

	INFORME EJECUTIVO AUDITORÍA INTERNA	Código:	
	EVALUACIÓN, SEGUIMIENTO Y CONTROL	Versión:	
	UNIDAD BUSQUEDA DE PERSONAS DADAS POR DESAPARECIDAS	Fecha:	

1. OBJETIVO GENERAL

Evaluar, verificar y realizar seguimiento a los aspectos técnicos, organizacionales, normativos y contractuales, significativos y aplicables a los procesos a cargo de la Oficina de Tecnologías de la Información y Comunicaciones y en los que interviene para brindar soporte a las operaciones de la Unidad de Búsqueda de Personas dadas por Desaparecidas – UBPD.

OBJETIVOS ESPECIFICOS:

- Realizar seguimiento y verificación de la planificación y ejecución de ejercicios de protección de datos y de los análisis de vulnerabilidades, con el fin de proteger la integridad y la privacidad de la información de la UBPD en términos de confidencialidad, integridad y disponibilidad.
- Realizar verificación del estado de planificación, desarrollo e implementación en Seguridad de la Información, teniendo en cuenta el carácter y la naturaleza especial de la UBPD, especialmente la necesidad de reserva y la criticidad de la información registrada desde los procesos misionales de la entidad.
- Realizar verificación en la ejecución de los procedimientos de Gestión de Aprovisionamiento de Infraestructura, Gestión del Cambio y Gestión de la Capacidad.
- Determinar el conocimiento del área responsable del marco normativo aplicable y evaluar el estado de cumplimiento del mismo, al igual que evaluar la existencia de políticas, manuales o lineamientos de la entidad UBPD y la definición del marco y metodología usada para construir y actualizar el PETIC, según lo indicado en el Numeral 1 del Artículo No. 7 del Decreto 1393 de 2018.
- Hacer seguimiento y análisis periódico de la gestión del servicio de Mesa de Ayuda, teniendo en cuenta los Acuerdos de Niveles de Servicio - ANS contractuales.
- Revisar la ejecución y supervisión de una muestra de contratos celebrados con componente de TI y a cargo de la OTIC durante la vigencia de 2019, teniendo en cuenta la ejecución de recursos de proyectos de inversión, la ejecución del plan de acción y el plan anual de adquisiciones.
- Realizar seguimiento y verificación de los planes de Mantenimiento Preventivo y Correctivo de Equipos de Cómputo, Centros de Datos, UPS, Aires Acondicionados.
- Realizar pruebas de accesibilidad Web a la página de la UBPD, con el fin de establecer el nivel de accesibilidad a personas con diversos tipos de discapacidad.

www.ubpdbusquedadesaparecidos.co

servicioalciudadano@ubpdbusquedadesaparecidos.co / notificacionesjudiciales@ubpdbusquedadesaparecidos.co

- Realizar seguimiento y verificación del estado del inventario de equipos tecnológicos, propios y en alquiler, en lo que respecta a la correlación entre registros en la OTIC y la articulación con los procedimientos de Gestión de Recursos Físicos como lo son los inventarios de la Subdirección Financiera y Administrativa.
- Realizar seguimiento al proceso de transición al protocolo IPV6, teniendo en cuenta lo indicado por el Ministerio de las Tecnologías de la Información y las Comunicaciones – Min TIC mediante Resolución No. 2710 de 20171, donde se establecen los lineamientos para la adopción del protocolo IPV6.
- Realizar verificación a la planificación y gestión de las actividades relacionadas donde la OTIC apoya la Continuidad del Negocio.
- Realizar seguimiento a las estrategias de la OTIC con el fin de promover el uso correcto de las tecnologías de la información y la adquisición de conocimiento para tal fin.
- Efectuar encuestas de percepción a los servidores con relación al uso y al nivel de satisfacción de los servicios informáticos.
- Realizar seguimiento al desarrollo del sitio de la Intranet de acuerdo al alcance de cada uno de los responsables en las distintas etapas del proyecto.
- Verificar los marcos y las actividades de autodiagnóstico efectuados por el área.
- Realizar seguimiento a los proyectos de interoperabilidad con otras entidades, teniendo en cuenta la naturaleza y misión de la UBPD.
- Realizar la verificación y seguimiento de la metodología para la gestión de proyectos.
- Evaluar las actividades de control de riesgos levantadas por el proceso en las diferentes matrices de riesgo de la entidad, riesgos de TI, riesgos operativos, de corrupción y de prevención del daño antijurídico.
- Realizar verificación y seguimiento a lo indicado en el Artículo No. 7 del Decreto 1393 de 2018, en especial respecto a lo relacionado con los numerales 8 y 11 del citado artículo, respecto al establecimiento del Registro Nacional de Desaparecidos y a la implementación, mantenimiento y mejora del Sistema Integrado de Gestión.

¹ El Artículo No. 2 de la norma mencionada en el párrafo anterior indica “...Ámbito de Aplicación: Son sujetos obligados de las disposiciones contenidas en la presente Resolución las entidades de que trata el Artículo 2.2.9.1.1.2 del Decreto 1078 de 2015...”, el cual cita: “Serán sujetos obligados de las disposiciones contenidas en el presente capítulo, las entidades que conformen la Administración Pública en los términos del Artículo No. 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas.

2. ALCANCE

Gestión efectuada durante el periodo comprendido entre el 01 de enero de 2019 al 31 de diciembre de 2019.

3. METODOLOGIA

Para el desarrollo de las actividades presentadas en el Plan de Auditoría, se utilizaron técnicas de auditoría como lo son: Estudio General, Análisis, Inspección, Confirmación, Investigación, Observación y Calculo.

Teniendo en cuenta que al momento de ejecutar la presente auditoría y en razón a la declaratoria de pandemia del brote COVID-19 por la Organización Mundial de la Salud OMS el 11 de marzo de 2020, del aumento de contagiados a nivel nacional, la declaratoria de la emergencia sanitaria por causa del COVID-19 del Ministerio de la Salud y la Protección Social y las medidas de aislamiento preventivo obligatorio decretadas por las autoridades distritales y nacionales; no era posible desarrollar actividades presenciales, por lo que la mayor parte de la auditoría se ejecutó bajo la modalidad virtual.

La presente auditoría de gestión se desarrolló a través de la revisión de soportes documentales entregados por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC ;como lo son Análisis, Estudios, Planes, Modelos, Comunicados, Informes, Actas de Reunión, Presentaciones, Correos Electrónicos, Procedimientos, Formatos, Manuales, Guías, Matrices, Inventarios, Registros, Autodiagnósticos, Normograma, Proyectos, Pruebas; así como, seguimientos previos relacionados con el objetivo de la auditoría.

Por otro lado, se realizaron inspecciones a sitios específicos como lo son Centros de Datos, UPS y demás infraestructura durante la visita efectuada por la OCI al GITT de la ciudad de Cali entre el 24 al 26 de febrero de 2020; se realizaron entrevistas virtuales con cada uno de los referentes nombrados por la Jefatura de la OTIC según el ítem auditado; así mismo, se efectuaron entrevistas con los líderes de proceso de otras dependencias donde existen proyectos conjuntos con la OTIC; se desarrolló una encuesta a través de Google con el fin de conocer el nivel de percepción de los servidores con relación a los servicios informáticos a cargo de la OTIC.

De acuerdo con lo anterior y en base a lo expuesto, el plan de acción presentado por el área como respuesta al informe final de auditoría, debe ser analizado y diseñado para mejorar el proceso a nivel general y no limitarse solo a los aspectos identificados en el informe de auditoría.

4. ANALISIS HALLAZGOS DE AUDITORÍA

En el informe final de auditoría de gestión a la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, no se presentaron “No Conformidades”.

5. CONCLUSIONES

En administración de empresas, la gestión de proyectos es la disciplina que estudia el planeamiento, la organización, la motivación y el control de los recursos con el propósito de alcanzar uno o varios objetivos, en lo que respecta a las Tecnologías de la Información y las Comunicaciones los proyectos deben ser gestionados bajo la misma formalidad, la OTIC durante el 2019 y como lo evidencian los indicadores de gestión del mismo periodo, la ejecución de los proyectos presentó rendimientos “Óptimos”, lo anterior debido a que la estructura para la gestión de proyectos en la OTIC se encuentra enmarcada en metodologías de Formulación y Ejecución, apoyadas tecnológicamente en la herramienta “Plan View” y en procedimientos ubicados en el Sistema de Gestión, todo lo anterior ha conllevado a que la OTIC sea una de las áreas líderes en la gestión de proyectos en la UBPD.

Teniendo en cuenta la importancia y criticidad en la confidencialidad de la información que administra la UBPD, surge la necesidad de diseñar, planificar, probar e implementar medidas preventivas y reactivas en espacios físicos, recursos y servicios que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos; la OTIC durante el 2019 efectuó una serie de actividades de forma individual y conjunta con otras áreas, como lo fueron: análisis o diagnóstico que determinó un estado “Inicial”, proceso contractual de Consultoría que en el 2020 desarrollará el Modelo de Seguridad de la Información, reuniones en el 2019 con otras dependencias y la Dirección General con el fin de establecer el Comité de Seguridad de la Información formalizado en mayo de 2020, proyecciones de las Políticas de Seguridad de la Información y de Seguridad Informática, entre otras cosas; los resultados de la encuesta de percepción indican que muchos de los servidores de la UBPD no evidencian seguridad en la información y al usar el servicio de Internet; de acuerdo con lo anterior es vital que la OTIC como proceso estratégico de la UBPD y miembro del Comité de Seguridad de la Información, siga acompañando la construcción de políticas desde la perspectiva tecnológica y la respectiva implementación de las medidas técnicas que se requieran.

Durante el 2019, la OTIC ejecutó una serie de análisis, diagnósticos, proyectos de contratación, implementaciones, soporte en cumplimientos normativos, etc., que dentro de las etapas de planificación y ejecución se requería la definición de metodologías en muchos casos basadas en normas de tipo administrativo, técnicas y/o marcos internacionales y nacionales emitidas por entes de control y organismos especializados en reglamentaciones para el sector tecnológico, lo anterior ya sea aplicado totalmente, parcialmente o sea referente de buenas prácticas, permitió establecer una base normativa mínima, como resultado de la ejecución de la Consultoría en el 2019 todos los procedimientos de la OTIC publicados en el Sistema de Gestión relacionaron el Decreto 1393 de 2018 como marco normativo donde se establecen a través del Artículo No. 7 las funciones de la OTIC; de acuerdo a lo informado y definido en ámbitos como lo son el Comité de Gestión y el Comité Institucional de Coordinación de Control Interno, los procesos que hacen parte de primera y segunda línea de defensa deben establecer el marco normativo especializado y efectuar procedimientos de vigilancia normativa y en caso de requerirlo deben acudir a la Oficina Asesora Jurídica – OAJ para la asesoría en la interpretación del cumplimiento normativo teniendo en cuenta la naturaleza Especial y

Excepcional de la UBPD; por lo que es vital que la OTIC inicie la construcción del marco normativo y solicite la asesoría a la OAJ con el fin de evitar el riesgo de incumplimiento normativo.

Uno de los puntos y factores de éxito para el cumplimiento de la misión de la UBPD, es la articulación y acceso a la información a través de convenios interadministrativos con otras entidades, información que es relevante y de gran apoyo en las operaciones de búsqueda de personas dadas por desaparecidas; así como lo anteriormente dicho, esta información también es crítica y requiere de manejos conjuntos especiales de carácter administrativos, tecnológicos, jurídicos y bajo marcos de alta confidencialidad; escenarios donde la OTIC como proceso estratégico apoya de forma activa con el acompañamiento técnico y en la aplicación medidas preventivas y reactivas en la protección en la información en los proyectos de interoperabilidad y/o intercambio de información con otras entidades.

6. RECOMENDACIONES

A continuación, se relacionan las (25) recomendaciones realizadas de acuerdo con las situaciones evidenciadas frente a cada uno de los componentes y objetivos específicos:

6.1. Seguridad Informática

- Debilidades de control y seguimiento en los documentos referenciados en el procedimiento de Gestión de Eventos o Incidentes de Seguridad Digital, debido a que desde el mes de noviembre de 2019 a la fecha de la presente auditoría no se tiene claro el estado del trámite de las “Guía para la clasificación incidentes o eventos de seguridad” y “Guía para valoración incidentes de seguridad” ante la OAP; por lo anterior, este procedimiento se encuentra incompleto lo que puede generar un riesgo en la operación debido a que no se cuentan con la totalidad de los lineamientos oficiales y publicados para clasificar y evaluar los incidentes o eventos de seguridad informática, por lo anterior, se recomienda terminar de gestionar la publicación de las guías ante la OAP.
- Ampliar los ejercicios de búsqueda de vulnerabilidades y de simulacros controlados de eventos como lo son ataques de origen exterior e interior, donde efectúen análisis de causas, consecuencias, riesgos, recomendaciones, prioridades y el desarrollo de un plan de acción teniendo en cuenta lo anterior; así mismo, el desarrollo de estrategias documentadas con protocolos claros para ataques informáticos (Malware, Denegación de Servicios – DDoS, Ingeniería Social) de contención, erradicación, post incidente y de lecciones aprendidas con el fin de tomar medidas oportunamente, no solo de forma reactiva sino preventiva en el uso de herramientas de software especializado para el monitoreo y evitar la propagación de los incidentes (Ciberespionaje, Intrusión en la Red, DDoS, Phishing, Vulnerabilidades en el Software, Infección por Malware, Fuga de Información, etc.) y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información como pilares en la seguridad de la información, de acuerdo a lo indicado en la Guía No. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de las Tecnologías de la Información y las Comunicaciones – Min TIC (https://www.mintic.gov.co/gestionti/615/articulos-5482_G21_Gestion_Incidentes.pdf).

- Debido a la importancia del relacionamiento con los entes relacionados con la ciberseguridad, ciberdefensa y la seguridad digital del país y teniendo en cuenta que la toma de las decisiones estratégicas y las acciones a emprender que contribuyan a la seguridad de la infraestructura e integridad de la información de la UBPD está a cargo del Comité de Seguridad de la Información, conforme el literal a) del Artículo 5º, de la Resolución 537 de 11 de mayo de 2020, se recomienda que en el marco de dicho Comité se determine la interacción con otras agencias del Estado en los planes de acción, comunicaciones y en los procedimientos de reacción ante incidentes o eventos que atenten contra la infraestructura tecnológica y la información de la UBPD, conforme la naturaleza humanitaria y especial de la Unidad.

6.2. Gestión de Infraestructura, del Cambio y la Capacidad

- Efectuar el ajuste por presentación y correspondencia entre las cifras relacionadas en los documentos “Plan de Capacidad Tecnológica Diciembre 2019.pdf” y la “GTI-FT-012 V1 Matriz de Capacidad tecnológica 19-09-2019_1.pdf”, así mismo, incluir como informativo y de control una fecha de corte en el documento “GTI-FT-012 V1 Matriz de Capacidad tecnológica 19-09-2019_1.pdf” teniendo en cuenta los posibles cambios que se puedan presentar durante una vigencia determinada.

6.3. Marco Normativo

- Se recomienda a la luz del concepto dado por el MinTIC a la OTIC, la revisión y análisis de la aplicación y/o realización de la Política de Gobierno Digital en la UBPD.
- Realizar el ejercicio de la determinación de las normas que aplican al proceso y aquellas que han sido adaptadas y/o adoptadas para el desarrollo de las actividades del proceso junto con las buenas prácticas, teniendo en cuenta que de acuerdo al decidido por el Comité Institucional de Coordinación de Control Interno cada proceso deber tener la claridad sobre las normas que le aplican a su proceso.

6.4. Mesa de Ayuda

- Debilidades de control y seguimiento en los documentos referenciados en el procedimiento de Solicitudes de Servicios de TI, debido a que desde el mes de noviembre de 2019 a la fecha de la presente auditoría no se tiene claro el estado del trámite de las guías “Guía para la gestión de solicitudes TI” ante la OAP; por lo anterior, este procedimiento se encuentra incompleto y se presenta riesgo en la operación debido a que no se cuentan con la totalidad de los lineamientos oficiales y publicados para gestión de solicitudes ante la mesa de ayuda, por lo anterior se recomienda terminar de gestionar la publicación de las guía ante la OAP.

- Se recomienda concentrar los criterios de priorización y/o de categorización en un documento que sea una fuente de consulta única y oficial, esto con el fin de evitar el riesgo de confusiones al transmitir estos criterios de forma verbal y como apoyo para el personal técnico.
- Crear instructivos sencillos para el acceso y uso de la herramienta de Mesa de Ayuda, así mismo divulgarlos y publicarlos.
- Agregar textos adicionales en las notificaciones que llegan a través de correo electrónico donde se invite a los usuarios a efectuar seguimiento a los casos, así mismo, cuando se informa sobre la solución del requerimiento, indicar sobre la opción del rechazo del servicio, ya que el usuario solo accede a esta opción si se evalúa el servicio, debido a que en la notificación de solución no hay ninguna referencia hacia esta opción.
- Establecer puntos de control con periodicidades inferiores a un mes (semanal o quincenal) donde se revisen y analicen los casos con estado Abierto del mes y los acumulados de meses anteriores.
- Se recomienda que, para futuras contrataciones, los informes de gestión tanto para el nivel central y los GITT presenten una misma estructura, es importante presentar las estadísticas por tipos de casos, estados, relación de casos con estado abierto, gestiones por agente, cantidad de casos por dependencia etc., lo que permite tener una visión más global de la gestión periódica del servicio de Mesa de servicios.
- Impulsar la evaluación del servicio por parte del usuario final, a través de campañas y/o mensajes usando los distintos medios de comunicación que tiene la UBPD.

6.5. PETI

- Se recomienda que lo relacionado en el PETI corresponda a una serie de planes y estrategias claras y aprobadas, por lo que es necesario definir los marcos de referencia y metodologías que apoyan el PETI y a la OTIC en general, dado el caso si se efectúa un cambio en los distintos planes, estrategias y documentos, este debe reflejarse a través de una actualización oportuna del PETI.

6.6. Gestión de Contratos

- Implementar controles o actividades internas y adicionales para evitar que las órdenes de compra expiren en el tiempo de liquidación, realizando un seguimiento efectivo a la liquidación de las órdenes de compra por parte de los supervisores de la OTIC.

6.7. Planes de Mantenimiento

Extender las medidas de monitoreo y de registro diario de las variables de temperatura y humedad de los centros de comunicaciones de todos los GITT, creando formatos y procedimientos para tal fin.

6.8. Accesibilidad Web

- Desarrollar los respectivos análisis técnicos y tecnológicos que conlleven al desarrollo de un plan de diseño e implementación en la página web de la UBPD de los criterios de accesibilidad definidos en la Norma NTC 5854, lo anterior con el fin de evitar el riesgo de incumplimiento normativo y en consonancia con el principio humanitario que rige la UBPD para ofrecer una mejor experiencia en el uso de la página web por parte de personas con discapacidades y otras limitaciones.
- Se recomienda que la supervisión contractual sea compartida entre la OACP y la OTIC teniendo en cuenta el apoyo requerido por la OTIC, donde se deben definir los roles y responsabilidades de forma clara.

6.9. Transición IPV4 a IPV6

- Se recomienda a la luz del concepto dado por el MinTIC a la OTIC, la revisión y análisis de aplicación y/o realización de la Política de Gobierno Digital en la UBPD, en virtud del principio de coordinación y colaboración armónica, establecidos en la Constitución Política.

6.10. Planeación y Gestión de la Continuidad del Negocio

- Se recomienda que a través del líder del BCP se gestione la integración de los temas de Continuidad de Negocio hacia alguno de los Comités de tipo directivo y así mismo, proyectar un rubro dentro del presupuesto de la UBPD destinado a la Continuidad del Negocio, no solo ante un evento catastrófico, sino también para la implementación del DRP.

6.11. Uso y Apropiación

- Se recomienda como buena práctica establecer en un documento la planificación y la ruta de las actividades que hacen parte de la Estrategia de Uso y Apropiación, lo anterior con el fin de enmarcar lineamientos, actividades, proyectos, grupos de interés, medición de resultados etc.
- Continuar con el reforzamiento en el uso y apropiación de la G-Suite teniendo en cuenta las nuevas vinculaciones de servidores, así mismo ampliar la estrategia a través de un documento que también planifique y trace la ruta del 2020 para la estrategia de Uso y Apropiación hacia las demás tecnologías y servicios (Office, Adobe Acrobat, Navegadores, Antivirus, Compresores,

PDF Creator, Mesa de Ayuda, Internet, Equipos de Cómputo, Impresoras) con el fin de mejorar la experiencia, la productividad y el conocimiento en general de todas estas herramientas.

6.12. Mapas de Riesgos, Controles y Actividades

- Se recomienda una vez se inicie el proceso de monitoreo, revisión y seguimiento anual al Mapa de Riesgos por parte de la OTIC e indicado en la Política de Administración de Riesgos, se efectúen los respectivos análisis, valoraciones y actualizaciones a los riesgos y sus controles teniendo en cuenta que al momento de la valoración inicial efectuada en el 2019 no se contaba con algunos procedimientos, guías, formatos, manuales etc. y que a la fecha de la presente auditoría ya se cuentan, además del progreso evidenciado en los procesos que tiene a cargo la OTIC entre el 2019 y 2020 donde los riesgos identificados en los proyectos se encuentren integrados en el Mapa de Riesgos TIC; lo anterior con el fin de conducir el Mapa de Riesgos TIC a un estado donde la relación entre riesgos inherentes y residuales se encuentre debidamente tratados, así como la valoración de la solidez individual y conjunta de los controles no sea débil.
- Aplicar controles adicionales al ciclo de vida de los documentos generados por la OTIC, donde el área es la responsable de verificar la correspondencia entre el envío y la socialización y/o publicación en el Sistema de Gestión, así mismo de su monitoreo periódico con el fin de tener certeza del inventario de documentación en trámite y publicada en el Sistema de Gestión y en la Página Web de la UBPD.

6.13. Indicadores de Gestión

- De acuerdo a la lectura trimestral acumulada presentada en el archivo “Ficha Indicadores OTIC IV Trimestre.xlsx” el indicador se encuentra “Sobrestimado” teniendo en cuenta que el porcentaje en la medición (cumplimiento trimestral del área) siempre estuvo por encima del valor del porcentaje planificado; por lo anterior, se recomienda ajustar el valor planificado teniendo en cuenta el rendimiento promedio del indicador, durante el 2019 presentó una diferencia del 10%.

(ORIGINAL FIRMADO)
IVONNE DEL PILAR JIMÉNEZ GARCÍA
 Jefe Oficina de Control Interno

Elaborado por:	Carlos Andres Rico Reina	Auditor Líder	FIRMA:
	Natalia Sofía Beltrán Ballén	Equipo Auditor	FIRMA:
Aprobado por:	Ivonne del Pilar Jiménez García Jefe de Control Interno	Jefe Oficina de Control Interno.	FIRMA: