de Internet**

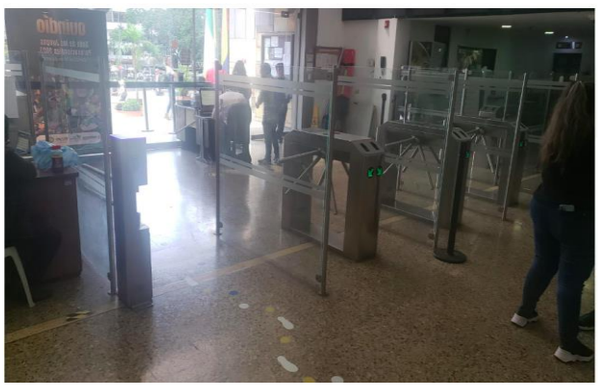
En la ficha de servicio se detalla que el servicio soporte lo realiza la empresa Une telecomunicaciones.

Observación
Se informa que la fichas se deben actualizar, ya que la empresa con la que se tiene el presente contrato para el servicio y soporte de Internet es AYA comunicaciones.

- Torniquetes

DESCRIPCION: Sistema de seguridad física dedicado al control de acceso a las instalaciones del centro administrativo departamental, Cuyo fin es el de tener un registro completo de todas las personas que ingresan al lugar para así poder aplicar los controles de seguridad pertinentes. El sistema de torniquetes funciona bajo un servidor y aplicación de software.

Observación
La entidad cuenta con 4 torniquetes trípodes de acceso doble brazo y una puerta de acceso personas discapacitadas de los cuales 2 se encuentran fuera de servicio o deshabilitados.
Es evidente que presenta fallas para el control de seguridad y los recursos para la mitigación y remediación establecido en el formato (***Gestión de incidentes de seguridad de la información O-TIC-02).***



- **Matriz de Riesgos de seguridad Digital**
  - **Fase de implementación**

Actualmente desde la secretaría TIC de la gobernación del Quindío ya se está haciendo un control sobre los riesgos identificados en las dos matrices de riesgos, reduciendo así la posibilidad de que los riesgos anteriormente mencionados puedan materializarse

Observación:
Para la fase de implementación el equipo auditor verifica en la intranet la Matriz de riesgos seguridad digital se encuentra cargada en el link Matriz Mapa de riesgos de gestión versión 04 fecha 10-mar-2023, se recomienda que la secretaría TIC verifique y actualice la información correspondiente al link establecido

Fuente: link Matriz de riesgos seguridad digital http://45.162.78.186:1882/sevenet/principal.php
Fuente: link Matriz Mapa de riesgos de gestión http://45.162.78.186:1882/sevenet/principal.php

- **Otros documentos valorados**
  Licencias de software
  Control de software P-TIC-14

Observación

El equipo auditor evidencia mediante información remitida a través de correo electrónico registros en Excel del total de software con que cuenta la Entidad y establecen a través de colores los estados de Soporte, Renovación licencia, Adquisición y soporte y por último compra. Estableciendo el control que se realiza a cada aplicativo.

No obstante, se recomienda a Secretaría TIC efectuar la revisión y obtener los certificados faltantes, estos deben especificar el software autorizado, la fecha de vigencia y la cantidad de licencias autorizadas así mismo, indicar el tipo de licenciamiento autorizado. Lo anterior, con el propósito de asegurar que el software instalado tiene los soportes adecuados. Adicionalmente, incluir en el reporte anexado por la secretaria, inventarios software un campo en el cual se especifiqué el tipo de licencia adquirida y mantenerlos actualizados.

- Los informes deben dar claridad sobre la situación real del Licenciamiento de software gestionado, generar alertas sobre situaciones que puedan generar sanciones o multas.

OCIG - SITUACIONES PRESENTADA (DEBILIDADES)

- Falta de mantenimiento regular y documentado que pueda llevar a un deterioro progresivo de los activos tecnológicos, aumentando la vulnerabilidad ante fallos técnicos que puedan resultar en una respuesta inadecuada ante eventos inesperados y en una mayor vulnerabilidad, reduciendo la eficiencia y eficacia operativa de los sistemas informáticos de la Gobernación del Quindío.
- La falta de adecuación y protección del sitio, junto con la ausencia de una planta eléctrica, sistema de refrigeración y seguridad física, deja a los equipos como la NAS y otros backups altamente vulnerables, lo que puede resultar en pérdida de datos y fallos en la continuidad operativa.
- Utilizar una guía desactualizada para la construcción y funcionamiento de políticas y planes puede resultar en la implementación de controles y prácticas que no cumplen con los requisitos actuales, aumentando la vulnerabilidad de la entidad ante riesgos emergentes y comprometiendo la efectividad de la gestión de riesgos.
- La ausencia de copias de seguridad incrementa significativamente el riesgo de pérdida de datos críticos, lo que puede afectar gravemente la gestión financiera y de nómina, así como otras operaciones dependientes de estos sistemas.
- La ubicación de equipos que no se encuentran en funcionamiento aumenta la vulnerabilidad de la entidad ante desastres que afecten el data center, reduciendo la efectividad del plan de contingencia y la capacidad de recuperación ante fallos.
- Lo anterior enfatiza la necesidad de una revisión exhaustiva y la actualización de políticas, planes y procedimientos, así como la mejora en la infraestructura física y las prácticas de mantenimiento para garantizar una gestión de riesgos eficaz y la continuidad operativa de la Gobernación del Quindío.

FORTALEZAS.

- La secretaria TIC ha demostrado un compromiso continuo con la implementación de políticas, planes y procedimientos relacionados con la seguridad y privacidad de la información. Esto incluye la articulación con otros procesos misionales y acciones encaminadas al mejoramiento de los procesos, con el objetivo de mejorar la satisfacción de los usuarios en términos de confidencialidad, integridad y disponibilidad de la información.
- La Secretaría TIC ha implementado una Matriz de Riesgos de Seguridad Digital, la cual está disponible en la intranet de la entidad. Esta herramienta es crucial para identificar, evaluar y gestionar los riesgos relacionados con la seguridad digital, permitiendo una respuesta rápida y efectiva a posibles amenazas.
- Lo anterior reflejan el compromiso de la Secretaría TIC y la Administración Departamental para mantener una gestión eficiente y segura de sus recursos tecnológicos, garantizando así la continuidad operativa y la protección de la información.

PRINCIPALES SITUACIONES ENCONTRADAS

OBSERVACIÓN N.1: CONTROLES AL PLAN DE CONTINGENCIA PCT Y COPIAS DE SEGURIDAD DE

LOS APLICATIVOS SEVENET, PCT, SISCAR, SISCAR WEB, ESTAMPILLA PRO-HOSPITAL Y PAGINA WEB E INTRANET.

Condición

- Una vez revisadas, verificadas y analizadas el reporte remitido a la oficina de control interno de gestión, NO evidencia copias diarias en los aplicativos Siscar web y estampilla Pro-hospital y Las copias diarias del Full PCT.

Criterio

- El Plan de contingencia PCT PL-TIC-07 versión 01 fecha: 07/04/2022.
- El Procedimiento P-TI C-01 versión 02, fecha 09/06/2022

Causa

- Procesos que no cumplen con el Plan y Procedimientos del Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital.

Efecto

- Perdida irreversible de los datos, ocasionando un paso atrás en todos los aspectos desde lo económico, tiempo hasta multas y sanciones.

OBSERVACIÓN N.2: PLAN QUE NO CONTEMPLA LA FRECUENCIA DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO

Condición

- En el segundo semestre de 2023 la secretaria TIC NO reporta contrato con la empresa encargada en realizar el mantenimiento y NO se evidencia el desarrollado de la actividad.

- No se tiene establecido controles sobre los activos con que cuenta la Entidad Territorial Gobernación del Quindío, los cuales NO se ven reflejados en los controles que se deben establecer como es la protección y adecuación que requiere el sitio instalado en el centro de convenciones donde se tienen ubicados equipos como la NAS y otros equipos (Backups) que se realizan diariamente a procesos y procedimientos desarrollados por todos y cada uno de los funcionarios y colaboradores de la Entidad Territorial Gobernación del Quindío.
- se evidencia que el cuarto de comunicaciones ubicado en el centro de convenciones NO tiene una adecuada instalación física y la protección requerida, la cual No posee una Planta eléctrica, sistema de refrigeración, Seguridad física, dejando ver lo vulnerable que es el sitio.
- No se ha realizado la baja definitiva de equipos que, de acuerdo con concepto técnico, análisis de uso y depreciación requiere de esta gestión tanto a nivel técnico, de recursos físicos y contable. Como se establece en la Política Nacional para la Gestión Integral de los Residuos de Aparatos Eléctricos y Electrónicos.

Criterio

- Plan de mantenimiento preventivo y correctivo PL-TIC-04 versión 01 fecha: 31/01/2022
- Procedimiento identificación y clasificación de activos de información P-TIC-21 versión 02 fecha:30/06/2022
- Procedimiento Protección de Activos Tecnológicos P-TIC-19 Versión 01 fecha: 30/11/2020

Causa

- No se está dando cumplimiento al Plan de mantenimiento preventivo y correctivo y al Procedimiento identificación y clasificación de activos de información
- Riesgo de incendio falta de sistemas de extinción (No se evidencia Extintores en los cuartos de Comunicaciones y Data center).

Efecto

- Ocasiona funcionamiento lento de los equipos, problemas de memorias, funcionamiento errático (bloqueos, programas que no se abren, virus, etc.)
- Posible pérdida de información

- Daños permanentes en las piezas básicas de la computadora (procesador, disco duro, tarjeta gráfica, memorias, etc.)
- Recursos necesarios en el manejo de presupuesto para la infraestructura (activos desactualizados) y sistemas vinculados.

Observación N. 3: RIESGOS RELACIONADO CON PRESENCIA DE FALLAS Y HURTOS EN HARDWARE Y SOFTWARE (BASES DE DATOS) EN CUSTODIA DE LA SECRETARIA TIC

Condición
- La Secretaría TIC cuenta con un aplicativo llamada OCSinventory1, cuya finalidad es levantar la información de hardware y software de cada equipo de la gobernación del Quindío, y establecer una base de datos actualizada de equipos de cómputo con que cuenta la Entidad Territorial Gobernación del Quindío. De acuerdo con evidencias reportadas, el software OCSinventory1, presentan inconsistencias ya que el equipo auditor ha tomado evidencia de algunos equipos los cuales no tienen instalado el antivirus.
- En consecuencia, el total de equipos con que cuenta la Entidad Territorial Gobernación del Quindío NO corresponde con el número que reporta la Secretaria TIC, ya que se evidencian a través del OCSinventory1 (reporte 31/08/2023) duplicidad de IP y casillas vacías en el archivo. Por lo anterior el total de equipos con que cuenta la Entidad no es exacto.

Criterio
- Procedimiento Administración de la Infraestructura Tecnológica P-TIC-02 Versión 02, Fecha:09/06/2022
- Protección de activos tecnológicos P-TIC-19 Versión 01 fecha: 30/11/2020

Causa
- Falta ejecución y seguimiento al Procedimiento P -TIC-02 Versión 02 Fecha:09/06/2022
- Falta apropiación de PETIC al interior de la oficina
- Falta de controles de seguridad apoyados en la tecnología que garanticen la seguridad de los bienes tecnológicos del edificio de la gobernación del Quindío.

Efecto
- Datos erróneos del total de equipos electrónicos con que cuenta la Administración Departamental.
- Vulnerabilidad ante posibles ataques cibernéticos y seguridad en toda la red de la Entidad.
- Incumplimiento de la Normatividad interna adoptada por a secretaría TIC.

Observación N. 4: GESTIÓN QUE NO CONTEMPLA LA PROTECCIÓN DE ACTIVOS TECNOLÓGICOS EN LAS ACTIVIDADES Y FLUJOGRAMAS.

Condición
- En la revisión y análisis al procedimiento Protección de activos tecnológicos P-TIC-19 se identificó que el flujograma desarrollado para el funcionamiento y cumplimiento de este no cumple con las descripciones planteadas por la secretaria TIC.

Criterio
- Procedimiento Protección de activos tecnológicos P-TIC-19 Versión 01 fecha: 30/11/2020

- Alcance
  Este procedimiento aplica para la gestión de protección de los activos tecnológicos de la gobernación del Quindío, como son: el acceso a las instalaciones de la data center de la entidad, la protección que tiene este contra acceso no autorizados, sobrecargas eléctricas y

condiciones ambientales correctas.

Causa
- Equipos susceptibles a fallos electrónicos.
- Falta de controles de seguridad.

Efecto
- Incumplimiento de la Normatividad interna adoptada por a secretaría TIC.

CONCLUSIONES

El Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital PL-TIC-02 establecido por la secretaría TIC muestra un enfoque adecuado hacia la protección y conservación de sus activos informáticos y la continuidad operativa en caso de incidentes externos. Sin embargo, se identifican áreas clave que requieren atención inmediata:

1. **Mantenimiento Programado y Consistente:** Es esencial incluir todas las ubicaciones de UPS en el cronograma de mantenimiento y garantizar que se realice de manera regular y documentada. Por otra parte, es vital la actualización del inventario de equipos y sus hojas de vida, y realizar la baja definitiva de equipos obsoletos según las políticas nacionales.

2. **Actualización de Políticas y Procedimientos:** Es imperativo actualizar las políticas y procedimientos de acuerdo con la versión más reciente de las normativas vigentes para asegurar el cumplimiento legal y la eficacia en la gestión de riesgos.

3. **Copias de Seguridad y Planes de Contingencia:** Es crucial implementar y monitorear de manera efectiva las copias de seguridad diarias para todos los aplicativos y asegurar que los equipos de contingencia estén ubicados externamente.

4. **Adecuación del Cuarto de Comunicaciones:** Se debe mejorar la instalación física y las medidas de protección del cuarto de comunicaciones y aumentar el número de cámaras de seguridad. Para reducir la vulnerabilidad de los equipos allí ubicados.

5. **Gestión Rigurosa del Antivirus:** Monitorear y administrar rigurosamente la instalación y funcionamiento del antivirus en todos los equipos.

6. **Actualización de Fichas de Servicios:** Revisar y actualizar las fichas de servicios tecnológicos, asegurando que reflejen los contratos actuales y el estado operativo de los sistemas de seguridad física, como los torniquetes de acceso.

Estas acciones son fundamentales para fortalecer el marco de gestión de riesgos y garantizar la resiliencia de la entidad frente a amenazas y vulnerabilidades. y asegurar el cumplimiento de las normativas vigentes. La implementación efectiva de estas medidas fortalecerá la seguridad, privacidad y disponibilidad de la información y servicios tecnológicos, contribuyendo significativamente a la mejora continua de los procesos misionales de la entidad.

EVIDENCIAS Y ANEXOS

Para el presente informe se anexa oficio CIG 13.31.01-00457 de 19 de octubre de 2023 Notificación de auditoria N. 012 Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital, PL-TI-02de 2023, con el Plan de auditoria
- Acta de reunión del 20 de octubre de2023 correspondiente a la instalación de la auditoria N. 012 y listado de asistencia
- Oficio S.TIC – 62.217.00 – 0756 de 04 de julio de 2023 correspondiente a los avances

realizados por la secretaria TIC correspondientes a la auditoria N. 04 Política de privacidad de seguridad de la información - Privacidad y confidencialidad.

NOMBRE RESPONSABLE REUNIÓN	CARGO	FIRMA
José Duván Lizarazo Cubillos	Jefe de Oficina	 JOSE DUVAN LIZARAZO CUBILLOS Jefe de Oficina de Control Interno De Gestion

ELABORACIÓN	REVISIÓN	APROBACIÓN
Elaborado Por: Juan Carlos Suarez Izquierdo	Revisado por: José Duván Lizarazo Cubillos	Aprobado por: José Duván Lizarazo Cubillos
Cargo: Profesional Universitario	Cargo: Jefe de Oficina	Cargo: Jefe de Oficina