	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017 Página 1 de 11

PROCESO O ÁREA AUDITADA: Secretaría de Hacienda – Tesorería	FECHA DE ELABORACIÓN: 09 de enero de 2025
---	---

DIRECTIVO RESPONSABLE: Dr. José Duván Lizarazo Cubillos	DESTINATARIO: Secretaría de Hacienda – Tesorería Secretaría TIC
---	--

ASPECTOS GENERALES DEL PROCESO DE AUDITORÍA

OBJETIVO:

Construcción de informe final de la Auditoría No. 08 al seguimiento y verificación de la aplicación del Protocolo de Seguridad establecido por la Secretaría de Hacienda – Tesorería, Dirección TIC y las Entidades Financieras autorizadas por el Departamento, en uso de Plataformas y medios electrónicos para pagos y movimientos bancarios e interbancarios.

ALCANCE:

La auditoría se realizará del 23 de octubre al 13 de noviembre de 2024, en las instalaciones de la Tesorería del Departamento del Quindío y se enfocará en los controles implementados en el Protocolo de seguridad.

METODOLOGÍA:

Conforme a la Guía de Auditoría Basada en Riesgos, indica requerir de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada:

- Paso 1. Política de Administración del Riesgo
- Paso 2. Identificación del riesgo y
- Paso 3. Valoración del Riesgo

Una vez establecidos los riesgos; se procederá en la recolección de evidencias que permitan verificar el cumplimiento del protocolo de seguridad adoptado por la tesorería Departamental para crear condiciones de seguridad de los recursos y las transacciones del departamento, minimizando los riesgos de fraude y evitando que se materialicen.


Criterios de la Auditoría:

- Artículo 269 de la constitución Política de Colombia.
- Ley 87/1993 – Decreto 1537/2001.
- Decreto 1078 de 2015.
- Decreto 648 de 2017.
- Guía N. 3 Procedimientos de seguridad de la Información.
- Guía N. 12 Seguridad en la Nube.
- Matriz de riesgos Institucional – MR-TIC-08-V11 Fecha: 08-agosto-2024.
- Matriz de riesgos Seguridad Digital

DESARROLLO DE LA AUDITORIA

El equipo auditor de la oficina de Control Interno de Gestión consultó los procesos y procedimientos establecidos por las Secretarías de Hacienda y TIC publicados en la ventanilla virtual y la existencia del documento de Protocolo de seguridad establecido por la Secretaría –Hacienda – Tesorería, Dirección TIC y las Entidades Financieras autorizadas, en uso de Plataformas y medios electrónicos para pagos y movimientos bancarios e interbancarios. para la respectivo revisión y análisis y con el fin de alcanzar el objetivo de la auditoría

1. Revisión del Protocolo de Seguridad establecido por la Secretaría de Hacienda – Tesorería, Dirección TIC
2. Revisión y análisis de los usuarios autorizados
3. Verificación de las actualizaciones de los antivirus
4. Verificación de las certificaciones expedidas por el Banco de Occidente, Tesorería y las TIC.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 2 de 11

5. Verificación del cumplimiento de los protocolos de seguridad (Cámaras de Seguridad, Cajas fuertes, claves, mantenimiento a los equipos y a la red.
6. Verificación de la custodia de títulos valores, (Estampillas, cheques, mandamientos de pago)
7. Revisión custodia y manejo de Token
8. Verificación de la realización de los Backup
9. Revisar la identificación de la gestión del riesgo, operatividad de los controles y el mejoramiento continuo.

1. Revisión del Protocolo de Seguridad establecido por la Secretaría de Hacienda - Tesorería, Dirección TIC.

En prueba de recorrido practicada en el periodo de ejecución de auditoría, con el Tesorero y el Director financiero, se pudo evidenciar que en la actualidad el Protocolo de Seguridad para las transacciones financieras en los portales electrónicos, se cuenta con las certificaciones que expide el Banco de Occidente, el tesorero y las TIC mensualmente.

En la descripción del Control en el MAPA DE RIESGOS DE GESTIÓN MR-HAC-01, el Tesorero General aplicará estrictamente el protocolo adoptado por el Departamento, basado en recomendaciones hechas por la Dirección TIC y las Entidades Financieras autorizadas por la Gobernación del Quindío, para los pagos y transferencias electrónicas a través de la banca virtual, de lo cual, quedará evidencia a través de un informe trimestral que enviará a la Secretaría de Hacienda.

OBSERVACIÓN:

Se evidencia que para ellos el Protocolo de Seguridad son las tres certificaciones, (banco, tesorería y las TIC), por lo que se desconoce el Protocolo documentado y adoptado por el Departamento, que incluya los parámetros, procedimientos y componentes generales de seguridad, los cuales, permitan minimizar la probabilidad de vulnerabilidad al fraude informático a través de los portales electrónicos de las entidades financieras y proteger la confidencialidad, autenticidad y/o integridad de los archivos que ordenan operaciones de tesorería. No obstante, en la certificación de Tesorería se refieren al Protocolo de seguridad informática 2021.

2. Revisión y análisis de los usuarios autorizados

La potestad y competencia para solicitar creación, modificación o inactivación de los usuarios y contraseñas del aplicativo PCT ENTERPRISE, es del Jefe encargado de cada área funcional, para el caso de Tesorería, es del señor Tesorero. Cuando así, lo requiere, remite a la Secretaría TIC, a través de correo electrónico, mesa de ayuda o aplicativo controldoc, la solicitud, indicando el nombre del funcionario o contratista, los módulos, permisos y vigencias que deben ser activados, modificados o inactivados.


Se cuentan con usuarios de Administrador, de Autorizados, y de preparadores registrados en el Portal del Banco, siendo el administrador quien realiza el reporte ante la entidad bancaria. El usuario de administrador es diferente al usuario de autorizador, por lo que se evidencia que se tiene un control dual para el proceso de transferencias electrónicas.

Son usuarios preparadores personal de planta y contratistas.

OBSERVACION:

En la prueba de recorrido realizada a la Secretaria de Hacienda — Tesorería- se evidenció que el personal que maneja transacciones bancarias y el registro de información, como usuarios de Autorización y preparadores, se encuentra a la vista las claves de acceso de dichos usuarios en los respectivos equipos de cómputo.

De conformidad con el Manual de Funciones y Competencias de la Administración Central del Departamento del Quindío, respecto a la responsabilidad de preparar los pagos electrónicos y convencionales por transferencias la tiene sólo el cargo Auxiliar Administrativo código 407 grado 04, cargo que está vacante. El profesional universitario código 219 grado 03 y el Técnico Operativo grado 314 código 01 quienes realizan esta responsabilidad no está incluida en las funciones esenciales.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 3 de 11

3. Verificación de las actualizaciones de los antivirus

Para el control que establece la secretaría TIC, en la infraestructura tecnológica, manifiesta que se está llevando a cabo un proceso contractual para la adquisición de un software antivirus tipo EDR en la nube, con esta actualización en la infraestructura de ciberseguridad, se busca incorporar capas adicionales de seguridad informática avanzadas basadas en inteligencia artificial, lo que permitirá mitigar los riesgos de seguridad cibernética. El sistema EDR (Endpoint Detection and Response) será clave para enfrentar los crecientes delitos cibernéticos, la expansión de redes y las nuevas formas de trabajo.

OBSERVACION:

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 período 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".

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 encuentra 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.

Dichos servidores son fundamentales para el funcionamiento de la Tesorería, debido a las transacciones y el manejo de información crítica que realiza la Entidad Territorial Gobernación del Quindío. Lo que representa un riesgo alto para la integridad, disponibilidad y confidencialidad de la información institucional. Esta situación vulnera los controles establecidos en las *Políticas de Seguridad de la Información* (POL-TIC-02, versión 04, de fecha 31/10/2022), el marco normativo de la Ley 1581 de 2012 sobre protección de datos personales y CONPES 3701 de 2011 Lineamientos de política para Ciberseguridad y Ciberdefensa.

4. Verificación de las certificaciones expedidas por el Banco de Occidente, Tesorería y las TIC. Certificación del Banco:

El Banco de Occidente expide una certificación mensual de Protocolo de seguridad, que consiste en realizar periódicamente evoluciones de seguridad sobre los sistemas y plataformas transaccionales que ha habilitado para el uso de sus clientes, con el propósito de verificar constantemente su estado y mitigar de manera oportuna las falencias que sean detectadas. El banco cuenta con un modelo basado en el estándar ISO 27001, que además de dar cumplimiento a la normatividad regulatoria nacional (Circular Básica Jurídica 029, Circular 007 emitidas por la Superintendencia Financiera de Colombia e internacional SOX) que permite contar con herramientas de seguridad perimetral para controlar el acceso seguro de la información, logrando que a ella solo accedan las personas que se encuentran debidamente autorizadas.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 4 de 11

El banco de Occidente realiza monitoreo de la costumbre transaccional del cliente y ha habilitado los siguientes controles que garantizan mayor seguridad en las transacciones que realizan los clientes empresariales y gubernamentales en este caso:

- Registro de direcciones IP, desde las cuales se efectúan las transacciones
- Definición de horarios para efectuar operaciones
- Uso de segundo factor de autenticación
- Posibilidad de establecer doble intervención para transacciones
- Uso de Ropport, herramienta sin costo para el cliente, que se debe estar instalada en el equipo desde el cual se realizan las operaciones que permite:
 - Prevenir ataques de día cero
 - Alertar al usuario de sitios Phishing
 - Evitar el robo de claves por Phishing
 - Evitar robo de información
 - Reportar el Malware financiero

Certificación de Tesorería:

“El Tesorero de la Secretaria de Hacienda del Departamento del Quindío hace constar mensualmente en relación con el Informe de aplicación de Protocolos de Seguridad informática para las transacciones financieras en los portales electrónicos lo siguiente:

Que el **Protocolo de seguridad informática 2021**, que tiene como objetivo establecer los lineamientos y procedimiento que permiten fortalecer y asegurar la gestión de la tesorería Departamental del Quindío, para las transacciones financieras en los portales electrónicos y un archivo en Excel llamado “lista de Chequeo

Dando estricto cumplimiento al protocolo, se procede a realizar una retroalimentación con los funcionarios adscritos a la tesorería General con el objetivo de que cada uno continúe con el estricto cumplimiento de los objetivos y los componentes generales de seguridad.

Se continúa diligenciando en compañía con la Secretaria de las TIC, la lista de chequeo mensualmente, en ejercicio se realiza un día al azar para cada periodo, teniendo estricto cuidado en el chequeo de la categoría física, software y navegadores web. En el presente periodo no se evidencia inconsistencia alguna en dicha categoría y por parte de la Secretaria TIC se informa que para la revisión física de los componentes de la red, se dispone de un (1) ingeniero que está revisando continuamente los elementos propios de la red de datos de la administración.

Consecuente al protocolo, se han realizado los trámites correspondientes ante la Secretaría de las TIC (mesa de ayuda), cuando se ha requerido cualquier tipo de soporte técnico, accesos de permisos (para el aplicativo PCT Enterprise módulo de egresos, ingresos y SISCAR), para los nuevos usuarios e igualmente para el retiro, actualizando la información del directivo activo de la entidad por parte del ingeniero especializado en el proceso.


Se realiza monitoreo constantemente a la IP pública fija, la cual es de uso exclusivo para los equipos preparadores y pagador.

Todos los equipos de cómputo de la tesorería General, siguen con la credencial de usuario para autenticar fecha de inicio de sesión.

Certificación TIC

La secretaria de la TIC, presenta un listado en Excel nombrado Verificación Equipos de Cómputo de Hacienda Oficina Tesorería (Verificación de Equipos de uso exclusivo y su ubicación) mensualmente y reporta el informe cada tres meses.

Este listado contiene las siguientes columnas: nombre de la persona, usuario, sistema operativo activo y versión, si tiene activa las actualizaciones automáticas, estado de los cables eléctricos, versión del antivirus, firewall antivirus activo, firewall Windows activo, puertos USB activos.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 5 de 11

OBSERVACION:

Certificación del Banco:

El banco certifica que cuenta con un modelo basado en el estándar ISO 27001, que además de dar cumplimiento a la normatividad regulatoria vigente.

Certificación Tesorería:

En la certificación que expide y firma el Tesorero y/o el director Financiero como encargado de la tesorería hacen mención al Protocolo de seguridad informática 2021, documento que a la fecha no fue evidenciado en esta auditoría.

La certificación de las TIC

En visita realizada a la Secretaría de Hacienda - Tesorería, el equipo auditor evidenció que, aunque los equipos de cómputo ubicados dentro de las instalaciones cuentan con direcciones IP fijas proporcionadas por el proceso de gestión de la Secretaría TIC, los equipos utilizados para el registro e ingreso de transacciones tienen habilitados los puertos USB, así como los quemadores de CD y DVD. Esta situación representa un riesgo por malware, originada a través de dispositivos de almacenamiento para la seguridad de la información, ya que podría facilitar, pérdida de datos sensibles, debido a la extracción no autorizada mediante dispositivos USB, e infección extraíbles o medios físicos no seguros.


La secretaria TIC manifiesta que: “la política y controles de acceso a puertos USB, quemadores de CD y DVD en los equipos dedicados a las transacciones con bancos, en recomendación y mejora continua del protocolo de seguridad de los proceso de tesorería, en común acuerdo se dispone a dar seguimiento al proceso, y realizar la respectiva inclusión en la matriz de evaluación realizada cada trimestre desde el área de sistemas a la tesorería departamental, este punto quedó como compromiso de implementación para el próximo corte de evaluación de protocolos en la matriz de protocolos de seguridad.

Verificada la matriz de verificación de equipos de cómputo de la secretaria de Hacienda - Tesorería correspondiente al periodo del 1 de octubre de 2024 al 31 de octubre de 2024, reportada por la Secretaria de las TIC, en las instalaciones de la Tesorería, se encontraron diferencias entre los datos registrados en la matriz y la asignación real de usuarios a los equipos de cómputo, es decir, los nombres de los usuarios registrados en la matriz no coinciden con los usuarios asignados a los equipos.

Adicionalmente, se identificó que algunos usuarios no tienen acceso, ni manejo a la banca virtual de las entidades financieras, éstos figuran asignados en la matriz, lo que genera dudas sobre la exactitud y confiabilidad de la información registrada. Esta inconsistencia podría indicar un posible desajuste en los controles internos de asignación y gestión de los equipos, lo que requiere corrección para garantizar la precisión y coherencia de la matriz de verificación y asegurar que la asignación de usuarios a equipos se realice de acuerdo con las responsabilidades y accesos correspondientes, como se detalla en la Tabla No. 1.

Tabla N. 1 matriz verificación de equipos de cómputo de hacienda oficina Tesorería

PERSONA	INGRESE UN USUARIO DENTRO DEL DOMINIO	
	USUARIO	EVIDENCIA OCIG
KAREN MONARD	DIRHAHACIENDA 06	Auxhacienda79
MARINA GÓMEZ	AUXHACIENDA33	Trabaja en archivo
MARINA GÓMEZ	DIRHACIENDA09	Trabaja en archivo
DANIELA CÁRDENAS	AUXHACIENDA71	No maneja plataforma de bancos
SANDRA MARIN	AUXEDUCACION25	Nomina – Secretaría de Educación

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 6 de 11

FELIPE BEDOYA	AUXHACIENDA55	No maneja plataforma de bancos
ISABEL VANEGAS	DIRHACIENDA04	No maneja plataforma de bancos
NUBIA CEBALLOS	AUXHACIENDA62	No maneja plataforma de bancos
ISOLEY SALAZAR	AUXHACIENDA77	No maneja plataforma de bancos

Fuente: reporte OCIG asignación de usuarios que no coinciden con reporte de la secretaria TIC

5. Verificación del cumplimiento de los protocolos de seguridad (Cámaras de Seguridad, Cajas fuertes, claves, mantenimiento a los equipos y a la red.

Cámaras de Seguridad:

Se evidenciaron dos cámaras de seguridad ubicadas en la tesorería Departamental del Quindío.

Cajas fuertes:

Se cuentan con dos cajas fuertes

OBSERVACION:

Se consultó con la empresa VIPCOL LTDA, el funcionamiento de las cámaras de seguridad e informaron "... que dichas cámaras no funcionan, al parecer se encuentran desconfiguradas de su conexión IP, desde el pasado mes de diciembre"... , este reporte lo hacen a través del oficio radicado con el Id: 106803 con fecha 2024-10-07, a la Directora Administrativa de Recursos Físicos Departamental Señora Maira Alejandra Noreña.

En cuanto a las cajas fuertes se encuentran inoperables

6. Verificación de la custodia de títulos valores, (Estampillas, cheques, mandamientos de pago)


Estampillas:

El equipo auditor de Control Interno, en la visita de recorrido realizada en la Oficina de Tesorería de la Secretaría de Hacienda, en conversación con la Profesional Universitaria y el Técnico Operativo encargados del manejo de los títulos valores (Estampillas: Pro Adulto Mayor, Pro Cultura, Pro desarrollo, Pro Universidad y Pro Hospital), se constató, que manejan un control manual en un libro en el cual registran las entregas a las cajas del Banco de Occidente, y en los cuadros diarios que reporta el Banco quedan registrados la cantidad de las estampillas vendidas diariamente con el valor de los mismos. igualmente atienden las solicitudes de las estampillas en consignación con los municipios en convenio, mediante el oficio de solicitud, anexo la consignación del pago de las estampillas que habían sido dado en consignación y la solicitud de un nuevo pedido; y procede a entregar el nuevo pedido en consignación.

OBSERVACION:

Se pudo evidenciar que las personas encargadas del proceso de control, seguimiento y registro de las Estampillas, desconocen el Procedimiento de Estampilla Código: P-HAC-01, Versión: 04 del 16 de mayo de 2023, y el Procedimiento Inventarios Código: P-HAC-49, Versión: 02 del 20 de diciembre de 2022, al no operar el Módulo de Inventario de las Estampillas, conforme a lo establecido en los Procedimientos citados.

Lo anterior, conlleva a deficiencias en el control y seguimiento al inventario de Estampillas, dificultando conocer el inventario actual de la estampilla en tiempo real.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 7 de 11

Cheques:

En la prueba de recorrido el tesorero informo que la chequera permanece en el cajón de su escritorio, y en cuanto a los cheques de las cuentas para pagar ya diligenciados, se evidenció que permanecen encima de un archivador en la oficina del Tesorero

OBSERVACION:

Se evidencia que el manejo de los cheques no presenta una adecuada custodia de los mismos, dado que son títulos valores.

7. Revisión custodia y manejo de Token

En mesa de trabajo realizada con el director financiero y el tesorero se informó que se tienen asignados tres tipos de token, los cuales están distribuidos así;

- Token para el administrador (Director financiero)
- Token para el Autorizador (Tesorero), encargado de realizar los pagos
- Token para Preparadores (contratistas y/o funcionarios de planta) encargados de registrar información en los portales de los bancos.

OBSERVACION:

Se evidenció que los token para los preparadores no se guardan bajo seguridad permanecen encima de los escritorios y es utilizado para dos usuarios, dado que los Token son dispositivos diseñados para aumentar la seguridad de las transacciones de los usuarios, minimizando el riesgo de fraude y otros delitos electrónicos, se deben manejar buenas prácticas de seguridad informática para hacer buen uso de este, y a su vez protegerlo. La custodia de los tokens debe estar en un lugar seguro.

8. Verificación de la realización de los Backup

En mesa de trabajo realizada con la secretaría TIC informa que diariamente se realiza copia de seguridad dos (2) veces al día, a los aplicativos PCT y Humano, los cuales comparten una misma Base de datos. Y a través del convenio que se tiene establecido con la entidad bancaria del recaudo del impuesto vehicular se maneja el aplicativo Siscar, que posterior se realiza un copia de seguridad 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 (NAS).


OBSERVACION:

Conforme al análisis realizado para analizar el proceso de backups se toma de referencia el proceso **P - TIC - 01 - Copias de Seguridad y Recuperación de Información**

Se han identificado deficiencias en la Gobernación del Quindío que afectan la seguridad de la información. En el ámbito de seguridad física, existen vulnerabilidades en el Datacenter y el sitio de almacenamiento externo. Además, el proceso de copias de seguridad presenta fallas como registros desactualizados, falta de capacitación y la ausencia de pruebas de restauración. También, tras la finalización del contrato de soporte del antivirus, los sistemas quedaron sin protección adecuada. Asimismo, aunque se tiene un proceso de gestión de incidentes, no se implementan ni documentan adecuadamente, lo que limita la capacidad de respuesta ante incidentes de seguridad. Estas deficiencias exponen a la entidad a riesgos significativos que deben ser abordados con urgencia para garantizar la seguridad y continuidad operativa.

Una vez revisado el **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, Código: PL-TIC- 001**, Versión: 04, Fecha; 31/01/2024, se contempla la implementación del Modelo de seguridad y Privacidad MSPI, donde establecen un cronograma de actividades a desarrollar en la vigencia 2024.

En cuanto al convenio establecido con el Banco para el manejo del aplicativo Siscar, No se evidencio la monitorización de los servicios proporcionados y los informes del proveedor sobre el nivel del servicio prestado.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 8 de 11

9. Revisar la identificación de la gestión del riesgo, operatividad de los controles y el mejoramiento continuo.

El equipo auditor en la prueba de recorrido realizada en el periodo de ejecución de auditoría, identifico que la Secretaría de Hacienda tiene el siguiente riesgo:

Riesgo identificado: Posibilidad de afectación económica y reputacional por pagos y transferencias electrónicas realizadas a través de los portales electrónicos de las entidades financieras autorizadas en el Departamento del Quindío, sin aplicación de los protocolos de seguridad implementados por la Dirección TICs del Departamento y la Entidades Financieras autorizadas debido a falta de implementación de los protocolos de seguridad establecidos por el Ente Territorial a través de la Dirección TICs y la banca virtual de las entidades financieras.

Causa: Falta de implementación de los protocolos de seguridad establecidos por el Ente Territorial a través de la Dirección TICs y la banca virtual de las entidades Financieras.

Nivel del Riesgo: Alto.

OBSERVACIÓN: Se pudo verificar por parte del equipo auditor la identificación del riesgo que tiene la Secretaría de Hacienda, con relación a la posibilidad de afectación económica y reputacional por pagos y transferencias electrónicas

Operatividad de los controles

La secretaría de Hacienda en la Jefatura de Tesorería tiene establecido el control para el riesgo identificado el cual es:

Control: El Tesorero General aplicará estrictamente el protocolo adoptado por el Departamento basado en recomendaciones hechas por la Dirección TICs y las Entidades Financieras autorizadas por el Departamento, para los pagos y transferencias electrónicas, a través de la banca virtual, de lo cual, ***“quedara evidencia a través de un informe trimestral que enviara a la secretaría de Hacienda”***. En caso de evidenciar alguna inconsistencia, al momento de aplicar el protocolo, el Tesorero General solicitará apoyo a la Dirección TICs y/o Entidad Financiera responsable.


OBSERVACIÓN: El equipo auditor pudo verificar en la prueba de recorrido que el tesorero aplica unas actividades, pero no se evidenció en ningún momento el Protocolo de Seguridad Informática 2021, el cual está adoptado por la Gobernación del Quindío, por lo cual no se pudo establecer si son operantes los controles implementados.

Referente al informe trimestral que enviará el Tesorero General a la Secretaría de Hacienda, en ningún momento el equipo auditor pudo verificar la existencia del informe como evidencia de la operatividad del control realizado.

Mejoramiento continuo.

El equipo auditor en el recorrido realizado, no evidencia un mejoramiento continuo en el proceso de administración del riesgo.

OBSERVACION: Se pudo evidencia que no se ve mejoramiento continuo para la mitigación del riesgo, por lo cual, el riesgo sigue siendo ALTO.

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 9 de 11

--

HALLAZGOS ADMINISTRATIVOS

HALLAZGO N. 1 Protocolo de seguridad: Ausencia y/o desconocimiento del Protocolo de seguridad.

Condición:

En la descripción del Control en el MAPA DE RIESGOS DE GESTIÓN MR-HAC-01, el Tesorero General aplicará estrictamente el protocolo adoptado por el Departamento, basado en recomendaciones hechas por la Dirección TIC y las Entidades Financieras autorizadas por la Gobernación del Quindío, para los pagos y transferencias electrónicas a través de la banca virtual, de lo cual, quedará evidencia a través de un informe trimestral que enviará a la Secretaria de Hacienda; en la certificación expedida por el Tesorero hace mención del Protocolo de Seguridad informática 2021, no obstante en la prueba de recorrido el Tesorero y/o el Director Financiero como encargado de la tesorería hacen mención al Protocolo de seguridad informática 2021, documento que a la fecha no fue evidenciado en esta auditoría.

Criterio:

- MAPA DE RIESGOS DE GESTIÓN MR-HAC-01
- PL-TIC-01 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- POL-TIC-02 POLICAS DE SEGURIDAD
- P-TIC-07 PROTOCOLOS DE SEGURIDAD EQUIPO DE PAGOS VIRTUALES TESORERIA.
- PROCEDIMIENTO DESEMBOLSOS CODIGO: P-HAC-13 VERSIÓN 02 DEL 30/07/2018.
- Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"
- Modelo Integrado de Planeación y Gestión MIPG
- Guía para la gestión por procesos en el marco del modelo integrado de planeación y gestión (MIPG)

Causa:

- Desconocimiento del Protocolo de Seguridad
- Desconocimiento de las buenas prácticas de seguridad informática dadas por el banco
- Desconocimiento de la incorporación del sistema de gestión de la calidad en el sector público
- Desconocimiento de las directrices del Departamento Administrativo de la Función Pública para la gestión por procesos en el marco del modelo integrado de planeación y gestión (MIPG)
- Desconocimiento de las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones.


Efecto:

- Accesos no autorizados a una red informática o a los equipos que en ella se encuentran pueden ocasionar pérdidas económicas, retrasos en los pagos, pérdida de información confidencial.

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 instalados en los servidores y equipos de la Entidad, dejando los sistemas

	FORMATO	Código: F-CIG-02
	Informe de auditoría interna	Versión: 04 Fecha: 01/12/2017
		Página 10 de 11

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 Backup

Condición:

Se han identificado deficiencias en la Gobernación del Quindío que afectan la seguridad de la información. En el ámbito de seguridad física, existen vulnerabilidades en el Datacenter y el sitio de almacenamiento externo. Además, el proceso de copias de seguridad presenta fallas como registros desactualizados, falta de capacitación y la ausencia de pruebas de restauración. También, tras la finalización del contrato de soporte del antivirus, los sistemas quedaron sin protección adecuada. Asimismo, aunque se tiene un proceso de gestión de incidentes, no se implementan ni documentan adecuadamente, lo que limita la capacidad de respuesta ante incidentes de seguridad. Estas deficiencias exponen a la entidad a riesgos significativos que deben ser abordados con urgencia para garantizar la seguridad y continuidad operativa.

Criterio:

- La Norma ISO 27001 — All (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
- Plan de Seguridad y privacidad de la Información — 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.
- Recursos insuficientes 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.
- Deficiencias en realización de pruebas de restauración y recuperación de información en caso de un incidente.
- Fallos operativos.
- Desactualización de los inventarios de bases de datos

RECOMENDACIONES

De conformidad al presente informe final de auditoría se recomienda a las secretarías de Hacienda – Tesorería y 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 termino será de veinte (20) días hábiles para su formulación y remisión a la oficina de control interno de gestión.

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

Por último se recomienda lo siguiente:

- Incluir en el Manual de Funciones y Competencias de la Administración Central del Departamento del Quindío, respecto a la responsabilidad de preparar los pagos electrónicos y convencionales por transferencias.
- Poner en funcionamiento las cámaras de seguridad en el área de Tesorería
- Actualizar los Procedimientos de Estampilla Código: P-HAC-01, Versión: 04 del 16 de mayo de 2023, y el Procedimiento Inventarios Código: P-HAC-49, Versión: 02 del 20 de diciembre de 2022, y poner en funcionamiento el Módulo de Inventario de las Estampillas, conforme a lo establecido en los Procedimientos citados.

CONCLUSIONES

La Secretaria de Hacienda — Tesorería tiene adoptado un Protocolo de seguridad Informático 2021, documento que es desconocido por los funcionarios de Tesorería, dificultando que el personal tenga presente las pautas y reglas claras de buenas prácticas de seguridad como en el manejo de los tokens, restricción de usuarios y claves, manejo de las cámaras de seguridad, cajas fuertes y títulos valores entre otros. Dicho documento tampoco fue evidenciado en la auditoría realizada.

Desde la secretaria TIC se cuentan con planes, políticas y protocolos de seguridad que a la fecha están desactualizados y en su implementación se evidencian deficiencias en el manejo del antivirus y backups; no obstante, se observa que en el PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, CODIGO PL – TIC-001 VERSION 04 FECHA: 31/01/2024 se contempla la implementación del Modelo de Seguridad y Privacidad MSPI, donde establecen un cronograma de actividades a desarrollar en la vigencia 2024.

La auditoría de protocolos de seguridad basada en riesgos fue notificada con el informe preliminar Acta N. 207 del 16 de diciembre de 2024, y a la fecha no se presentaron objeciones u observaciones, por lo tanto, el equipo auditor de la oficina de control interno de gestión deja en firme el informe final de auditoría, el cual se notifica a cada una de las secretarías y se les recomienda elaborar el plan de mejoramiento y remitirlo a esta oficina.

FIRMA:



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

ELABORACIÓN	REVISIÓN	APROBACIÓN
Elaborado Por: Juan Carlos Suarez Izquierdo	Revisado por: Jose Duvan lizarazo Cubillos	Aprobado por: Jose Duvan lizarazo Cubillos
Cargo: Profesional Universitario	Cargo: Jefe de Oficina	Cargo: Jefe de Oficina