Código:GE-FR-013
Vigente a partir de: 16/10/2024
Versión: 1

INFORME "FINAL"

Auditoría Proceso Tecnología de la Información y Comunicaciones.

Fecha: 24/12/2024

Tabla de contenido

1. Objetivo

Evaluar de manera integral la gestión y el uso de las tecnologías de la información y comunicación (TIC) en el Fondo Rotatorio de la Policía, con el fin de garantizar que los sistemas de información sean adecuados, eficientes y estén alineados con los objetivos estratégicos y operativos de la entidad. Además, se busca asegurar que los recursos tecnológicos se empleen de manera efectiva y que los riesgos asociados con las TIC estén controlados.

2. Contenido del informe.

2.1. Alcance.

Evaluación de todos los sistemas de hardware, software y redes utilizadas por la organización, incluyendo servidores, estaciones de trabajo, bases de datos, sistemas de comunicación y aplicaciones críticas que serán evaluadas durante el proceso. En este caso, el periodo comprendido entre el 1 de enero de 2023 y el 31 de octubre de 2024 será el marco temporal de la auditoría, de igual manera se constatara y documentara el actual funcionamiento de los sistemas informáticos durante el proceso de auditoría.

2.2. Justificación.

La Oficina de Control Interno, en el ejercicio de su función evaluadora e independiente y conforme al Plan de Auditoría 2024, aprobado por el Comité de Coordinación de Control Interno, incluyo la Auditoría Proceso Tecnología de la Información y Comunicaciones. Esta tiene como objetivo evaluar el cumplimiento de las disposiciones legales y normativas que regulan las actividades contractuales desarrolladas por el Grupo de Tecnología de la Información y Comunicaciones.

2.3. Criterios.

- Constitución Política.
- Ley 80 de 1993.
- Ley 1150 de 2007.
- Ley 1474 de 2011.
- Ley 1437 de 2011.
- Ley 1882 de 2018.
- Ley 2022 de 2020.
- Decreto 310 de 2021.
- Decreto 1082 de 2015.
- Decreto 1822 de 2019.
- Decreto 1860 de 2021.
- Guía de Roles y Responsabilidades del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).
- Guía de Procedimientos de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).
- Resolución 00299-31-07-23.
- Articles-5482_G3_Procedimiento_de_Seguridad
- Documento maestro del modelo de seguridad y privacidad de la Información (MINTIC).
- Mapas de riesgos

3. Desarrollo de la Auditoría.

El 12 de noviembre de 2024 se realizó reunión de apertura con la Coordinadora del Grupo de Tecnologías de la Información y Comunicaciones. Durante este encuentro, se presentó el plan de auditoría, se dio a conocer al equipo auditor designado y se entregó la carta de compromiso correspondiente. Esta reunión permitió establecer un marco de colaboración, además de aclarar los objetivos y el alcance de la auditoria.

El 13 de noviembre de 2024 se inició con la prueba de recorrido, la cual consistió en verificar los procesos clave relacionados con el área auditada. También se realizaron entrevistas con el personal responsable de las actividades que forman parte del proceso de auditado, de acuerdo con el cronograma establecido. Estas entrevistas facilitaron la obtención de información detallada sobre los procedimientos operativos, la identificación de posibles riesgos y evaluar el cumplimiento de los procedimientos internos establecidos.

Se garantizaron condiciones adecuadas para la recopilación de datos, y se establecieron canales de comunicación abiertos con los involucrados para resolver dudas y asegurar la transparencia durante todo el proceso. No obstante, pese a los anteriores requerimientos el Grupo de Tecnologías de la Información y las Comunicaciones no allegó la totalidad de la información solicitada, lo que afectó el cronograma que tenían establecido el equipo auditor y limitó el trabajo de auditoría.

Con la información allegada y analizada durante la ejecución de la auditoría, se elaboró el informe preliminar, obteniendo los siguientes:

4. Hallazgos.

Hallazgo 1: Ingreso a la Sede Administrativa de personal desvinculado.

Durante la revisión de los accesos y autorizaciones de ingreso a las instalaciones de la entidad, así como de permisos, claves, usuarios y correos electrónicos, se identificó que se mantiene un buen control. Sin embargo, algunos ex funcionarios que ya no están activos siguen teniendo acceso, a pesar de que estos ya no forman parte de la planta de personal. Además, las autorizaciones de ingreso no han sido actualizadas, canceladas o revocadas tras la finalización de su relación laboral. Del mismo modo, los correos y permisos en los sistemas de información se mantienen vigentes.

Cuadro. 1. Personal desvinculado.

NO CRUZARON
DOS EXFUNCIONARIOS DEL GRUPO - ADCON
DOS EXFUNCIONARIOS DEL GRUPO - DIGEN
UN EXFUNCIONARIO DEL GRUPO - OCOIN

Al respecto, el documento maestro del modelo de seguridad y privacidad de la Información, en sus numerales A.5.1.2, A9.1.2, A.9.2.1, A.9.2.2 y A.9.2.6, refieren: *(…) "Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas" (…), (…) "**Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente"** (…), (…) "**Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios**, para posibilitar la asignación de los derechos de acceso" (…), (…) "**Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los***

derechos de acceso *a todo tipo de usuarios para todos los sistemas y servicios" (…) y (…) "**Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo,** o se deberían ajustar cuando se hagan cambios" (…)* Negrilla fuera del texto.

El articles-5482_G3_Procedimiento_de_Seguridad (MINTIC) PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO, alude: *(…) "En este procedimiento **se debe describir como se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado**. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas etc..." (…)* Negrilla fuera del texto.

Así mismo la resolución del FORPO 00299-31-07-23 por la cual SE CREAN Y REORGANIZAN LOS GRUPOS", menciona en su numeral 1.3 funciones del grupo tecnologías de la información y las comunicaciones, apartados E y J *(…) "E. Realizar la mejora continua del proceso de seguridad de la información bajo las normas y regulaciones vigentes según corresponda a los lineamientos del Gobierno Nacional con el fin de salvaguardar la información de la entidad" (…) y (…) "J. **operar y controlar los sistemas de acceso y seguridad de la entidad"** (…)* Negrilla fuera del texto.

Conforme a los argumentos expuestos, es crucial que la entidad implemente controles más estrictos y eficientes en el proceso de gestión de accesos, a fin de garantizar que únicamente el personal autorizado pueda ingresar a las instalaciones y hacer uso de sus servicios. Estos controles deben incluir la actualización periódica de los registros de personal y la correcta desactivación de los accesos de exfuncionarios que ya no pertenecen a la entidad, con el propósito de evitar posibles incidentes que puedan comprometer la seguridad de la información y los activos tecnológicos de la entidad.

El ingreso no autorizado de personal desvinculado o no registrado constituye un riesgo tecnológico, debido a la inobservancia de los principios de confidencialidad de los datos y disponibilidad del sistema, afectando tanto la seguridad física como la protección de los activos de la entidad, ya que se permite el acceso indebido a las instalaciones, al correo institucional y a los servicios de red, comprometiendo la integridad de la información y la seguridad de los recursos tecnológicos. *(Soportes-Anexo-1)*

Hallazgo 2: Falta de adquisición o contratación para el licenciamiento del antivirus de la entidad.

Durante la revisión de los sistemas de protección tecnológica, se identificó que el personal del área de telemática mantiene un control de la seguridad de los sistemas de información pero el software antivirus instalado en los equipos de la entidad no cuenta con una licencia renovada. Lo que impide acceder a actualizaciones esenciales o a la activación de funciones críticas, comprometiendo la efectividad del antivirus en la prevención y detección de amenazas.

Al respecto, el documento maestro del modelo de seguridad y privacidad de la Información, en sus numerales A.6.1.1, A.9.4.4, A.12.2.1, A.17.1.2 y A.17.1.3 donde refieren: *(…) "Se deben definir y asignar todas las responsabilidades de la seguridad de la información" (…), (…) "Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones" (…), (…) "**Se deben implementar controles de detección, de prevención y de recuperación**, combinados con la toma de conciencia apropiada de los usuarios,*

para proteger contra códigos maliciosos" *(…), (…) "**La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información** durante una situación adversa" (…) y (…) "La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas" (…)*Negrilla fuera del texto.

Así mismo la resolución del FORPO 00299-31-07-23 por la cual SE CREAN Y REORGANIZAN LOS GRUPOS Menciona en sus numeral 1.3 funciones del grupo tecnologías de la información y las comunicaciones. En su apartado A, B, C, D y G *(…) "**Planificar y ejecutar acciones destinadas a asegurar el correcto funcionamiento de la plataforma tecnológica** según los requerimientos normativos y lineamientos del Gobierno Nacional" (…), (…) "Avalar con informe técnico la funcionalidad e idoneidad de las herramientas informáticas y tecnológicas adquiridas por la entidad" (…), (…) "**Planificar y coordinar las actividades técnicas y administrativas necesarias para atender las necesidades de software y hardware**, y demás tecnologías de la información que requiere la entidad para su funcionamiento y mejora continua" (…), (…) "Realizar evaluación, seguimiento y control al inventario de hardware, software y demás recursos ofimáticos de la entidad" (…), (…) "**asesorar a la alta dirección sobre las adquisiciones de software, hardware y demás tecnologías de la información**" (…)*Negrilla fuera del texto.

Es importante que la Entidad a través del GUTIC tome medidas correctivas para asegurar que todos los equipos cuenten con la protección adecuada, a fin de evitar vulnerabilidades que puedan ser explotadas. Estas medidas se pueden adelantar con la adquisición de las licencias correspondientes para garantizar que todos los sistemas estén debidamente protegidos, mitigando así, riesgos asociados con la exposición a ataques o pérdidas de información crítica. La inoperabilidad del antivirus representa un riesgo tecnológico, debido a la inobservancia de los principios de integridad y disponibilidad del sistema, lo que podría afectar la seguridad de la información dentro de la entidad exponiéndola a posibles ataques cibernéticos*. (Soportes-Anexo-2)*

Hallazgo 3: Falla en el canal dedicado y backup de internet de la sede principal.

Durante el proceso de auditoría, se identificó que el riesgo tecnológico asociado con la falla en el canal de internet se materializó, afectando de manera significativa la operatividad de los sistemas que dependen de la conectividad externa. El incidente, que tuvo lugar entre el 20 y el 22 de julio de 2024, ocasionó la pérdida de acceso a sistemas críticos, la interrupción de las operaciones y el tiempo de inactividad de diversas aplicaciones y servicios, entre otros efectos.

A pesar de que existen protocolos establecidos para la gestión de incidentes tecnológicos, el Fondo Rotatorio de la Policía no contaba con el personal idóneo para realizar los ajustes manuales pertinentes a los diferentes dispositivos para poder realizar el cambio automático o inmediato al momento de ser percibida la falla. La respuesta ante este evento fue insuficiente, lo que retrasó la restauración del servicio y exacerbó las consecuencias operativas. Esto indica una posible deficiencia en la planificación de contingencia y la capacidad de respuesta ante fallas en la infraestructura tecnológica.

Al respecto, el documento maestro del modelo de seguridad y privacidad de la Información, en sus numerales A.6.1.1 A.13.1.1, A.17.1.1, A.17.1.2 y A.17.1.3 refieren: *(…) "Se deben definir y asignar todas las responsabilidades de la seguridad de la información" (…), (…) "**Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones"** (…), (…) "**La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre**" (…), (…) "**La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa"** (…) y (…) "La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas" (…)* Negrilla fuera del texto.

Así mismo la resolución del FORPO 00299-31-07-23 por la cual SE CREAN Y REORGANIZAN LOS GRUPOS Menciona en sus numeral 1.3 funciones del grupo tecnologías de la información y las comunicaciones. En su apartado A, B, C y D *(…) "Planificar y ejecutar acciones destinadas a **asegurar el correcto funcionamiento de la plataforma tecnológica** según los requerimientos normativos y lineamientos del Gobierno Nacional" (…), (…) "Avalar con informe técnico la funcionalidad e idoneidad de las herramientas informáticas y tecnológicas adquiridas por la entidad" (…), (…) "**Planificar y coordinar las actividades técnicas y administrativas necesarias para atender las necesidades de software y hardware**, y demás tecnologías de la información que requiere la entidad para su funcionamiento y mejora continua" (…) y (…) "Realizar evaluación, seguimiento y control al inventario de hardware, software y demás recursos ofimáticos de la entidad" (…)* Negrilla fuera del texto.

Aunque la entidad cuenta con procedimientos establecidos para gestionar este tipo de incidentes, la respuesta ante la interrupción no fue lo suficientemente ágil ni eficiente. Este hecho pone en evidencia la necesidad urgente de mejorar los planes de contingencia, la contratación de personal especializado y la resiliencia tecnológica de la organización. La falta de una respuesta rápida y adecuada ante este tipo de fallas subraya la importancia de reforzar estos aspectos para evitar interrupciones en el servicio que afecten las operaciones cotidianas.

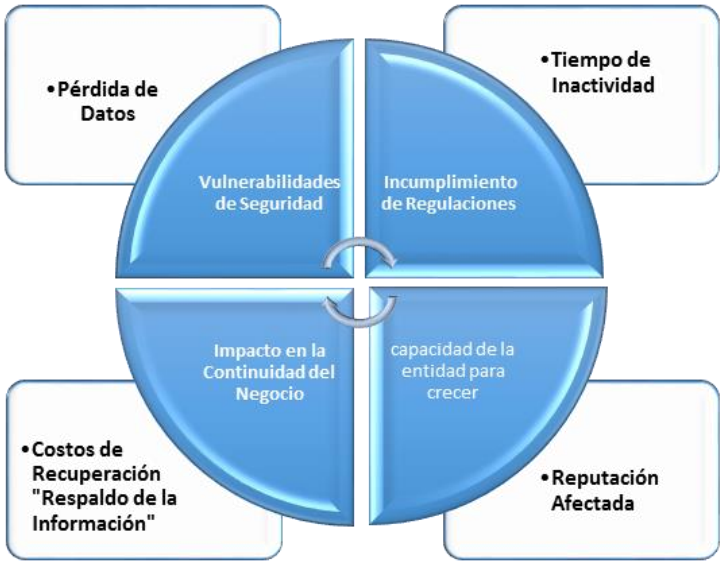
La materialización del riesgo de falla en el canal de internet ha evidenciado una vulnerabilidad significativa en la infraestructura tecnológica de la organización, lo que ha generado un riesgo tecnológico, afectado gravemente los principios de integridad de los datos y disponibilidad del sistema, comprometiendo la continuidad de las operaciones y generando impactos negativos en la productividad y en la confianza de los usuarios. *(Soportes-CONCEPTO INFORME FALLO INTERNET del 23 de agosto de 2024).*

Hallazgo 4: Debilidades en la identificación de vulnerabilidades y amenazas de la arquitectura tecnológica Hardware y Software de la entidad.

En la revisión del funcionamiento de los diferentes servicios tecnológicos del Fondo Rotatorio de la Policía, se evidenció que los servidores presentaron fallas en dos ocasiones diferentes: una desde el 2 de septiembre de 2023 hasta el 13 de septiembre de 2023, y la otra desde el 19 de enero de 2024 hasta el 14 de marzo de 2024.

Durante un período crítico de 55 días sin servicios informáticos, el diagnóstico reveló una progresión en el deterioro de los sistemas de información. Inicialmente, se detectaron 14 discos en estado de alarma, cifra que cambió a 9, luego a 21, y finalmente a 19 discos, superando los límites de capacidad de almacenamiento del 80% y 90%.

Cuadro. 2. Riesgo Técnico



Teniendo en cuenta lo anterior, se verificaron los últimos mantenimientos de los equipos de data-center de la entidad, a través de los procesos contractuales adelantados, evidenciando que se cuentan con dos proyectos que impactan directamente en el correcto funcionamiento de estos equipos, MANTENIMIENTO HARDWARE ORACLE PARA EL FONDO ROTATORIO DE LA POLICÍA y MANTENIMIENTO PLATAFORMA TIC (UPS, A.A, TELÉFONOS IP Y SALA MULTIPROPÓSITO, ESCÁNER, DRONES, ACCESO FACIAL) con lo corrido de la vigencia 2023, para el primer proyecto van 3 años y para el segundo van 2 años sin realizarse actividades de mantenimiento preventivo y/o correctivo.
En la revisión de anteriores procesos relacionados, se identificó que desde el 2021 no se paga el Oracle Support, y que la última contratación fue soporte netamente de software al aplicativo INFORPO

De igual manera el en el contrato CTO 111-6-2022 se constató que el contratista identificó un error crítico. Este fue detallado en el “Informe de Intervención Técnica en noviembre de 2022*”, (…) “al ingresar se evidencia un* ***error de suma criticidad el cual radica en que el storage*** *solo tiene una controladora activa, la numero (01), el controlador que en sí mismo es un servidor físico” (…) lo cual no fue informado en el informe de supervisión de (noviembre y diciembre 2022) De las advertencias y recomendaciones señaladas por “Server Tech Soluciones Informáticas el 07 de noviembre de 2022”, se evidenció que el supervisor del contrato, en los informes correspondientes a noviembre y diciembre, no comunicó o alerto a cerca de (…) “****las fallas en los sistemas de información y la urgencia para que fueran intervenidos y reparados antes de un Crash down****” (…). De igual manera informan en el contrato de mantenimiento infraestructura tecnológica Forpo 2023 con la empresa COINSA SAS informando que: (…) “Lamentamos informar que técnicamente no podemos ejecutar*

ninguna otra acción de recuperación de la integridad en funcionamiento de la infraestructura." Situación que no garantizo un seguimiento técnico adecuado en la ejecución del contrato. Dejando como una única opción de ***recuperación la asistencia del fabricante SUN –ORACLE"*** *(…)* Negrilla fuera del texto.

Al respecto, el documento maestro del modelo de seguridad y privacidad de la Información, en sus numerales A.8.1.3, A.11.2.4, A.12.1.3, A.12.3.1, A.12.7.1, A.17.1.2, A.17.1.3 Y A.18.2.3 *(…) "Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información" (…), (…) "****Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas****" (…), (…) "****Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones*** *de los requisitos sobre la capacidad futura" (…), (…) "****Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas****, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada" (…), (…) "Los requisitos y actividades de auditoría que* ***involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio****" (…), (…) "****La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa****" (…), (…) "****La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados****, con el fin de asegurar que son válidos y eficaces durante situaciones adversas" (…) y (…) "****Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información****" (…)* Negrilla fuera del texto.

Así mismo la resolución del FORPO 00299-31-07-23 por la cual SE CREAN Y REORGANIZAN LOS GRUPOS menciona en su numeral 1.3 funciones del grupo tecnologías de la información y las comunicaciones, en sus apartados A, B, C y D *(…) "****Planificar y ejecutar acciones destinadas a asegurar el correcto funcionamiento de la plataforma tecnológica*** *según los requerimientos normativos y lineamientos del Gobierno Nacional" (…), (…) "****Avalar con informe técnico la funcionalidad e idoneidad de las herramientas informáticas y tecnológicas adquiridas por la entidad****" (…), (…) "****Planificar y coordinar las actividades técnicas y administrativas necesarias para atender las necesidades de software y hardware, y demás tecnologías de la información*** *que requiere la entidad para su funcionamiento y mejora continua" (…) y (…) "Realizar evaluación, seguimiento y control al inventario de hardware, software y demás recursos ofimáticos de la entidad" (…)* Negrilla fuera del texto.

Dada la magnitud del impacto y la crítica importancia de los activos de información involucrados en los procesos afectados por la falla, así como la necesidad esencial de asegurar la continuidad del negocio y la integridad de la información para el desarrollo adecuado de las operaciones, tanto en las áreas misionales como de apoyo, se ha identificado un riesgo tecnológico significativo. Este riesgo resalta la incapacidad de la entidad para cumplir con sus objetivos estratégicos y satisfacer las necesidades derivadas de su misión institucional, lo que podría afectar el funcionamiento de los sistemas de información de manera crítica.

Adicionalmente, se ha identificado un riesgo de imagen, ya que las expectativas y percepciones negativas de las partes interesadas incluyendo entidades de control y clientes internos y externos están afectando de manera desfavorable el prestigio y la reputación de la entidad. Estas percepciones pueden generar desconfianza y reducir la credibilidad de la organización ante sus stakeholders, impactando negativamente en sus relaciones tanto internas como externas.

Los hechos mencionados evidencian deficiencias en la entidad en cuanto a la implementación de medidas oportunas para el desarrollo continuo e ininterrumpido de las actividades relacionadas con la seguridad de los sistemas de información. La falta de acciones preventivas y correctivas ha dejado expuestos los activos críticos de la organización a riesgos operativos y reputacionales.

A partir de las situaciones identificadas por el equipo de auditoría, se ha determinado que este hallazgo corresponde a un tipo administrativo, dado que se relaciona con la gestión interna de los recursos, la planificación y la ejecución de las políticas necesarias para garantizar la seguridad y continuidad operativa de los sistemas de información. *(Soportes-INFORME PRELIMINAR GESTIÓN DEL RIESGO SISTEMAS DE INFORMACIÓN).*

Hallazgo 5 Debilidades en la supervisión y falta de capacitación del contrato de adquisición, instalación y puesta en funcionamiento del ERP para el Fondo Rotatorio de la Policía.

En la revisión de los informes de supervisión contenidos en las carpetas contractuales, correspondientes al contrato de *"adquisición, instalación y puesta en funcionamiento del ERP (Enterprise Resource Planning) de la Entidad",* se evidenció que no se encuentran en la carpeta fisica ni en la plataforma SECOP II los informes correspondientes a los meses octubre y noviembre del presente año; al igual, se realizó encuesta con los diferentes grupos de la entidad para conocer de antemano el conocimiento y las capacitaciones recibidas para el uso del nuevo ERP, encontrando que los Grupos de Gestión Documental y Atención al Ciudadano, Infraestructura, Central de Cuentas, Oficina Jurídica y Presupuesto no han recibido capacitación alguna sobre el uso y funcionamiento de la nueva ERP.

Para el ejercicio y la responsabilidad en la supervisión de contratos, los Artículos 83 y 84 de la Ley 1474 de 2011, establecen: *(…) "Artículo 83. Supervisión e Interventoría Contractual. Con el fin de proteger la moralidad administrativa, de prevenir la ocurrencia de actos de corrupción y de tutelar la transparencia de la actividad contractual,* ***las entidades públicas están obligadas a vigilar permanentemente la correcta ejecución del objeto contratado a través de un supervisor****" "Artículo 84. Facultades y Deberes de los Supervisores y los Interventores.* ***La supervisión e interventoría contractual implica el seguimiento al ejercicio del cumplimiento obligacional por la entidad contratante sobre las obligaciones a cargo del contratista.****"* (…).Negrilla fuera del texto.

Así mismo la resolución del FORPO 00299-31-07-23 por la cual SE CREAN Y REORGANIZAN LOS GRUPOS Menciona en sus numeral 1.3 funciones del grupo tecnologías de la información y las comunicaciones. En su apartado A y *D (…) "****Planificar y ejecutar acciones destinadas a asegurar el correcto funcionamiento de la plataforma tecnológica*** *según los requerimientos normativos y lineamientos del Gobierno Nacional" (…) y (…) "Realizar evaluación, seguimiento y control al inventario de hardware, software y demás recursos ofimáticos de la entidad" (…)* Negrilla fuera del texto.

Al respecto, el documento maestro del modelo de seguridad y privacidad de la Información, en sus numerales A.14.2.3, A.14.2.6, A.14.2.7 y A.14.2.9 *(…) "**Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio**, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización" (…), (…) "Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas" (…), (…) "**La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente**" (…) y (…) "**Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba** para aceptación y criterios de aceptación relacionados" (…)* Negrilla fuera del texto.

Entiéndase que la falta de capacitación adecuada podría dar lugar a la materialización de riesgos tanto de imagen como tecnológicos. En primer lugar, el riesgo de imagen se deriva de la incapacidad de la entidad para garantizar que su personal esté suficientemente preparado para utilizar el sistema de manera efectiva desde el comienzo de la nueva vigencia. Esto podría generar un impacto negativo en la percepción pública y de los usuarios sobre la capacidad operativa de la entidad.

Por otro lado, el riesgo tecnológico se refiere a la integridad y disponibilidad de la información, ya que la falta de conocimiento del personal podría ocasionar errores en la gestión de datos y en la supervisión de los procesos críticos. Este escenario también afecta la supervisión adecuada de las operaciones, lo que compromete la correcta vigilancia y control de la actividad contractual, incrementando el riesgo de incumplimiento de las obligaciones pactadas en el contrato de administración delegada.

En conclusión, se evidencia que los términos de ejecución contractual no se cumplieron según el cronograma de ejecución, presentado retrasos en el desarrollo e implementación definitiva del sistema, lo que se evidencia según comunicado dirigido a las distintas oficinas y coordinaciones quienes manifiestan que no se han realizado pruebas ni capacitaciones al personal de cada dependencia sobre el uso ni se han realizado pruebas para determinar el correcto funcionamiento de la ERP, se recomienda realizar seguimiento continuo y detallado a la ejecución contractual, evitar saltar procesos e improvisar en la puesta en funcionamiento del ERP dada la importancia e impacto del mismo sobre la entidad. *(Soportes-Anexo-5).*

Hallazgo 6: Deficiencias en la administración del sistema de información y ausencia de personal idóneo.

Durante la auditoría, se identificaron deficiencias en la administración del sistema de información. Adicionalmente, se constató que la oficina encargada de la gestión del sistema enfrenta graves limitaciones de recursos humanos. El personal disponible, aunque altamente comprometido, es insuficiente para atender la totalidad de los requerimientos tecnológicos, lo que genera una carga excesiva sobre los pocos miembros del equipo. A pesar de estos desafíos, el personal hace un esfuerzo considerable por mantener la entidad en funcionamiento tecnológico, respondiendo a las demandas operativas con los recursos limitados con los que cuentan. Sin embargo, esta sobrecarga laboral aumenta el riesgo de desatención de incidencias críticas, la falta de implementación de mejoras necesarias y dificulta la actualización de los sistemas en tiempo y forma.

La Guía de Procedimientos de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), en su numeral 6.2 y 6.10 sobre Gestión de Incidentes de Seguridad de la Información, definió: *(…) "El equipo de gestión del proyecto en cada una* ***de las entidades se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades*** *necesarias para adoptar el Modelo de Seguridad de la Información al interior de su entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo" (…) y (...) "Este procedimiento debe indicar cómo responde* ***la entidad en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad***. ***Deben especificarse los roles, las responsabilidades*** *y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información" (…)* Negrilla fuera del texto.

*Al respecto, el documento maestro del modelo de seguridad y privacidad de la Información, en sus numerales A.6.1.1, A.11.2.4 Y A.18.2.3 refieren: (…) "****Se deben definir y asignar todas las responsabilidades de la seguridad de la información****" (…), (…) "Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas" (…) y (…)* ***"Los sistemas de información se deben revisar periódicamente*** *para determinar el cumplimiento con las políticas y normas de seguridad de la información" (…)* Negrilla fuera del texto.

Se destaca que, para asegurar el cumplimiento de actividades críticas como el Responsable de Seguridad de la Información de la entidad, soporte de páginas web, el mantenimiento de la infraestructura/hardware y la administración de bases de datos, entre otras acciones, es fundamental detallar una estructura organizacional con funciones y responsabilidades definidas para la ejecución de las actividades que demanda el grupo GUTIC.

En consonancia con lo anterior, la Guía de Roles y Responsabilidades del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) señala lo siguiente: *(...) "En aquellas entidades que así lo justifiquen, por ejemplo, con insuficiencia de recursos técnicos o experticia,* ***se recomienda la definición de un responsable de seguridad*** *que responda simultáneamente para un conjunto de entidades que acuerden agruparse" (…)* Negrilla fuera del texto.

Dentro de la definición de responsables en cada uno de los Dominios entregados en el Marco de Arquitectura Empresarial, está contemplado el papel del responsable de seguridad y privacidad de la información de la entidad, de esta forma se tienen las siguientes responsabilidades específicas de acuerdo con el Dominio: SERVICIOS TECNOLÓGICOS, ESTRATEGIA TI, GOBIERNO TI, SISTEMAS DE INFORMACIÓN, DE INFORMACIÓN, USO Y APROPIACIÓN".

Es fundamental señalar que el Grupo de Tecnologías de la Información y las Comunicaciones (GUTIC) es el responsable principal de la administración del sistema de información de la entidad, proporcionando soporte esencial para las operaciones diarias y garantizando su funcionamiento eficiente. Sus responsabilidades incluyen la resolución de problemas técnicos, la actualización y monitoreo de software, y el mantenimiento de la infraestructura tecnológica, que abarca servidores, equipos de red y sistemas de almacenamiento. De esta manera, el grupo GUTIC asegura

que los recursos tecnológicos estén disponibles y operativos para satisfacer las necesidades de la entidad en todo momento.

Sin embargo, tras revisar las funciones asignadas a los miembros del GUTIC, se ha identificado que no hay un funcionario especializado para las funciones clave mencionadas anteriormente. La ausencia de personal con habilidades técnicas especializadas ha resultado en una gestión deficiente de los sistemas de información, lo que ha derivado en un impacto negativo en los procesos administrativos del Fondo Rotatorio de la Policía. Esta falta de especialización ha generado un riesgo tecnológico importante, especialmente en lo que respecta a la disponibilidad de la información y la continuidad operativa de los sistemas.

Como consecuencia directa de esta carencia, se han experimentado fallas e interrupciones en la disponibilidad de los sistemas, lo que ha afectado gravemente la operación de la entidad y sus procesos. La falta de personal adecuado y capacitado para administrar y mantener los sistemas tecnológicos de manera eficiente compromete la estabilidad y el correcto funcionamiento de los recursos digitales críticos para la entidad.

Los hechos descritos evidencian deficiencias por parte de la entidad en la implementación de medidas oportunas para asegurar el desarrollo continuo y sin interrupciones de las actividades relacionadas con la seguridad, mantenimiento y operación de los sistemas de información. *(Soportes-FUNCIONES ACTUALES PERSONAL GUTIC).*

Hallazgo 7: Retraso en la implementación de la APP FORPO PLUS y vencimiento próximo de la garantía técnica y de cumplimiento.

Durante la revisión del contrato Orden de Compra 122836-2023, “SERVICIO DE SUSCRIPCIÓN DE CRÉDITOS NUBE PÚBLICA PARA EL DESARROLLO E IMPLEMENTACIÓN DE LA APLICACIÓN MÓVIL Y WEB DEL FONDO ROTATORIO DE LA POLICÍA”, iniciado el 21 de diciembre de 2023, se constató que, hasta la fecha, no se ha llevado a cabo la implementación ni la puesta en producción de la APP FORPO PLUS.

En el informe RAD. Nro. 242 FORPO - GUTIC - 302-10-29º del 11 de diciembre de 2024, entregado por el grupo GUTIC, se indicó que aún se encuentra pendiente la implementación del botón PSE para habilitar la compra o adquisición de uniformes y enseres por parte de los usuarios, así como la integración de un web servicie con la Policía Nacional para la autenticación del personal activo, pensionado o en uso de buen retiro. Asimismo, se señaló que la póliza de cumplimiento fue extendida hasta el 29 de diciembre de 2024, con el entendimiento de que, si para esa fecha la aplicación no entra en funcionamiento, no se podría generar ninguna reclamación ante un eventual incumplimiento.

Sumado a lo anterior, en las especificaciones del mencionado acuerdo se definió que el contratista otorgaría garantía técnica de mínimo un (1) año para la calidad de las actividades realizadas, la cual contaría a partir de la terminación del plazo de ejecución establecido en el contrato, previa firma del acta de recibido a satisfacción por parte del supervisor, la cual fue realizada el 29 de diciembre de 2023. Por lo tanto, dicha garantía iría hasta el 29 de diciembre de 2024. Sin embargo, hasta la

fecha de la revisión, no se ha cumplido con este compromiso, ya que la aplicación no está en funcionamiento en el entorno de producción.

Conforme a la ley 80 de 1993 en sus artículos 3 y 26 en su numeral 1, enfatizan: *(…) "artículo 3.De los Fines de la Contratación Estatal. Los servidores públicos tendrán en consideración que al celebrar contratos y con la ejecución de los mismos, las entidades buscan* ***el cumplimiento de los fines estatales, la continua y eficiente prestación de los servicios públicos y la efectividad de los derechos e intereses de los administrados que colaboran con ellas en la consecución de dichos fines****" (…) y (…) "artículo 26. Principio de responsabilidad. 1.* ***Los servidores públicos están obligados a buscar el cumplimiento de los fines de la contratación, a vigilar la correcta ejecución del objeto contratado*** *y a proteger los derechos de la entidad, del contratista y de los terceros que puedan verse afectados por la ejecución del contrato.*

Frente al alcance del principio de planeación en la contratación estatal, el Consejo de Estado, sala de lo Contencioso Administrativo, Sección Tercera- Subsección C, radicado 88001-23-31-000-2011-00021-01 (54.415), refiere: *(…) "En efecto, los contratos del Estado "****deben siempre corresponder a negocios debidamente diseñados, pensados, conforme a las necesidades y prioridades que demanda el interés público****; en otras palabras, el ordenamiento jurídico busca que* ***el contrato estatal no sea el producto de la improvisación ni de la mediocridad,"*** *razón por la cual en todos ellos se impone el deber de observar el principio de planeación. Para cumplir con el principio de planeación deben observarse* ***"parámetros técnicos, presupuestales, de oportunidad, de mercado, jurídicos, de elaboración de pliegos y términos de referencia" puesto que así se aseguran la prestación de los servicios públicos y la preservación de los recursos del Estado****." (…)* Negrilla fuera del texto.

Al respecto, el documento maestro del modelo de seguridad y privacidad de la Información, en sus numerales A.12.1.3, A.14.2.7 y A.14.2.9, refieren: *(…) "****Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos****, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura" (…), (…) "****La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente****" (…) y (…) "Para los sistemas de información nuevos, actualizaciones y nuevas versiones,* ***se deben establecer programas de prueba*** *para aceptación y criterios de aceptación relacionados" (…)* Negrilla fuera del texto.

Es de precisar que en los Estudios Previos del, en su *"Identificación y Descripción de la Necesidad"*, definieron: *(…) "Esta plataforma, está en la capacidad de* ***acceso tanto web, como a través de una aplicación móvil multiplataforma****, que trabaja en conjunto con* ***sistemas de información externos como lo son SIATH, centrales de riesgo, CIFIN, nómina de la Policía, mensajería OTP*** *(para la validación del usuario en cada transacción), además, esta aplicación debe contar con los módulos necesarios para la ejecución de una tienda virtual, la cual incluye plataforma de venta de productos, solicitud de adquisición de prendas, adquisición de productos y servicios de aliados comerciales, la posibilidad de realizar pagos a través* ***del botón PSE y solicitud de financiamiento****" (…)* Negrilla fuera del texto.

A su vez, las Especificaciones Técnicas del Acuerdo Marco, numeral II. Funcionalidad requerida de la necesidad, estipularon: *(…)* "*crédito rápido FORPO Plus – simulación de créditos: Calculo de la tasa*

de interés y el total desembolsable” (…) y *(…) “el servicio debe integrar el web servicie con el operador de las firmas electrónicas. Este proceso se pagara una vez se evidencie en la plataforma esta integración lo cual según el informe antes mencionado no se ha logrado la implementación del web service” (…)*

Se destaca que en el informe de supervisión de diciembre de 2023, el supervisor del contrato alude que la aplicación fue recibida a satisfacción y pagada en su totalidad el 14 de marzo de 2024. Posteriormente, la aplicación estuvo disponible para su descarga en plataformas desde el 17 de junio de 2024, con una actualización realizada el 19 de junio del mismo año en servicios móviles y web. El personal de la entidad fue notificado el 20 de junio de 2024 de que la aplicación ya estaba prestando servicios en la nube, aunque aún no se encontraba en producción.

No obstante, a la fecha, la aplicación FORPO PLUS sigue sin estar operativa, lo cual no se ajusta a lo estipulado en el contrato. Se ha identificado que la falta de implementación de dicha aplicación afecta significativamente la operatividad y los plazos establecidos para la entrega del servicio, lo que podría materializarse en un riesgo fiscal, toda vez que el atraso en la implementación y uso de la APP resultaría en un eventual detrimento patrimonial en los recursos invertidos por el Fondo Rotatorio de la Policía, ya que estos no están siendo usados de forma eficiente. Además, el vencimiento de las garantías técnicas y la póliza de cumplimiento podrían impedir que la entidad gestione el riesgo ante un eventual incumplimiento contractual. *(Soportes-RAD. Nro. 242 FORPO - GUTIC - 302-10-29, Anexo 7).*

Hallazgo 8: Protocolos de seguridad de los servidores y rack de la entidad.

Durante la evaluación de la infraestructura tecnológica de la entidad, se verificó que los protocolos de seguridad implementados en los servidores y racks están en su mayoría debidamente resguardados mediante sistemas de seguridad biométrica. Sin embargo, se identificó una excepción en el rack ubicado en el almacén general, el cual presenta deficiencias tanto en su materialización como en su aplicación. A pesar de que existen políticas establecidas para proteger estos recursos críticos, no se evidenciaron medidas físicas y operativas adecuadas que aseguren su integridad y seguridad en un entorno operativo real.

En particular, se observó que el acceso al rack del almacén general no está restringido de manera apropiada mediante controles de acceso físico, y que los procedimientos establecidos para garantizar la seguridad de la información y proteger contra accesos no autorizados no se están cumpliendo de manera consistente. De igual manera, se evidenció humedad en la pared del cuarto del servidor principal, la cual puede generar daños en los equipos que se encuentran allí. Además, el rack ubicado en el primer piso de la sede principal se encuentra expuesto, ya que está adyacente a una ventana de la entrada principal, lo que lo pone en riesgo de sufrir actos de vandalismo, daños por terceros o incluso afectaciones debido a condiciones climáticas adversas.

Por otro lado, se identificó la presencia de basura electrónica en todos los cuartos de servidores y racks, como equipos de cómputo, cableado, canaletas, entre otros. Esta acumulación de residuos no solo obstruye el libre acceso a los equipos, sino que también impide mantener un área de trabajo limpia y ordenada.

Al respecto, el documento maestro del modelo de seguridad y privacidad de la Información, en sus numerales A 11.1.2 , 11.13, 11.14 y 11.1.5 refieren: *(…) "**Las áreas seguras se deben proteger mediante controles de entrada apropiados** para asegurar que solamente se permite el acceso a personal autorizado" (…), (…) "**Se debe diseñar y aplicar seguridad física** a oficinas, recintos e instalaciones" (…) , (…) "**Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes**" (…) y (…) "Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras" (…)* Negrilla fuera del texto.

Así mismo la resolución del FORPO 00299-31-07-23 por la cual SE CREAN Y REORGANIZAN LOS GRUPOS, menciona en su numera 1.3 funciones del grupo tecnologías de la información y las comunicaciones numerales B, C y J : *(…) "**Avalar con informe técnico la funcionalidad e idoneidad de las herramientas informáticas y tecnológicas adquiridas por la entidad**" (…), (…) "**Planificar y coordinar las actividades técnicas y administrativas necesarias para atender las necesidades de software y hardware**, y demás tecnologías de la información que requiere la entidad para su funcionamiento y mejora continua" (…) y (…) "operar y controlar los sistemas de acceso y seguridad de la entidad" (…)* Negrilla fuera del texto.

De conformidad a los criterios antes aludidos, es fundamental que el Grupo GUTIC garantice la seguridad en los cuartos donde se encuentren los servidores y Racks, y que estos se mantengan libres de residuos materiales y objetos que puedan obstaculizar la libre circulación y el acceso a los mismos; además se debe garantizar que todos los cuartos de servidores de la entidad se mantengan sin acumulación de basura electrónica. Las situaciones evidenciadas podrían conllevar a la materialización de un riesgo tecnológico, al exponerse la seguridad y operatividad de los sistemas tecnológicos de la entidad, comprometiendo el principio de disponibilidad de los sistemas, ya que puede interferir con el acceso adecuado a los servidores y su correcto funcionamiento. *(Soportes-Anexo 8)*

Hallazgo 9. Vigencia del Firewall adquirido mediante el contrato 076-6-2023 "*Mantenimiento a la página web, firewall, Inforpo del Fondo Rotatorio de la Policía*".

Durante la evaluación de la infraestructura tecnológica de la entidad, se revisaron los detalles del licenciamiento de los firewalls encargados de proteger la infraestructura de la red interna. La entidad cuenta con tres firewalls: dos 1500D en configuración de alta disponibilidad (HA) en la sede de la Calle 26 y un 601E en la sede de Venecia.

Se evidenció que el licenciamiento de los tres equipos fue renovado bajo el contrato 076-6-2023 objeto *"Mantenimiento a la página web, firewall, Inforpo del Fondo Rotatorio de la Policía"***,** con una vigencia hasta el 23 de septiembre de 2024**,** según el informe de supervisión de diciembre de 2023, en su sección n° 5.1, resalta: *(…) "Para los 3 Firewall 1500D de la sede de la Calle 26, a continuación, en la ilustración 2, se presenta la evidencia del licenciamiento directamente desde el equipo donde se evidencia que se encuentra correctamente sincronizado y **con vigencia hasta el 23 de septiembre de 2024…"** (…) Negrilla fuera del texto.*

Sin embargo, en el Anexo n°1 ESPECIFICACIONES TÉCNICAS MÍNIMAS, ÍTEM 1 sobre la renovación de licencias y soporte de los firewalls Fortinet, se especificó lo siguiente: *(…) "ítem para renovar los Fortigate, FortiAnalizer y FortiADC **por 12 meses"** (…) Negrilla fuera del texto.*

Conforme a lo anteriormente expuesto, se presenta una dicotomía en cuanto a las fechas de cobertura y vigencia del licenciamiento de los firewalls, ya que, según las especificaciones técnicas del contrato, la vigencia debería ser hasta el 26 de diciembre de 2024, según el acta de recibido a satisfacción del 26 de diciembre de 2023**.** Sin embargo, en las actividades ejecutadas por el contratista y relacionadas por el supervisor, se menciona que la vigencia sería hasta el 23 de septiembre de 2024**.**

Al respecto, la ley 80 de 1993 en su artículo 26 del Principio de Responsabilidad, numeral 1, define: *(…) "1.* ***Los servidores públicos están obligados a buscar el cumplimiento de los fines de la contratación, a vigilar la correcta ejecución del objeto contratado y a proteger los derechos de la entidad****, del contratista y de los terceros que puedan verse afectados por la ejecución del contrato."* *(…) Negrilla fuera del texto.*

La ley 1474 de 2011, artículo 83 de la Supervisión e interventoría contractual, dice: *(…) "****Con el fin de proteger la moralidad administrativa, de prevenir la ocurrencia de actos de corrupción y de tutelar la transparencia de la actividad contractual, las entidades públicas están obligadas a vigilar permanentemente la correcta ejecución del objeto contratado*** *a través de un supervisor" (…) Negrilla fuera del texto*

La ley 1952 de 2019 por la cual se expide el Código General Disciplinario, artículo 54. Faltas relacionadas con la Contratación Pública, en su numerales 6 y 7: *(…) "6. No exigir, el supervisor o el interventor, la calidad de los bienes y servicios adquiridos por la entidad estatal,* ***o en su defecto, los exigidos por las normas técnicas obligatorias, o certificar como recibida a satisfacción obra que no ha sido ejecutada a cabalidad.****" "7. Omitir, el supervisor o el interventor,* ***el deber de informar a la entidad contratante los hechos o circunstancias que puedan constituir actos de corrupción tipificados como conductas punibles, o que puedan poner o pongan en riesgo el cumplimiento del contrato, o cuando se presente el incumplimiento.****" (…) Negrilla fuera del texto.*

De acuerdo con las especificaciones técnicas definidas en el contrato 076-6-2023, se estableció que la renovación y vigencia de las licencias de los firewalls sería por un periodo de 12 meses, los cuales debían contarse a partir del recibido a satisfacción. Según consta en la carpeta contractual, dicho recibido a satisfacción se formalizó el 26 de diciembre de 2023, por lo que la vigencia del licenciamiento debía extenderse hasta el 26 de diciembre de 2024.

Sin embargo, en el informe de supervisión del mes de diciembre de 2023, se indicó que las actividades ejecutadas por el contratista describían que la vigencia de las licencias se extendería únicamente hasta el 23 de septiembre de 2024, lo que genera una discrepancia significativa con lo estipulado en las especificaciones técnicas del contrato.

Al realizar el cálculo de la cobertura proporcionada por los 365 días (12 meses) contratados, se observa que, de estos, 266 días (equivalentes a 8 meses y 27 días) fueron efectivamente cubiertos. Esto deja un total de 99 días sin cumplir, lo que representa un incumplimiento respecto a lo pactado en el contrato, lo cual se constató mediante reporte solicitado al grupo GUTIC evidenciando que efectivamente las licencias se encontraban expiradas.

El valor del contrato fue de $456.700.000, correspondiente a los 12 meses de cobertura definidos en las especificaciones técnicas. Este monto fue pagado en su totalidad, como se evidencia en la factura electrónica n° FE 6811 del 27 de diciembre de 2023, por un valor de $456.699.999, emitida por el contratista COINSA S.A.S y pagada por el Fondo Rotatorio de la Policía en febrero de 2024, según consta en el informe de supervisión de ese mismo mes. Sin embargo, a pesar de que se pagó la totalidad del contrato, los tiempos definidos en las especificaciones técnicas del contrato 076-6-2023 no se cumplieron de acuerdo a lo pactado, ya que hubo una discrepancia en la vigencia de las licencias. Estas situaciones no fueron observadas ni advertidas por la supervisión designada, lo que indicaría una deficiencia en el control y seguimiento del cumplimiento a la ejecución contractual.

Con los hechos evidenciados, estaríamos frente a la materialización de un riesgo fiscal en este caso radica en el hecho de que se haya aprobado el pago de un contrato por un monto de $456.700.000**,** sin que se haya cumplido con las condiciones y tiempos estipulados en las especificaciones técnicas del mismo. Esto puede implicar que el Fondo Rotatorio de la Policía haya realizado un desembolso de recursos públicos sin recibir la totalidad del servicio pactado. *(Soporte Carpeta Contractual, Tomo 2, fl 226 a 228 Especificaciones Técnicas. fl, 241 Recibido a Satisfacción. fl, 242 a 243 Facturas COINSA SAS. fl, 285 a 306 Informes de Supervisión Diciembre 23, Enero y Febrero 24)*

Además de la potencial materialización de un riesgo tecnológico al quedar desprotegida la red informática y por ende vulnerable la información y dados contenidos en la entidad

5. Conclusiones

- El hallazgo relacionado con el acceso de personal que ya no forma parte de la entidad resalta una deficiencia en los controles de acceso. Esto expone a la entidad a posibles riesgos de seguridad y acceso no autorizado a información confidencial. Es necesario revisar y actualizar los procedimientos para garantizar que solo el personal autorizado pueda acceder a las instalaciones.

- La falta de licenciamiento del antivirus pone en riesgo la protección de los sistemas de la entidad frente a posibles amenazas cibernéticas, como virus o malware. Es crucial que se adquiera y mantenga el software adecuado para proteger los sistemas y datos sensibles de la entidad.

- La falla en el canal dedicado y el backup de internet de la sede principal pone en evidencia una debilidad en la infraestructura tecnológica, lo que genero interrupciones operativas importantes. Se recomienda tomar medidas para garantizar la estabilidad y redundancia de la conectividad a internet.

- Las debilidades en la identificación de vulnerabilidades y amenazas en la arquitectura tecnológica, tanto en hardware como en software, presentan un riesgo elevado de ataques cibernéticos. Es esencial implementar procesos proactivos de detección y mitigación de vulnerabilidades, como auditorías periódicas y el uso de herramientas avanzadas de monitoreo de seguridad.

- Las deficiencias en la supervisión y capacitación del proceso de adquisición, instalación y puesta en marcha del ERP para el Fondo Rotatorio de la Policía indican una falta de control en proyectos

tecnológicos clave. Se debe mejorar la capacitación del personal involucrado y reforzar la supervisión de estos procesos para garantizar su éxito y efectividad.

- La falta de personal especializado en la administración de los sistemas de información afecta la capacidad de la entidad para gestionar, mantener y mejorar sus plataformas tecnológicas. Se recomienda contratar personal capacitado o invertir en la formación continua del equipo existente.

- La no implementación de la APP FORPO PLUS refleja un retraso en la modernización de las herramientas tecnológicas. La puesta en marcha de esta aplicación debe ser prioritaria para optimizar los procesos y mejorar la eficiencia operativa.

- Los protocolos de seguridad insuficientes en los servidores y racks de la entidad aumentan la exposición a posibles brechas de seguridad. Es crucial implementar políticas y procedimientos rigurosos para asegurar físicamente los equipos y protegerlos de accesos no autorizados o daños

- Respecto a la ejecución y cumplimientos de las condiciones pactadas en el contrato O.C 122836-2023, objeto *"servicio de suscripción de créditos nube pública para el desarrollo e implementación de la aplicación móvil y web del Fondo Rotatorio de la Policía"* y 076-6-2023, objeto *"Mantenimiento a la página web, firewall, Inforpo del Fondo Rotatorio de la Policía"*, se podría presentar la materialización de riesgos con incidencias fiscal y tecnológicas; toda vez, que los servicios contratos fueron suspendidos fuera de los términos pactados.

6. Recomendaciones

- Es urgente revisar y actualizar los procedimientos de control de acceso a las instalaciones para evitar la entrada de personal que ya no forma parte de la entidad. Se recomienda mantener una comunicación constante entre el grupo de las tecnologías de la información y las comunicaciones y los proveedores de información, y realizar auditorías periódicas para verificar que sólo el personal autorizado pueda ingresar a áreas sensibles.

- Se debe proceder a la adquisición inmediata de las licencias correspondientes para el antivirus y firewall de la entidad. Es esencial garantizar que todos los sistemas estén protegidos contra amenazas cibernéticas mediante una solución de seguridad confiable y actualizada, con políticas de protección activas en todos los equipos.

- Es fundamental reforzar los protocolos de seguridad tanto física como lógica de los servidores y racks de la entidad. Se deben establecer políticas estrictas para proteger estos activos, incluyendo controles y medidas de seguridad informática, como la encriptación de datos y la monitorización continua de los sistemas.

- Se recomienda realizar una revisión y mejora de la infraestructura tecnológica, específicamente en lo que respecta a la conectividad a internet. Es importante asegurar la continuidad operativa mediante la instalación de un sistema de respaldo para la conexión automática a internet (backup) y la verificación periódica de la estabilidad del canal dedicado y del backup para evitar interrupciones en el servicio.

- Es fundamental mejorar la capacitación del personal involucrado en la gestión de proyectos tecnológicos clave, como la implementación del ERP para el Fondo Rotatorio de la Policía. Además, se recomienda fortalecer la supervisión de estos procesos para asegurar que se lleven a cabo de manera eficiente y con el debido control de calidad, minimizando el riesgo de fallos en su implementación.

- Se recomienda contratar personal especializado en administración de sistemas de información para gestionar adecuadamente los recursos tecnológicos de la entidad. La falta de personal capacitado afecta la capacidad de la entidad para responder a incidentes tecnológicos y gestionar sus sistemas de manera efectiva.

- Es necesario priorizar la implementación de la APP FORPO PLUS, asegurando que se pongan en marcha o en producción para optimizar los procesos operativos de la entidad. Este tipo de herramientas tecnológicas es crucial para mejorar la eficiencia y la modernización de las operaciones diarias.

- Es recomendable desarrollar y poner en práctica un plan de contingencia que contemple situaciones como la caída de la infraestructura tecnológica, pérdida de conectividad o incidentes de seguridad. Este plan debe incluir procedimientos detallados para la recuperación de datos y la reactivación de sistemas críticos, minimizando el impacto en las operaciones de la entidad.

- Actualizar la matriz de riesgos tecnológicos de la entidad

- Establecer controles que permitan contrarrestar proveer y/o mitigar los efectos derivados de la materialización de los riesgos

- Se debe establecer un proceso sistemático para la identificación, evaluación y gestión de vulnerabilidades en la arquitectura tecnológica, tanto en hardware como en software. La implementación de herramientas avanzadas de escaneo de vulnerabilidades, junto con un plan de respuesta ante incidentes, contribuirá a reducir los riesgos.

- Diseñar procedimientos para la realización de análisis y diagnósticos periódicos que permitan tener una visión más clara y precisa del estado de la infraestructura tecnológica del FORPO que permita mejorar los procesos de planeación de necesidades tecnológicas de la entidad anticipando los riesgos.

- Respecto a la ejecución y cumplimientos de las condiciones pactadas en el contrato O.C 122836-2023, objeto *"servicio de suscripción de créditos nube pública para el desarrollo e implementación de la aplicación móvil y web del Fondo Rotatorio de la Policía"* y 076-6-2023, objeto *"Mantenimiento a la página web, firewall, Inforpo del Fondo Rotatorio de la Policía"*, se recomienda a la Dirección iniciar con los trámites administrativos que consideran pertinentes, a fin de determinar las presuntas incidencias fiscales evidenciadas por la Oficina de Control Interno.

7. Anexos

- Excel - Anexos
- PDF - CONCEPTO INFORME FALLO INTERNET
- Word - FUNCIONES ACTUALES PERSONAL GUTIC
- PDF - INFORME GESTIÓN DEL RIESGO SISTEMAS DE INFORMACIÓN
- PDF - RAD. Nro. 242 FORPO - GUTIC - 302-10-29

Elaborado por:
Ingeniero en Sistemas. Rubén Darío Díaz Jiménez
Abogado- Especialista en Contratación Estatal. Juan David Cardona Marín

Revisado y aprobado: Contador Público. **Juan Jairo Gil Rodríguez**, Jefe Oficina de Control Interno.