	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 1 de 15

PROCESO O ÁREA AUDITADA: PROCEDIMIENTO DE COPIAS DE SEGURIDAD Y RECUPERACIÓN DE LA INFORMACIÓN. P-TIC-01	FECHA DE ELABORACIÓN: 17 de enero de 2025
DIRECTIVO RESPONSABLE: Dr. José Duván Lizarazo Cubillos	DESTINATARIO: SECRETARIA DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES - TIC

ASPECTOS GENERALES DEL PROCESO DE AUDITORÍA

OBJETIVO:

Construcción de informe final de la Auditoria No. 11 al seguimiento y verificación de la aplicación al procedimiento de copias de seguridad y recuperación de la información en los aplicativos que se manejan en todas las dependencias de la Administración Central Departamental, asegurando que se realicen de manera oportuna, segura y conforme a las normativas vigentes. Gestionado por la secretaria TIC

ALCANCE:

El presente análisis abarcará la verificación de la ejecución de copias de seguridad y recuperación de la información en la infraestructura tecnológica, tanto en servidores locales como en la nube. También comprende la evaluación de la seguridad y la integridad de los respaldos, así como la revisión de los procedimientos para su almacenamiento, manejo y restauración. Este procedimiento se extiende a todas las áreas operativas de la Administración Central Departamental, asegurando que los datos críticos se mantengan protegidos contra pérdidas, daños o accesos no autorizados, y que se cumpla con las normativas legales y regulatorias pertinentes en materia de protección de datos.


METODOLOGÍA:

La oficina de Control Interno de Gestión adelantó las siguientes actividades para el presente informe abarcará la revisión del procedimiento – Copias de seguridad y recuperación de información – P-TIC – 01 Versión: 02 Fecha: 09/06/2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI), adoptado por la secretaria TIC. Esto incluirá la verificación del proceso de respaldo tanto en servidores locales como en la nube, ajustándose a las necesidades particulares de cada dependencia.

Criterios de la Auditoria:

Facultades de Auditar otorgadas a la OCIG: artículo 269 de la Constitución Política de Colombia;

- Ley 87 de 1993 – Por la cual se establecen normas para el ejercicio de control interno en las entidades y organismos del estado.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1273 de 2009 – De la Protección de la Información y de los datos,
- P – TIC – 01 - Copias de Seguridad y Recuperación de Información
- PL - TIC- 01 - Plan de seguridad y privacidad de la información
- PL – TIC – 02 Plan gestión riesgos seguridad, privada de la información y seguridad digital
- POL - TIC – 01 – Tratamiento datos personales
- POL – TIC – 02 – Políticas de seguridad DE LA INFORMACION
- O – TIC – 02 – Gestión Incidentes Seguridad Información
- Modelo de seguridad y privacidad de Información.
- La norma ISO/IEC 27001.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 2 de 15

- Guía de Auditoría de la Función Pública Versión 4 de julio de 2020. Basada en riesgos.
- Constitución Política de Colombia.

DESARROLLO DE LA AUDITORIA

El equipo auditor de la Oficina de Control Interno de Gestión llevó a cabo la presente auditoría al proceso de Gestión TIC, en cumplimiento con el Plan de Auditoría correspondiente a la vigencia 2024. En este informe se ha analizado el proceso P-TIC-01 denominado "Copia de Seguridad y Recuperación de la Información", de acuerdo con su versión 02, con fecha del 09 de junio de 2022.


La auditoría se centró en evaluar el proceso implementado por la Secretaría TIC, específicamente en los controles establecidos para la protección de la información. Asimismo, se verificaron los procedimientos definidos para las copias de seguridad y la recuperación de la información, con el fin de alcanzar el objetivo de la auditoría

1. Verificar que se estén realizando copias de seguridad conforme a los procedimientos establecidos en la Administración departamental y las normativas vigentes.
2. Asegurar que las copias de seguridad se realicen de manera oportuna, cubriendo todos los datos críticos e importantes para las operaciones de las dependencias, y que se mantenga la frecuencia indicada en los procedimientos.
3. Comprobar que las copias de seguridad estén protegidas mediante métodos adecuados de seguridad, como cifrado y almacenamiento seguro, para prevenir el acceso no autorizado y asegurar la integridad de la información.
4. Asegurar que exista un procedimiento claro y funcional para la recuperación de información en caso de pérdida o contingencia, y que los sistemas puedan restaurar datos de manera efectiva dentro de los tiempos establecidos.
5. Evaluar que las actividades de copias de seguridad y recuperación de la información se realicen en cumplimiento de las normativas vigentes relacionadas con la protección de datos y seguridad de la información.
6. Garantizar que el personal encargado de la gestión de copias de seguridad y recuperación de información reciba la formación necesaria para ejecutar correctamente los procedimientos, y que todas las dependencias estén conscientes de su rol en el proceso.

1. VERIFICAR QUE SE ESTÉN REALIZANDO COPIAS DE SEGURIDAD CONFORME A LOS PROCEDIMIENTOS ESTABLECIDOS EN LA ADMINISTRACIÓN DEPARTAMENTAL Y LAS NORMATIVAS VIGENTES.

En mesa de trabajo realizada con el personal encargado del proceso de copias de seguridad, se informó sobre los aplicativos que se respaldan. Los aplicativos y sus respectivas copias de seguridad son los siguientes:

- **PCT y Humano:** Se realiza una copia de seguridad dos (2) veces al día, compartiendo una misma base de datos.
- **SGDA (ControlDoc):** La copia de seguridad se realiza dos (2) veces al día.
- **SISCAR:** Esta copia de seguridad es gestionada por la empresa **Datasoft**, que se encarga de realizarla. Una vez realizada la copia, Datasoft informa a la Secretaría TIC, para que guarde las copias en el lugar correspondiente.
- **Sevenet:** Este aplicativo, destinado a realizar consultas y registrar procesos del fondo de pensiones, tiene una copia de seguridad una vez al día. Se aclara que este aplicativo desde el 11 de septiembre de 2023, dejó de realizar procesos de

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 3 de 15

PQRSD y se tiene para realizar consultas y paso a realizar una parte del proceso del fondo de pensiones (Secretaría Administrativa).

Además, se informó que la **intranet** ya no es respaldada por la entidad, ya que, mediante el contrato con la empresa **Seven**, se acordó que la intranet se vinculó con el aplicativo ventanilla virtual. En consecuencia, **Seven** es la empresa encargada de realizar las copias de seguridad de la intranet. El personal de TIC indicó que, desde que Seven asumió este proceso, no realizan copias de seguridad relacionadas con la intranet.

Por lo anterior el equipo auditor procede a realizar la revisión del procedimiento copias de seguridad y recuperación de información, encontrando que;

P – TIC – 01 - Copias de Seguridad y Recuperación de Información

Objetivo: Este procedimiento tiene por objeto garantizar la salvaguarda y restauración de la información de las diferentes bases de datos archivados en medios magnéticos de los servidores de la entidad.

Controles


- a. Los medios de almacenamiento de las copias de seguridad estarán ubicados en sitios seguros para impedir el acceso a la información a personal no autorizado.
- b. 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.
- c. 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.
- d. 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.
- e. La secretaria 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.

Observaciones:

- ✓ Para el análisis al control del punto (a), el equipo auditor realiza visita al Datacenter ubicado en la Entidad Territorial Gobernación de Quindío y centros de comunicaciones ubicados en el Centro de convenciones evidenciando lo siguiente;

Se ha observado que el Datacenter de la Entidad presenta deficiencias en su seguridad perimetral, lo que compromete la protección de los equipos utilizados para las copias de seguridad y la recuperación de la información. A pesar de contar con un espacio designado para el almacenamiento de estos equipos, se evidencian falencias en la implementación de medidas de seguridad física esenciales, tales como cerraduras, alarmas y controles de acceso físico adecuados.

Es fundamental reforzar estas medidas de seguridad física para garantizar la protección de los equipos y la información almacenada, evitando accesos no autorizados y mitigando los riesgos que puedan comprometer la integridad, disponibilidad y confidencialidad de los datos.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 4 de 15

Conforme a lo establecido en la resolución N° 000448 del 14 de febrero de 2022, en los artículos 6 (Política de Gestión de Activos), 7 (Política de Control de Acceso) y 10 (Política de Seguridad Física y del Entorno), así como en la norma ISO 27001 A.11 (Seguridad Física del Entorno), se recomienda implementar controles físicos adecuados en el Datacenter para asegurar la continuidad y protección de los activos de información, alineándose a los estándares de seguridad establecidos.

- ✓ Así mismo, en visita realizada el 13 de noviembre al sitio externo designado para el resguardo de las copias de seguridad de los equipos (Centro de convenciones), se identificaron las siguientes falencias que afectan el cumplimiento de los controles establecidos por la norma ISO 27001 y la Resolución N°. 000448 del 14 de febrero de 2022, citadas anteriormente.

Seguridad de ingreso - Norma ISO 27001 - 11.1.1 Perímetro de seguridad

- Los cuartos de comunicaciones carecen de medidas adecuadas de control de acceso, permitiendo que cualquier persona pueda ingresar sin restricciones, lo que representa una vulnerabilidad significativa.

Condiciones ambientales – Norma ISO 27001 - 11.1.4 Protección contra amenazas externas y del ambiente. y 11.2.1 Ubicación y protección del equipamiento.

- Se observó una acumulación excesiva de polvo en las UPS, racks y otros equipos, lo que puede afectar su funcionamiento.
- No se dispone de sistemas de refrigeración adecuados (como aires acondicionados), lo que compromete las condiciones óptimas para el funcionamiento de los equipos.

Equipos fuera de servicio - Norma ISO 27001 -: 11.2.1 Ubicación y protección del equipamiento

- Existen equipos en desuso que no han sido dados de baja formalmente, ocupando espacio y representando posibles riesgos operativos.


Gestión del cableado- Norma ISO 27001 - 11.2.3 Seguridad en el cableado.

- Se evidencia un desorden significativo en el cableado, el cual carece de etiquetas y de una estructura adecuada, dificultando la gestión y aumentando los riesgos de interrupción

Áreas de trabajo no seguras – Norma ISO 27001 - 11.1.5 Trabajo en áreas seguras.

- Las condiciones observadas en las áreas no cumplen con los estándares mínimos de seguridad y orden requeridos para garantizar un entorno de trabajo seguro.


Imagen 1 -Sitio donde se tiene ubicada la NAS y demás equipos para copias de seguridad y recuperación de información

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04
		Fecha: 01/12/2017
		Página 5 de 15



Fuente: visita realizada OCIG a los Centros de Datos ubicados fuera de la Entidad Gobernación del Quindío

- ✓ Para el control (b) *Las copias de seguridad de los aplicativos Sevenet, PCT, Siscar, Siscar Web, Estampilla Pro-hospital y pagina web e intranet.*
El equipo auditor ha identificado diferencias entre lo establecido en el Proceso P-TIC-01 Copia de Seguridad y Recuperación de la Información y lo descrito en el Mapa de Riesgos de Gestión – MR-TIC-01 versión 05, específicamente en el Riesgo 3. Durante la revisión, se evidencio lo siguiente;
 - El equipo auditor evidencia que no se tiene actualizado el procedimiento, en cuanto al registro de los aplicativos con que cuenta la Entidad. Es decir, no se tiene incluido en el procedimiento el aplicativo SGDA, y el retiro de Siscar web, Estampilla pro- hospital y pagina web e intranet.
- ✓ Respecto a los controles (c) y (d) establecidos en el proceso de Copias de Seguridad y Recuperación de Información, se han identificado las siguientes observaciones:
 - **El control (c):** Establece que los servidores públicos deben efectuar las copias de seguridad bajo la supervisión del personal de la Secretaría TIC. Sin embargo, no se ha encontrado evidencia que respalde la ejecución y supervisión de esta actividad. Se aclara que la Secretaría TIC tiene el sistema "Mesas de Ayuda", el cual permite informar a la Secretaría sobre cualquier falla o inconsistencia en los equipos de la Entidad. A través de este proceso, la Secretaría TIC procede a realizar las solicitudes por funcionarios y/o contratistas de la entidad. No obstante, no se dispone de registros documentales que validen que las copias de seguridad estén siendo efectivamente supervisadas como parte de este proceso, lo que genera incertidumbre sobre el cumplimiento de este control.
 - **Control (d):** No se ha encontrado evidencia de las pruebas de restauración de los backups realizadas con la periodicidad establecida en el plan de copias de

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 6 de 15

seguridad. Esta falta de evidencia pone en riesgo la confiabilidad del proceso de recuperación de la información en caso de ser necesario.

Adicionalmente, no se ha encontrado el **"Plan de Copias de Seguridad"** en la intranet, actualmente Ventanilla Virtual, ni en el micrositio de la Secretaría TIC. En su lugar, se observa el proceso "P-TIC-01 Copias de Seguridad y Recuperación de Información", el cual no establece de manera explícita la actividad de restauración de backups ni el plan asociado a las copias de seguridad.

2. ASEGURAR QUE LAS COPIAS DE SEGURIDAD SE REALICEN DE MANERA OPORTUNA, CUBRIENDO TODOS LOS DATOS CRÍTICOS E IMPORTANTES PARA LAS OPERACIONES DE LAS DEPENDENCIAS, Y QUE SE MANTENGA LA FRECUENCIA INDICADA EN LOS PROCEDIMIENTOS

POL - TIC- 02 - Política de seguridad de la Información

Políticas de creación y restauración de copias de seguridad

La gobernación del Quindío a través de la Secretaría 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 diarias, la frecuencia de estas copias fue establecida 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 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

Política de medios de Almacenamiento externo

Política: Los funcionarios públicos que contengan información confidencial de propiedad de la entidad en medios de almacenamiento externo, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información. El medio de almacenamiento externo que conecte un funcionario en su equipo asignado es responsabilidad propia, por tal motivo la información que se encuentre allí y que por algún motivo sea modificada o borrada por accidente, no involucra ni compromete a la Secretaría TIC en ningún caso.

Controles


Todo medio de almacenamiento con copias de seguridad debe ser marcado de acuerdo a la información que almacena, detallando su contenido.

Toda copia de respaldo que se encuentre en medios de almacenamiento removible deberá ser guardada bien sea en caja bajo llave o en un lugar seguro, al cual solo tendrá acceso el responsable de esta.

Observaciones:

Secretaría TIC tiene establecidos los medios de almacenamiento para las bases de datos que se les realiza las copias de seguridad, no se mantiene un registro detallado sobre el contenido de dichos medios. Esto impide garantizar la fácil localización y correcta gestión de los respaldos, ya que no se cuenta con información clave como la descripción de los datos almacenados y otros detalles relevantes que permitan distinguir y verificar cada respaldo realizado.

En cuanto a los medios de almacenamiento removibles, como discos duros y cintas, no se tiene registro de si la Entidad cuenta con estos medios y si se almacenan de forma segura, como se establece en los controles de seguridad. La falta de esta

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04
		Fecha: 01/12/2017
		Página 7 de 15

información compromete la trazabilidad y protección adecuada de los respaldos realizados.

Además, a la fecha de la presente auditoría, se ha observado que no se están llevando a cabo copias de seguridad mediante discos duros externos, a pesar de que este procedimiento estaba estipulado en los lineamientos establecidos. La discontinuación de este proceso representa una brecha en la flexibilidad y redundancia del almacenamiento de las copias de seguridad, lo que limita la capacidad de recuperación ante posibles incidentes que afecten los medios de almacenamiento principales.

En base a lo establecido en la política anteriormente citada, se observa una falta de documentación adecuada en el proceso de copias de seguridad de la Gobernación del Quindío. En primer lugar, no se tiene claramente definida la periodicidad con la que deben realizarse las copias, ni la hora y fecha exacta de cada una de ellas. Además, no se especifica el tipo de copia de seguridad realizada (ya sea incremental, completa o diferencial), lo cual es esencial para una adecuada gestión de la información. A esto se suma la ausencia de una bitácora donde se registre si el proceso de restablecimiento de las copias de seguridad fue exitoso, las observaciones relevantes o las firmas correspondientes del supervisor o técnico de soporte.

En cuanto al Plan Estratégico de Tecnología de la Información (PETI) código: PL-TIC-01, versión: 02 fecha: 28/01/2022 detalla que la infraestructura tecnológica actualmente en la Gobernación del Quindío cuenta con 11 servidores físicos, de los cuales se evidencia lo siguiente: el 64% de los servidores soportan IPv6 de lo anterior presentan varios desafíos, particularmente en lo que respecta a los servidores físicos, “la infraestructura referente a los servidores físicos que posee la Gobernación del Quindío corre el riesgo de obsolescencia tecnológica, además de que no cuentan con servidores de respaldo, ocasionando retrasos en los servicios (tiempo que dure en montar la copia de seguridad). Caso contrario con servidores que se encuentran en la nube ya que al estar tercerizados este servicio el proveedor es responsable de la continuidad del servicio”.


Con base en lo anterior se constata las falencias que presenta y el riesgo en la infraestructura tecnológica de la Gobernación del Quindío, a medida que la tecnología avanza rápidamente, los servidores físicos se vuelven más difíciles de mantener, menos eficientes y vulnerables a fallos. Esto puede generar problemas de rendimiento, tiempo de inactividad y altos costos de mantenimiento. Además, la falta de actualización constante puede llevar a incompatibilidades con nuevos estándares y protocolos, lo que afectaría directamente la capacidad de la Entidad para adaptarse a las nuevas demandas tecnológicas.

3. COMPROBAR QUE LAS COPIAS DE SEGURIDAD ESTÉN PROTEGIDAS MEDIANTE MÉTODOS ADECUADOS DE SEGURIDAD, COMO CIFRADO Y ALMACENAMIENTO SEGURO, PARA PREVENIR EL ACCESO NO AUTORIZADO Y ASEGURAR LA INTEGRIDAD DE LA INFORMACIÓN.

La Secretaría TIC ha implementado un método binario para realizar las copias de seguridad de los datos. Este enfoque, aunque funcional, presenta varias desventajas que deben ser evaluadas y mitigadas para asegurar la integridad y la seguridad de la información.

Uno de los principales

Uno de los principales inconvenientes del método binario es que las copias de seguridad se realizan de manera íntegra, es decir, se copian todos los archivos tal como están, sin ningún tipo de filtrado. Esto genera un tamaño considerable de

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04
		Fecha: 01/12/2017
		Página 8 de 15

archivo, lo que aumenta significativamente el espacio de almacenamiento requerido. En muchos casos, los recursos de almacenamiento pueden ser insuficientes, lo que obliga a adquirir más capacidad de almacenamiento o a gestionar de manera menos eficiente los backups. Este factor también puede afectar los tiempos de transferencia de los datos, haciendo que las copias de seguridad tarden más en completarse.

Otro riesgo importante asociado con el método binario es que las copias de seguridad se realizan sin ningún tipo de cifrado. Como resultado, los datos quedan expuestos a cualquier persona que tenga acceso al medio de almacenamiento (ya sea en la nube o en almacenamiento local). Esta falta de protección pone en riesgo la confidencialidad y la integridad de la información, especialmente en un contexto donde se manejan datos sensibles o confidenciales. Sin un cifrado adecuado, los datos pueden ser vulnerables a accesos no autorizados, lo que podría generar brechas de seguridad, pérdida de información o incluso la exposición de datos críticos.

PL – TIC – 02 – Plan gestión riesgos seguridad, privada de la información y seguridad digital

IDENTIFICACION Y ANALISIS DE RIESGOS

Definición: La matriz de riesgos es una confrontación analítica de los posibles riesgos a los que se encuentra sometida el área tecnológica, este análisis nos permitirá evaluar la probabilidad de ocurrencia de los distintos riesgos para diseñar los controles preventivos y correctivos, los que se considera más críticos y causan más impacto para la gobernación del Quindío. En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, el Impacto y probabilidades de los riesgos, finalmente las alternativas de corrección de la anomalía

Mitigación del riesgo


Consiste en el establecimiento, desarrollo de estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas.

Virus informáticos Contra los virus informáticos, la gobernación del Quindío, cuenta con antivirus en todos los equipos de cómputo de la misma, que protegen los equipos en tiempo real. Además de lo anterior, cabe destacar que, a través del año, se está ejecutando

Observación

La Secretaría TIC ha informado que actualmente se encuentra en proceso de adquisición de un nuevo sistema que cumpla con los requisitos necesarios para salvaguardar la integridad de la información en la Entidad. Sin embargo, durante la auditoría realizada, se evidenció una situación relacionada con la continuidad en la protección de los sistemas de la entidad.

En la plataforma Siaobserva, se observó que, en el periodo comprendido entre el 10 de octubre y el 25 de noviembre de 2023, la entidad contaba con el contrato de compraventa No. 021 de 2023, para la “Renovación de Licencia y Soporte Técnico de Antivirus ESET Protect Entry (On-Prem), para Equipos de Cómputo y Servidores propiedad de la Entidad Territorial Gobernación del Quindío”. No obstante, la Secretaría TIC remitió a esta oficina un documento de aceptación de la oferta al contrato de compraventa No. 022 de 2024, titulado “Adquisición de Licencias y Soporte Técnico de Software Antivirus EDR, para Estaciones de Trabajo y Servidores propios de la Gobernación del Quindío”.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 9 de 15

Al verificar en la plataforma Siaobserva, el equipo auditor no encontró evidencia del contrato de compraventa No. 022 de 2024, lo que genera una preocupación en relación con la cobertura continua en la protección de los equipos y servidores de la entidad. Como consecuencia, esta oficina informa que, durante el periodo comprendido entre la finalización del contrato de compraventa No. 021 de 2023 y la fecha de inicio con el proceso del contrato de compraventa N. 022 de 2024, la entidad no cuenta con una licencia de antivirus instalada en los servidores ni en los equipos de cómputo, lo que compromete la seguridad de la información y los sistemas tecnológicos

Esta situación pone en evidencia una brecha significativa en la implementación de controles de seguridad adecuados, lo que contraviene lo estipulado en el Modelo de Seguridad y Privacidad de la Información de la entidad, así como en la norma ISO 27001, específicamente en el Objetivo A.12, Seguridad de las Operaciones, y más específicamente el control 12.2.1 sobre el manejo de software malicioso.

La falta de un antivirus adecuado compromete la protección de los activos informáticos de la Entidad ante posibles infecciones por virus, malware u otros tipos de software malicioso, lo que puede afectar la **confidencialidad, integridad y disponibilidad** de la información crítica para la operación de la Gobernación del Quindío. Esta vulnerabilidad expone a la entidad a riesgos significativos de ciberataques y brechas de seguridad que podrían poner en peligro la continuidad de sus operaciones y el cumplimiento de normativas de seguridad.

Es crucial que se dé prioridad a la implementación de medidas de protección efectivas, como la adquisición e instalación urgente de un **antivirus adecuado** que cumpla con los estándares de seguridad necesarios, garantizando que los sistemas informáticos estén protegidos ante amenazas externas y se alineen con las normativas y buenas prácticas en ciberseguridad establecidas por el Modelo de Seguridad y la ISO 27001.

4. ASEGURAR QUE EXISTA UN PROCEDIMIENTO CLARO Y FUNCIONAL PARA LA RECUPERACIÓN DE INFORMACIÓN EN CASO DE PÉRDIDA O CONTINGENCIA, Y QUE LOS SISTEMAS PUEDAN RESTAURAR DATOS DE MANERA EFECTIVA DENTRO DE LOS TIEMPOS ESTABLECIDOS.


O – TIC – 02 – Gestión Incidentes Seguridad Información

OBJETIVO GENERAL Tener un enfoque claro y preciso de la gestión de incidentes de seguridad y privacidad de la información, que ayude a gestionar dichos incidentes de forma rápida y oportuna, con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la gobernación del Quindío.

ROLES Y RESPONSABILIDADES EN LA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Como parte de la gestión de incidentes de seguridad de la información y teniendo en cuenta que de acuerdo al **modelo de seguridad y privacidad de la información MSPI, que adoptó la entidad, ya existen roles y responsabilidades de seguridad de la información, se decide adoptar dentro del mismo equipo, el grupo de Respuesta a Incidencias de Seguridad Informática CSIRT (Computer Security Incident Response Team)**, enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica de la entidad la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 10 de 15

Con base a la Guía No 21, de Gestión de incidentes de seguridad de la información se adoptan las siguientes etapas dentro del plan propuesto por la gobernación del Quindío.

Observación:

La secretaría TIC evidencia el proceso de gestión de incidentes de seguridad, se comprobó que este proceso no se está implementando de manera adecuada. En particular, no se ha documentado ni monitoreado adecuadamente la gestión de incidentes de seguridad relacionados con las copias de seguridad, como los errores en los archivos generados (logs). La falta de registros formales y procedimientos claros para abordar, gestionar y resolver estos incidentes, así como la ausencia de análisis o evaluaciones posteriores, limita la capacidad de la Entidad para mejorar continuamente sus controles de seguridad.

Este incumplimiento de los procedimientos establecidos refleja una brecha crítica en el cumplimiento de los estándares de seguridad del Modelo de Seguridad y Privacidad de la Información, particularmente en lo relacionado con el control A.12 "Seguridad de las operaciones". La carencia de un proceso formal y la falta de una evaluación de incidentes expone a la Entidad a riesgos importantes, ya que no se está gestionando adecuadamente la seguridad de la información. Esto podría poner en peligro la confidencialidad, integridad y disponibilidad de los datos, así como la continuidad de las operaciones de la Entidad, ante posibles incidentes de seguridad no gestionados o no detectados a tiempo.

5. EVALUAR QUE LAS ACTIVIDADES DE COPIAS DE SEGURIDAD Y RECUPERACIÓN DE LA INFORMACIÓN SE REALICEN EN CUMPLIMIENTO DE LAS NORMATIVAS VIGENTES RELACIONADAS CON LA PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN.

PL - TIC- 01 - Plan de seguridad y privacidad de la información


Objetivo General

Establecer el Plan de Seguridad y Privacidad de la Información, el cual está dirigido a la implementación del modelo de seguridad y privacidad de la información MSPI y a todas las etapas que lo componen. Lo anterior en atención al contexto organizacional de la entidad, las capacidades técnicas y recursos disponibles.

Objetivos específicos

- Comunicar e implementar la estrategia de seguridad de la información.
- Identificar infraestructuras críticas en las entidades a través de la implementación de mejores prácticas de seguridad de la información.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

Observación

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 11 de 15

Para el análisis del PL-TIC-01 el equipo auditor toma de referencia la evaluación desarrolla por la secretaría TIC PETI evidenciado que; Ver imagen N.º 1 Evaluación MSPI

Evaluación de MSPI

Tabla 15 Evaluación de efectividad de controles

No.	Evaluación de Efectividad de controles			Evaluación de efectividad de control
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	Políticas De Seguridad De La Información	100	100	OPTIMIZADO
A.6	Organización De La Seguridad De La Información	81	100	OPTIMIZADO
A.7	Seguridad De Los Recursos Humanos	84	100	OPTIMIZADO
A.8	Gestión De Activos	77	100	GESTIONADO
A.9	Control De Acceso	77	100	GESTIONADO
A.10	Criptografía	40	100	REPETIBLE
A.11	Seguridad Física Y Del Entorno	66	100	GESTIONADO
A.12	Seguridad De Las Operaciones	71	100	GESTIONADO
A.13	Seguridad De Las Comunicaciones	53	100	EFFECTIVO
A.14	Adquisición, Desarrollo Y Mantenimiento De Sistemas	43	100	EFFECTIVO

Fuente: reporte secretaria TIC evaluación MSPI

En relación a la imagen N° 1, se evidencia que la secretaría TIC, conforme a la evaluación realizada al MSPI para la vigencia 2023, obtiene un puntaje del 68 esto sugiere que el nivel de madurez de las prácticas de seguridad de la información en la organización es relativamente **intermedio** o **en desarrollo**, pero aún no ha alcanzado un nivel alto de madurez. Por lo tanto, un **68** sugiere que la organización ha avanzado en la implementación de medidas de seguridad, pero aún tiene áreas de mejora para optimizar sus prácticas y alcanzar un nivel más alto de madurez. Esto podría incluir la formalización de procesos, la mejora de la capacitación o la actualización de tecnologías y procedimientos de seguridad.

6. GARANTIZAR QUE EL PERSONAL ENCARGADO DE LA GESTIÓN DE COPIAS DE SEGURIDAD Y RECUPERACIÓN DE INFORMACIÓN RECIBA LA FORMACIÓN NECESARIA PARA EJECUTAR CORRECTAMENTE LOS PROCEDIMIENTOS, Y QUE TODAS LAS DEPENDENCIAS ESTÉN CONSCIENTES DE SU ROL EN EL PROCESO.


Matriz Mapa de Riesgos de Gestión- MR- TIC-01 versión 05 Riesgo No. 3

Descripción del Riesgo: Posibilidad de afectación económica y reputacional asociado a la falta de copias de seguridad permanente a los sistemas de información y equipos de cómputo que se encuentran en la gobernación del Quindío, debido a la baja capacitación en el manejo y realización de copias de seguridad a los diferentes funcionarios de la Secretaría TIC.

Plan de acción: Realizar capacitaciones para el aprendizaje en copias de seguridad diarias de la base de datos en custodia de la Secretaría TIC, a través de discos duros externos. (PCT, Humano, Sevenet, SISCAR). Realizar la bitácora diariamente.

Seguimiento:

- Nro de capacitaciones realizadas / Nro de capacitaciones programadas
- Nro de copias de seguridad realizadas/ No de copias de seguridad programadas
- Nro de bitácoras realizadas / Nro de bitácoras programadas

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 12 de 15

Observaciones:

Para el seguimiento realizado al Mapa de Riesgos de Gestión correspondiente al primer semestre de 2024, la Secretaría TIC ha presentado únicamente la evidencia del total de las copias de seguridad realizadas. Sin embargo, no se ha proporcionado información o documentación relacionada con los otros dos controles establecidos para mitigar el riesgo en cuestión. Se aclara que esta acción tiene un plazo establecido hasta el 31 de diciembre de 2023, cuando esta oficina realice el seguimiento al segundo semestre de 2024.

Por otro lado, aunque la Secretaría cuenta con un proceso de capacitación constante para el personal de TI, no se ha presentado evidencia que respalde la realización de capacitaciones a los funcionarios en relación con el manejo y la realización de copias de seguridad, tal como se establece en el plan de gestión de riesgos de seguridad, privacidad de la información y seguridad digital (PL-TIC-02). La falta de formación formal en este ámbito puede poner en riesgo la correcta ejecución de los procesos de copia de seguridad, afectando la protección de los datos y la continuidad de los servicios en caso de incidentes.

HALLAZGOS ADMINISTRATIVOS

HALLAZGO N. 1 Falencias en la Implementación de Copias de Seguridad y Seguridad Física de los Equipos.

Condición

Se ha identificado una serie de deficiencias tanto en los controles de seguridad física como en el proceso de copias de seguridad de la Entidad. En cuanto a la seguridad física, se observó que el Datacenter (medidas adecuadas de control acceso) y el sitio externo de almacenamiento de equipos presentan vulnerabilidades significativas, como la falta de medidas adecuadas de control de acceso y protección ambiental (falta de refrigeración y acumulación de polvo). Respecto al proceso de copias de seguridad, se encontró que el registro de inventario de bases de datos está desactualizado, no se cuenta con evidencia de capacitación del personal ni se realizan las copias de seguridad según lo establecido en los procedimientos, como el uso de discos duros externos. Además, no se documentan las pruebas de restauración ni se lleva un formato estandarizado para registrar la ejecución de las copias

Criterio:


- La Norma ISO 27001 – A11 (Seguridad Física y del Entorno),
- 11.1.1 sobre Perímetros de Seguridad Física
- A.12 de Seguridad de las Operaciones
- Plan Estratégico de Tecnología de la Información – PETI -PL-TIC-01
- Modelo de seguridad y privacidad de la información.

Causa

- La falta de un plan de seguridad física adecuado, junto con una ausencia de procedimientos documentados claros y la desactualización de los registros de copias de seguridad.
- carencia de recursos y enfoque en la capacitación del personal y en la implementación efectiva de medidas de seguridad.

Efecto

- Deficiencias en la seguridad física
- Pérdida de datos
- La falta de un proceso de copias de seguridad documentado.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 13 de 15

- Deficiencias en realización de pruebas de restauración y recuperación de información en caso de un incidente.
- Fallos operativos.
- Desactualización de los inventarios.

Hallazgo N. 2: Brecha en la Continuidad de Protección Antivirus en la Gobernación del Quindío

Condición:

Durante el período comprendido entre el 10 de octubre y el 25 de noviembre de 2023, la Gobernación del Quindío contó con el contrato de compraventa No. 021 de 2023 para la renovación de la licencia y soporte técnico del antivirus ESET Protect Entry. Sin embargo, tras la finalización de este contrato y hasta la fecha de inicio del contrato de compraventa No. 022 de 2024, no se evidenció la existencia de licencias antivirus vigentes instaladas en los servidores y equipos de la Entidad, dejando los sistemas tecnológicos expuestos.

Criterio:

- El Modelo de Seguridad y Privacidad de la Información.
- Norma ISO 27001, Objetivo A.12 (Seguridad de las Operaciones) y el control 12.2.1 (Protección contra software malicioso).

Causa:

- Falta de planeación y gestión oportuna en la transición entre el contrato de compraventa No. 021 de 2023 y el contrato No. 022 de 2024.

Efecto:

- Debilidad en la planificación para garantizar la continuidad de las medidas de seguridad tecnológica, así como en el monitoreo del cumplimiento de los procesos contractuales
- Riesgos significativos de ciberataques, interrupciones operativas y posibles sanciones por incumplimiento de normativas de seguridad.

Hallazgo N. 3: Incumplimiento en la Gestión de Incidentes de Seguridad de la Información

Condición


La entidad ha informado que cuenta con un proceso de gestión de incidentes de seguridad. Sin embargo, el equipo auditor ha evidenciado que los roles y responsabilidades establecidos en dicho proceso no se cumplen adecuadamente. Además, aunque se menciona que se ha adoptado un modelo de seguridad y privacidad de la información, se ha constatado que dicho modelo no ha sido formalmente implementado ni documentado. En particular, no se ha documentado ni gestionado ningún incidente de seguridad de la información, y no existe evidencia de análisis o evaluación de los incidentes ocurridos.

Criterio

- Resolución número 00500 de marzo 10 de 2021
- Modelo de Seguridad y Privacidad de la Información.
- Norma ISO 27001.

Causa

- Falta de implementación formal

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 14 de 15

- Falta de documentación adecuada del proceso de gestión de incidentes de seguridad.
- Falta de registros y análisis de los incidentes ocurridos.

Efecto:

- La falta de un proceso formal y documentado para la gestión de incidentes de seguridad de la información
- Deficiencia a respuesta oportuna y eficaz ante incidentes de seguridad.
- Limitada capacidad de identificar y mitigar vulnerabilidades.
- Ausencia de registros y análisis de incidentes.

RECOMENDACIONES

De conformidad al presente informe final de auditoría se recomienda a la secretaría de Tecnología de la Información y comunicaciones - TIC, que adopten el plan de Mejoramiento conforme a los documentos adoptados para ello, el cual debe contener las acciones preventivas y correctivas que ataquen la causa de los Hallazgos administrativos estructurados por la oficina de control interno de gestión, en un plazo de quince (15) días hábiles siguientes a la fecha de recibido el informe final de auditoría, salvo que involucre a otros procesos o dependencias, caso en el cual el término será de veinte (20) días hábiles para su formulación y remisión a la oficina de control interno de gestión.

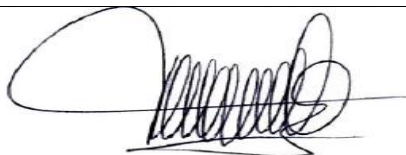
CONCLUSIONES

El informe de auditoría ha identificado una serie de deficiencias críticas en la gestión de la seguridad física y el proceso de copias de seguridad en la Entidad. En cuanto a la seguridad física, se detectaron vulnerabilidades en el Datacenter y en el sitio externo de almacenamiento de equipos, debido a la falta de controles adecuados de acceso y protección ambiental. En el proceso de copias de seguridad, se observó que el registro de inventario de bases de datos está desactualizado, y no se siguen los procedimientos establecidos para la ejecución de las copias de seguridad ni para la prueba de restauración, lo que pone en riesgo la integridad y disponibilidad de la información.

Se evidenció que durante el período entre la finalización del contrato de soporte antivirus (ESET) y el inicio de uno nuevo, los sistemas quedaron sin protección antivirus adecuada, lo que expone a la Entidad a posibles vulnerabilidades de seguridad. En relación con la gestión de incidentes de seguridad, a pesar de existir un proceso formal, no se están cumpliendo adecuadamente los roles y responsabilidades establecidos, y no se ha documentado ni gestionado ningún incidente relevante, lo que refleja un incumplimiento de los procedimientos en materia de seguridad de la información.


Por último, el Mapa de Riesgos de Gestión, aunque se presentó evidencia de copias de seguridad realizadas, no se proporcionó documentación suficiente sobre otros controles necesarios para mitigar riesgos relacionados. Finalmente, la falta de formación continua sobre el manejo de copias de seguridad para el personal de TI, como se establece en el plan de gestión de riesgos, representa una debilidad significativa en la implementación de buenas prácticas de seguridad de la información.

FIRMA:



JOSE DUVAN LIZARAZO CUBILLOS
Jefe de Oficina de Control Interno De Gestion

--	--	--

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 15 de 15

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