UNIDAD DE BÚSQUEDA DE PERSONAS DADAS POR DESAPARECIDAS EN EL CONTEXTO Y EN RAZÓN DEL CONFLICTO ARMADO – UBPD

UBPD

UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

INFORME DE SEGUIMIENTO A RIESGOS DE GESTIÓN RELACIONADOS CON LAS TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES TICS

BOGOTÁ, D.C., JUNIO DE 2023

UBPD
UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

TABLA DE CONTENIDO

1. INFORMACIÓN GENERAL DEL SEGUIMIENTO	
Informe Seguimiento	Riesgos de Gestión de las Tecnologías de la Información y las Comunicaciones TIC
Fecha	22 de junio de 2023

2. ASPECTOS GENERALES DEL PROCEDIMIENTO DE SEGUIMIENTO

2.1. OBJETIVO GENERAL

La Oficina de Control Interno OCI en cumplimiento de sus funciones señaladas en el Decreto 1393 de 2018, realiza seguimiento detallado a los Riesgos de Gestión definidos y usados por la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, lo anterior, en concordancia al componente de Actividades de Control del Plan MECI 2023 y a la actividad No. 11.4.

El propósito principal es verificar el estado de actualización, gestión y cumplimiento por parte de la UBPD, en lo que respecta al análisis, diseño, implementación y seguimiento a Riesgos de Seguridad Digital y de Tecnologías de la Información y las Comunicaciones.

2.2. ALCANCE

La Oficina de Control Interno OCI realiza la verificación de la información relacionada con Análisis, Lineamientos para el Diseño, Implementación y Seguimiento de Riesgos de Seguridad de la Información, Seguridad Digital, Documentación de Análisis de Riesgos de Gestión Tecnologías de la Información y las Comunicaciones, Riesgos Tecnológicos en Planes Institucionales, Gestión de la Información y Gobierno de Datos, al corte del 28 de abril de 2023.

2.3. MARCO LEGAL, ANTECEDENTES, CRITERIOS

- **Decreto 1599 de 2005**, “Por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano”.
- **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”.
- **Ley 1474 de 2011**, “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.”
- **Decreto 612 de 2018**, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.”
- DPE-PC-001 V2 Política de Administración de Riesgos, del 25 de agosto de 2021.

- GSI-PC-003 V1 Política General de Seguridad de la Información, del 09 de septiembre de 2022.
- GSI-PR-001 SGSI V1 Procedimiento Seguimiento al Sistema de Seguridad de la Información.
- GTI-PL-003 V1 Plan Estratégico de Seguridad Digital.
- GTI-PL-002 V1 Plan de Recuperación de Desastres Tecnológicos.
- GTI-MR-001 V3 Gestión de Tecnologías de la Información y Comunicaciones 05-11-2021.
- Plan de Implementación de Protección y Seguridad Digital 2022.
- GCO-FT-003 Matriz de Riesgos del Proceso de Contratación, según Procedimiento GCO-PR-010 V2 Solicitud de Inicio Trámite Contractual para Procesos de Selección.
- Informes de seguimiento de Riesgos de Gestión Relacionados con las Tecnologías de la Información y las Comunicaciones TIC, realizados por la OCI en las vigencias 2021 (UBPD 1200-3-202103893 del 12 de julio de 2021) y 2022 (memorando UBPD-3-2022-009133 del 28 de junio de 2022).

3. FUENTES DE INFORMACION

- Respuestas y soportes entregadas por la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, el Oficial de Seguridad de la Información OSI y el Grupo Interno de Trabajo de Gestión Contractual GITGC, como respuesta a las preguntas y solicitudes de información realizadas por la OCI durante la ejecución del presente seguimiento.

4. METODOLOGÍA

- Revisión, contraste y análisis de la información entregada por los responsables identificados como fuentes de información.
- Revisión, contraste y análisis de la información publicada en el Sistema Integrado de Gestión SIG de la UBPD.

5. DESARROLLO

El día 08 de mayo de 2023 y con fecha de entrega para el 31 de mayo de 2022, la OCI solicitó a la OTIC y al OSI, información relacionada con:

Oficina de Tecnologías de la Información y las Comunicaciones OTIC (información entregada con oportunidad el 29 de mayo de 2023 a través de correo electrónico).

- Mitigación de riesgos de programación relacionados con accesos no autorizados al Sistema de Información Misional SIM Busquemos.
- Gestión del riesgo a nivel de capa de telecomunicaciones.
- Priorización en encriptación de datos críticos.

- Estado de simulacros según el "Plan de Recuperación de Desastres Tecnológicos".
- Sistemas de detección de intrusos en red y dispositivos.
- Reportes de robo de dispositivos tecnológicos.
- Autorización de conexión para equipos personales.
- Estado de implementación del "Plan Estratégico de Seguridad Digital".
- Actividades desarrolladas según observaciones y/o recomendaciones de anteriores seguimientos.

Oficial de Seguridad de la Información OSI (Información entregada con oportunidad el 19 de mayo de 2023 a través de correo electrónico).

- Estado de evaluaciones de riesgo de seguridad de la información y de su respectiva documentación.
- Acciones sobre los resultados de evaluaciones.
- Plan de Tratamiento de riesgos.
- Estado de cumplimiento de actividades del procedimiento "Seguimiento al Sistema de Seguridad de la Información".

Por otro lado, el 05 de mayo de 2023 y con fecha de entrega para el 12 de mayo de 2023, la OCI solicitó al GITGC la base contractual con corte al corte del 30 de abril de 2023, información entregada por el responsable en la fecha precitada.

6. RESULTADOS POR COMPONENTES

6.1. Tecnologías de la Información y las Comunicaciones

Contexto: la Norma Técnica Colombiana NTC-ISO 31000 brinda los principios y las directrices genéricas sobre la gestión del riesgo, donde, el numeral 4.3 Diseño del Marco de Referencia para la Gestión del Riesgo indica que *"…Antes de empezar el diseño y la implementación del marco de referencia para la gestión del riesgo,* ***es importante evaluar y entender el contexto, tanto externo como interno de la organización****, dado que este puede tener influencia significativa en el diseño de dicho marco…"*, (negrita y subrayado fuera del texto original).

En lo que respecta a las Tecnologías de la Información y las Comunicaciones, el análisis del contexto externo (según NTC-ISO 31000) puede incluir aspectos como: *"…el ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico…*", tipologías que hacen parte también de la "Guía para administración del riesgo y el diseño de control en entidades públicas" del Departamento Administrativo de la Función Pública DAFP y a nivel interno esta tipología debe ser registrada en el formato de "Mapa de Riesgos", asimismo, la evaluación y entendimiento del contexto de los riesgos TI, también debe evaluar riesgos relacionados con factores internos como lo son: Alineación con Objetivos y Estrategias, Estructura Organizacional, Funciones, Políticas, Capacidades (en términos

de recursos y conocimiento como, por ejemplo: tiempo, personas, procesos y tecnologías de la información y las comunicaciones), donde, una materialización podría afectar el alcance de objetivos estratégicos, continuidad del negocio, credibilidad, confianza, y valor de la Unidad.

En este sentido, la OCI solicito a la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, dar respuesta soportada con evidencias a las siguientes preguntas:

- **P2. ¿Se realiza gestión del riesgo a nivel de capa de Telecomunicaciones?, en lo relacionado al análisis de diagramas de red y de protocolos de red etc., lo anterior, con el fin de comprender el tráfico de datos desde fuera y al interior de la Unidad.**

  Respuesta OTIC: *"Si se realiza gestión del riesgo a nivel de la capa de telecomunicaciones, para ello se ha implementado un esquema de monitoreo de la infraestructura de red y los canales de comunicación mediante las herramientas Nagios, Zabbix, Entuity y E Monitor para mitigar riesgos que se puedan presentar sobre el tráfico de la red.*

  - *Topología de Red*
  - *EMonitor*
  - *Entuity*
  - *Nagios*
  - *Alertas Nagios*
  - *Zabbix"*

- **P3. ¿Existe priorización en la encriptación de datos identificados como críticos?, si es afirmativa la respuesta, indique por favor, ¿cuáles datos están priorizados? y cómo se realiza la encriptación.**

  Respuesta OTIC: *"Con corte a la presentación de este informe, la OTIC no ha recibido ninguna indicación o directriz en este sentido por parte de la Dirección Técnica de Información, Planeación y Localización para la Búsqueda, en el marco del Gobierno de Datos implementado al finalizar el tercer trimestre del 2022. Por el contrario, el Oficial de Seguridad de la Información presentó un concepto en el que indica que todos los equipos institucionales y arrendados deben incluir la herramienta de cifrado, en respuesta la OTIC implementó lo requerido durante el 2022, lo que viabiliza la encriptación de la información que se tenga almacenada de manera local en los discos duros de los equipos de cómputo asignados a servidores y contratistas.*

  Los discos duros de los equipos de cómputo se cifran mediante la herramienta Trellix, con la cual se administra y realiza monitoreo al estado de cifrado de los mismos, la gestión de las llaves de cifrado, la asignación de los usuarios que tienen acceso al equipo de cómputo como control complementario a la gestión realizada por directorio activo, adicionalmente otorga la posibilidad de cifrar documentos a discreción del usuario."

De lo anterior, la OCI recomienda establecer el nivel de uso y apropiación de las herramientas de cifrado, asimismo, reforzar, comunicar y/o dar a conocer a la Unidad las herramientas con las que se cuenta, el objetivo, ventajas, riesgos y desafíos, como lo podrían ser: los nuevos tipos de ataques, dificultades para compartir información, pérdida de información y problemas relacionados con accesos indebidos o malas prácticas.

Por otro lado, resulta muy importante que, a todo nivel se identifiquen los datos e información crítica y establecer el protocolo de manejo de estos, acompañado del respectivo análisis de riesgos, lo anterior, correspondería a actividades de gestión y de gobernabilidad de toda la información de la Unidad; así las cosas, se requiere agilizar y dar prioridad a la implementación del modelo de Gobierno de Datos.

- **P6. ¿Han sido reportados a la Mesa de Ayuda robos de dispositivos móviles tipo "Celulares", "Tabletas" y/o "Portátiles" de propiedad de la Unidad?, si es afirmativa la respuesta, indique por favor ¿Cuántos y de que dependencias?**

  Respuesta OTIC: *"Con corte a la fecha de la presente respuesta, se han reportado a la Mesa de Servicios el hurto de dos (2) portátiles y tres (3) celulares de propiedad de la entidad, estos estaban asignados funcionarios adscritos la Dirección de Prospección y a la Subdirección Técnica y Territorial."*

- **P7. ¿Cuántos dispositivos móviles personales (Celulares, Tabletas y/o Portátiles) se encuentran autorizados para conexión y uso de los servicios de la Unidad?, indique por favor cuantos por cada tipo y aporte evidencia de la autorización.**

  Respuesta OTIC: ***"****Para dar respuesta a la pregunta,* ***se aclara que, actualmente no se tienen equipos autorizados para la conexión y uso de los servicios TIC institucionales a través de equipos personales desde la red LAN o Wifi de la Entidad****, la conexión a estas redes se válida para autorización o denegación de acuerdo a lo establecido en el procedimiento GTI-PR-012 Solicitud de Servicios de Seguridad Digital. Sin embargo, algunos contratistas que hacen parte de proyectos específicos utilizan equipos personales en los cuales se configura la VPN para acceso controlado a los servicios que son requeridos por parte del supervisor y/o dependencia responsable. Es importante considerar que, la OTIC no tiene control sobre la ejecución de proyectos específicos."* (Negrita y Subrayado por fuera del texto original)

Si bien, se establece el control de acceso desde equipos personales y que se conectan a las redes internas a través de la LAN y el Wifi, resulta importante tener en cuenta que, el acceso a servicios institucionales como lo son el "Correo Electrónico" y el "Drive" no solo se realiza a través de las redes institucionales, sino que, también se realiza a través de dispositivos móviles personales con conexión a redes públicas, donde, desde cualquier dispositivo tipo "Teléfono Celular" se accede a recursos y/o

documentos internos, por lo tanto, la OCI recomienda extender el control de acceso hacia los dispositivos móviles personales con acceso a redes externas.

6.1.1. Sistema de Información Misional SIM Busquemos

- **P1. En el marco del Contrato No. 0181 de 2021, indicar ¿cómo se mitigan o mitigaron los riesgos de errores de programación relacionados con accesos no autorizados al Sistema de Información SIM Busquemos y a la(s) bases de datos en lo concerniente a administración de seguridad.**

  Respuesta OTIC: *"Durante la fase de recibo de las funcionalidades desplegadas por el contratista en el ambiente de pruebas en la infraestructura de la UBPD, se evaluó cada componente con la ejecución de pruebas funcionales y técnicas por parte del equipo que apoya la Supervisión del contrato, incluyendo los líderes temáticos de cada módulo, pruebas funcionales. En tal sentido, dependiendo del cumplimiento evidenciado en las pruebas técnicas y funcionales se viabiliza el despliegue de las funcionalidades evaluadas en los ambientes UBPD de Preproducción y Producción. Adicionalmente, antes de la entrada en uso del sistema, se debe ejecutar un ejercicio de Hacking Ético, el inicio en operación del sistema depende que no tenga vulnerabilidades.*

  A continuación, se listan los principales atributos y condiciones específicas incluidas en los Requerimientos No Funcionales definidas en el ANEXO 1.2. Anexo Ficha Técnica asociadas al control de accesos no autorizados a BUSQUEMOS:

  - *Seguridad. Este atributo permite verificar el grado de protección de la información y los datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos. Esta característica se subdivide a su vez en las siguientes categorías:*
  - *Confidencialidad: grado de protección contra el acceso de datos e información no autorizados, ya sea accidental o deliberadamente.*
  - *Integridad: grado del sistema o componente para prevenir accesos o modificaciones no autorizados a datos o programas de software.*
  - *No repudio: grado en que se demuestran las acciones o eventos que han tenido lugar, para que estas no puedan ser rechazadas o negadas por un usuario posteriormente.*
  - *Auditabilidad: grado en que se logran rastrear las acciones realizadas por un usuario dentro del sistema.*
  - *Autenticación: grado en que se asegura la identidad de un usuario sobre un recurso protegido del sistema.*

  ***Nota**: BUSQUEMOS solo puede ser accedido de manera local (LAN institucional), los accesos remotos que se requieran se gestionan de manera exclusiva mediante el uso de la VPN.*

- *Almacenamiento de objetos físicos, el sistema permite relacionar dentro el proceso de búsqueda, objetos o documentos físicos de las personas aportantes y que estos cuenten con los respectivos controles de seguridad enfocados a que únicamente se de acceso a los roles que estén autorizados a dicha información y su respectiva caracterización, descripción y ubicación.*
- *Roles basados en control de acceso: El sistema permite definir los roles y perfiles de los usuarios acorde a modelos RBAC (Roles basados en control de acceso).*
- *Auditoría de accesos denegados: Registra los accesos que se consideren como denegados a las diferentes funcionalidades, manteniendo un registro en base de datos para que pueda ser consultado por el administrador del sistema.*
- *Listado de requerimientos de autenticación requeridos en el sistema: Todo acceso al sistema se realiza a través de un proceso de autenticación en el que cada usuario ingresa su nombre de usuario y contraseña.*
- *Permisos a nivel de secciones de formularios: El nivel de granularidad de los permisos establecidos para los roles se puede realizar a nivel de secciones de formularios, que así lo determinen. El no parametrizar permisos de modificación en ningún campo, se tratará como restrictivo por lo que no podrá modificar ninguno hasta que se habilite su edición.*
- *Hacking Ético: Una vez el sistema se encuentre desarrollado completamente, se debe realizar una ejecución de Hacking ético sobre los desarrollos hechos a la medida para garantizar que no se presente vulnerabilidades que puedan comprometer la seguridad del sistema.*

Aunado a lo ya indicado, es importante resaltar que la arquitectura tecnológica diseñada e implementada por la OTIC dispone para BUSQUEMOS tres (3) ambientes separados, pruebas, preproducción y producción, los citados ambientes operan bajo el mismo marco de seguridad de los demás sistemas y herramientas que actualmente son utilizados en la Unidad. Como política general de la OTIC, BUSQUEMOS está restringido para accesos externos, en caso de requerirse es viable siempre y cuando sea a través de la VPN institucional, y/o, utilizando la funcionalidad OnLine - OffLine incluida en el Sistema de Información, la gestión de usuarios de BUSQUEMOS desarrolló y configuró mediante la integración con el Directorio Activo institucional, el acceso a la base de datos solo es viable en LAN institucional, la cual corresponde a una red MPLS con monitoreo proactivo-reactivo mediante el servicio de un NOC, el cual a su vez, incluye la gestión del Firewall Core y la coordinación con el grupo de seguridad digital en la gestión de acciones asociadas con la administración de las herramientas de ciberseguridad que se han implementado en la Unidad, lo anterior, disminuye el riesgo de accesos no autorizados a la base de datos o al mismo sistema.

En cuanto a las evidencias que se requiere aportar, y considerando que a la fecha aún está en proceso de implementación el Sistema de Información Misional, por el momento, se incluyen pantallazos del Módulo de Administración, actualmente BUSQUEMOS controla de manera

correcta los roles, permisos, acceso al sistema y a la base de datos de acuerdo con lo requerido por la entidad. Así mismo, presentamos como evidencia el resultado que obtuvo el grupo de seguridad digital de la OTIC al realizar un ejercicio de ethical hacking proactivo, se detectaron cuatro (4) vulnerabilidades que actualmente el contratista se encuentra resolviendo, (como se documentó anteriormente, antes de la puesta en producción el contratista debe presentar el resultado de un ejercicio de ethical hacking).”

6.1.2. Seguridad Digital

- **P5. ¿La Unidad cuenta con sistemas, herramientas o mecanismos de Detección de Intrusos en Red y en Dispositivos?, ¿Cuáles y cómo se realizan estas actividades?**

  Respuesta OTIC: *“Para controlar el acceso a intrusos al esquema de servicios TIC institucionales, se cuenta con un Firewall de perímetro que controla las políticas para el acceso, publicación y/o denegación a los servicios de red y aplicaciones web publicadas, adicionalmente se realiza un control mediante la MAC para la conexión de equipos de cómputo, ipad, tablet y/o celulares a la red LAN y la red WIFI de la entidad, lo que permite que no se entregue servicios, accesos, o visualización de segmentos de red a equipos no autorizados que se conecten a estas.”*

  La OCI recomienda para la vigencia 2024, contratar un servicio especializado que realice las pruebas de vulnerabilidad a los sistemas de información de la Unidad, con el fin de identificar oportunidades de mejora y validar la suficiencia y efectividad de las herramientas de detección implementadas a la fecha. Esta recomendación se hace teniendo en cuenta que, los ataques cibernéticos avanzan y en esa misma medida, deben avanzar las acciones de identificación de nuevos riesgos y ataques, para fortalecer las medidas y mecanismos de seguridad.

- **P8. En el marco del Plan Estratégico de Seguridad Digital (GTI-PL-003 V1), por favor dar respuesta soportada a:**

  - **P8.1. ¿Cuál es el nivel general de implementación del plan?**

    Respuesta OTIC: “*Con corte diciembre de 2022 se implementó el 100% de las actividades programadas para ser ejecutadas en la citada anualidad.*

    Para el 2023 se está trabajando en la articulación de los componentes de seguridad de la información y seguridad digital por lo cual se creó el Plan_Implementacion_SSI_2023 el cual fue aprobado por el comité de Seguridad de la Información, y se realizó la medición a marzo de 2023 donde se obtuvieron los siguientes resultados:

    - *83% a nivel general del Sistema de Seguridad de la Información.*

- *62% a nivel de controles de seguridad de la información."*

- **P8.2: ¿Cuál es el nivel de avance de identificación de Infraestructura Crítica, para las metas Nivel 3 y Nivel 4?**

  Respuesta OTIC: *"En 2022 se alcanzó el Nivel 3, se realiza la identificación de la infraestructura a 2022, realizando la evaluación respectiva referente a 3 componentes internos (función, disponibilidad e impacto) y 3 componentes externos definidos por el Comando Conjunto Cibernético (Impacto social, económico y medio ambiental), adicionalmente se identifica si la infraestructura cuenta con copia de seguridad y/o réplica.*

  En 2023 se tiene como meta alcanzar el Nivel 4 para lo cual se realizará la actualización de infraestructura y nuevos servicios tecnológicos, evaluación de los mismos, articulación de la infraestructura con el plan de copias de seguridad de la información y plan de recuperación de desastres."

- **P8.3: ¿Cuál es el estado de avance, seguimiento y resultados del Plan de Protección y Seguridad Digital al corte del 30 de abril de 2023?**

  Respuesta OTIC: *"Con corte a diciembre de 2022 se implementó el 100% de las actividades programadas.*

  Para el 2023 se está trabajando en la articulación de los componentes de seguridad de la información y seguridad digital por lo cual se creó el Plan_Implementacion_SSI_2023 el cual fue aprobado por el comité de Seguridad de la Información, y se realizó la medición a marzo de 2023 donde se obtuvieron los siguientes resultados:

  - *83% a nivel general del Sistema de Seguridad de la Información.*
  - *62% a nivel de controles de seguridad de la información."*

- **P8.4: ¿Cuál es el nivel de avance en la implementación del Gobierno de seguridad Digital, para las metas Nivel 3 y 4?**

  Respuesta OTIC:

  *"**Política de Seguridad Digital:***
  En 2022 se realizó la unificación de la política de seguridad de la información mediante la resolución 1358 de 2022 la cual adopta la nueva Política General de Seguridad de la información y deroga las resoluciones 1140 y 1141 de 2021, la cuales adoptan la Política

General de Confidencialidad, Protección y Seguridad de la Información y la Política de Seguridad Digital.

Requisitos Legales:
En 2022 se solicitó incluir en el Normograma de la UBPD la normatividad inherente a Seguridad de la Información

Estrategias de Seguridad Digital:
A diciembre de 2022 se implementó el 100% de las actividades programadas de acuerdo a las estrategias establecidas

Roles y Responsabilidades de Seguridad Digital:
En 2022 se incluyó el documento de roles y responsabilidades de Seguridad Digital en el Sistema Integrado de Gestión de la UBPD."

- **P8.5: ¿Cuál es el nivel de avance en la Gestión de Riesgos? en lo referente a: identificación de vulnerabilidades, información de amenazas, identificación y evaluación de riesgos, planes de tratamiento y gestión del riesgo de seguridad digital en los proveedores.**

Respuesta OTIC: *"A continuación, se presenta lo requerido:*

Identificación de vulnerabilidades:
Se realizó ejercicio de retest en junio de 2022 del Ethical Hacking contrato en 2021 para la identificación de las vulnerabilidades de la infraestructura tecnológica.

Se realizó Ethichal Hacking en noviembre de 2022 para la identificación de las vulnerabilidades de la infraestructura tecnológica.

***Nota**: El archivo se encuentra en el repositorio diferente debido a su contenido, tamaño, cantidad de archivos o estructura para seguimiento, serán garantizados los accesos a los mismos para la respectiva revisión por parte de la Oficina de Control Interno.*

Información de amenazas:
Se realiza monitoreo de alertas emitidas por fabricantes, entidades, organizaciones o grupos respecto a vulnerabilidades que pueden afectar la infraestructura tecnológica de la entidad.

Identificación y evaluación de riesgos:
Se realizó la identificación y evaluación de los riesgos de seguridad digital

Gestión del riesgo de seguridad digital en los proveedores:
Dentro de las obligaciones generales del clausulado en los contratos se especifica la obligación que hacen referencia al lineamiento de seguridad de la información "Suscribir el acuerdo de confidencialidad con la UBPD" en el cual se especifican los compromisos, obligaciones y prohibiciones respecto a la seguridad de la información."

- **P8.6: ¿Cuál es el nivel de avance en la implementación para la Gestión de Identidad y Control de Acceso, para las metas Nivel 3 y Nivel 4?**

  Respuesta OTIC: *"A continuación se presenta lo requerido:*

  Gestión de credenciales:
  Los accesos a los sistemas de información y servicios tecnológicos de la entidad se gestionan de acuerdo a las novedades administrativas (ingresos, vacaciones, licencias, retiros, entre otros) reportados por Recursos Humanos y las novedades de los Contratos de Prestación de Servicios enviados por el grupo de contratos.

  Aseguramiento físico de los activos tecnológicos:
  Los servidores y equipos de comunicación se encuentran ubicados en centros de datos con acceso controlado por llave y/o lector de huella digital y/o clave.

  Los equipos cuentan con guaya para ser asegurados a los puestos de trabajo y para ser retirados de las instalaciones se debe diligenciar el formato GRF-FT-009 AUTORIZACIÓN DE SALIDA DE BIENES DE LA ENTIDAD el cual debe ser autorizado por la OTIC para el nivel central y por el coordinador del equipo territorial.

  Accesos remotos:
  Los accesos remotos son gestionados mediante conexión VPN donde se establecen los servicios o infraestructura tecnológica a la que se tiene acceso.

  Segmentación de la Red:
  Se tiene segmentada la red por tipo de infraestructura (Servidores, equipos de cómputo, red wifi, entre otros) y los accesos a cada segmento se establecen de acuerdo a las necesidades de cada usuario."

- **P8.7: ¿Cuál es el nivel de implementación para Conciencia y Capacitación, para las metas Nivel 3 y Nivel 4?**

Respuesta OTIC: *"A continuación se presenta lo requerido:*

En 2022 se realizó las actividades establecidas en el Plan de Uso y Apropiación 2022 dentro de las cuales se generaron piezas de comunicación, capacitación en equipos territoriales, desarrollo de la semana de la seguridad.

En 2023 el Plan de Uso y Apropiación el cual se están desarrollando las actividades programadas en el mismo."

- **P8.8: ¿Cuál es el nivel de implementación para Seguridad de Datos, para las metas Nivel 3 y Nivel 4?**

Respuesta OTIC: ***"****A continuación, se presenta lo requerido:*

Protección de datos en reposo:
Actualmente la entidad cuenta con 97 memorias y discos duros cifrados que permiten almacenar información en reposo de manera segura

Protección de datos en tránsito:
Las redes de la UBPD están protegidas mediante el uso de protocolos seguros de comunicación, los datos transferidos a GSuite se realizan de manera segura y cifrada.

Eliminación, transferencias y/o disposición final de activos de información:
A los equipos devueltos al proveedor y los equipos propios que presenten condiciones de daño, cambio de tecnología, mal funcionamiento y/o finalización de la vida útil, se les realiza el proceso de borrado seguro certificado.

Protección contra filtraciones de datos:
Mediante la herramienta de Prevención de fuga de información DLP se administra la conexión y permisos de transferencia de información desde y hacia los equipos de cómputo desde dispositivos como memorias USB, discos, celulares, ipads, iphones, CD, DVD, entre otros. Así mismo se establecen las políticas para la transferencia de información en redes, repositorios en la nube, servidores, entre otros."

- **P8.9: ¿Cuál es el nivel de implementación para Protección de la Información? En lo referente a: Desarrollo Seguro, Control de Cambios, Copias de Seguridad, Plan de Respuesta a Incidentes, Plan de Recuperación de Desastres, Líneas Base para las etas Nivel 3 y Nivel 4.**

Respuesta OTIC: *"A continuación se da respuesta a lo requerido:*

Control de cambios:
Los cambios en la infraestructura tecnológica y sistemas de información se analizan, para ser aprobados o denegados en la mesa de control de cambios que realiza la OTIC cada vez que se requiere.

***Nota**: El archivo se encuentra en el repositorio diferente debido a su contenido, tamaño, cantidad de archivos o estructura para seguimiento, serán garantizados los accesos a los mismos para la respectiva revisión por parte de la Oficina de Control Interno.*

Copias de seguridad:
Se realizan réplicas de servidores y copias de seguridad de servidores, adicionalmente se realizan copias de base de datos o repositorios de acuerdo al plan de copias de seguridad que actualmente se está actualizando.

Líneas base:
Se realizaron las plantillas de línea base para sistemas Windows Server, Directorio Activo, Windows 10, linux, Ipads y MAC."

- **P8.10: ¿Cuál es el nivel de implementación para Mantenimiento de los Activos de Información Tecnológicos?**

  Respuesta OTIC: *"Durante el año 2022 se realizaron mantenimientos preventivos a los equipos de cómputo y la infraestructura tecnológica de la entidad, así mismo durante el primer semestre del año 2023 se tienen programados estos mantenimientos de acuerdo a los cronogramas adjuntos."*

- **P8.11: ¿Cuál es el nivel de implementación para Tecnologías de Protección? En lo referente a: Registros de Auditoría, Medios de Almacenamiento Extraíbles, Protección de Redes, Redundancia de Dispositivos, Defensa en Profundidad.**

  Respuesta OTIC: *"A continuación se presenta lo requerido:*

  Registros de Auditoría:
  Se llevan registros de auditoría a nivel de los eventos en servidor de Bases de Datos, Servidor de Directorio Activo y herramienta de Prevención de pérdida de datos DLP

  Medios de Almacenamiento Extraíbles:

Actualmente la entidad cuenta con 97 memorias y discos duros cifrados que permiten almacenar información en reposo de manera segura los cuales están habilitados en modo lectura y escritura

Adicionalmente se encuentra habilitado en modo lectura (sólo se puede copiar información del medio de almacenamiento externo hacia el computador) para las áreas misionales y la Oficina Asesora de Comunicaciones y Pedagogía, teniendo en cuenta las labores que estas realizan, para las demás áreas se realiza bajo demanda.

Protección de Redes:
Actualmente la UBPD cuenta con el Firewall donde se establecen las políticas para el acceso, publicación y/o denegación a los servicios de red y aplicaciones web publicadas, así como la detección y bloqueo de amenazas a nivel perimetral.

Defensa en Profundidad:
Se ha implementado la estrategia defensa en profundidad en los siguientes ítems:
Políticas y Procedimientos los cuales se encuentran en el sistema integrado de gestión

Gestión de riesgos:
Se realizó la identificación y evaluación de los riesgos de seguridad digital

Seguridad Perimetral:
Actualmente la UBPD cuenta con el Firewall donde se establecen las políticas para el acceso, publicación y/o denegación a los servicios de red y aplicaciones web publicadas, así como la detección y bloqueo de amenazas a nivel perimetral.

Se implementó el WAF para la protección de las aplicaciones web de la UBPD

Seguridad en el Host:
Se tiene implementado el DLP y EDR en los equipos de cómputo"

- **P8.12: ¿Cuál es el nivel de implementación para Anomalías y Eventos? En lo referente a: Reporte de Eventos e Incidentes, Monitoreo de Seguridad, Detección de Código Malicioso, Monitoreo de Conexiones No Autorizadas, Revisión y Análisis de Logs de Auditoría, Pruebas de Seguridad y Validaciones.**

  Respuesta OTIC: *"Se da respuesta a lo requerido de la siguiente manera:*

  Reporte de Eventos e Incidentes:
  Se realiza la gestión de los eventos de seguridad de la información reportados, realizando el análisis y evaluación de estos

Monitoreo de Seguridad:
Se realiza monitoreo de las herramientas de ciberseguridad y los planes de remediación de vulnerabilidades

***Nota**: El archivo se encuentra en el repositorio diferente debido a su contenido, tamaño, cantidad de archivos o estructura para seguimiento, serán garantizados los accesos a los mismos para la respectiva revisión por parte de la Oficina de Control Interno*

Detección de Código Malicioso:
Se realiza la detección de código malicioso mediante el EDR, identificando alertas, ajuste de políticas y excepciones.

Monitoreo de Conexiones No Autorizadas:
Se realiza un control mediante la MAC para la conexión de equipos de cómputo, ipad, tablet y/o celulares a la red LAN y la red WIFI de la entidad, lo que permite que no se entregue servicios, accesos, o visualización de segmentos de red a equipos no autorizados que se conecten a estas.

Revisión y Análisis de Logs de Auditoría:
Se llevan registros de auditoría a nivel de los eventos en servidor de Bases de Datos, Servidor de Directorio Activo y herramienta de Prevención de pérdida de datos DLP

Pruebas de Seguridad y Validaciones:
Se realizó ejercicio de retest en junio de 2022 del Ethical Hacking contrato en 2021 para la identificación de las vulnerabilidades de la infraestructura tecnológica.

***Nota**: El archivo se encuentra en el repositorio diferente debido a su contenido, tamaño, cantidad de archivos o estructura para seguimiento, serán garantizados los accesos a los mismos para la respectiva revisión por parte de la Oficina de Control Interno*

Se realizó Ethichal Hacking en noviembre de 2022 para la identificación de las vulnerabilidades de la infraestructura tecnológica.

***Nota**: El archivo se encuentra en el repositorio diferente debido a su contenido, tamaño, cantidad de archivos o estructura para seguimiento, serán garantizados los accesos a los mismos para la respectiva revisión por parte de la Oficina de Control Interno*

Información de amenazas:
Se realiza monitoreo de alertas emitidas por fabricantes, entidades, organizaciones o grupos respecto a vulnerabilidades que pueden afectar la infraestructura tecnológica de la entidad.

***Nota**: El archivo se encuentra en el repositorio diferente debido a su contenido, tamaño, cantidad de archivos o estructura para seguimiento, serán garantizados los accesos a los mismos para la respectiva revisión por parte de la Oficina de Control Interno."*

- **P8.13: ¿Cuál es el nivel de implementación para Gestión de Eventos e Incidentes?, en lo referente a: Planificación de la Respuesta, Comunicaciones, Análisis, Mitigación, Mejoras.**

  Respuesta OTIC: *"A la fecha se encuentra implementado y operando las actividades establecidas para la gestión de un evento o incidente, no se han presentado incidentes de seguridad de la información, se han realizado y están programados para 2023 escenarios de pruebas, lo que permite verificar las actividades establecidas y mejorar los procedimientos y respuestas."*

- **P8.14: ¿Cuál es el nivel de implementación para Recuperación de Eventos e Incidentes? En lo referente a: Planificación de la Recuperación, Mejoras, Comunicaciones.**

  Respuesta OTIC: *"A la fecha se encuentra implementado y operando las actividades establecidas para la recuperación ante un evento o incidente, no se han presentado incidentes de seguridad de la información, se han realizado y están programados para 2023 escenarios de pruebas, lo que permite verificar las actividades establecidas y mejorar los procedimientos y respuestas."*

- **P8.15: ¿Cuál es el nivel de implementación para Ciber Resiliencia?**

  Respuesta OTIC: *"Para la implementación de la ciber resiliencia se han realizado las actividades enumeradas en puntos anteriores.*

  - *Defensa en profundidad*
  - *Copias de seguridad*
  - *Plan de recuperación de desastres*
  - *Identificación de vulnerabilidades*
  - *Gestión de eventos e incidentes"*

6.1.3. Recuperación de Desastres

- **P4. En el marco del Plan de Recuperación de Desastres Tecnológicos (GTI-PL-002 V1), por favor dar respuesta soportada a:**

  - **P4.1. ¿Se han llevado a cabo algún tipo de simulacros controlados según los escenarios o eventos fijados en el Plan? y/o ¿Se tienen planificados durante la presente vigencia?**

Respuesta OTIC: *"Para dar respuesta a lo indicado, la OTIC se permite confirmar que, sí se han ejecutado simulacros con el DRP, para ello se precisa que, durante la vigencia 2022 se ejecutaron las pruebas que se listan a continuación:*

- *Prueba restauración y replica servidor 172.16.30.3.*
- *Prueba restauración CPP-CMP-P02 (2022-08-17 10_21 GMT-5).*

La ejecución de las pruebas del DRP (simulacros) están programados entre el 01 de junio y el 30 de noviembre de 2023 de conformidad con lo indicado en el Plan_Implementacion_SSI_2023.xlsx, el cual fue aprobado por el comité de Seguridad de la Información del 1 de febrero de 2023 como está registrado en el acta 001 2023."

- **P4.2. ¿Para la ejecución de los simulacros se requirieron o se requieren recursos económicos?, si la respuesta es afirmativa, indicar por favor el valor ejecutado o planificado a ejecutar.**

  Respuesta OTIC: *"La OTIC se permite aclarar que, no se consideró necesario disponer de recursos adicionales a los que ya cuenta la Unidad, los simulacros se planearon y se han ejecutado en la infraestructura institucional y con la activa participación del Talento Humano adscrito a la OTIC, entre otros aspectos, por considerar que estos deben ser lo más realista posible, facilitando la evaluación de su efectividad y oportunidades de mejora."*

6.1.4. Gestión Contractual TIC

De acuerdo con la información suministrada por el Grupo Interno de Trabajo de Gestión Contractual GITGC, durante la vigencia 2023 y al corte del 30 de abril de 2023, se observaron un total de 30 procesos contractuales relacionados con las Tecnologías de la Información y las Comunicaciones TIC, distribuidos así, por según dependencia de Supervisión Contractual y clase contrato:

DEPENDENCIA SUPERVISION CONTRACTUAL	CLASE DE CONTRATO	CANT.	VALOR CONTRATOS
OFICINA DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES OTIC	ORDEN DE COMPRA	1	$ 27.819.167,17
	PRESTACIÓN DE SERVICIOS	2	$ 210.073.344,00
	PRESTACIÓN DE SERVICIOS PROFESIONALES Y DE APOYO A LA GESTIÓN	13	$ 783.503.000,00
TOTAL		**16**	**$ 1.021.395.511,17**

DEPENDENCIA SUPERVISION CONTRACTUAL	CLASE DE CONTRATO	CANT.	VALOR CONTRATOS
OFICINA DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES OTIC SUBDIRECCION DE GESTION DE LA INFORMACION PARA LA BUSQUEDA SGIB	PRESTACIÓN DE SERVICIOS PROFESIONALES Y DE APOYO A LA GESTIÓN	4	$ 204.924.000,00
TOTAL		**4**	**$ 204.924.000,00**

DEPENDENCIA SUPERVISION CONTRACTUAL	CLASE DE CONTRATO	CANT.	VALOR CONTRATOS
SUBDIRECCION DE GESTION DE LA INFORMACION PARA LA BUSQUEDA SGIB	PRESTACIÓN DE SERVICIOS PROFESIONALES Y DE APOYO A LA GESTIÓN	10	$ 501.960.000,00
TOTAL		**10**	**$ 501.960.000,00**

TOTAL	**30**	**$ 1.728.279.511,17**

Fuente: archivo "BASE DE DATOS CONTRATACION 2023 - OCI 12052023.xlsx"

De lo anterior, se observó que con corte al 30 de abril de 2023, el 10 % (3) de los contratos corresponden a bienes intangibles (software) y el 90 % (27) de los contratos a OPS, en este sentido, se realizó la verificación del cumplimiento de requisitos establecidos en el "Manual de Contratación y Supervisión" GCO-MN-01 V2 del 21 de agosto de 2020, donde, en los numerales "3 - Actuaciones en las etapas del proceso contractual" y "3.1 Requisitos Mínimos Generales para iniciar un proceso de contratación, se indica: *"…Estudios y documentos previos con sus correspondientes soportes y/o anexos, incluida la matriz de análisis de riesgos en los formatos: "GCO-FT-010, Estudios Previos para Contratos de Prestación de Servicios Profesionales y Apoyo a la Gestión", "GCO-FT-001 o Estudios y Documentos Previos para Procesos de Licitación, Concurso de Méritos, Selección Abreviada y Contratación Directa Diferente a PSP*", y "*GCO-FT-010 Matriz de riesgos anexo N° 1 del estudio previo para la contratación de servicios profesionales y de apoyo a la gestión" o "GCO-FT-003 Matriz de riesgos del proceso de contratación, según corresponda*…", como resultado de la verificación, se observó cumplimiento al requisito y la publicación de 29 matrices de riesgos en la plataforma "SECOP II" y correspondientes a los contratos de clase: Prestación de Servicios y Prestación de Servicios Profesionales y de Apoyo a la Gestión, por otro lado, al contrato de clase: Orden de Compra no se observó matriz de riesgo publicada en el portal de "Colombia Compra Eficiente".

Ahora bien, la OCI realizo la verificación individual de las 29 matrices de riesgo y se observó lo siguiente:

- **Inconsistencias entre el tipo de riesgo identificado y la descripción:** la Matriz de Riesgo soporte del contrato No. 123 de 2023 con objeto *"Renovación del licenciamiento del software como servicio SaaS Planview para la gestión de proyectos de la Unidad de Búsqueda de Personas Dadas por Desaparecidas en el contexto y en razón del conflicto armado."*, **el riesgo No. 2** se tipifico como "Social/Político" y en la descripción se registró: *"…RIESGOS OPERACIONALES: Incumplimiento con la entrega de la renovación del licenciamiento adquirido por parte del proveedor…"*; **el riesgo No. 4** se tipifico como "Regulatorio" y en la descripción se registró: *"…RIESGOS OPERACIONALES: Falla en la herramienta de software adquirida…"*; **el riesgo No. 5** se tipifico como "Regulatorio" y en la descripción se registró: *"…RIESGOS OPERACIONALES: Falla en la calidad y/o oportunidad en la prestación del servicio de soporte contratado…"*; De acuerdo con lo anterior, no se observó pertinencia entre las descripciones y las tipologías asignada a los riesgos.

- **Posibles fallas en la identificación de riesgos:** del total de 30 procesos contractuales identificados en la vigencia 2023, relacionados con las Tecnologías de la Información y las Comunicaciones y bajo la supervisión de individual de: la Oficina de Tecnologías de la Información y las Comunicaciones OTIC o la Subdirección de Gestión de la Información para la Búsqueda SGIB o conjunta entre estas dependencias, se identificó un total de 104 riesgos registrados en las 29 matrices de riesgos (publicados en la plataforma SECOP II) correspondientes a los procesos contractuales para "Prestación de Servicios Profesionales y de Apoyo a la Gestión" y de "Prestación de Servicios", donde, se observaron las siguientes cifras:

Económicos	Sociales o Políticos	Operacionales	Financieros	Regulatorios	Naturaleza	Ambientales	Tecnológicos	Total
1	5	86	3	5	0	4	0	104
0,96 %	4,81 %	82,69 %	2,88 %	4,81 %	0,00 %	3,85 %	0,00 %	100 %

Fuente: formatos "GCO-FT-003 V1 matriz de riesgos del proceso de contratación" publicados en SECOP II

De lo anteriormente presentado, se puede observar que de los 29 procesos contractuales que cuentan con matrices de riesgo contractuales y publicadas en la plataforma "SECOP II", el 86,29 % (25) cuentan únicamente con 1 solo tipo de riesgo identificado y las 4 restantes presentan otros análisis de riesgos.

Nº DE CONTRATO INTERNO	Económicos	Sociales o Políticos	Operacionales	Financieros	Regulatorios	Naturaleza	Ambientales	Tecnológicos
031-2023-UBPD			3					
032-2023-UBPD			3					
042-2023-UBPD			3					

Nº DE CONTRATO INTERNO	Económicos	Sociales o Políticos	Operacionales	Financieros	Regulatorios	Naturaleza	Ambientales	Tecnológicos
046-2023-UBPD			3					
047-2023-UBPD			3					
048-2023-UBPD			3					
049-2023-UBPD		2	2	1	2		1	
050-2023-UBPD			3					
054-2023-UBPD			3					
059-2023-UBPD			3					
061-2023-UBPD			3					
063-2023-UBPD			3					
070-2023-UBPD			3					
071-2023-UBPD			3					
072-2023-UBPD			3					
073-2023-UBPD			3					
074-2023-UBPD			3					
076-2023-UBPD			3					
077-2023-UBPD			3					
078-2023-UBPD			3					
079-2023-UBPD		2	2	1	2		1	
080-2023-UBPD			3					
081-2023-UBPD			3					
082-2023-UBPD			3					
083-2023-UBPD			3					
099-2023-UBPD			3					
117-2023-UBPD			3					
123-2023-UBPD	1		5	1	1		1	
142-2023-UBPD		1	2				1	
OC-108231								
Total Contratos: 30	**1**	**5**	**86**	**3**	**5**	**0**	**4**	**0**
	0,96%	**4,81%**	**82,69%**	**2,88%**	**4,81%**	**0,00%**	**3,85%**	**0,00%**

Fuente: formatos "GCO-FT-003 V1 matriz de riesgos del proceso de contratación" publicados en SECOP II; tipificaciones de riesgos extraídas del Numeral 2 Identificar y clasificar los Riesgos, según Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación M-ICR-01 de Colombia Compra Eficiente

De lo anterior y tal como lo muestra la anterior tabla, resulta importante mencionar, que las tipificaciones de los riesgos de las 29 matrices de riesgos, se observaron agrupadas en 2 tendencias de análisis de riesgos, así: i) 25 matrices de riesgo con un solo tipo de riesgo identificado como "Operacionales" y ii) 4 matrices de riesgo con más de un tipo de riesgo identificado y repetitivos, situaciones que, corresponderían a un posible ejercicio sistemático de cumplimiento de requisitos contractuales y de ausencia de análisis más amplios de riesgos, por otro lado, y lo que resulta aún

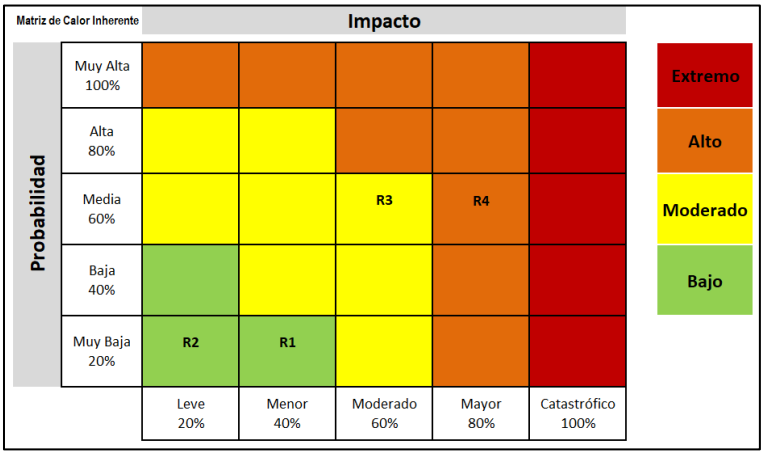
más preocupante es que, ninguna matriz cuenta con identificación de riesgos de tipo “Tecnológicos”, más aún, cuando se trata de procesos contractuales directamente relacionados con las Tecnologías de la Información y las Comunicaciones.

Así las cosas, los análisis de riesgo deben reflejar la mayor parte de la(s) situación(es) de impacto y probabilidad que puedan afectar los procesos contractuales, asimismo, del sector de origen (TIC) o en el que se va a desarrollar o ejecutar el bien y/o servicio contratado, por lo tanto, se recomienda realizar análisis de riesgos más amplios y pertinentes.

6.1.5. Riesgos de Gestión TI

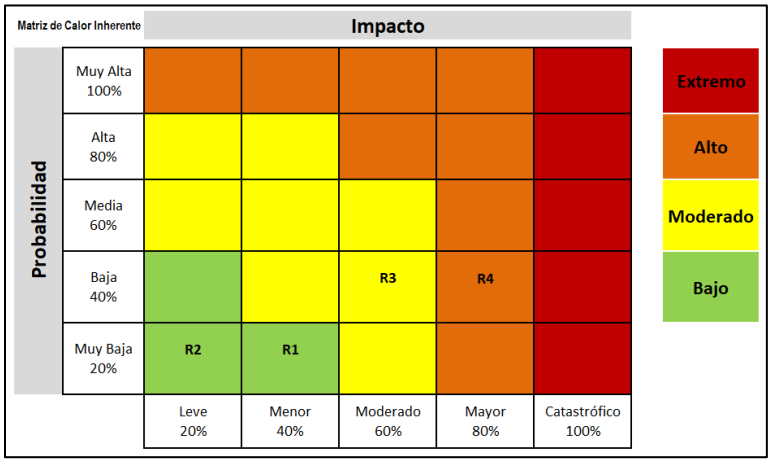
La Oficina de Tecnologías de la Información y las Comunicaciones OTIC, al corte del presente seguimiento tiene publicado en el Sistema Integrado de Gestión SIG, el formato “GTI-MR-001 V3” correspondiente a la “Matriz de Riesgos de Gestión” con fecha de actualización del 05 de noviembre de 2021, donde, se observó un total de 4 riesgos y se ubican en los Mapas de Calor así:

- Mapa de Calor – Riesgo Inherente (antes de Controles)



Fuente: archivo “GTI-MR-001 V3 Gestión de Tecnologías de la Información y Comunicaciones 05-11-2021.xlsx”

- Mapa de Calor – Riesgo Residual (después de Controles)



Fuente: archivo "GTI-MR-001 V3 Gestión de Tecnologías de la Información y Comunicaciones 05-11-2021.xlsx"

En lo relacionado a Riesgos tipificados como "Altos" ubicados en zona de riesgos inherentes y residuales, se observó el riesgo No. 4 "Posibilidad de afectación reputacional por la vulneración de la seguridad digital de la entidad debido al inadecuado establecimiento y aplicación de los mecanismos, directrices y estrategias necesarios para la gestión de la seguridad digital", donde, el líder del proceso identificó y estableció lo siguiente:

Impacto	Causa Inmediata	Causa Raíz
Reputacional	vulneración de la seguridad digital de la entidad	Inadecuado establecimiento y aplicación de los mecanismos, directrices y estrategias necesarios para la gestión de la seguridad digital.

Controles:

- El Experto Técnico designado para los temas de seguridad digital del proceso de Gestión de TIC analiza cuando se requiera durante la vigencia, el diseño e implementación de los mecanismos directrices y lineamientos de manera articulada, teniendo en cuenta el contexto de la UBPD en materia de seguridad de la información y seguridad digital, los estándares o buenas prácticas en esta materia y la legislación, vigente, con el fin de proteger la información de la entidad, dejando como evidencia la documentación sobre lo realizado; en caso de no contar con los mecanismos, directrices o lineamientos implementados se deberá monitorear el comportamiento de las herramientas tecnológicas para identificar debilidades o situaciones anómalas y en el marco de las posibilidades generar acciones sobre las mismas.

- El Experto Técnico designado para los temas de seguridad digital del proceso de Gestión de TIC anualmente diseña y ajusta en caso de requerirse las políticas de seguridad digital y las pone a

consideración de las instancias respectivas para su aprobación, posteriormente realiza la implementación durante la vigencia, de las acciones necesarias que permitan dar cumplimiento a las políticas institucionales de seguridad de la información y seguridad digital, en caso de no contar con políticas aprobadas se deberá formular un plan para la identificación e implementación de controles tecnológicos en las diferentes dependencias de la Entidad. Como evidencia se tendrá correos, actas, modificaciones de política de seguridad digital, presentaciones, listas de asistencia o grabaciones según aplique.

De acuerdo con lo observado, los riesgos de gestión de la Oficina de Tecnologías de la Información OTIC con corte al presente seguimiento, se mantienen iguales en cuanto a identificación, análisis y estado de actualización de riesgos, lo anterior, teniendo en cuenta que el formato "GTI-MR-001 V3" correspondiente a la "Matriz de Riesgos de Gestión" presenta fecha del 05 de noviembre de 2021, hecho igualmente comunicado por la OCI en el informe de seguimiento de la vigencia 2022, comunicado a través de memorando UBPD-3-2022-009133 del 28 de junio de 2022.

De acuerdo con lo anterior, y para las Tecnologías de la Información y las Comunicaciones TIC ya existentes, por adquirir y/o implementar en la unidad y que, asimismo, se encuentran identificadas como "Emergentes" por MinTIC (https://gobiernodigital.mintic.gov.co/692/articles-160829_Guia_Tecnologias_Emergentes.pdf), en este sentido, se recuerda que la OCI realizó un análisis relacionado en el numeral 7 y lo recomendó en el numeral 9, del informe de seguimiento al uso y apropiación de bienes y tecnologías que apoyan la misión en la vigencia 2022, comunicado a la OTIC a través de memorando UBP-3-2022-009263 del 30 de junio de 2022, así: *"… Para las etapas de Análisis, Desarrollo, Implementación y Sostenimiento de "Tecnologías Emergentes" en la UBPD, se recomienda hacer uso como buena práctica del documento "Guía con lineamientos generales para el uso de tecnologías emergentes" del MinTIC, donde, se define la ruta para la implementación de este tipo de tecnologías…",* lo anterior y como bien se sabe, la industria de las tecnologías de la información y las comunicaciones, son susceptibles a cambios muy frecuentes por innovaciones y/o nuevas tendencias, por lo que se generan riesgos no contemplados en la gestión general.

6.1.6. Estado de Actividades según Observaciones y/o Recomendaciones OCI

- **P9: Indicar por favor, si la OTIC ha adelantado actividades relacionadas con las observaciones y/o recomendaciones emitidas por la OCI en el Informe de seguimiento liberado el 28 de junio de 2022 mediante memorando UBPD-3-2022-009133.**

  Respuesta OTIC: *"Para dar respuesta a lo requerido es menester indicar que, mediante Memorando UBPD-3-2022-009636 con asunto "Respuesta: Informe de Seguimiento a los Riesgos de Gestión relacionados con las Tecnologías de la Información y las Comunicaciones" y fechado del 11 de julio de 2022, la OTIC informó las acciones inmediatas que se ejecutan de conformidad con el referido informe, así mismo, se indicó la pertinencia de las observaciones y recomendaciones de la OCI, en tal sentido, se listan a continuación las acciones que se implementaron por parte de la OTIC:*

Para la vigencia 2022 desde la oficina asesora de planeación se realizó el monitoreo de mapa de riesgos de gestión donde se analizó el cumplimiento a la ejecución de los 4 riesgos, 6 controles y 2 acciones de tratamiento formuladas para la mitigación del riesgo.

Observaciones:

No se observó avales, firmas o aprobaciones por parte del Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC en los documentos de "Plan de Implementación de Protección y Seguridad Digital 2022" y en el "Informe Ejecutivo", solo se observó la firma del Experto Técnico que lo elaboró.

El Plan Estratégico de Seguridad Digital contiene la aprobación por parte del Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, de este se desprende del Plan de Implementación de Protección y Seguridad Digital 2022 entre otros documentos que fueron revisados y aprobados con el Plan Estratégico de Seguridad Digital.

Para el 2023 se unifica el en el "Plan_Implementacion_SSI_2023.xlsx", el cual fue aprobado por el comité de Seguridad de la Información del 1 de febrero de 2023 como está registrado en el "acta 001 2023", y se programa dentro de este para el mes de mayo 2023 la inclusión del Plan Estratégico de Seguridad Digital dentro del Plan Estratégico de Seguridad de la Información - PESI, continuando con la unificación y consolidación del Sistema de Seguridad de la Información.

Proyectó: Juan de Jesús Aponte Buitrago, Contratista-. 20/12/2021
Revisó: Cristian Eduardo Zanguña Ruiz- Experto Técnico 22/02/2022
Aprobó: Oscar Javier Suarez Ramos- Jefe OTIC 25/03/2022

Para las actividades "Actualización de riesgos de Seguridad Digital de los procesos de la UBPD Identificados" y "Elaboración de planes de tratamiento de riesgo (si aplica) resultantes del retest." del Plan de Implementación de Protección y Seguridad Digital 2022, no se observó avance registrado en el Informe Ejecutivo presentado por la OTIC, teniendo en cuenta que el alcance hace parte de los periodos de ejecución indicados en el informe precitado.

Dentro de los seguimientos realizados para la remediación de las vulnerabilidades del retes se realiza registro en las matrices por cada responsable de los avances y evidencias de las actividades realizadas, así como resultado de las mismas, adicionalmente se genera un informe mensual.

Si bien el Plan de Protección y Seguridad Digital se estructura en 6 componentes, dentro del Plan, no se presenta una descripción de cada uno, donde es muy importante incluir una definición del componente, de modo que para el lector se pueda identificar con claridad qué se busca con el

mismo y si las actividades propuestas responden a tal objetivo. Dentro del Plan de Implementación de Protección y Seguridad Digital 2022, se encuentran planes de Sensibilización, Transferencia de Conocimiento y Comunicación, de los cuales solo el último cuenta con una breve definición. Al igual que con los componentes, es necesario que se definan estos planes de forma que sea claro cuál es el objetivo de su diseño e implementación y el vínculo con los componentes señalados. De otro lado, la tabla de contenido presente en el Plan de Implementación de Protección y Seguridad Digital 2022, no da cuenta de la totalidad de componentes en los que se organiza el Plan, así como sugiere una estructura incorrecta, pues se entiende que los planes de Sensibilización, Transferencia de Conocimiento y Comunicación están contemplados dentro del último componente, el de Seguimiento.

En el Plan Estratégico de Seguridad Digital del cual se desprende el Plan de Protección y seguridad Digital 2022 se define cada uno de los componentes y los elementos que se deben desarrollar en cada uno de ellos.

Dentro del Plan de Protección y seguridad Digital 2022, se incluyen las actividades pertenecientes al plan de Sensibilización, Transferencia de Conocimiento y Comunicación; para el 2023 se crea un documento denominado Plan de Uso y Apropiación de seguridad de la Información el cual se encuentra en ejecución en su primera versión y actualmente se está actualizando por parte de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC; las actividades allí contempladas se han venido ejecutando conforme lo programado.

Actualizar la información registrada en la herramienta "ISOLUCION" tipo Saas (Software como un Servicio), utilizada para la gestión, monitoreo y evaluación anual de los riesgos de Seguridad Digital y de Gestión por parte de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC.

Se realizó cargue de los riesgos de Seguridad Digital en la herramienta ISOLUCION.

Mantener anualmente y de forma programada, los espacios de capacitación y de comunicación, relacionados con los Riesgos de Seguridad Digital o Ciberseguridad, asimismo, en el uso de las Tecnologías de la Información y las Comunicaciones.

Plan de Uso y Apropiación de seguridad de la Información el cual se encuentra en ejecución en su primera versión y actualmente se está actualizando parte de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, las actividades allí contempladas se han venido ejecutando conforme lo programado.

***Nota**: El archivo se encuentra en el repositorio diferente debido a su contenido, tamaño, cantidad de archivos o estructura para seguimiento, serán garantizados los accesos a los mismos para la respectiva revisión por parte de la Oficina de Control Interno."*

6.2. Análisis y Evaluación de Riesgos de Seguridad de la Información

Contexto: "*La Norma ISO 27001 establece la necesidad de un proceso de evaluación de riesgos de seguridad de la información, el cual debe*

- *Establecer y mantener los criterios de riesgo de seguridad de la información, los cuales deben incluir los criterios de aceptación del riesgo y los criterios para realizar evaluaciones de riesgo de seguridad de la información.*
- *Asegurar que las evaluaciones de riesgo de seguridad de la información repetidas produzcan resultados consistentes, válidos y comparables.*
- *Identificar los riesgos de seguridad de la información, así como aplicar el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados con pérdida de confidencialidad, integridad y disponibilidad de la información.*
- *Identificar a los propietarios de los riesgos.*
- *Evaluar las consecuencias potenciales que resultarían si los riesgos identificados fueran a materializarse, evaluando la probabilidad realista de ocurrencia de los riesgos identificados, determinando los niveles de riesgo.*

El proceso de evaluación de riesgos de seguridad de la información está directamente relacionado con la Norma ISO 31000 de Gestión de Riesgos, pues la misma contiene los lineamientos fundamentales para gestionar el riesgo al que se enfrenta cualquier tipo de organización, dado que proporciona un enfoque común para gestionar cualquier tipo de riesgo, ya que no es específico de un sector o industria en particular."[1]

En este sentido, la OCI solicito al Oficial de Seguridad de la Información OSI, dar respuesta soportada con evidencias a las siguientes preguntas:

- **P10: ¿Se han establecido evaluaciones de riesgo de seguridad de la información a intervalos planificados o cuando ocurren cambios significativos?**

  Respuesta OSI: *"El primer ejercicio de identificación de riesgos de seguridad de la información fue adelantado en el año 2020 por medio de la consultoría en el marco de la ejecución del contrato 183-2019, los cuales se encuentran registrados en la plataforma de gestión ISOlución. Posterior a esto, luego de la actualización de la metodología de riesgos de seguridad de la información, se realizó un segundo ejercicio de identificación de riesgos de seguridad en la vigencia 2022, posterior al ejercicio de identificación, clasificación y aceptación de activos de información".*

[1] Guía de Seguridad de la Información, Autor: www.auditool.org

- **P11: ¿De qué forma se documentan las evaluaciones de riesgos de seguridad de la información realizadas por la Unidad?**

  Respuesta OSI: *"De acuerdo con lo definido en el documento Metodología Gestión de Riesgos de Seguridad de la Información, el cual se encuentra dentro de la documentación del SSI y está publicado en el Sistema Integrado de Gestión, esta se definió de acuerdo con los lineamientos emitidos por la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por del DAFP, en su versión más reciente. Adicionalmente, se incluyó dentro del procedimiento DPE-PR-008 Administración de Riesgos, el componente de seguridad de la información con el fin de mantener de forma articulada con la Oficina Asesora de Planeación, las actividades requeridas para la administración del riesgo. Finalmente, estas estrategias se ven plasmadas dentro de la matriz de riesgos de seguridad de la información, tomando como insumo la identificación de activos de información de cada uno de los procesos, como elementos a evaluar, los que cuentan una calificación en alta.".*

- **P12: ¿Se toman acciones específicas sobre los resultados de las evaluaciones de riesgo de seguridad de la información realizadas?**

  Respuesta OSI: *"A la fecha se han adelantado ejercicios de identificación y definición de tratamiento de riesgos de seguridad de la información en cada uno de los procesos de la Entidad donde la criticidad del activo sea Alta; lo previsto para esta vigencia de acuerdo a lo definido en el plan de trabajo del sistema de seguridad de la información, es ejecutar las acciones definidas en la matriz de riesgos de seguridad de la información, tal como la implementación de controles establecidos en el plan de tratamiento de cada uno de los procesos en que se hayan identificado los riesgos, Se adjunta la matriz de riesgos consolidada a la fecha.".*

- **P13: ¿Existe un plan de tratamiento de riesgos de seguridad de la información formalmente establecido y documentado?**

  Respuesta OSI: *"En el proceso de identificación de los riesgos de seguridad de la información se establece un plan de tratamiento de riesgos, de acuerdo a lo definido en la metodología de riesgos de seguridad de la información la cual se encuentra formalizada dentro del Sistema de Seguridad de la Información".*

- **P14: ¿Se toman acciones sobre los riesgos identificados y no cubiertos, y sobre los riesgos residuales existentes? ¿Cómo se documentan las acciones acordadas?**

Respuesta OSI: *"A la fecha se han adelantado ejercicios de identificación y definición de tratamiento de riesgos de seguridad de la información en cada uno de los procesos de la Entidad, no se han identificado riesgos que no estén cubiertos, en cuanto al riesgo residual, una vez finalice la implementación de los controles que reducirán el riesgo, se realizará una nueva valoración de los riesgos.".*

- **P15: en el marco del procedimiento "Seguimiento al Sistema de Seguridad de la Información" GSI-PR-001 SGSI V1, donde, el responsable de las actividades es el Oficial de Seguridad de la Información OSI, por favor aportar evidencia de:**

  - **P15.1: Actividad 11 Realizar seguimiento a los planes de acción de tratamiento de los riesgos (sin registro identificado en el procedimiento)**

    Respuesta OSI: *"Debido a que a la fecha no se ha realizado la implementación del plan de tratamiento de riesgos de seguridad de la información, no se ha realizado seguimiento a los mismos.".*

  - **P15.2: Actividad 12 Generar informe ejecutivo de los seguimientos realizados a los planes de acción (registro: Informe ejecutivo del monitoreo de los indicadores del Sistema de Seguridad de la Información).**

    Respuesta OSI: *"Debido a que a la fecha no se ha realizado la implementación del plan de tratamiento de riesgos de seguridad de la información, no se ha realizado seguimiento a los mismos.".*

  - **P15.3: Actividad 13 Informar al Comité de Seguridad de la Información (registro: Acta del Comité de Seguridad de la Información).**

    Respuesta OSI: *"Si bien a la fecha no se ha realizado la implementación del plan de tratamiento de riesgos de seguridad de la información, en la sesión 1 para la vigencia 2023 se informó al comité de seguridad de la información, que el año inmediatamente anterior se adelantó el ejercicio de identificación y definición de tratamiento de riesgos de seguridad de la información en cada uno de los procesos de la Entidad".*

  - **P15.4: Actividad 14 Revisar informes e identificar las oportunidades de mejora (registro: Acta del Comité de Seguridad de la Información).**

    Respuesta OSI: *"Dentro de las oportunidades de mejora que ha tenido el sistema de seguridad de la información, se realizó la unificación y fortalecimiento de las políticas de seguridad la información junto con la de seguridad digital, adicionalmente la actualización de controles y lineamientos en concordancia a lo establecido por la normativa vigente y las*

buenas prácticas de seguridad de la información como es la NTC ISO 27001:2022. Adicionalmente se actualizó el instrumento de autodiagnóstico con el fin de verificar el estado de implementación de los controles de acuerdo con las necesidades en materia de protección de información en la Unidad.".

- **P15.5: Actividad 15 Realizar seguimiento a medidas a partir de oportunidades de mejora identificadas (sin registro identificado en el procedimiento), de lo anterior, resulta importante mencionar que, la descripción de la actividad hace mención del documento "Metodología de Seguimiento al Sistema de Seguridad de la Información", el cual no fue observado en los documentos del SIG del proceso de Gestión de Seguridad de la Información, por lo cual, agradecemos adicionalmente nos informe sobre el estado del documento precitado.**

  Respuesta OSI: *"Como se indica en la respuesta anterior, se han adelantado actividades de mejora continua en el Sistema de Seguridad de la Información y se tomó como referencia el documento Metodología de Seguimiento al Sistema de Seguridad de la Información, adelantado por la consultoría realizada en el marco del contrato 183-2019, al ser un documento de referencia, y dado que el seguimiento lo realiza el Oficial de seguridad de la información, no se requirió codificarlo ya que es categorizado como un documento de apoyo.".*

De acuerdo con lo anterior, se observaron procesos documentados de identificación, análisis y valoración de riesgos al corte de 2022, asimismo, de ejercicios de identificación y definición de tratamientos de riesgo identificados con criticidad "Alta", lo anterior, en el marco de las actividades para el tratamiento de riesgos definidas en la "Metodología de Gestión de Riesgos de Seguridad de la Información".

Por otro lado, el cierre del ciclo de la gestión del riesgo se da una vez sea implementado el Plan de Tratamiento de Riesgos de Seguridad de la Información y posteriormente su respectivo proceso de seguimiento, actividades que al corte del presente seguimiento no se han realizado, según lo informado por el Oficial de Seguridad de la Información OSI; Así las cosas y como bien se sabe, es muy importante implementar las actividades que permitan que el ciclo de gestión del riesgo este completo, lo anterior, con el fin de determinar con suficiencia de datos, la efectividad de los controles establecidos en los tratamientos de riesgos, asimismo, obtener retroalimentación de los procesos con el fin de apoyar la toma de decisiones y la mejora continua.

6.3. Planes Institucionales

A continuación, se presenta el inventario de riesgos identificado:

6.3.1. Plan Anticorrupción y de Atención al Cliente – Mapa de Riesgos de Corrupción.

El Articulo No. 73 – Plan Anticorrupción y de Atención al Cliente de la Ley No. 1474 de 2011, establece que *"…Cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. Dicha estrategia contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias antitrámites y los mecanismos para mejorar la atención al ciudadano.*

El Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción señalará una metodología para diseñar y hacerle seguimiento a la señalada estrategia.

PARÁGRAFO. En aquellas entidades donde se tenga implementado un sistema integral de administración de riesgos, se podrá validar la metodología de este sistema con la definida por el Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción…".

Por otro lado, el Numeral 2.2.22.3.14 - Integración de los planes institucionales y estratégicos al Plan de Acción, del Articulo No. 1 del Decreto 612 de 2018, indica que *"…Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:*

…
9. Plan Anticorrupción y de Atención al Ciudadano
10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI
11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
12. Plan de Seguridad y Privacidad de la Información …"

En cuanto al "Plan Anticorrupción y de Atención al Ciudadano" de la UBPD para la vigencia 2023, este instrumento no tiene como objetivo realizar análisis y plantear el tratamiento de riesgos de anticorrupción, estas actividades se registran en el "Mapa de Riesgos de Corrupción", donde, para la vigencia 2023 se observó el riesgo "…*Posibilidad de pérdida de confidencialidad y/o de integridad de los archivos de información para favorecimiento propio o de terceros…*", con causas identificadas de: *"No aplicación de las políticas de protección y seguridad digital y general de seguridad, protección y confidencialidad de la información por parte de los servidores de la entidad.", "Alteración no autorizada de la configuración de los controles existentes" y "Ausencia o debilidades en el monitoreo oportuno y la definición de derechos de uso y acceso."*, donde, para mitigar y controlar el riesgo se definieron 6 actividades de control, bajo la responsabilidad de: Oficial de Seguridad de la Información OSI, Oficina de Tecnologías de la Información y las comunicaciones OTIC y la Dirección Técnica de Información Planeación y Localización para la Búsqueda DTIPLB, asimismo, el riesgo tiene tipificadas consecuencias de: Afectación Legal, Afectación Económica, Afectación Reputacional, Riesgo Físico a Personas, Pérdida de Confianza, y Retraso en la Búsqueda.

- Como cumplimiento normativo, el Plan Anticorrupción y de Atención al Ciudadano, se encuentra publicado en la página de la Unidad, en el siguiente link:

  https://ubpdbusquedadesaparecidos.co/wp-content/uploads/2023/01/Plan-Anticorrupcion-y-de-Atencion-al-Ciudadano-UBPD-2023.xlsx

- El Mapa de Riesgos de Corrupción, se encuentra publicado en la página de la Unidad, en el siguiente link:

  https://ubpdbusquedadesaparecidos.co/wp-content/uploads/2023/01/Mapa-Riesgos-de-Corrupcion-UBPD-2023.xlsx

6.3.2. Plan de Acción 2023

En lo relacionado con las Tecnologías de la Información y las Comunicaciones, se observaron 3 metas así:

- **Meta No. 20 (Indicador):** 100% de los datos en gobierno de datos (Sistema de Información Misional - SIM en uso, tableros de indicadores asociados a la búsqueda) y modelo de analítica de datos implementado.

  Riesgos básicos identificados: en matrices de riesgos de cada uno de los procesos contractuales, así: Contrato No. 181 de 2021, Contrato No. 229 de 2021, Orden de Compra No. 98967 del 09 de noviembre de 2022, matrices de riesgo relacionadas para la Oficina de Tecnologías de la Información y las Comunicaciones OTIC y la Subdirección de Gestión de la Información para la Búsqueda SGIB.

- **Meta No. 21 (Indicador):** Un (1) mecanismo de monitoreo y seguimiento del cumplimiento de la política seguridad de la información implementado (asegurar que no se impongan más restricciones al acceso a la información de las que ya están contempladas).

  Riesgos básicos identificados: matriz de riesgo relacionadas con el proceso de Gestión de Seguridad de la Información y matrices de riesgo correspondientes a procesos contractuales bajo su supervisión contractual.

- **Meta No. 28 (Indicador):** Meta 28. 100% de implementación del PETI de acuerdo con lo planeado en la vigencia 2023.

  Riesgos básicos identificados: matrices de riesgo relacionadas con la Oficina de Tecnologías de la Información OTIC y demás procesos con proyectos incorporados en el PETI, asimismo,

matrices de riesgo correspondiente a los procesos contractuales bajo la supervisión de los procesos responsables.

Si bien, en el Plan de Acción para la vigencia 2023, se estableció una meta relacionada con el 100 % de datos en el modelo de Gobierno de Datos, resultaría también muy importante, que se fijaran indicadores y/o metas relacionadas con la Gestión de la Información y de la Calidad del Dato a nivel funcional y técnico, lo anterior, teniendo en cuenta los problemas de atraso en el procesamiento y disposición de la información recibida y/o recolectada en aplicación de la misión de la Unidad. Asimismo, es vital que el resultado del procesamiento de la información sin importar su estructuración, responda a criterios definidos de calidad del dato, lo que mitigaría riesgos de análisis y presentación sin oportunidad, confiabilidad, completitud, pertinencia y utilidad; gestión de la información sin control o gobernanza; reputacionales; pérdida de confianza e incumplimiento al mandato.

6.3.3. Plan Estratégico de Tecnologías de la Información PETI 2021 - 2024

"…la UBPD mediante un formato desarrolla un esquema completo acorde con los contenidos metodológicos de la Guía para la Administración del Riesgo y el diseño de controles V5. El formato cuenta con celdas parametrizadas y permite contar con los respectivos mapas de calor para riesgo inherente y riesgo residual.

Riesgos para la OTIC:

Posibilidad de afectación económica por la inadecuada Identificación de necesidades tecnológicas debido a que las dependencias de la entidad no tienen claro las necesidades que pretenden satisfacer en términos de servicios tecnológicos.

Posibilidad de afectación económica por la inadecuada planeación de los proyectos de la OTIC, debido a cambios en las variables de tiempo, alcance, costos y actividades establecidas en la etapa de planificación de los proyectos de la OTIC.

Posibilidad de afectación reputacional por indisponibilidad de servicios tecnológicos debido a falla en los servicios prestados por el tercero u operador.

Posibilidad de afectación reputacional por la vulneración de la seguridad digital de la entidad debido al inadecuado establecimiento y aplicación de los mecanismos, directrices y estrategias necesarios para la gestión de la seguridad digital…"

Lo anterior corresponde a la identificación de los riesgos de gestión del proceso de Gestión de Tecnologías de la Información y las Comunicaciones, ampliados e identificados en los numerales 6.1.5 y 6.3.2 del presente informe.

6.3.4. Plan de Tratamientos de Riesgos de Seguridad de la Información

El documento "Metodología gestión de riesgos SI V2 30112022", contempla en el numeral 6.4 las actividades para realizar el tratamiento de riesgos, como lo son: la definición del tipo de tratamiento del riesgo y la elaboración del plan de tratamiento; asimismo, de la aceptación de planes de riesgos y del respectivo seguimiento, en este sentido se establecen las responsabilidades así:

i) Registro y documentación por parte de procesos que hacen parte de la "Primera Línea de Defensa" a través del *"…instrumento **GTI-MR-001 Mapa de Riesgos** en la sección que corresponda al PLAN DE TRATAMIENTO DE RIESGOS…*" (Negrita y Subrayado por fuera del texto original).

ii) Aceptación de Planes de Tratamiento, el Oficial de Seguridad de la Información OSI realiza la consolidación de los riesgos y los planes de tratamiento y comunica a los lideres de proceso el resultado para su aprobación.

iii) Seguimiento y validación a la efectividad de los controles del Plan de Tratamiento por parte del Oficial de Seguridad de la Información OSI.

De lo anterior resulta importante mencionar que, algunos documentos que soportan el proceso de Gestión de Seguridad de la Información y que se encuentran publicados en el Sistema Integrado de Gestión de la Unidad, se encuentran en proceso de actualización, lo anterior con el fin de que, se encuentren alineados a las necesidades y los objetivos estratégicos de la Unidad.

6.4. Gobierno de Datos

El programa de Gobierno de Datos en la Unidad debe dar la capacidad de gestionar el conocimiento sobre la información que se recibe, produce y se entrega, esto a partir de los lineamientos generados a partir del contrato No. 0229 de 2021, los que permitirán fijar una serie de procesos y responsabilidades de aseguramiento, calidad y la seguridad de los datos; asimismo, responder preguntas como:

- ¿Qué sabemos sobre nuestra información?
- ¿De dónde provienen esos datos?
- ¿Están estos datos alienados con nuestra política institucional?

En este sentido *"…La confianza de una empresa en sus datos tiene mucho que ver con llevar a cabo una gestión adecuada de los mismos. y, en este aspecto, el gobierno de datos juega un rol muy importante…"*, ahora bien, "… ***¿Qué sucedería si el gobierno de datos estuviese desligado a la***

gestión del riesgo? *Las consecuencias afectarían desde la calidad de datos a la arquitectura de sistemas, o de la administración de contenidos en línea a la gestión de metadatos…*".[2]

Por lo tanto, existen estrategias de apoyo en la gestión del riesgo para Gobierno de Datos, que deberían contemplar actividades de cálculo como lo podrían ser:

- **El valor de los datos:** *"…Si la empresa no sabe reconocer qué tipo de información tiene valor, no puede mejorar, proteger o medir sus datos…"*.

- **La probabilidad de riesgo:** *"…Saber cómo los datos se han usado y abusado en el pasado es un indicador de cómo podrían verse comprometidos en el futuro…"*.

- **El monitoreo en la eficacia de los controles:** *"…El gobierno de datos trata en gran medida sobre el comportamiento organizacional. Las organizaciones cambian todos los días, y por lo tanto sus datos, su valor y el riesgo también cambian rápidamente. Por desgracia, la mayoría de las organizaciones se evalúan a sí mismas sólo una vez al año. Pero en materia de datos, es necesario realizar controles organizacionales para satisfacer las demandas con una periodicidad diaria o semanal. Sólo así se podrá gobernar el cambio…". [3]*

De acuerdo con lo anterior, y tal como se estableció en la estrategia de "Acciones Concretas" y se ha observado por parte de la Oficina de Control Interno OCI, a través de los seguimientos al estado de desarrollo, implementación y uso del ecosistema tecnológico que apoya la misión de la Unidad, los procedimientos y demás documentación de Gobierno de Datos, la cual se encuentra en construcción y ajuste por parte de la Subdirección de Gestión de la Información para la Búsqueda SGIB y de la Oficina Asesora de Planeación OAP desde octubre de 2022; ahora bien y, como se argumentó anteriormente, es vital que se adelante y se materialice la gestión del riesgo propia al modelo de Gobierno de Datos y de esto, no es suficiente con la gestión del riesgo valorada en el mapa de riesgos del proceso de la SGIB.

7. CONCLUSIONES

- **6.1 Tecnologías de la Información y las Comunicaciones**

    - **P3. Encriptación de Datos Críticos:** se recomienda establecer el nivel de uso y apropiación de las herramientas de cifrado, asimismo, reforzar, comunicar y/o dar a conocer a la Unidad las herramientas con las que se cuenta, el objetivo, ventajas, riesgos y desafíos, como lo podrían ser: los nuevos tipos de ataques, dificultades para compartir información, perdida de información y problemas relacionados con accesos indebidos o malas prácticas.

[2] https://blog.es.logicalis.com/analytics/gobierno-de-datos-y-gestion-del-riesgo-una-union-indeleble
[3] https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/logra-un-gobierno-de-datos-que-asegure-la-calidad-de-la-informacion

Por otro lado, resulta muy importante que, a todo nivel se identifiquen los datos e información crítica y establecer el protocolo de manejo de estos, acompañado del respectivo análisis de riesgos, lo anterior, correspondería a actividades de gestión y de gobernabilidad de toda la información de la Unidad, así las cosas, se requiere agilizar y dar prioridad a la implementación del modelo de Gobierno de Datos.

- **P7. Acceso a través de dispositivos móviles personales:** resulta importante tener en cuenta que, el acceso a servicios institucionales como lo son el "Correo Electrónico" y el "Drive" no solo se realiza a través de las redes institucionales, sino que, también se realiza a través de dispositivos móviles personales con conexión a redes públicas o externas, donde, desde cualquier dispositivo tipo "Teléfono Celular" se accede a recursos y/o documentos internos, por lo tanto, se recomienda extender el control de acceso hacia los dispositivos móviles personales con acceso a redes externas.

- **6.1.4 Gestión Contractual TI:** se realizó la verificación individual de 29 matrices de riesgo y se observó lo siguiente:

  - **Inconsistencias entre el tipo de riesgo identificado y la descripción:** no se observó Pertinencia entre las descripciones y las tipologías asignada a los riesgos.

  - **Posibles fallas en la identificación de riesgos:** resulta importante mencionar, que las tipificaciones de los riesgos de las 29 matrices de riesgos, se observaron agrupadas en 2 tendencias de análisis de riesgos, así: i) 25 matrices de riesgo con un solo tipo de riesgo identificado como "Operacionales" y ii) 4 matrices de riesgo con más de un tipo de riesgo identificado y repetitivos, situaciones que, corresponderían a un posible ejercicio sistemático de cumplimiento de requisitos contractuales y de ausencia de un análisis más amplio de riesgos; por otro lado y, lo que resulta aún más preocupante, es que, ninguna matriz cuenta con identificación de riesgos de tipo "Tecnológicos", más aún, cuando se trata de procesos contractuales directamente relacionados con las Tecnologías de la Información y las Comunicaciones.

  Así las cosas, los análisis de riesgo deben reflejar la mayor parte de la(s) situación(es) de impacto y probabilidad que puedan afectar los procesos contractuales, asimismo, del sector de origen (TIC) o en el que se va a desarrollar o ejecutar el bien y/o servicio contratado, por lo tanto, se recomienda realizar análisis de riesgos más amplios y pertinentes.

- **6.1.5 Riesgos de Gestión TI:** para las Tecnologías de la Información y las Comunicaciones TIC ya existentes, por adquirir y/o implementar en la unidad y que, asimismo, se encuentran identificadas como "Emergentes" por MinTIC

(https://gobiernodigital.mintic.gov.co/692/articles-160829_Guia_Tecnologias_Emergentes.pdf), la OCI reitera la recomendación relacionada en el numeral 9, del informe de seguimiento al uso y apropiación de bienes y tecnologías que apoyan la misión en la vigencia 2022, comunicado a la OTIC a través de memorando UBP-3-2022-009263 del 30 de junio de 2022, lo anterior y como bien se sabe, la industria de las tecnologías de la información y las comunicaciones, son susceptibles a cambios muy frecuentes por innovaciones y/o nuevas tendencias, por lo que se generan riesgos no contemplados en la gestión general.

- **6.2 Seguridad de la Información**

  - **P15. Seguimiento al Sistema de Seguridad de la Información:** es muy importante implementar las actividades que permitan que el ciclo de gestión del riesgo este completo, lo anterior, con el fin de determinar con suficiencia de datos, la efectividad de los controles establecidos en los tratamientos de riesgos, asimismo, obtener retroalimentación de los procesos con el fin de apoyar la toma de decisiones y la mejora continua.

    La OCI recomienda para la vigencia 2024, contratar un servicio especializado que realice las pruebas de vulnerabilidad a los sistemas de información de la Unidad, con el fin de identificar oportunidades de mejora y validar la suficiencia y efectividad de las herramientas de detección implementadas a la fecha. Esta recomendación se hace teniendo en cuenta que, los ataques cibernéticos avanzan y en esa misma medida, deben avanzar las acciones de identificación de nuevos riesgos y ataques, para fortalecer las medidas y mecanismos de seguridad.

- **6.3 Planes Institucionales**

  - **6.2.2 Plan de Acción 2023:** se recomienda que, se fijen indicadores y/o metas relacionadas con la Gestión de la Información y de la Calidad del Dato a nivel funcional, lo anterior, teniendo en cuenta los problemas de atraso en el procesamiento y disposición de la información recibida y/o recolectada en aplicación de la misión de la Unidad. Asimismo, es vital que el resultado del procesamiento de la información sin importar su estructuración responda a criterios definidos de calidad del dato, lo que mitigaría riesgos de análisis y presentación sin oportunidad, confiabilidad, completitud, pertinencia y utilidad; gestión de la información sin control o gobernanza; reputacionales; pérdida de confianza e incumplimiento al mandato.

- **6.4 Gobierno de Datos**

- Tal como se estableció en la estrategia de “Acciones Concretas” y se ha observado por la Oficina de Control Interno OCI a través de los seguimientos al estado de desarrollo, implementación y uso del ecosistema tecnológico que apoya la misión de la Unidad, los procedimientos y demás documentación del modelo de Gobierno de Datos, se encuentran en etapas de construcción, ajuste y aprobación por parte de la Subdirección de Gestión de la Información para la Búsqueda SGIB y de la Oficina Asesora de Planeación OAP desde octubre de 2022; ahora bien, es vital que se adelante y se materialice la gestión del riesgo propia al modelo de Gobierno de Datos y de esto, no es suficiente con la gestión del riesgo valorada en el mapa de riesgos del proceso de la SGIB.

Cordialmente,

DIANA MARIA CALDAS GUALTEROS
Jefe Oficina de Control Interno.

Elaborado por:	Carlos Andres Rico Reina	**Experto Técnico**	FIRMA: 
Aprobado por:	Diana María Caldas Gualteros Jefe Oficina de Control Interno	**Jefe Oficina de Control Interno**	FIRMA: