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 Y CONTRACTUALES RELACIONADOS CON LAS TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES TICS

BOGOTÁ, D.C., JUNIO DE 2021

UBPD
UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

TABLA DE CONTENIDO

1. INFORMACIÓN GENERAL DEL SEGUIMIENTO	
Informe Seguimiento	Riesgos de Gestión y Contractuales de las Tecnologías de la Información y las Comunicaciones
Fecha	24 de junio de 2021

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 y Contractuales 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 2021 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, asimismo, a los riesgos que soportan la gestión contractual desarrollada por la OTIC.

2.2. ALCANCE

La Oficina de Control Interno OCI, realiza la verificación de la información relacionada con Lineamientos para el Diseño, Implementación y Seguimiento de Riesgos de Seguridad Digital, Documentos de análisis de Riesgos de Seguridad Digital, Documentación de análisis de Riesgos de Tecnologías de la Información y las Comunicaciones, Documentación de análisis de Riesgos en el marco del Contrato 0186 de 2019 (entregables o productos) y Análisis de Riesgos que hacen parte de la Gestión Contractual de la OTIC para la vigencia 2020 y al corte de abril de 2021.

2.3. MARCO LEGAL O ANTECEDENTES

- **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 Política de Administración de Riesgos, del 06 de noviembre de 2019
- GSI-PC-002 V1 Política de Protección y Seguridad Digital, del 23 de diciembre de 2020

3. FUENTES DE INFORMACION

- GTI-MR-001 V1 Mapa de Riesgos Gestión TIC 12-09-2019.pdf.
- GTI-MR-001 V2 Mapa de Riesgos de Gestón_OTIC.pdf
- Plan de Mejoramiento de la Contraloría General de la Republica – CGR, suscrito el 18 de diciembre de 2020, así:
    - **Hallazgo No. 5.** Pone en riesgo la implementación de los sistemas de información de la entidad, a través de los cuales se establezca estrategias, procesos y controles tecnológicos que permitan proteger la información y mitigar los riesgos y amenazas inherentes al uso de los sistemas de información:
        - **Acción de Mejora No. 6.** Política de seguridad digital. **Actividad.** Aprobación de la Política de seguridad digital.
        - **Acción de Mejora No. 7.** Política de seguridad digital. **Actividad.** Seguimiento a la implementación de la política de seguridad digital-
        - **Acción de Mejora No. 8.** Implementación y seguimiento de los controles tecnológicos sobre los sistemas que actualmente tiene la UBPD y apoyan el proceso de búsqueda con el fin de mitigar los riesgos y amenazas inherentes al uso de estos sistemas. **Actividad.** Definición de un plan de protección y seguridad digital 2021.
        - **Acción de Mejora No. 9**. Implementación y seguimiento de los controles tecnológicos sobre los sistemas que actualmente tiene la UBPD y apoyan el proceso de búsqueda con el fin de mitigar los riesgos y amenazas inherentes al uso de estos sistemas. **Actividad.** Implementación del plan de protección y seguridad digital 2021.
- Entregables correspondientes a Análisis de Riesgos en el marco del Contrato de Consultoría No. 186 de 2019
- GCO-FT-003 Matriz de Riesgos del Proceso de Contratación, según Procedimiento GCO-PR-010 V1 Solicitud de Inicio Trámite Contractual para Procesos de Selección.
- Soportes entregados por la Oficina de Tecnologías de la Información y las Comunicaciones OTIC como respuesta a la solicitud de información de la OCI realizada el 25 de mayo de 2021.

4. METODOLOGÍA

- Revisión, contraste y análisis de la información entregada por la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, como respuesta a solicitud de información realizada por la OCI.

- Revisión, contraste y análisis de la información publicada en el Sistema de Gestión de la UBPD, correspondiente a las versiones históricas de los Mapas de Riesgos de Gestión de la OTIC y su alineación con la Política de Administración de Riesgos y Planes Institucionales.

5. DESARROLLO

El día 25 de mayo de 2021 y con fecha de entrega para el 31 de mayo de 2021, la OCI solicitó a la OTIC la información relacionada con: Lineamientos para el Diseño, Implementación y Seguimiento de Riesgos de Seguridad Digital, Documentos de análisis de Riesgos de Seguridad Digital, Documentación de análisis de Riesgos de Tecnologías de la Información y las Comunicaciones, Documentación de análisis de Riesgos en el marco del Contrato 0186 de 2019 (entregables o productos) y Análisis de Riesgos que hacen parte de la Gestión Contractual de la OTIC al corte de abril de 2021; el 02 de junio de 2021 y ante la falta de respuesta por parte de la OTIC, la OCI reitera la solicitud de información realizada el 25 de mayo de 2021, donde, como respuesta el 03 de junio de 2021 la OTIC solicita un espacio de mesa de trabajo para la aclaración de dudas, para lo cual, la OCI y la OTIC acordaron realizarla el 04 de junio de 2021; como resultado de la mesa de trabajo anteriormente mencionada, la OTIC hizo entrega de la información solicitada el 10 de junio de 2021.

La información aportada por la OTIC fue revisada, contrastada y analizada bajo segmentaciones de Análisis del Diseño, Implementación y Seguimiento de Riesgos de Seguridad Digital, Análisis de Riesgos de Gestión TI, Análisis Independientes Riesgos TI, Análisis de Riesgos Contractuales TI y Planes Institucionales y los Riesgos TI.

6. RESULTADOS

6.1. Análisis del Diseño, Implementación y Seguimiento de Riesgos de Seguridad Digital

La Oficina de Tecnologías de la Información y las Comunicaciones OTIC, presentó el borrador del documento "*Metodología de Gestión de Riesgos de Seguridad de la Información y Seguridad Digital*", el cual, al corte del presente seguimiento se encontraba en trámite de formalización ante el Sistema de Gestión de Calidad.

El objetivo de la Metodología anteriormente mencionada, es "…*Definir la metodología de gestión de riesgos de seguridad de la información y seguridad digital, estableciendo de manera estructurada este documento con los diferentes lineamientos para identificar, analizar, valorar, tratar y dar seguimiento a los riesgos de seguridad que se presenten en la Unidad de Búsqueda de Personas Dadas por Desaparecidas – UBPD...*", más adelante, la Metodología contempla los siguientes capítulos:

- 6.1 Identificación de Riesgos
- 6.1.1 Identificación de Riesgos de Activos de Información
- 6.1.2 Identificación de Áreas de Impacto

- 6.1.3 Identificación de Factores de Riesgo
- 6.1.4 Identificación del Riesgo
- 7 Valoración de Riesgos
- 7.1 Análisis de Riesgos
- 7.2 Evaluación de Riesgos
- 8 Consolidación de Riesgos
- 9 Tratamiento de Riesgos
- 10 Hoja de Ruta para la Aplicabilidad e Implementación de Controles
- 11 Seguimiento

De acuerdo a la organización de la UBPD, la definición y perfeccionamiento de metodologías, políticas, planes, gestión de riesgos, etc., relacionadas con la Seguridad Informática o Seguridad Digital están a cargo de la OTIC, esto en concordancia con lo establecido en el Decreto No. 1393 de 2018, Artículo No. 7 Funciones de la Oficina de la Oficina de Tecnologías de la Información y numeral 4 "…*Diseñar e implementar las políticas de seguridad informática y los planes de contingencia de la UBPD...*".

Por otro lado, lo correspondiente a la gestión de la Seguridad de la Información le compete al "*Comité de Seguridad de la Información*", conformado mediante la Resolución No. 0537 del 11 de mayo de 2020, donde la Gestión de Riesgos se estableció en el Articulo No. 5 - Asuntos a tratar por el Comité de Seguridad de la Información y en el literal b) "*Prevenir, proteger y mitigar los riesgos y reaccionar frente a estos, priorizando la salvaguardia de la información que reciba, recaude o produzca la UBPD, preservando el carácter de entidad humanitaria y extrajudicial*", posteriormente, el 08 de junio de 2020 mediante la Resolución No. 0588 de 2020, se definió la estructura y los roles del Sistema de Seguridad de la Información SSI, donde, uno de sus principios es "…*garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y mitigados por la UBPD, de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, en el entorno y en las tecnologías...*".

En lo que respecta a funciones de los miembros del Comité de Seguridad de la Información y relacionadas con Gestión del Riesgo, se observó lo siguiente:

- El (la) Oficial de Seguridad de la Información: "*h. Dirigir, coordinar o supervisar (según el caso) las medidas y respuestas frente a ataques, amenazas y escenarios de riesgos contra la seguridad de la información de la UBPD, con el apoyo de la Oficina de Tecnologías de la Información y las Comunicaciones y/o de la Dirección Técnica de Información, Planeación y localización para la Búsqueda de acuerdo con los criterios y principios definidos".*
- La (el) Subdirectora (r) General Técnica y Territorial: "*b. Hacer seguimiento a la observancia y advertir sobre los riesgos en materia de protección de la Información.*".
- El (La) Subdirector (a) de Gestión de Información para la Búsqueda: "*c. Hacer seguimiento al cumplimiento de las directrices en materia de protección de la información y advertir riesgos*."

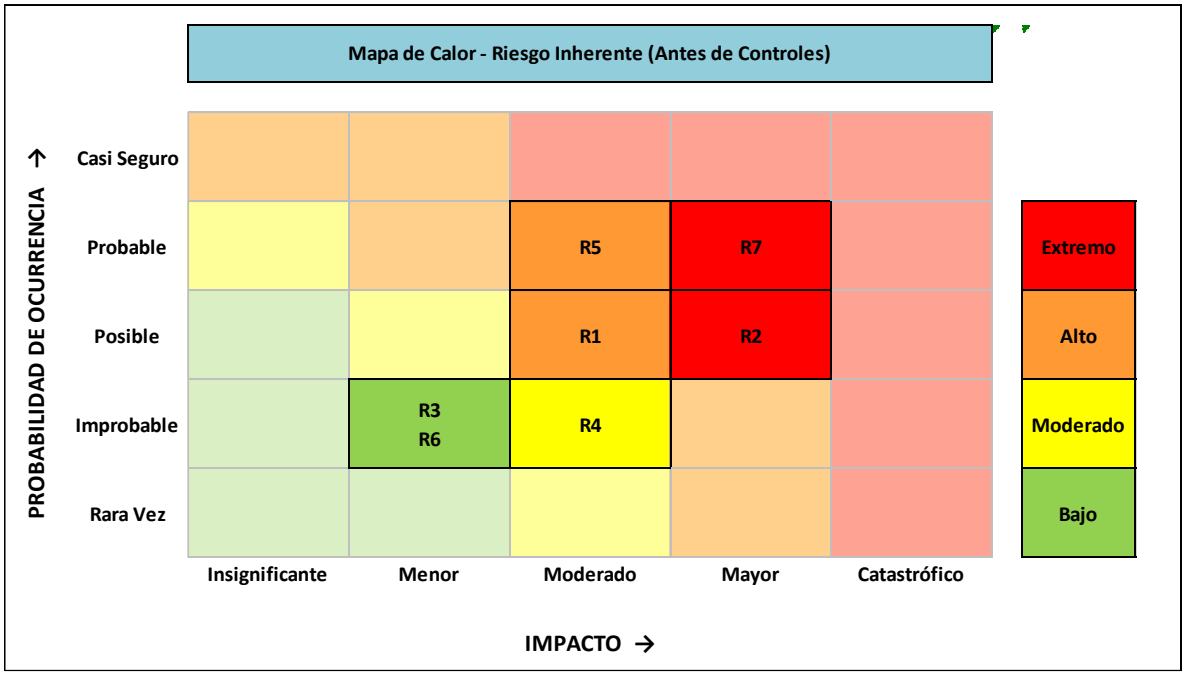
El Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC es miembro del Comité de Seguridad de la Información y lo concerniente hacia la Seguridad Digital, tiene asignadas las siguientes funciones:

- a) Diseñar e implementar las políticas de seguridad digital de la UBPD de acuerdo con los criterios y principios definidos.
- b) Desarrollar estrategias para garantizar la seguridad digital de la UBPD.
- c) Coordinar o implementar, según el caso y concertadamente con el Oficial de Seguridad de la Información, las acciones, medidas o planes de contingencia para la seguridad digital.

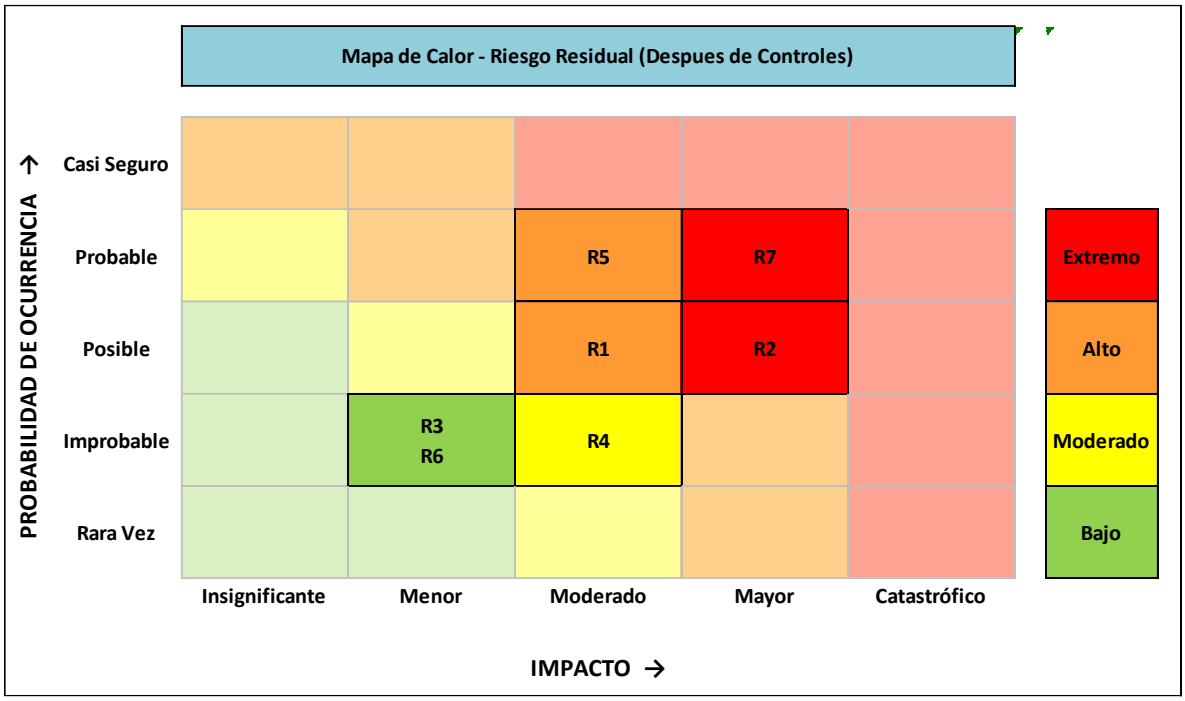
6.2. Análisis de Riesgos de Gestión TI

La Oficina de Tecnologías de la Información y las Comunicaciones OTIC, al corte del presente seguimiento tiene publicados en el Sistema de Gestión, (2) versiones del Mapa de Riesgos de Gestión TIC, correspondientes a los análisis de las vigencias de 2019 (primer ejercicio realizado con equipo consultor) y 2020 (monitoreo y actualización según metodología de la Oficina Asesora de Planeación OAP), donde, como resumen de la gestión de análisis de los Riesgos TI realizados durante las vigencias anteriormente mencionadas, se presenta el siguiente contraste de resultado entre los tratamientos aplicados, así:

- Tratamiento de Riesgos TI - Vigencia 2019



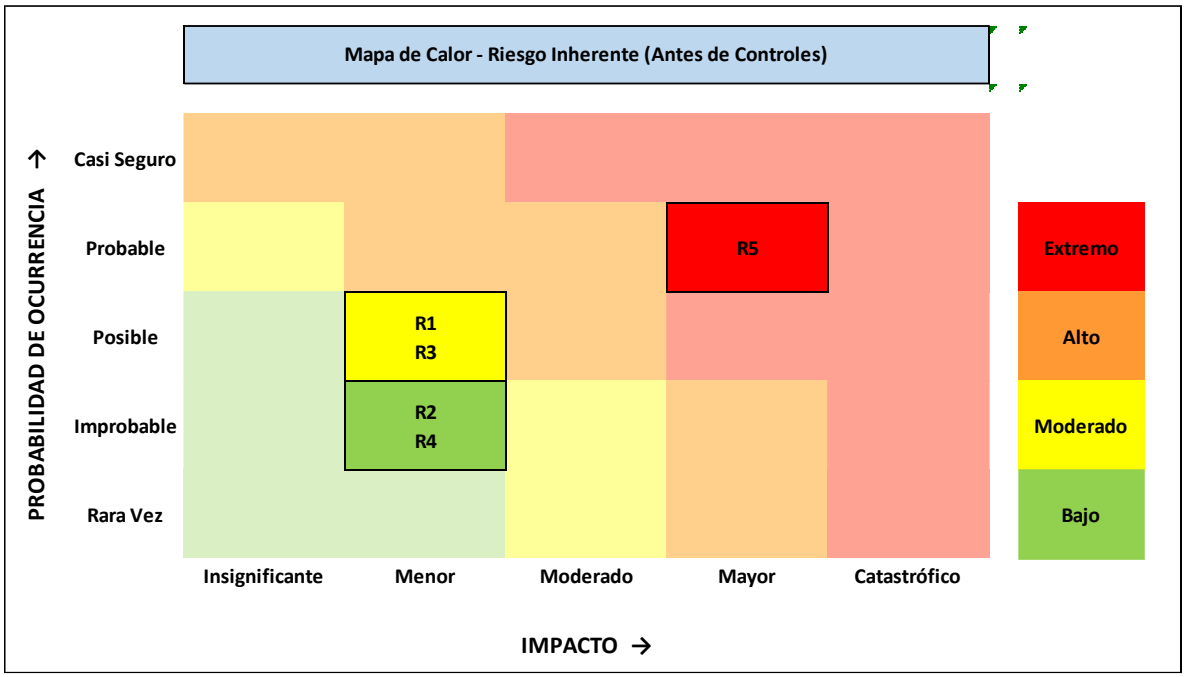
Fuente: archivo "GTI-MR-001 V1 Mapa de Riesgos Gestión TIC 20-09-2019"



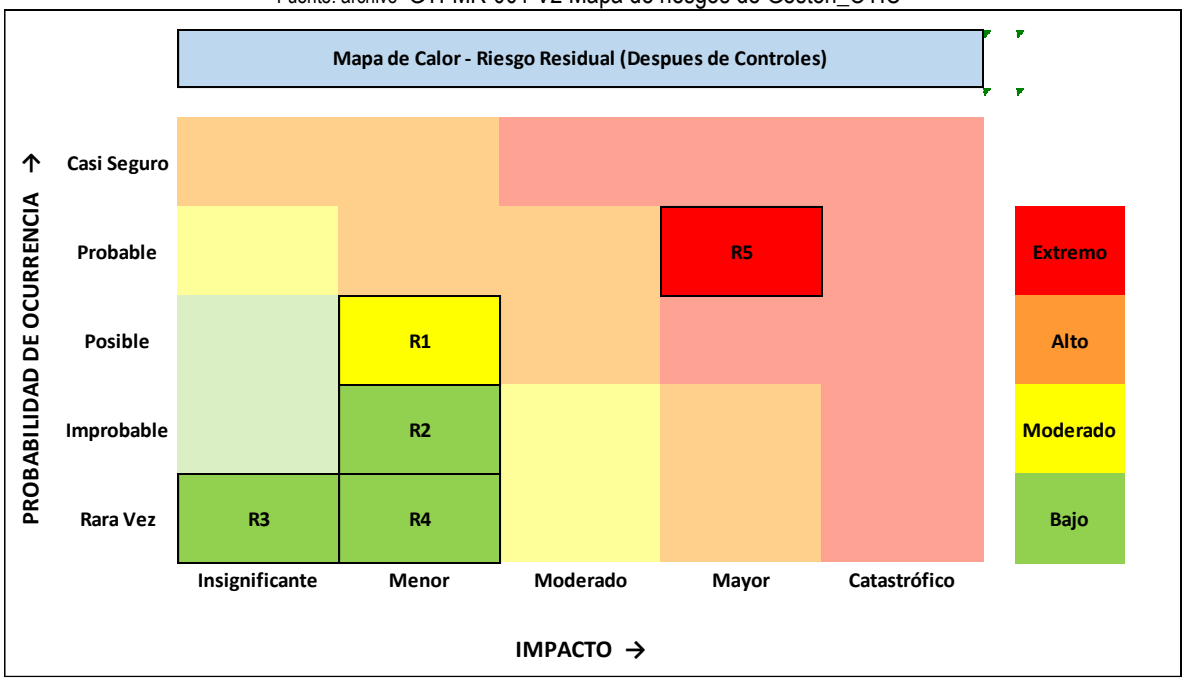
Fuente: archivo "GTI-MR-001 V1 Mapa de Riesgos Gestión TIC 20-09-2019"

De acuerdo con lo anterior, se observó que los (7) riesgos inherentes y residuales identificados, para la vigencia 2019, estaban ubicados en los mismos cuadrantes, luego del tratamiento dado al riesgo inherente identificado y una vez planificadas y desarrolladas todas las respuestas y acciones planificadas para mitigarlo, estas no fueron suficientes para reducir el impacto en la vigencia 2019.

- Tratamiento de Riesgos TI - Vigencia 2020



Fuente: archivo "GTI-MR-001 V2 Mapa de riesgos de Gestón_OTIC"



Fuente: archivo "GTI-MR-001 V2 Mapa de riesgos de Gestón_OTIC"

De acuerdo con lo anterior, se observó que los (5) riesgos inherentes y residuales identificados para la vigencia 2020, donde, una vez planificadas, desarrolladas todas las respuestas y acciones planificadas para mitigar los riesgos, los riesgos Nos. 3 y 4 surtieron cambios en su tipología, el riesgo No. 3 paso de Moderado (Probabilidad "Posible" e Impacto "Menor") a Bajo y el riesgo No. 4 se mantuvo como Bajo, sus cambios obedecieron a cambios en su Probabilidad (de Improbable a Rara Vez).

En lo relacionado a Seguridad Digital, se observó en el Mapa de Riesgos de Gestión de la OTIC el Riesgo No. 5 "Vulneración de la seguridad digital de la entidad", en el que el proceso identificó y estableció lo siguiente:

Causas:

- No. 1 Inadecuado establecimiento y aplicación de los mecanismos, directrices y estrategias necesarios para la gestión de la seguridad digital.
- No. 2 Falta de implementación de controles en las herramientas tecnológicas sobre los activos de información.
- No. 3 Inexistencia de políticas de seguridad digital que permitan soportar la implementación de acciones tecnológicas enfocadas en preservar la integridad, confidencialidad y autenticidad de los activos de información.

Consecuencias Potenciales:

- Perdida de confiabilidad, confidencialidad y disponibilidad de la información de la UBPD.
- Aseguramiento tecnológico inefectivo de los activos de la información de la UBPD.
- Afectación de la imagen de la UBPD frente al manejo de la reserva y la seguridad de la información.

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 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. (para Causas No. 1 y 2).
- 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. (para Causa No. 3)

Para la vigencia 2021, la Oficina Asesora de Planeación OAP se encuentra desarrollando el monitoreo de los controles y de los planes de tratamientos de los Riesgos de Gestión de la UBPD, bajo una metodología enfocada en la primera y segunda línea de defensa, lo anterior, se desarrolló entre el 12 de abril al 17 de mayo de 2021 y los resultados del monitoreo serán entregados a la primera y tercera línea de defensa para su análisis y fines pertinentes.

6.3. Análisis Independientes de Riesgos TI

En este componente, se presentan los análisis de riesgos realizados al interior de la OTIC como resultado de ejercicios independientes a los análisis base y obligatorios como lo son: Riesgos de Gestión y de Riesgos transversales e institucionales como los de Anticorrupción, Comité de Seguridad de la Información y Contratación, asimismo, la identificación de herramientas tecnológicas para el apoyo en la gestión de todos los riesgos de Tecnologías de la Información y las Comunicaciones.

- **Contrato No. 0186-2019** - Contratar los servicios de Consultoría para diseñar el sistema de información misional de la UBPD, el modelo estratégico de tecnologías de la información, el modelo de seguridad de la información y el componente de intercambio de información que incluya la implementación de servicios en un esquema de fábrica de software por demanda.

  En el marco del contrato anteriormente mencionado, se desarrollaron una serie de documentos definidos como entregables del Contrato y correspondientes a análisis de riesgos, así:

  - P18 Documentos con la evaluación de los riesgos internos y externos de seguridad de la información
    - ✓ UBPD P18_RiesgosSistemaMisional_V.2.0_20201126.xlsx
    - ✓ UBPD P18_Matriz de Inventario de activos sistema Misional_v2.0_20201125.xlsx
  - P43 Modelo metodología para gestión de riesgos de seguros de seguridad de la información
    - ✓ UBPD P43 – Metodología de Gestión de Riesgos de Seguridad_V1.1. 2020_04_08.pdf
  - P44 Riesgos de seguridad de la información identificados
    - ✓ UBPD P44_Documento con los Riesgos de seguridad de la información identificados_V2.1_20201120.xlsx
  - P45 Planes de tratamiento de riesgos
    - ✓ UBPD P45_Planes de Tratamiento de Riesgos_V.2.0_20201022.xlsx

- **Contrato No. 105-2021 –** Renovar la suscripción para uso y soporte de la herramienta tipo SaaS ISOLUCION para gestión del Modelo de Seguridad de la Información de la UBPD.

  La UBPD cuenta con una herramienta tecnológica de tipo SaaS (Software como un Servicio), el cual es un software para la administración de Sistemas de Gestión como ISO 9001, SG-SST, ISO 45001, HSEQ,

Medio Ambiente, Gestión de Riesgos, MIPG, SARLAFT, ISO 27001, Continuidad de Negocio, Control Interno y demás cumplimiento normativo; en lo referente a Tecnologías de la Información y las Comunicaciones, el software ISOLUCION es usado para la Gestión de Riesgos de Seguridad de la Información.

6.4. Análisis de Riesgos Contractuales TI

De acuerdo con el procedimiento GCO-PR-010 V1 Procesos de Selección con fecha del 27 de agosto de 2019, publicado en el Sistema de Gestión de la UBPD y perteneciente al proceso de Gestión Contractual, en la actividad No. 12 "*Radicar los documentos para inicio del proceso*" se observó cómo registro el formato "*GCO-FT-003 Matriz de riesgos del proceso de contratación*", así las cosas, y con el fin de verificar el cumplimiento de lo anteriormente mencionado por parte de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, el 25 de mayo de 2021, la OCI solicitó a la OTIC la matriz de riesgos para cada uno de los procesos de contratación de bienes y/o servicios para la vigencia 2020 y al corte del 30 de abril de 2021, presentando la OTIC las siguientes matrices de riesgos:

Vigencia 2020 (11 matrices de riesgo):

- **Contrato No. 234-2020:** Adquirir la suscripción a publicaciones en materia legislativa, jurisprudencial, doctrinal y normativa.
- **Contrato No. 196-2020:** Adquisición, implementación y puesta en funcionamiento de un sistema de vídeo conferencia que incluya herramientas de hardware y software integradas y compatibles que permitan la interoperabilidad y comunicación simultánea bidireccional de audio y vídeo entre todas las sedes a nivel nacional y renovación de licencias SaaS de herramientas colaborativas G-Suite y servicios conexos de Google.
- **Contratos No. 193-2020 y 194-2020:** Prestar los servicios de hosting, actualización, mantenimiento preventivo y mantenimiento correctivo del Portal Web e Intranet de la Unidad de Búsqueda de Personas dadas por Desaparecidas en Contexto y Razón del Conflicto Armado (UBPD) y el desarrollo de Micrositios, como la implementación de características para la visualización en dispositivos móviles.
- **Contrato No. 151-2020:** Adquirir Tabletas digitalizadoras y táctiles para la Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado (UBPD), de conformidad con lo señalado en las especificaciones técnicas.
- **Contrato No. 147-2020:** Adquisición de licenciamiento de herramienta de compresión y descompresión de archivos digitales, para la Unidad de Búsqueda de Personas Dadas por Desaparecidas en el Marco y en Razón del Conflicto Armado.
- **Contrato No. 113-2020:** Adquisición de Licencia de software de fotogrametría para la gestión y procesamiento de imágenes de drones para la Unidad de Búsqueda de Personas Dadas por Desaparecidas en el contexto y en razón del conflicto armado.
- **Contrato No. 092-2020:** Adquirir dispositivos de seguridad (cifrados) de almacenamiento externo.

- **Contrato No. 087-2020:** Adquirir un (1) Certificado digital SSL tipo Wildcard para el dominio de la Unidad de Búsqueda de Personas Dadas por Desaparecidos en razón y en contexto del conflicto armado.
- **Contrato No. 074-2020:** Renovación del licenciamiento del software como servicio SaaS Planview.
- **Contrato No. 073-2020:** Prestar los servicios de conectividad y seguridad centralizada, y demás servicios conexos, requeridos para la operación de las sedes de la UBPD.
- **Contrato No. 152-2020:** Adquirir Licenciamiento Adobe (Photoshop e Ilustrator) para la Unidad de Búsqueda de Personas Dadas por Desaparecidas en el contexto y en razón del conflicto armado.

Vigencia 2021 con corte al 30 de abril de 2021 (5 matrices de riesgo):

- **Contrato No. 070-2021:** Renovación del licenciamiento del software como servicio SaaS Planview.
- **Contrato No. 076-2021:** Adquirir licencias de PDF Element para la UBPD.
- **Contrato No. 105-2021:** Renovar la suscripción para uso y soporte de la herramienta tipo SaaS ISOLUCION para gestión del Modelo de Seguridad de la Información de la UBPD.
- **Contrato No. 115-2021:** Suscribir el derecho al uso de las herramientas de Adobe Creative para la UBPD.
- **Contrato No. 121-2021:** Prestar los Servicios Integrados de Tecnologías de Información y Comunicaciones (TIC), así como los demás bienes y servicios requeridos para la operación y mejora continua de servicios TIC de la UBPD, en todas sus sedes y lugares en que la entidad cumpla las funciones a su cargo.

6.5. Planes Institucionales y los Riesgos TI

El Articulo No. 73 de la Ley No. 1474 de 2011 (Plan Anticorrupción y de Atención al Cliente) 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 la verificación de los Planes Anticorrupción y de Atención al Cliente de la UBPD para las vigencias 2019, 2020 y 2021, no se observaron actividades específicas lideradas o de responsabilidad directa de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC y/o del Comité de Seguridad de la Información.

Evidencias de Publicaciones:

- Planes Anticorrupción y Atención al Ciudadano: https://www.ubpdbusquedadesaparecidos.co/transparencia/planeacion/
- Políticas de Seguridad de la Información: https://www.ubpdbusquedadesaparecidos.co/transparencia/planeacion/

7. RECOMENDACIONES

Del presente análisis, la OCI emite las siguientes recomendaciones:

- Hacer uso de la herramienta "ISOLUCION" tipo Saas (Software como un Servicio) para la gestión, monitoreo y evaluación anual de los riesgos de Seguridad Digital y de Gestión de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC.
- Realizar la aplicación de las metodologías, análisis y planes de acuerdo a los productos generados a través del Contrato de Consultoría No. 0186 de 2019.
- 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.

8. CONCLUSIONES

- Se observó cumplimiento en la definición de los riesgos a nivel contractual, según lo indicado en el procedimiento GCO-PR-010 V1 Procesos de Selección con fecha del 27 de agosto de 2019.
- No se observaron actividades específicas lideradas o de responsabilidad directa de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC y/o del Comité de Seguridad de la Información en el Mapa de Riesgos de Corrupción, en lo que respecta por ejemplo a: Acceso

fraudulento (intromisiones maliciosas, ataques informáticos etc.) a la información de las bases de datos y/o repositorios de la UBPD generando posible robo de información institucional (desde el interior o exterior), uso inadecuado a los recursos tecnológicos y sobrecostos en la adquisición de tecnologías de la información.

- La UBPD cuenta con una herramienta tecnológica que permite realizar la gestión de riesgos de Tecnologías de la Información y las Comunicaciones.

Cordialmente,

IVONNE DEL PILAR JIMÉNEZ GARCÍA
Jefe Oficina de Control Interno.

Elaborado por:	Carlos Andrés Rico Reina	**Experto Técnico**	FIRMA:
Aprobado por:	Ivonne del Pilar Jiménez García Jefe Oficina de Control Interno	**Jefe Oficina de Control Interno**	FIRMA: