TIPO DE INFORME:	Preliminar		Final	x

Tabla de contenido

Índice de tablas

Índice de gráficos

1. TÍTULO DE LA AUDITORÍA

Auditoría al Modelo de Privacidad y Seguridad de la Información (MSPI) / Norma ISO 27001: Seguridad de la Información.

2. FECHA DE LA AUDITORÍA

Del 1 de octubre al 30 de noviembre de 2024

3. PERIODO EVALUADO

Del 1 de abril de 2023 al 30 de septiembre de 2024.

4. UNIDAD AUDITADA

Gestión de Recursos Administrativos - Sistemas

5. LÍDER DE LA UNIDAD AUDITADA

Javier Augusto Medina Parra – Subdirector Administrativo / Mauris Antonio Ávila - Profesional de Sistemas.

6. AUDITORES

Diana del Pilar Romero Varila - Jizeth Hael González Ramírez

7. OBJETIVO DE LA AUDITORÍA

Verificar la apropiación de diferentes lineamientos en el marco de la implementación MSPI por parte de los colaboradores de Capital; adicionalmente, verificar si hay posibles riesgos de seguridad de la información que no hayan sido identificados, monitoreados y/o que se hayan materializado en la entidad.

8. ALCANCE DE LA AUDITORÍA

Abarca las actividades ejecutadas para la implementación y sostenibilidad del Modelo de Seguridad y privacidad de la información (MSPI) en Capital para el periodo comprendido entre el 1 de abril de 2023 al 30 de septiembre de 2024.

9. CRITERIOS

- ✓ Constitución política de Colombia

- ✓ 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"
- ✓ Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG - Versión 5 - 2023.
- ✓ Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6
- ✓ NTC ISO 27001:2013/2022.
- ✓ Resolución 500 de 2021 del Ministerio de las TI, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
- ✓ Modelo de Seguridad y Privacidad de la Información (MSPI) - MINTIC
- ✓ Manual metodológico para la Administración del riesgo - Canal Capital.
- ✓ Política de administración de riesgos - Canal Capital.
- ✓ Procedimientos, manuales, políticas, guías y demás documentos del Sistema Integrado de Gestión de Capital relacionados con el objetivo de la auditoría.
- ✓ Las demás normas pertinentes relacionadas con el objetivo de la auditoría.

10. METODOLOGÍA

De conformidad con la Guía de Auditoría Interna basada en riesgos para entidades públicas expedida por el Departamento Administrativo de la Función Pública – DAFP (versión 4, 2020), concordante con los lineamientos señalados en la norma ISO 19011-2018 y demás lineamientos establecidos al interior de Capital para el ejercicio de la auditoría interna, se emplearon los procesos de Planificación, Ejecución, Informe de Auditoría y Seguimiento del progreso de la auditoría interna basada en riesgos, de la siguiente manera:

Planificación

- Elaboración del Plan de Auditoría Individual [CCSE-FT-012].
- Definición del objetivo, alcance, riesgos, recursos y programa de trabajo.
- Preparación de papeles de trabajo de la revisión documental y procedimental sobre la unidad auditada.
- Preparación de solicitudes de información a la unidad auditada y áreas involucradas con el proceso.

Ejecución

- Solicitud de información mediante correo electrónico a las áreas de Contratación y Técnica.
- Solicitud de información al área de Sistemas a través del memorando 887 del 18 de octubre de 2024.

- Revisión documental de la unidad auditable asociados a la implementación del modelo de privacidad y seguridad de la información – ISO 27001.
- Entrevista a funcionarios y contratistas de Capital, sobre lineamientos del Manual de Políticas Complementarias.
- Solicitud de diligenciamiento de encuestas sobre riesgos de seguridad de la información a los líderes de proceso del canal.
- Análisis de la información remitida (soportes) por las unidades auditables, en herramienta digital (Drive), información tomada durante las entrevistas, así como de correos electrónicos, con el fin de validar el cumplimiento de las disposiciones legales vigentes y demás normas aplicables en materia de ISO 27001 – Modelo MSPI.

Informe de Auditoría

- Consolidación y entrega del informe preliminar de auditoría a los líderes y/o responsables de los procesos auditados en el formato CCSE-FT-016.
- Análisis de las respuestas remitidas por los líderes de proceso y equipos de trabajo frente a las observaciones señalas en el informe preliminar.
- Consolidación y entrega del informe final de auditoría a la Gerente, líderes y/o responsables de la unidad auditable y procesos adyacentes evaluados, en los formatos dispuestos para tal fin [CCSE-FT-016] y [CCSE-FT-024].

Seguimiento del progreso

- Solicitud de la formulación del Plan de Mejoramiento en el formato CCSE-FT-001 frente a las actividades que eliminen las causas de las observaciones encontradas.
- Acompañamiento de la formulación del Plan de Mejoramiento al área.
- Análisis de la evaluación de la auditoría CCSE-FT-018 y presentación al Comité Institucional de Coordinación de Control Interno para implementación de mejoras en el ejercicio de auditoría.

11. SITUACIONES GENERALES

11.1. DOCUMENTOS DEL PROCESO

Durante el desarrollo de la auditoría se adelantó la revisión de los documentos:

- **Manual de Políticas Complementarias, versión 3 del 10/12/2024:**
  Se identifican las siguientes debilidades:

    - En las definiciones de algunos términos relacionados en el glosario, así como que no se relaciona la fuente de información de donde fue extraída.

- De igual manera, durante las pruebas adelantadas con los diferentes responsables mencionados en el documento (Servicios Administrativos – Recursos Humanos), se indicó que no fueron consultados durante el levantamiento del documento, respecto a los lineamientos determinados.

Por lo anterior, deberá revisarse y ajustarse en el documento que se viene construyendo de actualización del publicado vigente, de manera que se revisen las obligaciones identificadas de cada área involucrada, teniendo en cuenta lo que efectivamente se adelanta por cada una.

- Guía de incidentes de reporte de incidentes de seguridad, versión 3 del 14/09/2023. Numeral 11.4. del presente informe.

11.2. AUTODIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Teniendo en cuenta las actividades formuladas como resultado de la auditoría adelantada al proceso de Sistemas de Gestión de Seguridad y Salud en el trabajo - SGSST y Norma ISO 27001: Seguridad de la Información efectuada en la vigencia 2023, y que a la fecha se encuentran en proceso de ejecución al interior del Plan de Mejoramiento por Procesos, se adelanta la revisión de los avances alcanzados durante el periodo comprendido entre el 1 de abril de 2023 y el 30 de septiembre de 2024.

Para lo anterior, se realizó la revisión de los resultados consignados por parte del área de Sistemas en el *autodiagnóstico del MSPI* del primer semestre de 2024 realizado en el instrumento del MinTic, encontrando que:

a. Se registran controles calificados entre el 60% y 90% sin reporte de evidencia o identificación de las brechas existentes al interior del canal respecto a lo requerido en la norma, lo cual fue mencionado en la auditoría de la vigencia anterior; sin embargo, a la fecha de evaluación no se han tenido en cuenta las recomendaciones dadas sobre el diligenciamiento de la herramienta [actividad formulada en plan de mejoramiento], ejemplo de lo anterior:

Ilustración 1. Herramienta MSPI (junio 2024)

ID. ITEM	CARGO	ITEM	ISO	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 2700
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN						
AD.2.1.2	Responsable de SI	Separación de deberes / tareas	A.6.1.2			80
AD.4.2	**Responsable de SI**	**Clasificación de información**	**A.8.2**			87
AD.4.2.2	Responsable de SI	Etiquetado de la información	A.8.2.2			60

b. Se identifica el cumplimiento al 100% de 12 controles y al 80% de 3 controles de la norma ISO 27001:2013, para los cuales se indicó que el control se cumplía a través de los lineamientos y controles definidos en el *Manual de políticas complementarias* y la Guía de Reporte de Incidentes de Seguridad, como se resume a continuación:

Tabla 1. Controles con calificación superior . MSPI

Identificación del control – Herramienta MinTic	Ítem	Descripción	Porcentaje de Cumplimiento de Capital
AD.1.2	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	100%
AD.2.1.3	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).	100%
AD.2.2.1	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	100%
AD.3.2.3	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	100%
AD.4.1.3	Uso aceptable de los activos	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.	100%

Identificación del control – Herramienta MinTic	Ítem	Descripción	Porcentaje de Cumplimiento de Capital
T.1.1.2	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	100%
T.1.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	100%
T.1.4.4	Uso de programas utilitarios privilegiados	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	100%
T.3.1.1	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	100%
T.3.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	100%
T.3.1.5	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	100%
T.7.1.1	Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	100%
T.3.1.2	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	80%
T.3.1.6	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	80%
T.3.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	80%

Sin embargo, no se indica en la herramienta diligenciada de qué manera se cumple el control al 100%, y para aquellos controles con calificación inferior a dicho valor, no se mencionan las actividades faltantes que permitan dar cabal cumplimiento a lo requerido normativamente. Lo anterior, mencionado durante la auditoría ejecutada en la vigencia 2023, y sobre lo cual no se han adelantado las mejoras formuladas en el plan de mejoramiento por procesos.

Es importante que se ajuste la debilidad mencionada en cuanto al diligenciamiento de la herramienta de autodiagnóstico en el próximo reporte del plan de mejoramiento por procesos [corte a 31 de diciembre de 2024], de manera que se pueda adelantar el cierre efectivo de lo formulado.

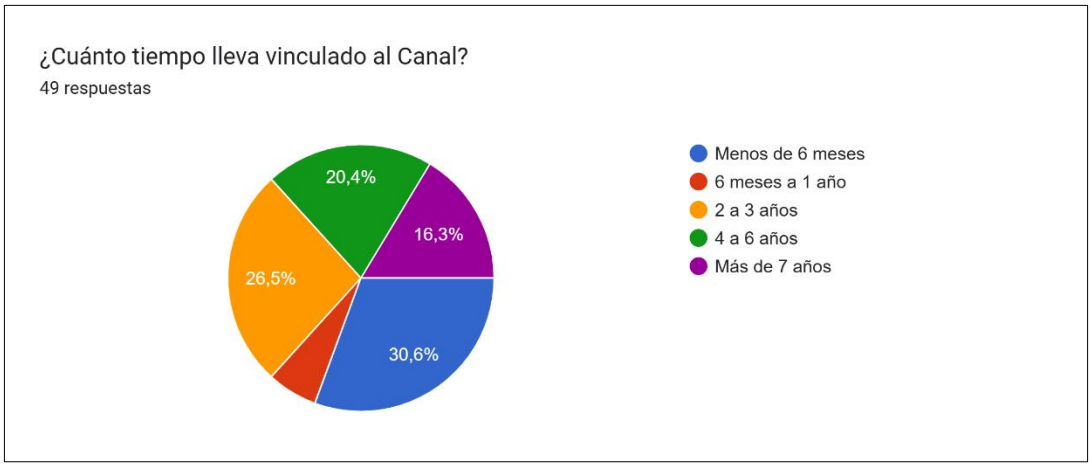
11.3. EVALUACIÓN DEL MANUAL DE POLÍTICAS COMPLEMENTARIAS

De conformidad con lo mencionado en el numeral anterior, se adelantaron pruebas que permitieran verificar si los controles descritos en el “Manual de políticas complementarias” en su versión 3 del 10 de diciembre de 2021 y la “Guía de incidentes de reporte de incidentes de seguridad” son conocidos y ejecutados por los responsables definidos en los lineamientos, obteniendo los siguientes resultados:

A. Resultados evaluación normas - colaboradores de Capital

Se adelantó la consolidación del formulario prueba "Manual de Políticas Complementarias", cuyo objetivo se enmarcaba en conocer el nivel de implementación en Capital por parte de los contratistas, colaboradores y terceros respecto a las *“Normas Dirigidas a Todos los Colaboradores, Contratistas y Terceros”*.

Teniendo en cuenta lo indicado previamente, se recopilaron (49) respuestas dadas por los colaboradores vinculados a la entidad con diferentes tiempos de vinculación a la entidad, establecidos en rangos desde menos de seis (6) meses a más de siete (7) años como se presenta a continuación:



Fuente: Google forms – Manual de políticas complementarias

Sobre las respuestas obtenidas de los colaboradores mencionados previamente en el formulario respecto a las normas generales para el uso de dispositivos móviles no corporativos se destaca que:

- El 56.3% de los colaboradores indican que al término de su vinculación se adelantó la devolución del carné, tarjeta de acceso u otro dispositivo de identificación entregado.

- Para ciertas políticas de transferencia de información algunos de los colaboradores cierran el correo al término de la jornada, algunos indican que adelantan adicionalmente:

  - Análisis de virus sobre documentos adjuntos recibidos por correo electrónico
  - Apaga el equipo asignado al término de la jornada.
  - Realiza análisis de virus sobre dispositivos externos (USB, DVD, CD, u otro) requerido, y, de igual manera no adelanta remisión de cadenas políticas, religiosas o publicitarias desde el correo institucional, así como tampoco adelanta actividades personales haciendo uso del correo institucional.

- Respecto a las políticas de mantenimiento de escritorio y pantalla limpia los colaboradores mantienen los puestos de trabajo libres de elementos que limitan el movimiento, que bloquean los equipos al momento de levantarse del puesto, y, que no cuentan con stickers, afiches u otros elementos no autorizados en los componentes físicos de los puestos de trabajo.

Por otro lado, respecto a los diferentes lineamientos considerados en el documento, se indicó por parte de los colaboradores que:

- El 49% del total de los respondientes **no** conoce el documento “Manual de Políticas Complementarias”.

- El mismo porcentaje (49%) **no** ha recibido capacitaciones, socializaciones u otras respecto a los lineamientos consignados en el documento.

- Algunos de los respondientes desconocen lineamientos relacionados con el uso de redes inalámbricas únicamente para actividades laborales, que no debe adelantarse modificaciones a la configuración de los equipos de la entidad, que no debe guardarse información personal en los equipos asignados por Capital y que los dispositivos móviles asignados por la entidad no deben conectarse a redes públicas o gratuitas.

- Respecto a las normas generales de uso de dispositivos móviles no corporativos definidos en el manual, se desconoce la normatividad dada por Capital para el uso de dispositivos móviles, las condiciones de legalidad con las que debe contar el software instalado en los dispositivos propios de los contratistas vinculados a la entidad, el evitar el almacenamiento de información de propiedad del Canal en dispositivos propios, el requerimiento de contar con la instalación, licenciamiento y

actualización de antivirus en los equipos de cómputo, así como que no debe instalarse aplicaciones que ponga en riesgo la seguridad de la información de la entidad.

- Que respecto al lineamiento *"Al finalizar la vinculación con Capital, se obliga al colaborador permitir la revisión final del dispositivo móvil con el fin de borrar de forma segura los recursos de red y la información propia de la entidad"*, el 56.3% de los respondientes indica que no se adelantó dicha revisión y que el 35.4% de los contratistas considera que lo definido "No aplica".

- Respecto a las normas generales para el *Uso de Dispositivos Móviles no Corporativos*, dado que no se establece claridad sobre cuáles son los acuerdos de confidencialidad exigidos por Capital, en dónde se documentan o si son adicionales a los determinados en las minutas de la entidad, los colaboradores que respondieron la prueba indican que al momento de la vinculación **no** adelantaron la suscripción adicional de acuerdos de confidencialidad y no divulgación de la información.

- Algunos de los respondientes desconoce los lineamientos definidos en el apartado de normas *Generales para el Teletrabajo y Conexiones Remotas* como por ejemplo: mantener la confidencialidad de la información, que toda la información gestionada por Capital debe ser utilizada para cumplir con sus obligaciones, desconoce cómo debe verificar que las conexiones sean cerradas de manera adecuada, que las conexiones deben establecerse por medio de VPN seguras, y, que no debe adelantarse el uso de conexiones remotas sin que se autorice por parte del supervisor del contrato y el área de Sistemas.

  Aunado a lo anterior, se indica por parte de los colaboradores que desconoce los lineamientos de control de acceso respecto a que debe hacerse responsable de las actividades efectuadas sobre los recursos compartidos e infraestructura tecnológica, sobre el hacerse cargo sobre los usuarios y contraseñas que le son asignados al momento de la vinculación, que no debe compartirse la cuenta de usuario a recursos de red, infraestructura, correo u otro asignado, y, que no debe compartirse o hacer préstamo del carné u otro recurso de identificación asignado para uso personal.

- A pesar de los lineamientos que se ejecutan por parte de los colaboradores, se hace necesario que se revisen aspectos respecto a la política para transferencia de información identificada, teniendo en cuenta que no se adelanta el cambio de contraseña cada 30 días, que en una

proporción similar a aquellos que dan cumplimiento, se indica que algunos no adelantan análisis de virus sobre documentos adjuntos recibidos por correo electrónico, no apagan el equipo asignado al término de la jornada, no realizan análisis de virus sobre dispositivos externos (USB, DVD, CD, u otro) requerido, y, que ha adelantado la remisión de archivos ejecutables por correo electrónico.

- El 65.3% desconoce las normas existentes para adelantar Backup y/o restauración de información, lo que se articula con el 83.7% de los colaboradores que no adelanta solicitudes de respaldo de información.

- Por último, se identificó que el 32% de colaboradores encuestados ingieren bebidas y comidas en los puestos de trabajo, aun cuando es una prohibición estipulada en el Manual, no se observan piezas informativas al respecto, así como tampoco socializaciones por parte de los responsables.

Lo anterior, deberá revisarse de manera que se establezcan lineamientos claros, principalmente en lo que respecta a las políticas que cuentan con lenguaje técnico (principios de lenguaje claro), así como que estos sean socializados (interiorizados) en todos los niveles organizacionales haciendo uso de los diferentes canales de comunicación del canal, así como de la infraestructura tecnológica disponible como por ejemplo: piezas compartidas vía Whatsapp (grupo de comunicaciones), fondos de pantalla de los equipos de cómputo (corporativos), carteleras físicas y digitales, redes sociales, piezas exclusivas vía correo electrónico (facilitando visualización e interiorización), socializaciones cortas con Tips en materia de lineamientos establecidos en materia de seguridad y privacidad de la información, así como socialización de dichos lineamientos dentro de las jornadas y comunicaciones de inducción y/o bienvenida remitidas a los colaboradores que se vinculan a la entidad.

B. Resultados evaluación de normas - Servicios Administrativos

Se adelantó la construcción de la prueba "Manual de Políticas Complementarias" – Administrativa con el fin de conocer el nivel de conocimiento e implementación de los lineamientos determinados en el documentos sobre actividades ejecutadas por el área, obteniendo como resultados:

- El área desconoce el documento, así como las obligaciones asignadas; sin embargo, se cumplen algunas de estas como parte del quehacer diario del proceso, como por ejemplo:

- Respecto a la norma *"Velar por que las estaciones de trabajo e Infraestructura Tecnológica de propiedad de Capital posean pólizas de seguro vigentes"*, Capital incluye todos los bienes de Propiedad. Planta y Equipo en la póliza Todo Riesgo de Daño Material de la entidad desde el momento de realizar la entrada al almacén. Así mismo, se maneja un cronograma de contratación del área para velar que el contrato de seguros se encuentre vigente y sin interrupciones. **(Se cumple)**

- Las normas de *"Mantener en buen funcionamiento los controles de acceso instalados en el ingreso y salida de los centros de datos y cableado de Capital"* y *"Velar por el correcto funcionamiento de las cámaras de seguridad instaladas en los centros de datos y cableado"*, se adelanta mediante el contrato de servicio de vigilancia y seguridad privada, el cual se adelanta con la empresa TAC – Seguridad privada. **(Se cumple)**

Adicionalmente, se presentan debilidades en el establecimiento de normas, teniendo en cuenta que:

- Sobre la norma *"Garantizar la asignación de escarapelas de identificación a todos los Colaboradores, Contratistas y Terceros para el desplazamiento por las instalaciones de la entidad"*, el área de Servicios Administrativos no realiza la asignación de escarapelas de identificación a colaboradores, contratistas o visitantes. En la actualidad se realiza la entrega de carnet con tarjetas control de acceso para colaboradores y/o contratistas y para visitantes, se asigna carnet de identificación como visitante. **(No se aplica)**

- Sobre la norma *"Señalizar de forma adecuada los elementos de seguridad física que se encuentren al interior de los centros de datos y cableado"*. Se indica por el área que en la actualidad el centro de datos de la sede calle 26 cuenta con un biométrico para el control de entrada de funcionarios. En todo caso, es importante especificar a que se refiere estos elementos. **(No es entendible)**

- Respecto a *"Proveer y velar por el correcto funcionamiento de extintores de incendio probados y verificados mínimo 3 veces en el año"*, se indica que el área de Servicios Administrativos no realiza la revisión del correcto funcionamiento de los extintores de la entidad. **(No se aplica)**

Lo anterior, denota la falta de articulación en la identificación de obligaciones, así como el poco conocimiento de las actividades adelantadas por cada proceso y la necesidad de mejorar la interrelación al interior de la entidad. Por

lo tanto, se recomienda se adelanten mesas de trabajo, socialización del documento, solicitud de información respecto a las actividades ejecutadas por cada área, con el fin de que estas sean acordes con la realidad de la entidad, lo anterior previo a su adopción e integración como documento oficial el Sistema de gestión del Ca

C. Resultados evaluación de normas - Recursos Humanos

Se adelantó la prueba "Manual de Políticas Complementarias" - Recursos Humanos, con el fin de identificar la interiorización y conocimiento de las normas asignadas al área en el numeral 5.2. Política de seguridad de los recursos humanos del documento citado. Como resultado de lo anterior se obtuvieron los siguientes resultados:

- Respecto a la norma *"El área de Recursos Humanos y Gestión Contractual, deben establecer mecanismos o controles necesarios para proteger la confidencialidad y privacidad de la información contenida en las historias laborales y expedientes contractuales"*, el área de Recursos Humanos cuenta con carpeta en drive [esta sin permisos], ERP de Sistemas, contratos laborales cláusula de confidencialidad, en todas las encuestas ley habeas, bases de datos solo compartida con las personas del área. **(Se aplica)**

- Sobre las normas contenidas en el numeral 5.2.3. Terminación y cambio de empleo, se desconocen las normas identificadas:

  - Asegurarse que el trabajador entrega la información propiedad de Capital que se encuentra bajo su gestión al momento del retiro, investigación, inhabilidades o cambio de funciones.
  - Recoger y custodiar la información de Capital una vez terminado o cedido el contrato.
  - Solicita la creación de copia de respaldo del correo electrónico.

Lo anterior, dado que no fueron consultadas las normas asignadas el área, así como tampoco se separan aquellas que le corresponden al profesional especializado de recursos humanos, al no ser claras respecto al responsable.

- Sobre la norma definida *"En periodo de vacaciones se debe informar al área de sistemas para que esta proceda a re-dirigir los correos a la cuenta de correo del funcionario que durante este periodo de tiempo sea asignado para el desarrollo de las actividades encomendadas"*, se remitió por parte del área la relación de correos en los cuales se comunicó la salida a vacaciones de los trabajadores de la entidad, sobre los cuales se tomó una

muestra de (10) correos, de los cuales, cinco (5) corresponden a la vigencia 2023 y cinco (5) de la presente [2024]; sin embargo, no es posible evidenciar que haya sido informada el área de Sistemas dentro de los correos. Por lo anterior, es importante que se coordinen acciones que permitan adelantar de manera clara las normas mencionadas. Se presentan a continuación ejemplos de lo indicado:

Ilustración 2. Correo vacaciones 2023

Disfrute de Vacaciones
5 mensajes

Carolina Vargas García <carolina.vargas@canalcapital.gov.co> 31 de octubre de 2023, 9:14
Para: Personal Planta <personalplantacc@canalcapital.gov.co>
Cc: Rocio Capador Riaño <rocio.capador@canalcapital.gov.co>, Paloma Solano López <paloma.solano@canalcapital.gov.co>, Luz Edid Suescún Cárdenas <luz.suescun@canalcapital.gov.co>, Vigilancia Canal Capital <vigilancia@canalcapital.gov.co>

Fuente: Correos remitidos por el área de RRHH

Ilustración 3. Correo vacaciones 2024

Disfrute de vacaciones
2 mensajes

Carolina Vargas García <carolina.vargas@canalcapital.gov.co> 27 de mayo de 2024, 11:46
Para: Personal Planta <personalplantacc@canalcapital.gov.co>
Cc: Natalia Paola Porras Cifuentes <natalia.porras@canalcapital.gov.co>, Rocio Capador Riaño <rocio.capador@canalcapital.gov.co>, Vigilancia Canal Capital <vigilancia@canalcapital.gov.co>, Laura María Montoya Vélez <laura.montoya@canalcapital.gov.co>, Tiziana Arevalo Rodríguez <tiziana.arevalo@canalcapital.gov.co>

Fuente: Correos remitidos por el área de RRHH

D. Resultados evaluación de normas – área Jurídica

Como resultado de la consulta de información con relación a las normas asignadas al área, se mencionó el desconocimiento de lo consignado; sin embargo, respecto a las normas:

- Velar por que todos los requerimientos legales y condiciones establecidos al momento de la contratación por la entidad sean cumplidos por parte de los proveedores. Se indicó por parte del área que:

> *"se concretan en la revisión que se efectúa de toda la documentación requerida y aportada por el futuro Contratista, para lo cual, se verifican que las cotizaciones o propuestas presentadas se ajusten a las exigencias de la Entidad, para lo cual, se apoya en el concepto técnico de las áreas; así mismo, se procede a examinar toda la documentación para determinar que el futuro contratista no se halle incurso en inhabilidades o incompatibilidades que no le permitan contratar con una entidad estatal y de otra parte, en caso de que el futuro proveedor tenga una condición especial, como la de proveedor exclusivo, se requiere para que mediante certificaciones demuestre tal condición e igualmente, si la actividad ejercida o los bienes ofrecidos por el cotizante son regulados por el Gobierno se*

procederá a verificar que efectivamente se ajusten a la regulación vigente y presenten la documentación que así lo pruebe.

De otra parte, la entidad establece en el contrato y especialmente, en la cláusula de obligaciones específicas a cargo del Contratista, la realización de todas las actividades que le permitan adelantar la ejecución del objeto contractual y de esta forma, la entidad pueda cubrir sus necesidades de bienes y servicios".

- El área de Recursos Humanos y Gestión Contractual, deben establecer mecanismos o controles necesarios para proteger la confidencialidad y privacidad de la información contenida en las historias laborales y expedientes contractuales. Sobre lo cual se respondió que:

"Sobre el particular es preciso señalar inicialmente que, por regla general, la información contendida en los expedientes contractuales es de carácter público, sin reserva, y en ese sentido lo señala el artículo 2 de la Ley 1712 de 2014, la cual prevé que: "Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley."

En concordancia, con ese principio universal, el artículo 10 de la citada norma señala que "En el caso de la información de contratos indicada en el artículo 9 literal e), tratándose de contrataciones sometidas al régimen de contratación estatal, cada entidad publicará en el medio electrónico institucional sus contrataciones en curso y un vínculo al sistema electrónico para la contratación pública o el que haga sus veces, a través del cual podrá accederse directamente a la información correspondiente al respectivo proceso contractual, en aquellos que se encuentren sometidas a dicho sistema, sin excepción.", en razón de lo cual, las entidades estatales nos vemos obligadas a publicar nuestros procesos contractuales en plataformas dispuestas para ello, tal como SECOP y en nuestras páginas web.

Ahora bien, en el entendido que el literal c) del artículo 6 de la Ley 1712 2014 define como: "c) Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;"

Y a su vez, el numeral 3 del artículo 24 de la Ley 1437 de 2011 indica que "Solo lo tendrán carácter reservado las informaciones y documentos expresamente sometidos a reserva por la Constitución Política o la ley, y en especial: (…)

3. Los que involucren derechos a la privacidad e intimidad de las personas, incluidas en las hojas de vida, la historia laboral y los expedientes pensionales y demás registros de personal que obren en los archivos de las instituciones públicas o privadas, así como la historia clínica."

En razón de la normatividad anteriormente señalada, se tiene que ante el pedido de información sobre las personas que han sido o son nuestros contratistas y con el objeto de evitarle daños, se ha solicitado autorización a la persona que pertenece esa información, en el entendido que está en custodia del Canal en razón de la relación derivada de la suscripción de los contratos de prestación de servicios profesionales o de apoyo a la gestión, por lo cual, se gestiona una autorización para que el Canal pueda entregar la información solicitada, lo cual ha sucedido en los casos de confirmación de vinculación al Canal mediante la figura del contratos de prestación de servicios.

De igual forma, desde el área de contratación se hizo una actualización a los formatos "listado documentos para contratar" tanto de persona jurídica como natural, estableciendo luego de un análisis, la calidad de documentos públicos y privados que se cargan en la plataforma Secop II, con base en lo establecido en la Ley 1712 2014.

Si bien se identifica que se adelantan acciones que dan cumplimiento a las normas definidas para el área, se hace necesario que se socialicen, y se complementen en el marco de lo que Capital ha venido implementando en materia de seguridad y privacidad de la información desde la protección de información de la gestión de contratación tanto del personal de planta como de los contratistas que prestan sus servicios a la entidad, contemplando los lineamientos y normatividad vigente.

E. Resultados evaluación de normas – Sistemas

Se adelantó solicitud de información sobre las normas establecidas para el área de Sistemas, así como de normas que deben ser aseguradas por el área, obteniendo como resultados algunas diferencias entre lo documentado y lo ejecutado como parte de los controles identificados en el marco del Modelo de Seguridad y Privacidad de la Información – MSPI para Capital. Lo anterior, teniendo en cuenta que:

Tabla 2. Normas - área de Sistemas

Norma identificada	¿Se cumple?		Observación
	Si	No	
Verificar el cumplimiento del Manual de Políticas Complementarias de Seguridad de la Información.			Se remite por parte del área de Sistemas la herramienta de diagnóstico del MSPI, así como el informe de controles de seguridad de la información implementados en Canal Capital de enero a junio de 2024; sin embargo, no se observa que haya sido socializado o remitido con conclusiones y recomendaciones, así como tampoco se observa que se incorpore la totalidad de normas relacionadas en el documento mencionado.
Configurar los dispositivos móviles de la entidad para que estos se bloqueen		x	Se indica por parte del área de Sistemas: *La política actual de bloqueo del Directorio Activo y del Servidor de Dominio para equipos*

Norma identificada	¿Se cumple?		Observación
	Si	No	
automáticamente después de un tiempo de inactividad no mayor a 30 segundos.			*portátiles y de escritorio está configurada para activarse automáticamente tras 3 minutos de inactividad. Una vez superado este límite, el equipo se bloqueará de forma automática.*
Dar a conocer las Políticas de Seguridad de la Información de Capital y asegurar que se cumpla esta normatividad.		x	Se remite por parte del área dos (2) listados de asistencia que no cuentan con encabezado o asunto al cual se pueda relacionar la temática tratada, así como un correo del 11 de septiembre de consulta de la Resolución 119 de 2024 *"Por la cual se adopta la Política de Seguridad y Privacidad de la Información de Canal Capital";* sin embargo, no se remiten documentos u otros que permitan evidenciar que se adelanta la revisión del cumplimiento de la normatividad vigente aplicable.
Asegurarse que el software instalado en los dispositivos móviles no corporativos cumpla con las normas de propiedad intelectual y su debida autenticidad.		x	Se indica por parte del área que: ***a.*** *El área de sistemas no contempla un procedimiento para la revisión de equipos no corporativos respecto al uso de software licenciado, debido a la autonomía en la propiedad, uso y privacidad de la información de dichos equipos. Por ello, se desincentiva el uso de software de pago, como Microsoft Office, Adobe, entre otros programas de oficina, fomentando el uso de los servicios adquiridos por la entidad.* ***b.*** *Además, en las minutas contractuales de la entidad se establece la siguiente obligación:* *(...)OBLIGACIONES GENERALES DEL CONTRATISTA: EL CONTRATISTA se obliga con CANAL CAPITAL a: (...) No instalar ni utilizar ningún software sin la autorización previa y escrita del área de sistemas del Canal; así mismo, responder y hacer buen uso de los bienes y recursos tecnológicos (hardware y software), y hacer entrega de los mismos en el estado en que los recibió.* Lo anterior, si bien hace parte de las acciones preventivas que permiten mitigar el uso de software que no esté debidamente licenciado **no** soporta adecuadamente que se adelanten actividades que permitan **asegurar** que los dispositivos que son propiedad de los colaboradores cuentan con el software bajo condiciones de autenticidad requeridas por la entidad, mencionadas en el Manual de Políticas Complementarias.

Norma identificada	¿Se cumple?		Observación
	Si	No	
Auditar la información almacenada en las unidades de red compartidas de la entidad con el fin de controlar y no permitir el almacenamiento de información que no sea estrictamente laboral.		x	Se indica por parte de Sistemas que: *El área de sistemas no audita el contenido de la información almacenada por los usuarios, ya que esta es responsabilidad exclusiva de cada funcionario, colaborador y contratista (propietarios y custodios de los activos de información)...*, lo cual es incoherente con lo identificado en el documento normalizado en el Sistema de Gestión de la entidad. Por lo que **no** es posible determinar que se dé cabal cumplimiento a la norma identificada.
Al finalizar la vinculación con Capital, se obliga al colaborador permitir la revisión final del dispositivo móvil con el fin de borrar de forma segura los recursos de red y la información propia de la entidad.		x	Se menciona por el área de Sistemas que: *No es necesario, ya que tanto la Política de Seguridad y Privacidad de la Información como la Guía de Conexiones Remotas establecen que los recursos deben gestionarse a través del Drive Institucional o las Carpetas de Red Compartidas. En este sentido, los equipos no corporativos se utilizan únicamente como una interfaz para conectarse de forma remota a los recursos de la entidad.* *Una vez finalizada la vinculación de los colaboradores, contratistas o terceros, se deshabilitan todos los accesos otorgados, lo que incluye la desactivación del usuario de Windows, el correo institucional y el acceso VPN (mediante el proceso de solicitud de Servicios TIC y Paz y Salvo). De este modo, aunque las unidades de red puedan aparecer en los equipos personales, no será posible acceder a los recursos compartidos o al Drive Institucional.* Lo anterior permite evidenciar la necesidad de revisar las diferencias entre lo documentado y lo ejecutado en la entidad, teniendo en cuenta que los colaboradores cuentan con dispositivos no corporativos en los cuales es posible almacenar información propia de la entidad, acceder a copias de respaldo de correos electrónicos u otros.
Llevar una bitácora donde se evidencie las conexiones remotas autorizadas y el motivo por el cual se realizó.		x	Se indica por parte del área que: *El área de sistemas habilita las conexiones remotas a solicitud de colaboradores y contratistas, ya sea a través del formulario de servicios TIC o por correo electrónico cuando así se requiere.* Una vez revisados los soportes remitidos no se observa que se haya dado respuesta a las solicitudes de conexión remota con el motivo por el cual se realizó, así como tampoco se cuenta con la bitácora mencionada en el manual, por lo cual se presentan

Norma identificada	¿Se cumple?		Observación
	Si	No	
			inconsistencias entre lo documentado y lo ejecutado por el área; así mismo, se identifican debilidades ya que no se indica quién debe ser el responsable de solicitar dicho servicio, tiempo de respuesta u otro que complemente el lineamiento a cumplir para conexiones remotas.
Definir estándares para la aplicación de controles criptográficos.			El área menciona como estándares: la protección de la información en el ERP de Canal Capital, dentro del cual se establecen el cifrado de datos en reposo, cifrado de datos en tránsito, gestión de accesos y autenticación, monitoreo y registro de accesos, respaldo y recuperación de datos, seguridad a nivel servidor y pruebas y vulnerabilidad y auditorías. Sin embargo, dentro de la herramienta de diagnóstico de MSPI se indica que el control de reglamentación de controles criptográficos **no aplica** para la entidad. Se reitera adelantar la revisión de los controles relacionados, aplicables e implementados al interior de la entidad, de manera que la información presentada sea coherente con lo que se ejecuta al interior de la entidad en materia de implementación de los controles de la norma ISO 27001.
Las firmas de correo electrónico deben estar estandarizadas y no deben ser modificadas por ningún motivo.		x	Se relaciona por parte del área el enlace de Google Workspace, y se menciona que *su diseño y uso están sujetos a los lineamientos establecidos por el área de Comunicaciones Internas*. Sin embargo, no se relacionan los soportes mediante los cuales se adelantó la socialización a los colaboradores de Capital, de manera que las firmas se estandaricen, por lo que **no** es posible evidenciar el cumplimiento de la norma relacionada en el manual.
Generar campañas para concientizar con respecto a las precauciones de uso que se deben tener sobre el correo electrónico.			El área de Sistemas indica que: *Durante el periodo del reporte se han realizado diferentes estrategias de socialización, capacitación y divulgación del uso adecuado de los recursos tecnológicos entre ellos el correo electrónico*. Se observa la solicitud de emisión de piezas informativas respecto a temas de seguridad de la información, listados de asistencia a jornadas de capacitación (sin que relacione a qué jornada corresponde el soporte), así como correos de alerta emitidos por parte del área respecto a los correos sospechosos; sin embargo, se recomienda al área fortalecer las

Norma identificada	¿Se cumple?		Observación
	Si	No	
			campañas adelantadas de manera que se trate de manera clara el tema de la norma identificada en materia de *"precauciones de uso que se deben tener sobre el correo electrónico"*.
Mantener mecanismos y controles que obliguen al usuario a cambiar sus contraseñas de accesos a red como mínimo cada 45 días.		x	El área de Sistemas indica en la respuesta a la solicitud de información que: *La configuración de la directiva de contraseñas en el controlador de dominio (Active Directory), en la sección de administración de Directivas de Grupo, establece una vigencia máxima de 90 días para las contraseñas.* Lo anterior, **no** permite observar que se adelante el cambio de contraseñas de conformidad con la norma identificada en el documento, por lo que es importante que se adelante la revisión de lineamientos presentados en el documento con el fin de que sea coherente lo documentado con lo implementado.
Realizar periódicamente mantenimientos preventivos y correctivos de la Infraestructura Tecnológica.	x		Se remiten los informes mensuales y anuales adelantados por el proveedor Web Solutions T.I. desde la vigencia 2022 respecto a los mantenimientos de software y hardware a los equipos de Capital teniendo en cuenta el inventario del parque informático asignado para la labor mensual.
Asegurar la adquisición de herramientas tales como antivirus y antispyware que permitan proteger y asegurar la seguridad de las estaciones de trabajo y servidores donde esta almacenada información de la entidad.			Se adelantó la adquisición del software LICENCIA ANTIVIRUS CLOUD GRAVITYZONE ELITE - GOV R BITDEFENDER (ENDPOINT CLOUD BITDEFENDER GRAVITYZONE ELITE). Se consulta con el área de Sistemas, para lo cual se indica la adquisición de 250 endpoints, 88 servidores y 375 buzones. El reporte se observa en la **Ilustración 4. Reporte antivirus.**
Generar reportes diarios de las copias de seguridad realizadas para así conocer el estado de estas.			Como respuesta al informe preliminar de auditoría se adelantó una mesa de trabajo el 6 de diciembre de 2024, en la cual, posterior a la revisión y análisis de lo observado, se estableció la necesidad de revisar y ajustar los lineamientos del proceso de copias de seguridad en el manual de políticas complementarias de seguridad de la información, para que quede claro y especifico en dónde se encuentra documentado el proceso mencionado y la razón por la cual se genera el reporte de las copias mencionadas en el manual evaluado.

Norma identificada	¿Se cumple?		Observación
	Si	No	
			Lo indicado, teniendo en cuenta que durante la revisión de los soportes entregados en la auditoría, se encontró que en el listado relacionado en la bitácora, se identifican (19) trabajos de copias de seguridad del periodo comprendido entre el 12/04/2023 y el 20/05/2024, así como el **reporte** de información de resumen de trabajos emitido por el programa "Veritas Backup Exe" no se adelanta diario, de conformidad con las normas responsabilidad del área de sistemas señaladas en el manual de políticas complementarias.
Realizar pruebas de restauración de información.			Respecto a la norma identificada en el manual para el área de tecnología no se establece de manera clara al área que se refiere; por lo anterior, se adelantó la consulta al área Técnica sobre el ejercicio presentándose confusiones respecto a la solicitud de información y desconocimiento del documento mencionado, de igual manera se consultó al área de Sistemas, siendo remitidos los soportes de restauraciones efectuadas durante el periodo comprendido entre el 4 de febrero de 2023 y 29 de septiembre de 2024. Teniendo en cuenta lo anterior, se recomienda que se revise el documento de manera que se establezcan las normas con responsabilidades claras, periodicidades, se adelante la consulta de obligaciones con las áreas involucradas y se documente con coherencia lo que se ejecuta a la realidad de la entidad.

Ilustración 4. Reporte antivirus

Fuente: Reporte antivirus- Sistemas.

Como resultados generales de la evaluación adelantada al conocimiento y apropiación del Manual de Políticas Complementarias por parte de los colaboradores de Capital se evidencia que:

- No es pertinente indicar en el autodiagnóstico que los controles se cumplen al 100% sólo porque se encuentran documentados en el Manual, es importante, adelantar pruebas y tener soportes de que estos son ejecutados de conformidad a la forma como se formularon, para poderlos calificar y que se soporte ese nivel de cumplimiento. Dados los resultados, es importante que se adelanten acciones que permitan uniformidad en el conocimiento e interiorización de las normas identificadas en el Manual.

- Teniendo en cuenta que en el Manual se le asignan responsabilidades a diferentes áreas de Capital, es necesario, su inclusión en la actualización del documento, pues como se evidenció en los casos de las áreas de Servicios Administrativos y Recursos Humanos, estas no ejecutan varios de los controles asignados de conformidad a como se estableció en el lineamiento, por lo tanto, se hace indispensable que el levantamiento de controles se realice con la participación y aprobación de las áreas a las que se les están asignando actividades específicas.

- Se recomienda al área de Sistemas incluir al área Técnica en la actualización del Manual, puesto que esta área realiza actividades diversas relacionadas con mantenimientos, adquisición de infraestructura, copias de seguridad, entre otras [especialmente de las áreas misionales], por lo cual puede aportar a la identificación y ejecución de controles en materia de Seguridad de la Información.

- Es necesario realizar campañas de sensibilización del Manual, debido al amplio número de controles que allí se establecen para colaboradores y funcionarios, así como generar espacios permanentes de capacitación [verificar el acceso a la intranet para consulta del documento en todos los equipos y sedes de la entidad].

11.4. EVALUACIÓN DEL PLAN DE SENSIBILIZACIÓN DEL SG-SPI 2024

Se adelantó la revisión del Plan de sensibilización del Sistema de Gestión de Seguridad y Privacidad de la Información (AGRI-SI-PL-005), versión 3 del 20 de febrero de 2024. Para lo cual se solicitó información respecto a la ejecución de actividades; sin embargo, no fue posible establecer la ejecución de lo formulado. Lo mencionado dado que:

- Las actividades mencionadas no cuentan con indicadores que permitan medir la eficiencia en su desarrollo o si se requieren actividades de mejoramiento.
- Se observa la falta de uso de métricas que permita determinar la cantidad de personas capacitadas o asistentes a dichas jornadas.
- La encuesta de satisfacción realizadas para el periodo evaluado a todos los grupos de interés de la entidad, para medir la percepción y apropiación sobre temas de seguridad de la información, fue aplicada a (27) personas, sin que se soporte de manera adicional si fue requerido su diligenciamiento vía comunicaciones internas, correo electrónico u otro medio.
- Falta la determinación de la periodicidad de la evaluación, mejora y seguimiento del plan, así como los responsables de dicha medición.
- El tiempo y cuando no cuenta con la integración de un cronograma que permita determinar a lo largo de la vigencia, los meses o semanas en las cuales se adelantarán las actividades identificadas.
- Las actividades carecen de la definición del público objetivo, no se relacionan en los soportes los resultados de evaluaciones de las jornadas adelantadas, entre otros que permitan medir el aporte generado en la entidad.
- Por último, se hace necesario que los soportes que se almacenan en el marco de la ejecución del Modelo de Seguridad y Privacidad de la Información – MSPI guarden lineamientos que permitan la identificación de estos, lo anterior, dado que los listados de asistencia remitidos no relacionan la jornada a la cual

pertenece, por lo que no es posible evaluar dichos soportes de manera adecuada.

Lo indicado, deberá tenerse en cuenta para la construcción del Plan de sensibilización de las vigencias futuras, al igual que los resultados del seguimiento que se delante de las actividades formuladas en el documento.

Mesa de trabajo 6 de diciembre de 2024: Se indicó por parte del área de Sistemas que las observaciones realizadas al plan de sensibilización del SGSI están relacionadas con la necesidad de contar con recursos humanos, técnicos y financieros robustos para garantizar la ejecución, el seguimiento y la mejora continua de las actividades previstas en dicho plan.

Sin embargo, como recomendaciones complementarias a lo mencionado en el informe, se indicó por parte de la Oficina de Control Interno que se deben revisar y definir actividades en el plan de sensibilización de acuerdo a las temáticas, con periodicidades explicitas y métricas de medición articuladas con el PIC de RRHH. Lo anterior, con la finalidad de que se logre monitorear la ejecución de lo formulado y sentar las bases de la planeación de las vigencias futuras.

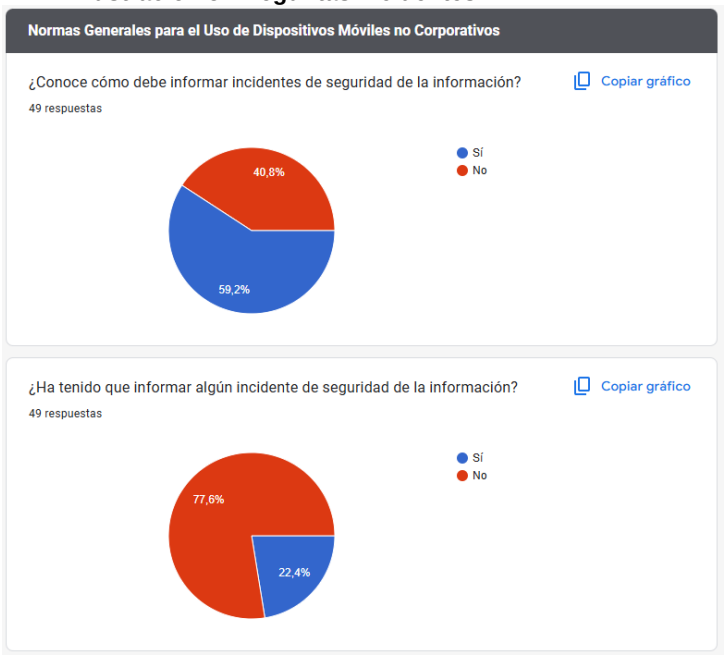
11.5. EVALUACIÓN DE LA GUÍA DE REPORTE DE INCIDENTES DE SEGURIDAD

Como parte de la evaluación adelantada a los controles indicados en la herramienta de diagnóstico del MSPI se adelantó la consulta a los colaboradores del Canal sobre el conocimiento de dicha guía, así como de conocimiento de los lineamientos establecidos para el reporte de incidentes del canal, lo anterior, mediante dos (2) preguntas [Ilustración 5].

Para ello, se contó con la participación de (49) respondientes a las preguntas adelantadas en materia de incidentes, obteniendo que el 59.2% de los participantes conoce el proceso para informar incidentes de seguridad de la información y que a la fecha el 77.6% de los colaboradores no ha tenido que reportar incidentes.

Respecto al 40.8% restante que indica que desconoce los lineamientos de la guía, se recomienda fortalecer las estrategias de comunicación y socialización al interior de la entidad, teniendo en cuenta la rotación de colaboradores con la que cuenta la entidad, tiempo de vinculación, responsabilidades, entre otros, que permitan interiorizar los conceptos de seguridad y privacidad de la información, así como mitigar riesgos en la materia.

Ilustración 5. Preguntas incidentes



11.6. EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Capital cuenta con tres (3) riesgos identificados desde el 16 de junio de 2023, cuyo plan de manejo cuenta con fecha de terminación el 13 de junio de 2024; durante el primer semestre de la vigencia se adelantó un seguimiento con corte a 31 de mayo, el cual arrojo como resultado un avance promedio del 55% a la fecha de corte, de igual manera las acciones formuladas en el plan de manejo alcanzaron las siguientes calificaciones:

- (2) calificadas con estado “Sin Iniciar”
- (2) calificadas con estado “En Proceso”
- (3) calificadas como “Terminada”

Sin embargo, en el marco de la presente auditoría se adelanta la revisión de la matriz de riesgos de seguridad digital identificados por parte de Capital bajo los lineamientos para la gestión de riesgos de seguridad digital en entidades públicas (Modelo de gestión de riesgos de seguridad digital – MGRSD).

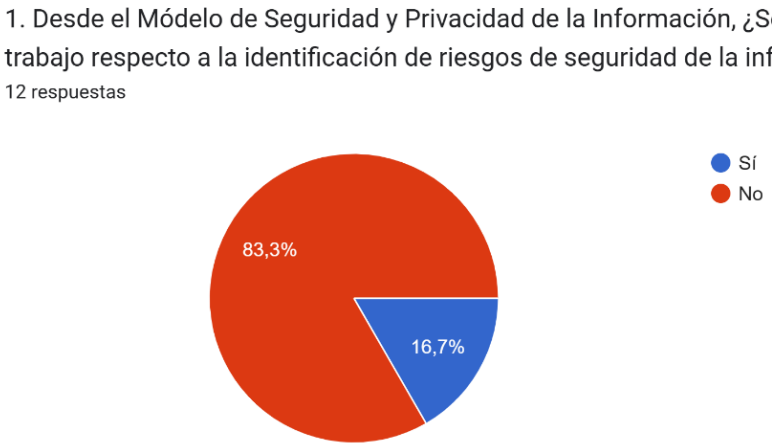
Teniendo en cuenta lo anterior, se observan debilidades en la identificación adecuada de riesgos, así como la coherencia de estos con la realidad del Canal. Para lo anterior, se adelantó una prueba de identificación de amenazas, materialización del riesgo y articulación entre áreas frente a la identificación de riesgos.

Dentro de lo identificado se menciona:

1. Dentro de los tipos de activos de información identificados en el documento “Formato para el inventario y clasificación de activos de información” (AGRI-SI-FT-038) se encuentran: Información y Software; sin embargo, en la matriz de identificación de riesgos se identifican activos adicionales como: *"COMPONENTE DE RED: *Firewall *Almacenamiento HARDWARE: Componentes de infraestructura del proceso * Infraestructura * Servicio de Comunicaciones y * Recursos de almacenamiento"*. Lo cual no es coherente entre documentos, por lo que deberá revisarse bajo los lineamientos de identificación de riesgos de seguridad digital.

2. Dada la revisión de amenazas relacionadas con los líderes de procesos [(12) respondientes] de Capital, se indicó por parte del 83.3% que no se adelantaron mesas de trabajo respecto a la identificación de riesgos de seguridad de la información.

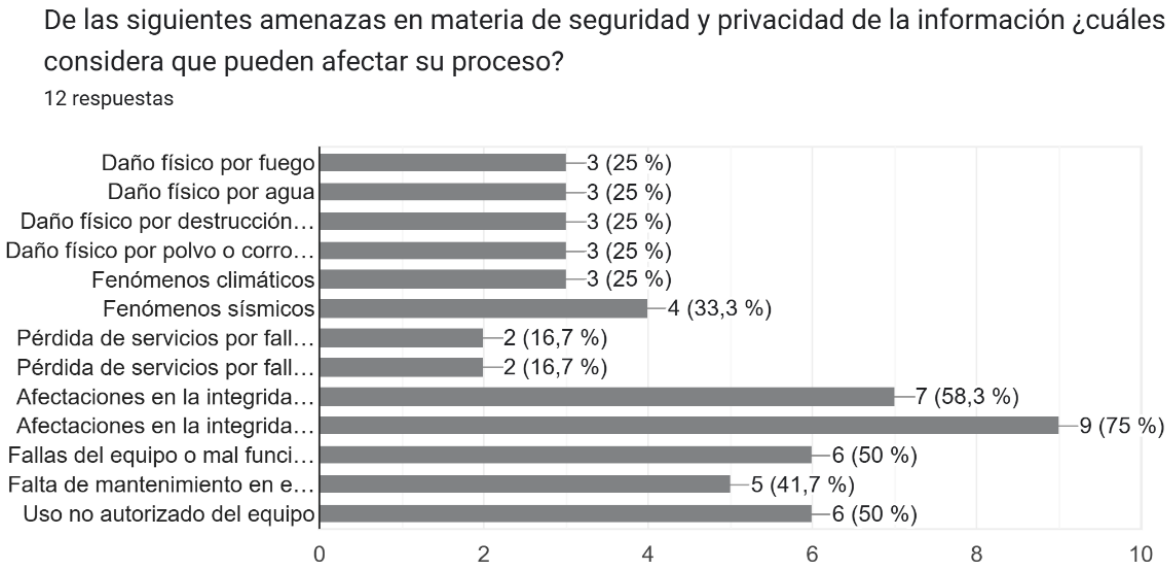
Ilustración 6. Prueba riesgos de seguridad



Fuente: Prueba de Riesgos de Seguridad Digital – 2024.

Teniendo en cuenta lo anterior, se consultó a los líderes de proceso respecto a las amenazas que pueden causar la materialización de un riesgo de seguridad digital al interior de las áreas, los cuales identificaron:

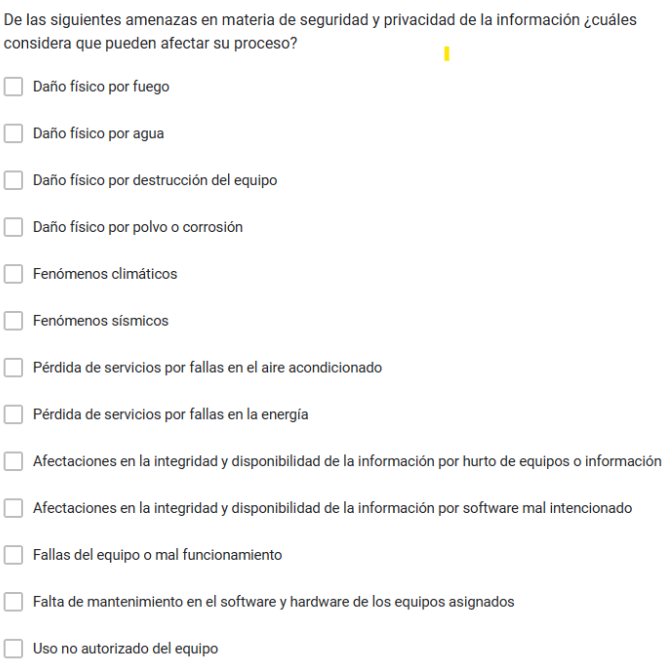
Ilustración 7. Prueba identificación de amenazas



Fuente: Prueba de Riesgos de Seguridad Digital – 2024.

Lo anterior, teniendo en cuenta el listado suministrado y filtrado a la realidad de Capital desde la tabla de amenazas del Modelo de gestión de riesgos de seguridad digital – MGRSD:

Ilustración 8. Listado de amenazas



Fuente: Prueba de Riesgos de Seguridad Digital – 2024.

3. Respecto a la identificación de los riesgos se hace necesario que se adelanten mesas de trabajo con las diferentes áreas de Capital. Es importante tener en cuenta que se identifican (14) procesos al interior del canal según Resolución 164 de 2023 “Por la cual se adopta el mapa de procesos de Canal Capital, se deroga la Resolución 073 de 2022, y se dictan otras disposiciones”. Lo anterior, teniendo en cuenta que el mapa de riesgos relaciona solo (12) procesos.

Macroproceso	Liderazgo estratégico	Procesos
Estratégico	Gerencia General	1. Planeación Estratégica 2. Gestión de marca y comunicaciones 3. Gestión de negocios y proyectos estratégicos
Misional	Dirección Operativa	1. Producción de contenidos 2. Gestión técnica para la producción, realización, emisión y circulación de contenidos 3. Diseño y ejecución de la estrategia de circulación de contenidos 4. Gestión digital para la creación, circulación y optimización de contenidos
Apoyo	Secretaría General	1. Gestión jurídica y contractual 2. Servicio al ciudadano
	Subdirección Administrativa	3. Gestión de recursos administrativos 4. Gestión de talento humano
	Subdirección Financiera	5. Gestión financiera y facturación
Evaluación (Control)	Control Interno	1. Control, Seguimiento y evaluación
	Control Disciplinario Interno	2. Control Disciplinario Interno

Fuente: Resolución 164 de 2023.

Adicionalmente, es importante tener en cuenta la descripción de la tipología del riesgo en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, versión 4.

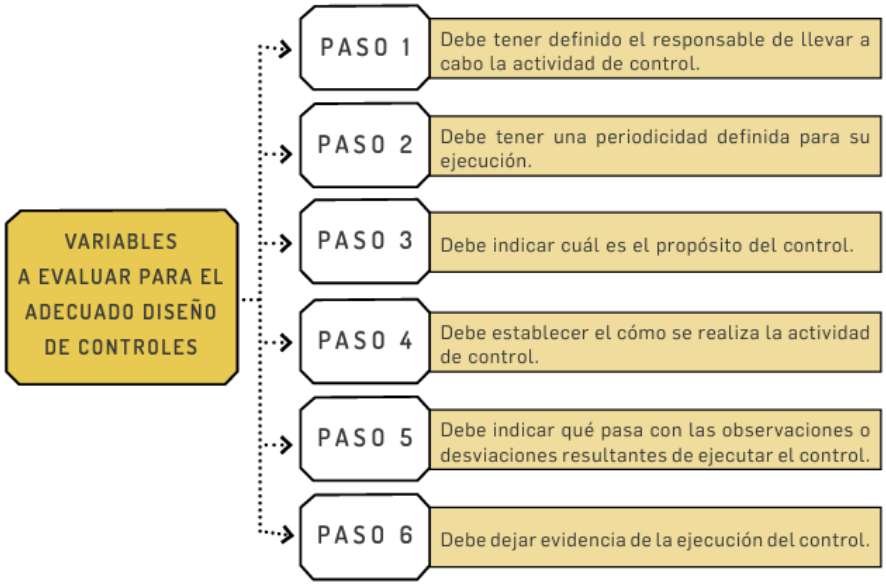
Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, versión 4

Por ejemplo:

- Perdida de disponibilidad, integridad y disponibilidad de la información almacenada, emitida y gestionada (tramitada) por los procesos de Capital por acceso no autorizado, falta de mantenimiento en el software y hardware de los equipos y servidores, fallas en los servicios de respaldo e indisponibilidad de parque tecnológico… (otras amenazas), a las herramientas de manejo de información dispuestas en la entidad.

4. Sobre los controles, es importante que se tengan en cuenta los pasos de valoración de controles, principalmente sobre lo faltante en la redacción como lo es la periodicidad de ejecución, cuál es la evidencia de ejecución del control, el propósito, entre otros. Lo anterior, teniendo en cuenta el esquema de valoración de controles de la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, versión 4.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, versión 4

5. Respecto al plan de manejo, es importante tener en cuenta que estos se diseñan adelantar acciones complementarias a los controles que permitan fortalecer el control o mantener el riesgo, y, que para el caso deben emplearse los controles definidos y aplicados en la entidad en el marco de la ISO 27001, así como del Modelo de Seguridad y Privacidad de la información – MSPI.

Teniendo en cuenta que actualmente se tiene suscrita una acción en el plan de mejoramiento por procesos relacionada con la actualización del mapa de riesgos de Seguridad Digital, se recomienda al área que de conformidad con los resultados obtenidos se incluyan actividades que abarquen las recomendaciones anteriormente indicadas y de ser necesario solicitar ampliación de la fecha de terminación.

12. OBSERVACIONES

Dado que las debilidades identificadas en el presente ejercicio de auditoría son reiteradas, y que las acciones formuladas para subsanar las causas de las observaciones se encuentran en el Plan de Mejoramiento por procesos cuya fecha de terminación es enero de 2025, no se adelanta la relación del cuadro de observaciones. Sin embargo, se definen a lo largo del documento las recomendaciones que deben ser tenidas en cuenta con el fin de asegurar la mejora continua del proceso de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la entidad, así como dar cumplimiento efectivo a las acciones formuladas.

13. CONCLUSIONES

Se dio cumplimiento al objetivo de la auditoría, el cual buscaba verificar el nivel de cumplimiento de los controles mencionados como parte de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI al interior de Capital. Dentro de lo evaluado se destacan aspectos como:

13.1. Capital adelantó el diligenciamiento de la herramienta de diagnóstico del Modelo de Seguridad y Privacidad de la Información – MSPI, habilitada por MinTic.

13.2. Se vienen adelantando actualizaciones a los documentos que soportan la implementación de controles definidos a la realidad de operación de Capital.

13.3. Se da cumplimiento a algunas normas definidas en el Manual de Políticas Complementarias por parte de las áreas responsables, así como de los colaboradores de la entidad.

13.4. Se viene construyendo la actualización de los activos de información por parte del área, con la consulta de las áreas de Capital.

13.5. Se han adelantado jornadas de sensibilización y comunicaciones sobre hábitos de seguridad digital, alertas de mensajes sospechosos y ciberataques, uso adecuado de la herramienta de Google drive.

De igual manera, se requiere la atención y ajuste de debilidades identificadas a lo largo de la evaluación de los controles consignados en la herramienta de diagnóstico como:

13.6. Se mantienen las debilidades de diligenciamiento de la herramienta de diagnóstico del MSPI al contar con reporte de controles en calificaciones entre el 60% y el 90% que no relaciona información respecto a cómo se da cumplimiento, y, en dado caso, qué falta para dar cabal cumplimiento.

13.7. Se desconoce por parte de los colaboradores del canal la documentación existente como controles en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI. Por lo que no es pertinente indicar que los controles se implementan al 100% en Capital.

13.8. Inconsistencias entre lo documentado y lo ejecutado efectivamente en el canal, respecto a ciertas políticas de uso de dispositivos móviles corporativos, backup y restauración de la información.

13.9. Se requiere la actualización de los términos del glosario del Manual de Políticas Complementarias, teniendo en cuenta la referenciación de la fuente y la correcta definición de los términos incluidos.

13.10. Es importante que se adelante la construcción de las normas del Manual de políticas complementarias con las áreas involucradas, de manera que se ajusten a la realidad de operación de la entidad, así como del quehacer de los colaboradores de Capital.

13.11. Revisión de los riesgos de seguridad digital, teniendo en cuenta que estos no cuentan con los lineamientos mínimos requeridos, y el plan de manejo se venció en junio de 2024, lo que implica que a la fecha de evaluación no se cuenta con actividades que mitiguen la materialización de riesgos en la materia.

13.12. Se requiere consultar a los líderes de proceso en la identificación de riegos de Seguridad Digital, teniendo en cuenta que cada área puede llegar a identificar riesgos aplicables a su propia actividad que no se encuentran en la matriz vigente de Capital.

13.13. Debilidades en la ejecución de las normas definidas para el área de Sistemas, teniendo en cuenta las inconsistencias indicadas en el informe sobre lo que se encuentra documentado en el Manual de políticas complementarias versus lo realmente ejecutado.

13.14. Debilidades en la constitución y ejecución del plan de sensibilización del SG- SPI de la presente vigencia, teniendo en cuenta las recomendaciones dadas en materia de mínimos de formulación.

13.15. Se requiere mayor socialización de los lineamientos construidos en el marco del MSPI, teniendo en cuenta que no todos los colaboradores tienen correo electrónico institucional, ni acceso a la intranet cuando se encuentran en las sedes de Capital, por lo que se deben buscar espacios de socialización diferentes.

14. RECOMENDACIONES

14.1. Revisar las debilidades que se mantienen en el diligenciamiento del diagnostico del MSPI, de manera que se refleje en la herramienta el reporte de cómo se da cumplimiento al control, así como las brechas que impiden contar con el cumplimiento al 100% de los controles mencionados.

14.2. Reforzar el conocimiento por parte de los colaboradores del canal sobre la documentación registrada como controles en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

14.3. Revisar y ajustar las inconsistencias entre lo documentado y lo ejecutado efectivamente en el canal, respecto a ciertas políticas de uso de dispositivos móviles corporativos, backup y restauración de la información, teniendo en cuenta la realidad de operación de la entidad.

14.4. Actualizar los términos del glosario del Manual de Políticas Complementarias, teniendo en cuenta la referenciación de la fuente y la correcta definición de los términos incluidos.

14.5. Concertar y coordinar la construcción de las normas del Manual de políticas complementarias con las áreas involucradas, de manera que se ajusten a la realidad de operación de la entidad, así como del quehacer de los colaboradores de Capital.

14.6. Revisar y actualizar los riesgos de seguridad digital, teniendo en cuenta que estos no cuentan con los lineamientos mínimos requeridos, y el plan de manejo se venció en junio de 2024.

14.7. Consultar a los líderes de proceso en la identificación de riegos de Seguridad Digital, teniendo en cuenta que cada área puede llegar a identificar riesgos aplicables a su propia actividad que no se encuentran en la matriz vigente de Capital.

14.8. Revisar la ejecución de las normas definidas para el área de Sistemas, teniendo en cuenta las inconsistencias indicadas respecto a lo indicado en el Manual de Políticas Complementarias.

14.9. Revisar y actualizar el plan de sensibilización del SG- SPI de la presente vigencia, teniendo en cuenta las recomendaciones dadas en materia de mínimos de formulación, así como la coordinación de actividades con áreas transversales como Recursos Humanos.

14.10. Fortalecer la socialización de lineamientos construidos en el marco del MSPI, teniendo en cuenta que no todos los colaboradores tienen correo electrónico institucional, ni acceso a la intranet cuando se encuentran en las sedes de Capital, por lo que se deben buscar espacios de socialización diferentes.

Revisó y aprobó:

Jefe Oficina de Control Interno

Preparó: Diana del Pilar Romero Varila – Profesional oficina de Control Interno, Cto 518 de 2024
Jizeth Hael González Ramírez – Profesional oficina de Control Interno, Cto 515 de 2024