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 2022

TABLA DE CONTENIDO

1. INFORMACIÓN GENERAL DEL SEGUIMIENTO	
Informe Seguimiento	Riesgos de Gestión de las Tecnologías de la Información y las Comunicaciones
Fecha	28 de junio de 2022

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 2022 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 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 Gestión Tecnologías de la Información y las Comunicaciones y Riesgos Tecnológicos en Planes Institucionales, al corte del 29 de abril de 2022.

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 V3 Gestión de Tecnologías de la Información y Comunicaciones 05-11-2021.
- 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.
- 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.
- 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 28 de abril de 2022.

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 28 de abril de 2022 y con fecha de entrega para el 27 de mayo de 2022, la OCI solicitó a la OTIC la información relacionada con:

- Descripción amplia del estado de avance, seguimiento y resultados del Plan de Protección y Seguridad Digital al corte del 29 de abril de 2022.
- Documentos de análisis de Riesgos de Seguridad Digital al corte del 29 de abril de 2022.
- Documentación de análisis de Riesgos de Tecnologías de la Información y las Comunicaciones al corte del 29 de abril de 2022.
- Documentación de análisis de Riesgos en el marco del Contrato 0181 de 2021.
- Análisis de Riesgos que hacen parte de la Gestión Contractual de la OTIC al corte del 29 de abril de 2022.

El 09 de junio de 2021 y ante la falta de respuesta por parte de la OTIC, la OCI reitera la solicitud de información realizada el 28 de abril de 2022, donde, como respuesta el mismo día la OTIC hizo entrega de la información solicitada.

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. Plan de Implementación de Protección y Seguridad Digital 2022.

La Oficina de Tecnologías de la Información y las Comunicaciones OTIC, presentó el documento precitado, donde se planteó lo siguiente:

Objetivo General

"Establecer las actividades a ejecutar durante la vigencia 2022 que permitan desarrollar las estrategias para fortalecer la Protección y Seguridad Digital de la Unidad de Búsqueda de Personas dadas por Desaparecidas".

Objetivos Específicos

"a. Definir las actividades a desarrollar en 2022 en materia de Protección y Seguridad Digital de acuerdo con lo establecido en las Estrategias de Implementación de Seguridad Digital asociadas al Modelo de Seguridad Digital de la UBPD.

b. Establecer las actividades para la implementación de controles tecnológicos que permitan mitigar los riesgos de seguridad digital y preservar la confidencialidad, disponibilidad e integridad de la información.

c. Establecer las actividades que permitan fortalecer la cultura del uso seguro de entornos digitales por parte de los servidorxs, contratistas, personal delegado y partes interesadas de la UBPD.

d. Gestionar de manera oportuna y adecuada los eventos e incidentes de seguridad digital que puedan presentarse en las plataformas tecnológicas de la UBPD."

Alcance

"El plan de protección y seguridad Digital 2022 de la Unidad de Búsqueda de Personas dadas por Desaparecidas, abarca las actividades a realizar desde la actualización de políticas, lineamientos y procedimientos, la actualización de activos de información y los riesgos de seguridad digital, continuando con la implementación y fortalecimiento de controles tecnológicos derivados de las líneas de acción establecidas en la política de Seguridad Digital con el fin de mitigar los riesgos asociados al uso de las plataformas tecnológicas y preservar la confidencialidad, integridad y disponibilidad de la información."

El Plan de Implementación de Protección y Seguridad Digital 2022, se encuentra dividido por los siguientes componentes: Identificar, Proteger, Detectar, Responder, Recuperar y Seguimiento, lo anterior, con un total de 86 actividades a llevar a cabo entre enero de 2022 a diciembre de 2022, de lo anterior, es importante mencionar que el Plan tiene fecha de marzo de 2022 y Planes de: Sensibilización, Transferencia de Conocimiento y Comunicación, en los que se detallan temas, grupos de interés y periodo de ejecución.

En lo referente a Riesgos de Seguridad Digital, se observó en el Plan precitado las siguientes actividades enmarcadas en el componente "Identificar":

E17	Identificación y Evaluación de riesgos de Seguridad Digital de los procesos y proveedores de Infraestructura, sistemas y servicios tecnológicos de la UBPD Identificados	Seguridad Digital	Enero - Abril	Evaluación de riesgos 7.4, 7.5, 8.4, 9.1, Actividades de control 12.2
E17	Actualización de riesgos de Seguridad Digital de los procesos de la UBPD Identificados	Seguridad Digital	Abril - Julio	Evaluación de riesgos 7.4, 7.5, 8.4, 9.1, Actividades de control 12.2
E17	Apoyo en el cargue en la herramienta de gestión del SSI de los riesgos identificados y su evaluación	Seguridad Digital	Julio - Agosto	
E17	Elaboración de planes de tratamiento de riesgo (si aplica) resultantes del retest	Seguridad Digital – OTIC – Partes Interesadas	Marzo - Mayo	Actividades de control 12.3
E17	Generación de planes de tratamiento de riesgo de seguridad digital de los procesos de la UBPD y proveedores de Infraestructura, sistemas y servicios tecnológicos (si aplica) en los nuevos riesgos identificados	Seguridad Digital - Servicios Tecnológicos - Proveedores	Julio – Septiembre	

Fuente: "Plan de Implementación de Protección y Seguridad Digital 2022"

Y para el Componente de "Proteger" se observó la siguiente actividad:

E17	Seguimiento a planes de tratamiento de riesgo	Seguridad Digital	Octubre – Diciembre	

Fuente: "Plan de Implementación de Protección y Seguridad Digital 2022"

Ahora bien, como evidencia del estado de avance y seguimiento del Plan, la OTIC presentó el documento "Seguimiento al plan de protección y seguridad digital330_04 (1).pdf", correspondiente a un reporte ejecutivo, donde, se detalla las estrategias sobre las cuales la OTIC basó las actividades adelantadas en el periodo de enero de 2022 a abril de 2022; Estas estrategias son: Seguridad Digital, Controles de uso de internet, Fortalecimiento de la infraestructura de seguridad digital, Respuesta a incidentes de seguridad digital, Seguimiento y evaluación de seguridad digital, Cultura de uso seguro de los entornos digitales, Prevención y gestión de riesgos, Control para el trabajo remoto seguro,

Copias de seguridad, Desarrollo seguro, Logs de auditoría, Uso de dispositivos móviles, Controles de acceso, Uso de dispositivos de almacenamiento externos, Línea base y Ciberresiliencia.

Por otro lado, y en lo relacionado con las 6 actividades presentadas anteriormente, el informe ejecutivo de seguimiento de la OTIC, registra el siguiente avance:

Actividad	Fecha Ejecución	% Avance
Identificación y Evaluación de riesgos de Seguridad Digital de los procesos y proveedores de Infraestructura, sistemas y servicios tecnológicos de la UBPD Identificados.	enero - abril	100
Actualización de riesgos de Seguridad Digital de los procesos de la UBPD Identificados.	abril - julio	Sin avance observado.
Elaboración de planes de tratamiento de riesgo (si aplica) resultantes del retest.	marzo - mayo	Sin avance observado.

Fuente: Seguimiento al plan de protección y seguridad digital330_04 (1).pdf

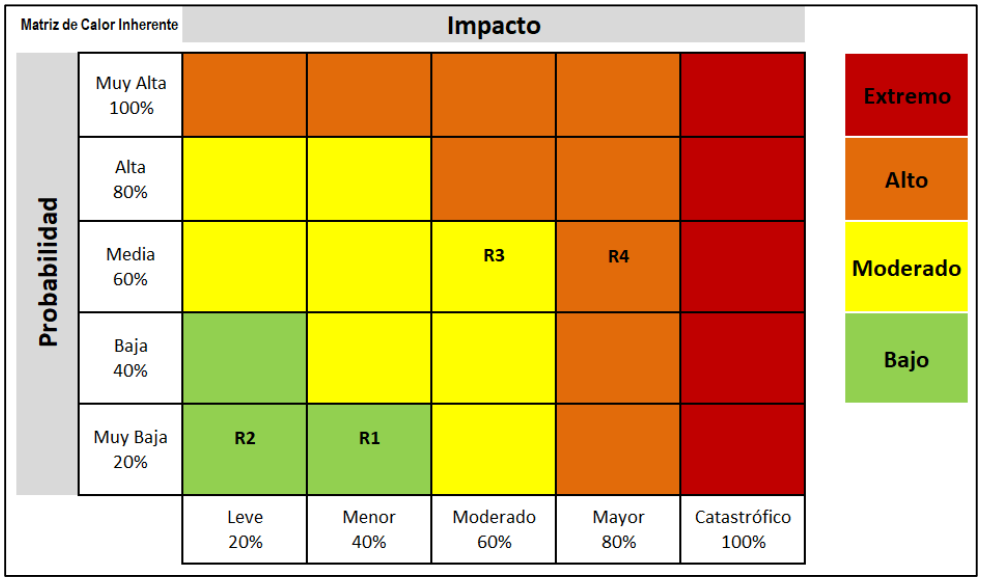
Las restantes actividades: "Apoyo en el cargue en la herramienta de gestión de SSI de los riesgos identificados y su evaluación", tiene como periodo de ejecución entre julio y agosto de 2022; "Generación de planes de tratamiento de riesgo de seguridad digital de los procesos de la UBPD y proveedores de infraestructura, sistemas y servicios tecnológicos (si aplica) en los nuevos riesgos identificados", tiene como periodo de ejecución entre julio y septiembre de 2022 y "Seguimiento a planes de tratamiento de riesgo", tiene como periodo de ejecución entre octubre y diciembre de 2022; actividades con periodos de ejecución por fuera del alcance y/o corte del presente seguimiento.

De lo anterior, resulta importante mencionar que 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." 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.

6.2. Análisis de Riesgos de Gestión TI

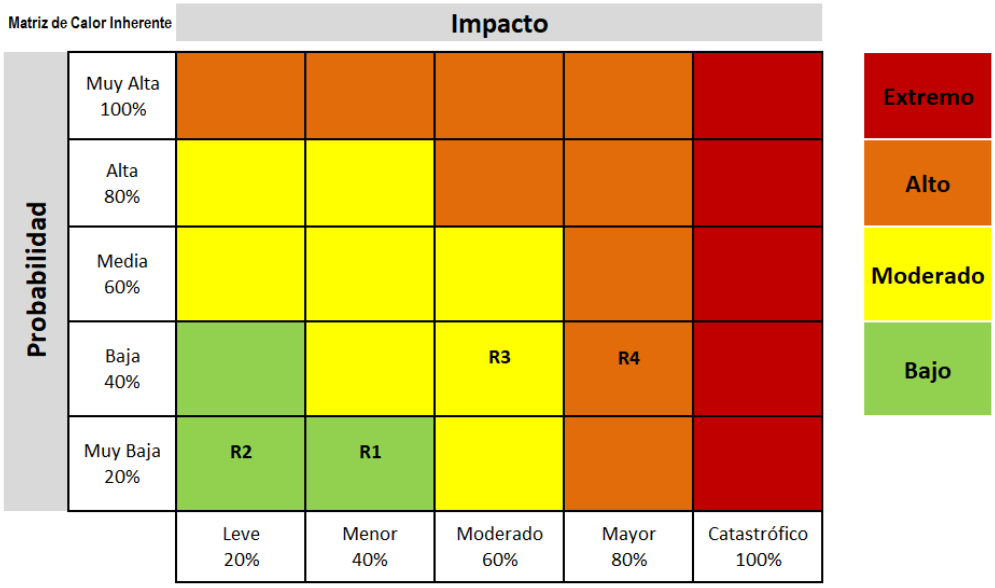
La Oficina de Tecnologías de la Información y las Comunicaciones OTIC, al corte del presente seguimiento tiene publicado en el Sistema de Gestión, (1) versión del Mapa de Riesgos de Gestión TIC, correspondiente al ejercicio de actualización del Mapa de Riesgos con corte al 05 de noviembre de 2021, donde, 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"

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

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 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.

6.3. Análisis de Riesgos de Seguridad Digital

La OTIC hizo entrega del archivo “1 - Riesgos OTIC.xlsx” y del link de acceso https://unidadbpd.isolucion.co/RiesgosDafp/frmFiltroRiesgos.aspx?TipoModulo=Mg%3d%3d , a la herramienta “ISOLUCION”, donde, se observó un filtro de 375 riesgos de “Seguridad de la Información” y fecha de identificación del 23 al 29 de octubre de 2020, de lo anterior, la OTIC indico que los riesgos registrados en la herramienta “ISOLUCION” fueron levantados a través del Contrato de Consultoría No. 0186 de 2019 y que serán actualizados en la presente vigencia.

Ahora bien, la matriz en hoja de cálculo "1 - Riesgos OTIC.xlsx" corresponde según lo indicado por la OTIC al inventario de riesgos de Seguridad Digital actualizado y se observó un total de 11 riesgos, sin embargo, se observó falta de completitud o ausencia de información en:

- Análisis de Riesgos Inherentes.
- Evaluación del Riesgo – Valoración de los Controles.
- Evaluación del Riesgo – Nivel del Riesgo Residual.
- Plan de Acción.

De lo anterior, es importante mencionar que la OTIC en la respuesta dada a la OCI el 09 de junio de 2022, no realizó ninguna aclaración o indicación relacionada a que la información registrada en el archivo "1 - Riesgos OTIC.xlsx" correspondía a un ejercicio en etapa de levantamiento o construcción.

6.4. Planes Institucionales y los Riesgos TI

El Articulo. 73 – Plan Anticorrupción y de Atención al Cliente de la Ley No. 1474 de 2011, establece:

> *"…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 del Plan Anticorrupción y de Atención al Ciudadano de la UBPD ,para la vigencia 2022, se observó el riesgo "*Posibilidad de pérdida de confidencialidad y/o de integridad de los activos de información para favorecer a un tercero a cambio de dádivas, favorecimientos o presiones externas.*", gestionado y bajo la responsabilidad del proceso de "Gestión de Seguridad de la Información", riesgo con consecuencias de: "Afectación Legal", "Afectación Económica", "Afectación Reputacional" y "Se Puede Generar Riesgo Físico a Personas" y con el siguiente tratamiento:

CAUSAS	ACTIVIDADES DE CONTROL	SOPORTE DE LA ACTIVIDAD	DEPENDENCIA RESPONSABLE	FECHA MÁXIMA DE EJECUCIÓN
No aplicación de las políticas de protección y seguridad digital y general de seguridad, protección y confidencialidad de la información por parte de los servidorxs de la entidad.	El Oficial de Seguridad de la información durante toda la vigencia realizará actividades de socialización para el fortalecimiento en estrategias de uso y apropiación en temas relacionados con seguridad de la información, con especial énfasis en la semana de la seguridad de la información. Dichas actividades serán dirigidas a todas las servidoras y servidores de la UBPD de manera presencial y/o virtual. Para aquellos que no puedan participar de su totalidad, el material y las grabaciones serán publicados. Como evidencia de las actividades se tendrá el desarrollo del plan de socialización y las diferentes presentaciones y materiales trabajados.	1. Plan de socialización documentado y desarrollado. 2. Presentaciones y material trabajado.	Dirección General - Oficial de Seguridad de la Información, Oficina de Tecnologías de Información y Comunicaciones	30/12/2022
	Los expertos técnicos y analistas de la Oficina de Tecnologías de Información y Comunicaciones y de la Dirección Técnica de Información, Planeación y Localización para la Búsqueda, cada vez que se construyan sistemas y software de información, implementan o incluyen en la construcción, los lineamientos establecidos en la guía de desarrollo seguro	Lineamientos establecidos en la guía de desarrollo seguro, incorporados en el proceso de construcción de sistemas y software de información.	Dirección General - Oficial de Seguridad de la Información, Oficina de Tecnologías de Información y Comunicaciones, Dirección Técnica de Información, Planeación y Localización para la Búsqueda	30/12/2022
	El experto técnico del equipo de seguridad digital de la Oficina de Tecnologías de Información y Comunicaciones y el Oficial de seguridad de la información de la Dirección General, cada vez que se realizan desarrollos de sistemas y software de información, dan la viabilidad mediante correo electrónico	Correos electrónicos de viabilidad de desarrollo de sistemas y software de información.	Dirección General - Oficial de Seguridad de la Información, Oficina de Tecnologías de Información y Comunicaciones	30/12/2022

CAUSAS	ACTIVIDADES DE CONTROL	SOPORTE DE LA ACTIVIDAD	DEPENDENCIA RESPONSABLE	FECHA MÁXIMA DE EJECUCIÓN
Alteración no autorizada de la configuración de los controles existentes	El experto técnico del equipo de seguridad digital de la Oficina de Tecnologías de Información y Comunicaciones, revisa como máximo semestralmente los usuarios, incluidos los administradores y los parámetros de autenticación en los activos de información cruzando contra el informe de revisión interna, el cual queda como evidencia, con el fin de establecer falencias y oportunidades de mejora en los mecanismos usados para la autenticación; en caso de identificar falencias u oportunidades de mejora, se informa y se solicita a los administradores la necesidad de ajuste.	Informe de revisión interna de usuarios, incluidos los administradores y los parámetros de autenticación	Dirección General - Oficial de Seguridad de la Información, Oficina de Tecnologías de Información y Comunicaciones	30/12/2022
	El experto técnico del equipo de seguridad digital de la Oficina de Tecnologías de Información y Comunicaciones, genera la excepción a las políticas y líneas de acción de protección y seguridad digital (bloqueos de puertos USB, navegación, dispositivos móviles entre otros), ante una solicitud realizada por los Jefes de dependencias; si en el análisis de dicha solicitud se identifican riesgos de seguridad de la información o seguridad digital, se responde al área mediante correo electrónico explicando la situación detectada. Como soporte se tiene la solicitud de la dependencia y el informe de revisión interna con la novedad.	1. Solicitud de la dependencia 2. Informe de revisión interna con la novedad.	Dirección General - Oficial de Seguridad de la Información, Oficina de Tecnologías de Información y Comunicaciones	30/12/2022
Ausencia o debilidades en el monitoreo oportuno y la definición de derechos de uso y acceso.	- La Oficina de Tecnologías de Información y Comunicaciones a través de los lideres de proceso (servicios tecnológicos, desarrollo de software y seguridad digital) revisan mensualmente los roles, perfiles y permisos otorgados a los usuarios, en caso de encontrar usuarios con roles, perfiles y/o permisos que no correspondan, la Oficina de Tecnologías de Información y Comunicaciones a través de los lideres de proceso (servicios tecnológicos, desarrollo de software y seguridad digital) realizará la respectiva depuración y notificara mediante correo electrónico al líder del proceso como evidencia se deja correo electrónico mensualmente con la respectiva depuración.	Correo electrónico mensualmente con la respectiva depuración	Dirección General - Oficial de Seguridad de la Información, Oficina de Tecnologías de Información y Comunicaciones	30/12/2022

Fuente: Archivo “Mapa-de-Riesgos-de-Corrupcion-2022.xlsx”, publicado en: https://ubpdbusquedadesaparecidos.co/transparencia/planeacion/

Evidencias de Publicaciones en Pagina Web:

- Plan Anticorrupción y Atención al Ciudadano: https://www.ubpdbusquedadesaparecidos.co/transparencia/planeacion/
- Política de Seguridad, Protección y Confidencialidad: https://www.ubpdbusquedadesaparecidos.co/transparencia/planeacion/

- Política de Protección y Seguridad Digital: https://www.ubpdbusquedadesaparecidos.co/transparencia/planeacion/

7. 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.
- 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.
- 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.

8. RECOMENDACIONES

Del presente análisis, la OCI emite las siguientes recomendaciones:

- 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 de la Oficina de Tecnologías de la Información y las Comunicaciones OTIC.
- 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.

- Agregar un link de acceso a las evidencias del avance reportado en el Informe Ejecutivo del Plan de Implementación de Protección y Seguridad Digital.

9. CONCLUSIONES

- En el Plan Anticorrupción y Atención al Ciudadano de la vigencia 2022, se concretaron un total de 5 actividades de control bajo la responsabilidad de dependencias o instancias estratégicas, de apoyo y misionales como lo son: Dirección General – Oficial de Seguridad de la Información OSI, Oficina de Tecnologías de la Información y las Comunicaciones OTIC y Dirección Técnica de Información Planeación y Localización para la Búsqueda DTIPLB, lo que demuestra un avance en el compromiso e involucramiento en la gestión de riesgos de la información en los procesos de la UBPD.

- La UBPD cuenta con una herramienta tecnológica que permite realizar la gestión de riesgos de Tecnologías de la Información y las Comunicaciones y que parte del éxito en la gestión de la misma, es que cuente con información actualizada.

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**	FIRMA: