UBPD

UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

MANUAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN-SSI

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

1. INTRODUCCIÓN

Este documento tiene una estructura que comprende su objetivo general y objetivos específicos, alcance, marcos de trabajo, estructura del Sistema de Seguridad de la Información, Metodología del Diseño y construcción del Sistema de Seguridad de la Información, Diseño del Ciclo de Vida del Sistema de Seguridad de la Información, Política General, Políticas de Seguridad de la Información y Políticas de Seguridad Digital, Matriz RACI de Roles y Responsabilidades de Seguridad de la Información, Indicadores del Sistema de Seguridad de la Información, Metodología de Seguimiento al Sistema de Seguridad de la Información y el Plan de Auditoría Interna del Sistema de Seguridad de la Información, que reflejan los aspectos más relevantes del documento.

De otro lado, es importante resaltar que el carácter humanitario y extrajudicial de la UBPD exige condiciones idóneas para la seguridad de la información, que garanticen su confidencialidad; por lo tanto, se hace necesaria la implementación y mantenimiento de este Sistema de Seguridad de la Información. Así mismo, entre las estrategias para la gestión de la información se dispondrá de mecanismos que garanticen su confidencialidad y anonimización, brindando así garantías a los aportantes.

Por lo anterior, con el fin de destacar la importancia que tiene la información en las labores de búsqueda, dentro de las líneas de acción que establece el Plan Nacional de Búsqueda – PNB, se encuentra el Fortalecer las estrategias, políticas, herramientas e instrumentos de seguridad, protección y confidencialidad de la información, ya que la UBPD tiene una importante responsabilidad con respecto a la información pues, si bien de ésta depende que pueda cumplir con sus funciones, también depende de su confidencialidad el garantizar las condiciones de seguridad de las personas, tanto de las que participan en la búsqueda, como de las que entregan información.

Así pues, la gestión de riesgos de seguridad de la información debe evaluar, por ejemplo, el fortalecimiento de las condiciones de seguridad necesarias para incentivar el suministro de información que contribuya a la búsqueda y localización de parte de las personas que aportan información que conduzca a la ubicación; lo anterior permite generar confianza en el suministro de datos sobre el paradero de las personas dadas por desaparecidas, sin temor a que las personas aportantes sean involucradas en procesos penales o perseguidos judicialmente.

Es por ello que la consolidación de un Sistema de Seguridad de la Información -SSI, es un paso fundamental para que la UBPD implemente una de las estrategias contenidas en el eje estratégico No. 1 del Plan Nacional de Búsqueda -PNB-, referente a la recolección, retroalimentación, seguridad de la información y construcción de confianza. Así, el SSI contribuye a fortalecer la construcción de confianza y permite dar certezas *"sobre los mecanismos estatales de protección de la información y de quienes la aportan, en el corto, mediano y largo*

plazo. Transmitir esta seguridad implica un incentivo para su suministro, no solamente para los familiares y organizaciones, sino para las personas que participaron directa o indirectamente en las hostilidades y la sociedad en general. La seguridad de la información incluye, desde la confidencialidad o reserva, hasta la permanencia de esta en la UBPD, que se constituyen en factores que tienden a brindar seguridad en quienes la proporcionan y, reducen la desconfianza que pueda generar su uso. Por su parte, la seguridad de quienes aportan información abarca, desde la protección de sus datos personales, hasta la garantía que no será utilizada en procesos judiciales"[1].

Precisamente, la relación de la esencia humanitaria y extrajudicial de la UBPD con la seguridad de la información puede verse en la dimensión que da el marco jurídico que la rige, sobre todo, porque la modalidad de trabajo de todos los equipos de la entidad tiene como base la confidencialidad. Así, con el fin de garantizar la efectividad del trabajo humanitario y extrajudicial de búsqueda, la información que reciba recaude o produzca, en el desarrollo de sus actividades misionales de búsqueda, es de carácter confidencial[2], no tiene valor probatorio, no puede ser utilizada a fines incriminatorio en procesos penales y no puede ser trasladado a las autoridades judiciales[3].

El Acto Legislativo 01 de 2017 estableció que la UBPD "tendrá carácter humanitario (…) con un mandato de búsqueda humanitaria". Por su parte el Decreto Ley 589 de 2017 estableció que la UBPD es una "entidad estatal de naturaleza humanitaria"[4]. Al respecto, la Corte Constitucional[5] precisó que la UBPD es un organismo humanitario y que, en consecuencia, sus labores misionales de búsqueda deben desarrollarse "en el marco de la confidencialidad"[6]. Así, la UBPD debe garantizar la confidencialidad, de las entrevistas de las personas para incentivar que voluntariamente sigan suministrando información, como otras informaciones confidenciales que reciba o recaude.

Respecto del régimen de confidencialidad de la información de la UBPD, la Corte Constitucional ha señalado que éste:

> *"resulta indispensable para generar confianza y lograr que los excombatientes, las propias víctimas y cualquiera en general suministren información sobre el paradero de las personas dadas por desaparecidas, sin temor a ser involucrados en procesos penales o perseguidos judicialmente. En el caso de los excombatientes que se sometan a la jurisdicción especial representa una oportunidad para obtener incentivos durante el juzgamiento, y para quienes no tengan que hacerlo, la posibilidad*

[1] Plan Nacional de Búsqueda de la UBPD, página 19, segundo párrafo.

[2] Su gestión se realiza conforme a lo establecido dentro del índice de información clasificada y reservada de la UBPD

[3] Sentencia C-080/18

[4] Artículo Transitorio 3°.

[5] Considerando 26. En el mismo sentido ver los considerandos 25 y 27.

[6] Sentencia C-080/18.

de aportar verdad en un escenario libre de persecución judicial. Para las víctimas y la sociedad en general se constituye en un espacio libre para aportar información sin temor a represalias"[7].

En consecuencia, el SSI debe involucrar, entre otros elementos, mecanismos que mitiguen los riesgos a los que está sometida la información que recibe y genera la UBPD. Una falla grave en el SSI que ponga en duda la capacidad de garantizar la confidencialidad de la información, entre otras consecuencias, pondría en riesgo la vida, la integridad y la libertad de las personas (tanto de quienes suministraron la información como de quienes trabajan en la entidad); y también, generaría desconfianza y daría al traste con la apuesta institucional de lograr que cualquiera en general suministre información sobre el paradero de las personas dadas por desaparecidas.[8]

2. OBJETIVOS

Se presenta a continuación el objetivo general, así como los objetivos específicos:

2.1 OBJETIVO GENERAL

El objetivo del presente documento es diseñar el Sistema de Seguridad de la Información (SSI) para la UBPD, a través del cual se establecen los lineamientos de alto nivel como las políticas de seguridad de la información y las políticas de seguridad digital, hasta los documentos que permitan su implementación, seguimiento y control como son el proceso de gestión de seguridad de la información, procedimientos, guías, formatos, indicadores y los roles que gestionen la seguridad de la información y la seguridad digital en la Entidad, hasta definir los mecanismos de revisión del SSI, de tal manera que permitan garantizar una permanente mejora continua de la gestión de la seguridad.

2.2 OBJETIVOS ESPECÍFICOS

1. Diseñar el Sistema de Seguridad de la Información de la UBPD.
2. Definir las Políticas de Seguridad de la Información y las Políticas de Seguridad Digital de la UBPD.
3. Definir la estructura organizacional de la Seguridad de la Información y la Seguridad Digital, estableciendo los roles y sus responsabilidades para la UBPD.
4. Definir los indicadores de seguridad para medir el desempeño y la gestión del Sistema de Seguridad de la Información.
5. Establecer la metodología de seguimiento al Sistema de Seguridad de la Información.
6. Definir el Plan de Auditoría Interna del Sistema de Seguridad de la Información.

[7] Sentencia C-067/18

[8] Documento "La importancia de la seguridad de la información para la UBPD", escrito por el Dr. Oscar Carbonell

3. MARCO DE TRABAJO

Existen a nivel global distintas normas, marcos de referencia o mejores prácticas que facilitan la estructura de un sistema de seguridad de la Información, por lo tanto, a continuación, se mencionan cuáles de estas se adoptaron como apoyo para el diseño del Sistema de Seguridad de la Información para la UBPD.

A nivel internacional, se tomaron como referencia los siguientes estándares:

- **Norma ISO/IEC 27001:2013:** es el estándar internacional que define los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). El estándar se ha concebido para garantizar la selección de controles de Seguridad adecuados y proporcionales, esto ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas. El estándar adopta un enfoque por procesos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI.

- **ISO/IEC 27002:2013:** guía de controles de seguridad de la información la cual se usa como referencia para seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO/IEC 27001, o como documento guía para organizaciones que implementan controles de seguridad de la información.

- **ISO/IEC 27004:2016:** estándar que contiene lineamientos para evaluar el desempeño de la seguridad de la información y la efectividad de un Sistema de Gestión de Seguridad de la Información para cumplir con los requisitos de ISO/IEC 27001:2013, en su numeral "9.1 monitoreo, medición, análisis y evaluación".

- **Norma ISO/IEC 27005:2018:** técnicas de Gestión para riesgos en seguridad de la información. Proporciona directrices para la gestión del riesgo en seguridad de la información en una organización, dando soporte particular a los requisitos de un Sistema de Gestión de Seguridad de la Información – SGSI de acuerdo con la norma NTC-ISO/IEC 27001.

- **Norma ISO/IEC 31000:2018:** es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones. Esta norma fue publicada por la Organización Internacional de Normalización (ISO) y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

- **ISO/IEC 27032:2012:** es un estándar que ofrece unas líneas generales de orientación para fortalecer el estado de la Ciberseguridad en una entidad, utilizando los puntos técnicos y estratégicos

más importantes para esa actividad y los que están relacionados con: la Seguridad en la Redes, Seguridad en Internet, Seguridad de la información y la Seguridad de las Aplicaciones.

- **ISO/IEC 22301:2012:** es una norma que proporciona un marco de referencia para gestionar la continuidad del negocio en una organización, disminuyendo la posibilidad de ocurrencia de un incidente disruptivo y, en caso de producirse, poder estar preparado para responder en forma adecuada y, de esa forma, reducir drásticamente el daño potencial de ese incidente.

- **ISO/IEC 19011:2018**: guía que contiene lineamientos para auditar sistemas de gestión, desde la definición del programa de auditoría, la ejecución de los planes de la auditoría, y la evaluación del equipo auditor.

- **COBIT 2019:** es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI).

- **Marco de Referencia de Ciberseguridad (Cybersecurity Framework) del NIST (National Institute of Standards and Technology):** marco basado en estándares, pautas y prácticas existentes para que las organizaciones administren y reduzcan mejor el riesgo de ciberseguridad.

- **Comité Internacional de la Cruz Roja-CICR:** Se tomaron como referencia algunos documentos en los que se encuentran aspectos relacionados con la seguridad y protección de la información sensible, como los siguientes:
    - Norma 117. Obligación de averiguar lo acaecido a las personas desaparecidas https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule117
    - DIH PRINCIPIOS BÁSICOS DE DERECHO INTERNACIONAL HUMANITARIO https://www.icrc.org/es/doc/assets/files/other/p0850.pdf
    - No discriminación y conflicto armado https://www.icrc.org/es/doc/resources/documents/misc/5tdpjk.htm La neutralidad como Principio Fundamental de la Cruz Roja https://www.icrc.org/es/doc/resources/documents/misc/5tdltx.htm

A nivel nacional, se tomaron como referencia los siguientes:

- **CONPES 3854 de 2016:** Política Nacional de Seguridad Digital.

- **CONPES 3995 de 2020** Política Nacional de Confianza y Seguridad Digital.

- **Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 4 - octubre de 2018:** documento del Departamento Administrativo de la Función Pública (DAFP) que

provee lineamientos a entidades públicas sobre los riesgos de gestión, corrupción y seguridad digital, y su **Anexo 5 - Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas - 2020:** documento del Departamento Administrativo de la Función Pública (DAFP) que permite Orientar a todas las entidades del Gobierno nacional, territoriales y sector público en la implementación de la gestión de riesgos de seguridad digital basada en la definición metodológica del Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) para, entre otros aspectos, incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en cada entidad pública.

- **Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) (2019):** marco de gestión de riesgos de seguridad digital desarrollado por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) el cual incluye los lineamientos en riesgos relacionados con seguridad digital.

4. ALCANCE

El Sistema de Seguridad de la Información SSI de la UBPD comprende todos los aspectos documentales, administrativos, físicos, geográficos y técnicos encaminados a la protección de la información que gira en torno a la búsqueda de las personas dadas por desaparecidas, el cual tiene como objetivo proteger todos los activos de información de los procesos de toda la Entidad incluidos en los niveles Estratégicos, Misionales, Apoyo, y Evaluación, los cuales se presentan en el Mapa de Procesos de la UBPD:

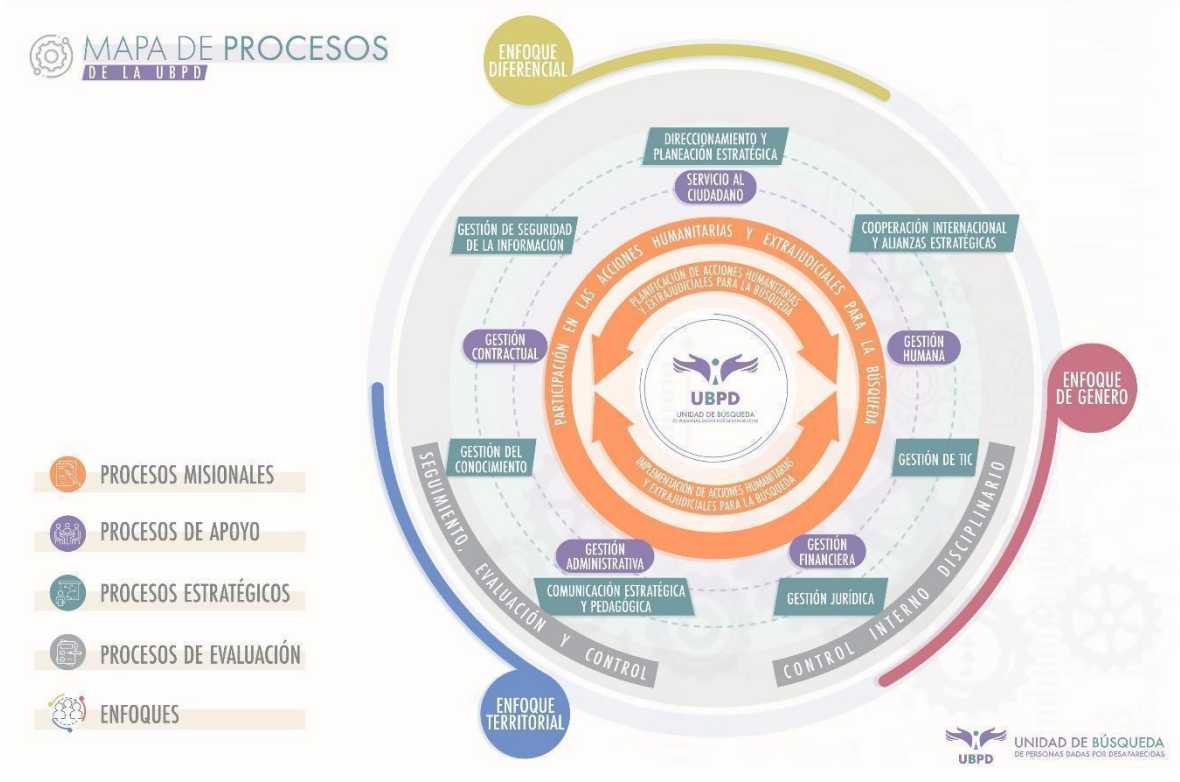


Ilustración 1 Mapa de Procesos para UBPD

Fuente: Información suministrada por la UBPD el 15 de abril de 2020

5. METODOLOGÍA DEL DISEÑO Y CONSTRUCCIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Para el diseño y construcción del presente Sistema de Seguridad de la Información, se establecen las siguientes fases, así:

Ilustración 2 Metodología del Diseño del Sistema de Seguridad de la Información Fuente: UT MYQ-ALINA TECH

- **Entendimiento del contexto:** Se revisa la documentación en torno a la misión, visión, organigrama, normatividad interna y externa aplicable, conocimiento de las fases a través de las cuales se hace la búsqueda (Recolección, organización y análisis de información, Localización, Prospección y Recuperación, Identificación y Reencuentro o Entrega Digna), conocimiento de los procesos Estratégicos, Misionales, Apoyo, y Evaluación.

  Además, se identifican los interesados internos y externos y sus necesidades en torno a Seguridad de la Información, se identifican las expectativas y necesidades de la Alta Dirección y de los Líderes de las distintas dependencias de la UBPD, en torno a los componentes del Sistema de Información Misional, al de Estrategia de TI y al de Seguridad de la Información, determinar y conocer los convenios y tratados internacionales en los que se definen lineamientos que pretenden proteger la información con carácter de reserva o confidencial.

- **Determinar Mejores Prácticas de Seguridad**: Para garantizar que el Sistema de Seguridad de la Información contemple todos los aspectos de seguridad aplicables a la UBPD, se identifican mejores prácticas a nivel mundial ampliamente reconocidas y aceptadas para poder contemplar: generalidades para el diseño, desarrollo, implementación, seguimiento y control del Sistema de Seguridad de la Información (ISO 27001:2013), gestión de riesgos de seguridad (ISO 27005:2018, ISO 31000: 2018, continuidad de la operación de los procesos soportados en tecnología (ISO 22301:2019), aspectos de ciberseguridad (ISO 27032:2012 y NIST CSF (Cybersecurity Framework)), indicadores de seguridad (ISO 27004:2016) auditoría al sistema de seguridad (ISO 19011:2018)controles a los procesos de las tecnologías de la información y las comunicaciones (COBIT 2019), y recomendaciones de entidades del gobierno nacional como CONPES 3854 de

2016: Política Nacional de Seguridad Digital, la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública, los lineamientos de Protección de Datos Personales de la Superintendencia de Industria y Comercio, los lineamientos de seguridad digital del Ministerio de las Tecnologías de la Información y las Comunicaciones, así como los lineamientos de protección de la información y del Derecho Internacional Humanitario emitidos por el Comité Internacional de la Cruz Roja, así mismo, el entendimiento de toda la información de los diferentes niveles directivo, ejecutivo y operativo que podría ser pertinente para el diseño y desarrollo del Sistema de Seguridad de la Información.

- **Diagnóstico de Seguridad de la Información**: El Diagnóstico de Seguridad de la Información comprende la identificación de las partes interesadas internas y externas, la solicitud de entrevistas e información, el análisis de la información y documentación y la generación del estado actual de la Seguridad de la Información, para este diagnóstico se toma como referencia principal las cláusulas y dominios de la norma ISO 27001:2013, los cuales se complementan con otros aspectos de los estándares internacionales como COBIT 2019, ISO 31000, ISO 22301 e ISO 27032, los cuales se detallan en el **UBPD Diagnóstico de Seguridad_V2.0.**

- **Desarrollo Propuesta de Estructura del SSI:** A partir de la estructura de alto nivel del Sistema de Seguridad de la información, descrita en el Diagnóstico de Seguridad de la Información, y la cual parte de la base de la Arquitectura de Seguridad, así como el análisis de aplicabilidad de dominios, objetivos de control y controles, la UT M&Q-ALINATECH desarrolla y deja a consideración de la UBPD, una propuesta que incluye: las políticas específicas de seguridad de la información, las políticas específicas de seguridad digital la estructura metodológica para la gestión de riesgos y activos de información, los roles y responsabilidades de la UBPD que van a gestionar la Seguridad en la Entidad, los procedimientos de seguridad que van a soportar la operación de la gestión de la seguridad, la continuidad de las operaciones de la UBPD, los indicadores que van a permitir medir y mejorar el Sistema de Seguridad de la Información, el Plan de Auditoría Interna, y la metodología de seguimiento del SSI.

- **Validación de Estructura del SSI:** La propuesta de la estructura de los diferentes aspectos de seguridad descritos en la fase anterior es presentada por la UT M&Q-ALINATECH a la UBPD, con el fin de dejar a consideración de la Entidad la adopción de esta propuesta, acordando la estructura y criterios de aceptación de criterios de aceptación de los diferentes documentos a desarrollar como parte del Sistema de Seguridad de la Información.

- **Desarrollo documentos del SSI**: Luego de haber acordado la estructura y los criterios de aceptación de los diferentes documentos a desarrollar como parte del Sistema de Seguridad de la Información, se desarrollan todos los entregables como son: la caracterización del proceso de gestión de la seguridad de la información, las políticas específicas de seguridad de la información,

y de seguridad digital, la estructura metodológica para la gestión de riesgos y activos de información, los roles y responsabilidades de la UBPD que van a gestionar la Seguridad en la Entidad, los procedimientos de seguridad que van a soportar la operación de la gestión de la seguridad, de la continuidad de las operaciones de la UBPD , los indicadores que van a permitir medir y mejorar el Sistema de Seguridad de la Información, el Plan de Auditoría Interna, y la metodología de seguimiento del SSI, así mismo, como parte del sistema también se desarrollan diferentes entregables relacionados con el Plan de Continuidad del Negocio, las herramientas de seguridad pertinentes al SSI, el desarrollo más detallado de la Arquitectura de Seguridad, la planeación y ejecución de pruebas de ethical hacking la planeación de la estrategia de defensa en profundidad para la plataforma tecnológica de la Entidad el plan de gestión de vulnerabilidades y el plan de respuesta a incidentes de seguridad.

- **Revisión y aprobación del SSI:** Luego del desarrollo de los diferentes documentos que establecen y soportan el Sistema de Seguridad de la Información son revisados y ajustados para su posterior aprobación y adopción.

- **Publicación y socialización del SSI:** Luego de ser aprobados los diferentes documentos que establecen y soportan el Sistema de Seguridad de la Información, éste se debe formalizar, publicar y socializar a las partes interesadas para su correspondiente conocimiento, entendimiento y cumplimiento.

6. SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Seguridad de la Información (SSI) de la UBPD tiene como objetivo proteger todos los activos de información de los procesos de la Entidad incluidos en los niveles Estratégicos, Misionales, Apoyo, y Evaluación, el cual tiene en cuenta lo siguiente:

- El carácter *humanitario y extrajudicial* de la Entidad, y que la información recibida y producida por la UBPD, que permita dar con el paradero de las personas dadas por desaparecidas en contexto y en razón del conflicto armado, así como su procedencia, *es totalmente confidencial y no puede ser utilizada como material probatorio en un proceso judicial*.

- En el ejercicio de sus funciones humanitarias, los Servidores de la UBPD pueden recoger, entregar, procesar y consultar informaciones que contienen *datos de carácter personal*. Estas informaciones y datos pueden incluir alegaciones extremadamente sensibles sobre abusos y violaciones a los derechos humanos, cuya divulgación puede conllevar riesgos para las víctimas, sus familiares, las personas que recogen estas informaciones y cualquier aportante de información. Por otra parte, constituirá una violación de su derecho de privacidad y a la protección de los datos personales. Por eso, es fundamental que los servidores (as), contratistas y personal delegado de la UBPD protejan los datos personales y confidenciales de las víctimas de conflictos armados y otras situaciones de violencia es parte integral de la protección y asistencia a estas víctimas.

- *Convenios y tratados internacionales* en los que se definen lineamientos que pretenden proteger la información con carácter de reserva o confidencial tales como GDPR (Reglamento General de Protección de Datos de la Unión Europea) que además tratan temas de Derecho Internacional y en cuanto a la protección de datos personales lo dispuesto por la Superintendencia de Industria y Comercio en el link Humanitario https://www.sic.gov.co/tema/proteccion-de-datos-personales y la demás normatividad vigente y aplicable.

- *Mejores prácticas o estándares* internacionales relacionados con protección y privacidad de la información tales como ISO 27001, ISO 22301, ISO 31000, COBIT 2019, NIST 800-39, aplicables dentro del contexto a la UBPD.

Por lo tanto, partiendo del contexto de la UBPD y sus necesidades de seguridad, la siguiente es la vista de la Arquitectura de Seguridad la cual contiene al Sistema de Seguridad de la Información:

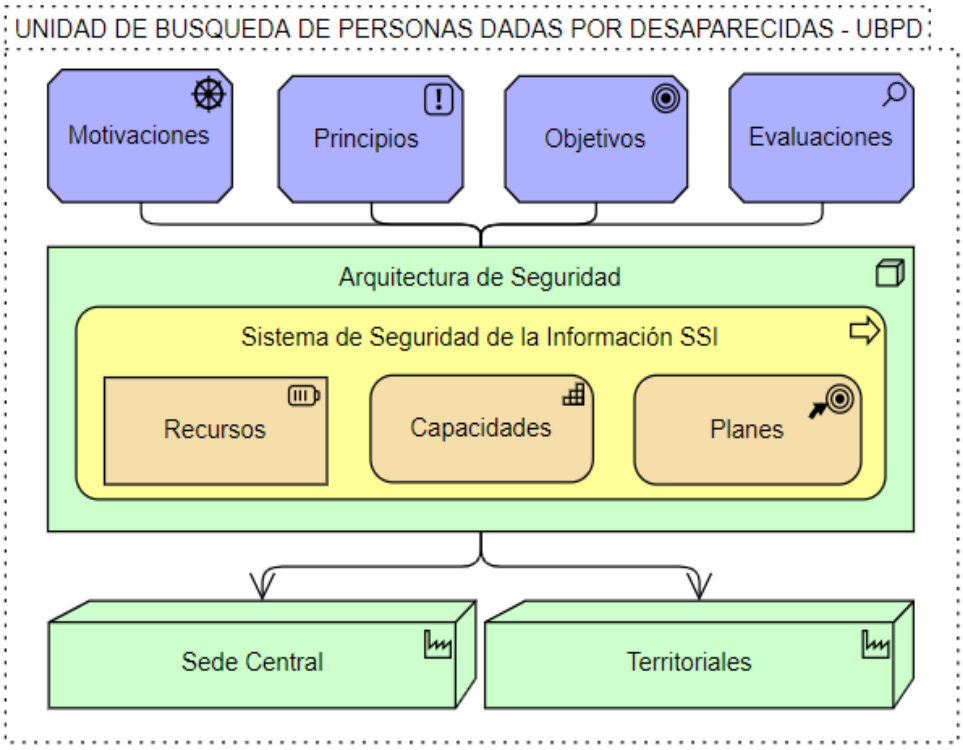


Ilustración 3 Vista Lógica Arquitectura de Seguridad dentro de la UBPD Fuente: Elaboración UT MYQ-ALINA TECH

Esta vista muestra cómo a partir de las motivaciones de la protección de la información que tiene la UBPD, los principios de la seguridad que le aplican, los objetivos estratégicos de la entidad y las evaluaciones de seguridad entre otros temas, se requiere definir una Arquitectura de Seguridad que responda a estos aspectos, y a partir de estos temas antes relacionados, estructurar la Arquitectura de Seguridad y a partir de esta también se determina el Sistema de Seguridad SSI, el cual debe establecer unos planes, actividades y además contar con una serie de capacidades y recursos para mantener una mejora continua, teniendo en cuenta además las capacidades del negocio del Plan Estratégico de Tecnologías de la Información; es de anotar, que el diseño de la Arquitectura de la Seguridad se desarrollará de manera completa y detallada en el entregable **P34 "Diseño Lógico y Físico de la Arquitectura de la Seguridad"**.

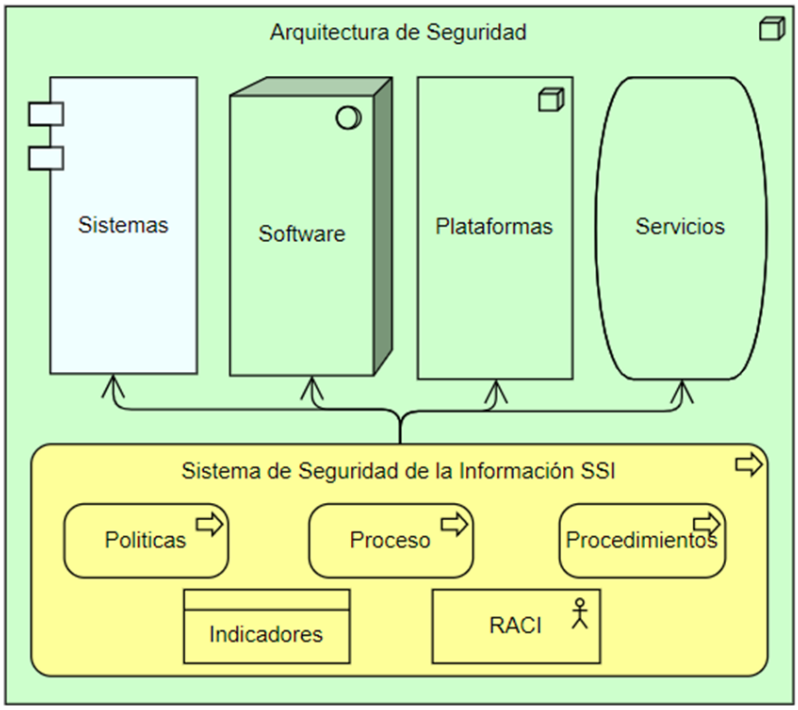


Ilustración 4 Vista Lógica de Alto Nivel de Arquitectura de Seguridad Fuente: Elaboración UT MYQ-ALINA TECH

Así mismo, la Arquitectura de Seguridad define aspectos de manera más específica alrededor de los sistemas de información, el software base, la plataforma tecnológica y los servicios tecnológicos, teniendo en cuenta los lineamientos o aspectos de alto nivel del Sistema de Seguridad de la Información SSI, el cual establece políticas de seguridad de la información, políticas de seguridad digital, el proceso de la Gestión de la Seguridad de la Información, los procedimientos de, los indicadores y los roles y responsabilidades del SSI, los cuales se visualizan en la siguiente gráfica y se detallan de manera más específica a continuación.

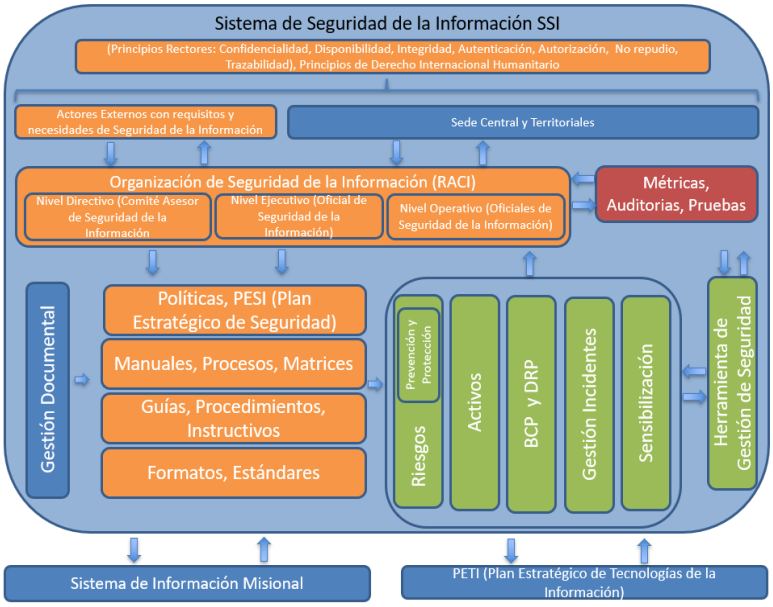


Ilustración 5 Estructura de Sistema de Seguridad de la Información de Alto Nivel Fuente: Elaboración UT MYQ- ALINA TECH

A continuación, se explican los componentes así:

Fase inicial de Diseño y Desarrollo del SSI (color naranja): Se realiza la identificación de los principios rectores, la identificación de todos los actores externos y sus necesidades o requisitos de seguridad, el desarrollo, formalización y divulgación de todos los documentos que soportan este Sistema.

Fase de implementación (color verde): En la que se gestionan aspectos de riesgos de seguridad, activos de información, continuidad del negocio, incidentes de seguridad, sensibilización en seguridad y la herramienta de gestión del Sistema.

Fase de Evaluación y Mejora continua (color Vinotinto): Se realiza el seguimiento de desempeño del sistema a través de mecanismos como métricas, auditorías y pruebas de seguridad las cuales arrojarán resultados que permitan identificar oportunidades de mejora y mantener en permanente evolución y madurez este Sistema de Seguridad de la Información.

Este Sistema es el que responde a las necesidades de seguridad de la información y seguridad digital de la Entidad, para proteger de manera adecuada la información, por lo que se requiere inicialmente una fase de diseño y desarrollo; luego una fase de implementación, y posteriormente una fase de evaluación y mejora continua, para así, cumplir un ciclo completo de implementación. Ahora bien, a partir de las oportunidades de

mejora que se vayan identificado, los nuevos riesgos presentados, los cambios y necesidades de la Entidad, se deberán rediseñar o fortalecer controles, implementarlos, medirlos y mejorarlos, con el fin de ir madurando los niveles de seguridad de la información de la UBPD.

Este Sistema de Seguridad de la Información está enmarcado en los principios rectores de seguridad tales como: Confidencialidad, Disponibilidad, Integridad, Autenticación, Autorización, No repudio y Trazabilidad, así como en los Principios Fundamentales del Derecho Internacional Humanitario (De humanidad:, de igualdad entre los beligerantes, de no discriminación:, de neutralidad y de prioridad humanitaria), a partir de estos principios los actores externos generan requisitos y necesidades de seguridad las cuales sirven de insumo para que la organización de seguridad de la información y de la seguridad digital, definan los diferentes lineamientos de seguridad como: Políticas, Manuales, Procesos, Matrices, Guías, Procedimientos, Instructivos, Formatos o Estándares, todos alineados con el Modelo operativo de gestión Documental.

Cada uno de estos lineamientos de diferente nivel de profundidad definen aspectos de temas como Riesgos de Seguridad, Activos de Seguridad, Continuidad del Negocio, Gestión de Incidentes, Sensibilización de Seguridad entre otros, los cuales, para contar con los registros y trazabilidad de su ejecución, deben gestionarse a través de una herramienta de gestión de seguridad.

En cuanto a la Organización de la Estructura de la seguridad (RACI) se definió por parte de la Entidad un Nivel Directivo en el cual se encuentra el Comité de Seguridad de la Información, siendo este el que asesora a (el) (la) Director (a) General, quien es la que adopta las decisiones relacionados con Seguridad de la Información, luego en el siguiente Nivel Ejecutivo se encuentra el Oficial de Seguridad de la Información quien coordina todos los aspectos de seguridad y finalmente en el Nivel Operativo se encuentran los Oficiales de Seguridad de la Información Operativos implementan y supervisan el cumplimiento de las directivas, circulares, instrucciones, planes y protocolos de seguridad de la información por parte de las/os servidoras/es públicos, contratistas o personal delegado de la UBPD de su respectiva dependencia.

De otro lado, para que se pueda evaluar el Sistema de Seguridad de la Información se deben llevar a cabo auditorías, pruebas de seguridad y métricas, todas estas gestionadas a través de la herramienta del SSI, y a partir de estas identificar oportunidades de mejora, para que los diferentes roles de seguridad de las diferentes áreas de la Entidad, incluidos los equipos territoriales deban hacer ajustes a la gestión de la seguridad y mantener y operar un Sistema de Seguridad en constante mejora y madurez.

Este Sistema de Seguridad definirá los lineamientos de Seguridad que debe cumplir el Sistema de Información Misional y los demás sistemas de información y componentes tecnológicos de la Entidad; y a su vez es insumo para que el PETI (P29 Plan Estratégico de las Tecnologías de la Información y el P28 Identificación de los proyectos necesarios para cerrar la brecha (mapa de ruta)), cumplan los lineamientos de seguridad y suplan algunas de las necesidades en cuanto a controles, soluciones o proyectos de seguridad

requeridos por este Sistema, esta comunicación es bidireccional, ya que en la medida que el Sistema de Información Misional evolucione y tenga cambios estos deberán tenerlos presente en el Sistema de Seguridad de la Información para que alrededor de ellos se definan los temas de seguridad que correspondan; de igual manera, el PETI en la medida que cambie generará necesidades en cuanto a planes, proyectos y programas que el Sistema de Seguridad de la Información debe blindar con las directrices de seguridad que correspondan.

Es de anotar, que este SSI aplica para toda la Entidad, incluyendo todas las sedes territoriales y satélites, a las cuales se les debe brindar los recursos humanos, tecnológicos, financieros, de infraestructura y administrativos para cumplir con todos los lineamientos de seguridad de este sistema, y que aplica, además, para todos los formatos en los cuales se encuentre la información.

A continuación, se detallan los aspectos contemplados para cada uno de los componentes del Sistema de Seguridad de la Información, así:

- **Arquitectura de Seguridad de la Información:** Define lineamientos de protección a todos los niveles de la Entidad de manera integral, para proteger los activos de información aplicando los controles adecuados y oportunos que correspondan, teniendo presente siempre los principios de seguridad como: Confidencialidad, Disponibilidad, Integridad, Autenticación, Autorización, No repudio, Trazabilidad.

- **Organización de Seguridad de la Información:** Define roles y responsabilidades y se mapean a través de una matriz RACI (Responsable, Aprobador, Consultado, Informado), para cada uno de los actores internos dentro del Sistema de Seguridad de la Información, así mismo, se deben tener en cuenta las necesidades, requerimientos y expectativas de seguridad de los diferentes actores externos, lo cual será desarrollado como parte de la ejecución del presente proyecto.

- **Riesgos:** Para el SSI el componente más relevante es la identificación, valoración y tratamiento de riesgos de seguridad de la información de manera oportuna y adecuada, lo cual será desarrollado como parte de la ejecución del presente proyecto, en la matriz de riesgos de seguridad de la información.

- **Activos:** Con el fin de contemplar todos los activos de seguridad de la información como son: información, personas, software, infraestructura, Hardware y servicios; éstos se deben identificar y valorar, para tenerlos presentes en el impacto asociado a los riesgos de seguridad de la información con los cuales tengan relación, lo cual será desarrollado como parte de la ejecución del presente proyecto, en la matriz de activos de información.

- **BCP (Plan de Continuidad de la Entidad) y DRP (Plan de Recuperación de Desastres):** Es muy importante poder realizar un análisis de impacto ante eventos adversos para los procesos de la Entidad, priorizarlos y tomar medidas que permitan garantizar la disponibilidad de la información y los servicios que requiere u ofrece la Entidad, lo cual será desarrollado como parte de la ejecución del presente proyecto, en el Plan de Continuidad del Negocio y en el Plan de Recuperación de Desastres.

- **Gestión de Incidentes:** La correcta y oportuna gestión de incidentes de seguridad de la información de acuerdo a como se defina en el Manual de equipo GRIES y el Plan de Respuesta a Incidentes IRP, permitirá mitigar el impacto en la disponibilidad, integridad y confidencialidad de la información y de los servicios, así mismo, permitirá ajustar, mejorar y madurar el Sistema de Seguridad de la Información.

- **Sensibilización en Seguridad de la Información:** Es muy importante el conocimiento y entendimiento de todos los lineamientos de seguridad emitidos por la Entidad por parte de cada uno de los servidores, contratistas y personal delegado, para su cumplimiento; así mismo, es muy relevante la constante concientización sobre las permanentes amenazas, con el fin de poder detectarlas y reportarlas de manera oportuna y así saber cómo proceder de manera adecuada y oportuna frente a estas. Este componente de sensibilización tiene gran importancia dentro del SSI, ya que las personas son el eslabón más débil en la cadena de protección de la información, por lo tanto, es indispensable mantenerlas actualizadas en los diferentes aspectos de seguridad de la información, a través de mensajes que usen un lenguaje común, sencillo y entendido por todos, por medio de los diferentes canales de comunicación que tenga establecidos la Entidad.

- **Métricas, Auditorías y Pruebas:** Permitirá detectar desviaciones del Sistema, evaluando y ajustando controles por quienes hacen parte de la estructura de la seguridad, con el fin de ir generando una mejora continua y madurez del Sistema de Seguridad de la Información, cada uno de estos aspectos se desarrolla con mayor detalle dentro de la Metodología de Seguimiento al Sistema de Seguridad de la Información descrita en este documento.

- **Políticas:** Son las directrices de alto nivel de seguridad de la información, que establecen los lineamientos que orientan las acciones de servidores contratistas y personal delegado para la protección de la información de la Entidad. Para lo cual se establecieron las Políticas de Seguridad de la Información y las Políticas de Seguridad Digital, que se relacionan y desarrollan en el capítulo 7.1 de este documento.

- **PESI:** Corresponde a los Planes Estratégicos de la Seguridad de la Información para mantenimiento y mejora continua del Sistema de Seguridad de la Información a nivel Estratégico, Táctico y Operativo. Estos planes corresponden a programas o proyectos que basado en la situación actual evidenciada en el

Diagnostico de Seguridad o en el resultado de las pruebas de seguridad se determinan las brechas y debilidades de seguridad, y a partir de estas se determina las necesidades para la debida y oportuna protección de la información, definiendo también las prioridades y así poder plasmarlas en un plan que permita cerrar la brecha de seguridad identificada.

- **Procesos:** En este caso para el SSI de la UBPD, se establece el Proceso de Gestión de Seguridad de la Información, el cual inicia con la identificación de necesidades de información, definición de la planeación estratégica, ejecución de planes, programas y proyectos a nivel de seguridad de la información, continúa con la verificación de los controles implementados a través de las pruebas de seguridad digital, auditorías, indicadores y planes de tratamiento de riesgos de seguridad, y termina con la identificación de oportunidades de mejora e implementación de acciones para contribuir a la mejora continua del Sistema de Seguridad de la Información.

- **Matrices:** Son instrumentos que permiten estructurar información relevante para el Sistema de Seguridad de la Información, los cuales normalmente hacen parte de los anexos que acompañan un procedimiento, guía o metodología, como parte del diseño y desarrollo del SSI se definieron la Matriz de Activos de Información y la Matriz de Riesgos de Seguridad de la Información.

- **Guías, Procedimientos:** Dependiendo del nivel de detalle y de la explicación de la ejecución de las actividades a documentar, se puede hacer uso de uno de estos tipos de documentos, los cuales se detallan más adelante dentro de este mismo capítulo como parte del SSI, algunos de estos procedimientos asociados a temas de seguridad tienen relacionadas guías que detallan más aspectos del procedimiento.

- **Formatos:** Son los documentos de menor nivel, que son anexos para diligenciar información o para registro de evidencia de solicitudes, ente otros. (Ej.: Formato de Solicitud de Asignación de Permisos), estos formatos normalmente hacen parte de los anexos que acompañan los procedimientos, guías o metodologías.

- **Estándares:** Son indicaciones técnicas de bajo nivel emitidas por los fabricantes para blindar la plataforma tecnológica, estos estándares establecen configuraciones seguras para no exponer los equipos o las aplicaciones a las amenazas permanentes del entorno tecnológico.

- **Confidencialidad:** significa que toda la información que reciba o produzca la UBPD no será entregada a persona alguna, ni autoridad judicial o de otra naturaleza, con excepción de los informes técnicos forenses. Este principio resulta indispensable para generar confianza y lograr que quien decida

suministrar información, que contribuya al proceso de búsqueda de las personas dadas por desaparecidas, lo haga sin temor.

- **Integridad:** Atributo que busca garantizar que la información sea completa, exacta y veraz, para que solo las personas autorizadas puedan modificar la información de la Entidad.

- **Disponibilidad:** Atributo que busca garantizar que la información y los servicios tecnológicos estén disponibles en el momento en que se requiera, por quienes estén autorizados.

- **Autenticación:** Permite validar la identificación de los servidores y contratistas que acceden a los diferentes servicios tecnológicos a fin de evitar suplantación de identidades.

- **Autorización:** Luego de la autenticación se lleva a cabo la autorización, la cual permite personalizar y de manera granular asignar los permisos y accesos a la información y a los servicios de acuerdo con los roles asignados.

- **No repudio:** Mecanismo para garantizar la confirmación de que quien genera la información o una comunicación, es quien dice ser, un ejemplo de un mecanismo que garantiza el no repudio es la firma digital.

- **Trazabilidad:** Mecanismos que permiten identificar las acciones realizadas por los servidores y contratistas, estos mecanismos deben a su vez garantizar la integridad de la información que demuestren las acciones de cada uno de estos actores.

Es necesario precisar, que todos los principios de seguridad se deben garantizar de manera transversal en todo el Sistema de Seguridad de la información; se considera la Confidencialidad de la Información como el de más relevancia sobre el de Integridad y Disponibilidad, sin que los demás dejen de ser importantes, dado que la información que se gestiona y que es obtenida en su mayoría de otras fuentes de información o es recolectada por la Entidad es reservada o confidencial y es el principal insumo para la planeación y ejecución de sus actividades.

Teniendo en cuenta todo lo anterior, a continuación, se detallan los componentes que hacen parte del diseño del Sistema de Seguridad de la Información:

- **Proceso de Gestión de Seguridad de la Información:** Este proceso es el documento que permite definir de manera general cómo se gestiona la seguridad de la información en la UBPD, el proceso inicia con la identificación de necesidades de información, definición de la planeación estratégica,

ejecución de planes, programas y proyectos a nivel de seguridad de la información, continúa con la verificación de los controles implementados a través de las pruebas de seguridad digital, auditorías, indicadores y planes de tratamiento de riesgos de seguridad, y termina con la identificación de oportunidades de mejora e implementación de acciones para contribuir a la mejora continua del Sistema de Seguridad de la Información, el cual se puede ver de manera específica en el Anexo **"GSI-CR-001 Caracterización Gestión de Seguridad de la Información"**.

- **Política General y Políticas de seguridad de la información y Políticas de seguridad digital:** Se define la Política General de Seguridad de la Información para el SSI, así mismo, se establecen los lineamientos de alto nivel que rigen todo lo relacionado con la seguridad en la UBPD, a través de las Políticas de seguridad de la Información y las Políticas de Seguridad Digital, las cuales se listan a continuación y se puede ver de manera específica en el ítem **"7. POLÍTICA GENERAL, POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y POLÍTICAS DE SEGURIDAD DIGITAL"** del presente documento, así:

En las Políticas de Seguridad de la Información se puede identificar la:

- Seguridad de las instalaciones
- Disponibilidad de la información
- Confidencialidad
- Privacidad
- Gestión de activos
- Gestión de incidentes de Seguridad de la Información
- Evaluación de Desempeño
- Escritorio limpio
- Relación con proveedores
- Organización en Seguridad de la Información
- Gestión de Riesgo
- Cultura de Seguridad de la Información

En las Políticas de Seguridad Digital se pude identificar:

- Control de acceso lógico
- Uso de credenciales de acceso
- Transferencia o intercambio de información
- Conexión remota segura
- Uso de controles criptográficos y gestión de llaves criptográficas
- Desarrollo seguro

- Dispositivos móviles
- Respaldo de la información
- Uso aceptable de activos digitales
- Servicios en la nube
- Disponibilidad de los servicios tecnológicos
- Seguridad de las comunicaciones
- Pantalla limpia
- No repudio

- **Procedimientos de Seguridad:** A través de los procedimientos de seguridad y en algunos casos a través de guías y formatos se permitirá materializar la aplicabilidad y control de las políticas de seguridad, para lo cual se diseñaron los siguientes procedimientos, los cuales se detallan en los correspondientes anexos, así:

    - Procedimiento de Seguimiento al Sistema de Seguridad de la Información GSI-PR-001
    - Procedimiento de Trabajo en Áreas Seguras GSI-PR-002
    - Procedimiento de Gestión de Incidentes de Seguridad de la Información GSI-PR-003
    - Procedimiento de Gestión de Activos de Información GSI-PR-004
    - Procedimiento de Etiquetado de Información GSI-PR-005
    - Procedimiento de Gestión de Eventos e Incidentes de Seguridad Digital GTI-PR-007
    - Procedimiento de Gestión de Cambios
    - Procedimiento de Instalación de Software
    - Procedimiento de Gestión de Acceso
    - Procedimiento de Conexión Remota Segura
    - Procedimiento de Gestión de Mecanismos Criptográficos

- **Roles y Responsabilidades de Seguridad:** Se diseñan los roles y responsabilidades de Seguridad teniendo en cuenta la estructura organizacional de la UBPD, a través de los cuales la Entidad gestionará desde diferentes niveles organizacionales la seguridad, los cuales se listan a continuación y se detallan en el ítem **"8. MATRIZ RACI DE ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN"** del presente documento, así:

    - Director (a) General
    - Secretario (a) General
    - Comité de Seguridad de la Información
    - Oficial de Seguridad de la Información

- Oficiales de Seguridad de la Información Operativos
- Subdirector (a) de Gestión Humana
- Subdirección Administrativa y Financiera
- Subdirector (a) General Técnica y Territorial
- Director (a) Técnico de Información, Planeación y Localización para la Búsqueda
- Subdirector (a) de Gestión de Información para la Búsqueda
- Jefe (a) de la Oficina de Tecnologías de la Información y las Comunicaciones
- Coordinador (a) de la Territorial
- Asesor (a) de Prevención y Protección
- Líder (esa) y Arquitecto de Seguridad Digital
- Administrador (a) en Seguridad Digital
- Administrador (a) de la Base de Datos DBA
- Jefe (a) de la Oficina Asesora Jurídica
- Jefe (a) de la Oficina Asesora de Comunicaciones y Pedagogía
- Jefe (a) de la Oficina de Control Interno
- Jefe (a) de la Oficina Asesora de Planeación
- Coordinador (a) de Mesa de Servicio (nivel central o territorial)
- Agente de soporte en Sitio
- Analista de Mesa de Servicio
- Coordinador (a) Gestión Global
- Gestor de Redes y Monitoreo (Coordinador del NOC)
- Analista de Aseguramiento
- Analista de Red
- Analista de Infraestructura
- Administrador (a) de Infraestructura (Experto 4, y Analista 2)
- Supervisores (as) de Contrato
- Usuarios (as)

- **Indicadores de Seguridad:** Se diseñan los indicadores de Seguridad con el fin de poder medir e ir mejorando los diferentes aspectos de seguridad, los cuales se listan a continuación y se detallan en el ítem **"9. INDICADORES DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN"**, del presente documento, así:

  - Sensibilización en Seguridad de la Información y Seguridad Digital
  - Cierre de Brechas Pruebas de Vulnerabilidades de Seguridad
  - Mantenimiento de Infraestructura Tecnológica

- Pruebas de Ingeniería Social
- Incidentes de Seguridad atendidos oportunamente
- Riesgos de Seguridad con Planes de Tratamiento ejecutados
- Pruebas de Restauración de Backups exitosas
- Conocimiento Políticas de Seguridad de la Información y Seguridad Digital
- Equipos con Antivirus Instalado y Actualizado
- Cambios en Plataforma Tecnológica con Análisis de Seguridad
- Áreas Seguras monitoreadas y con controles de acceso físico
- Sistemas de Información Seguros
- Permisos en Sistemas de Información

7. POLÍTICA GENERAL, POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y POLÍTICAS DE SEGURIDAD DIGITAL

La Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado - UBPD, tiene la responsabilidad de generar una Política General para el Sistema de Seguridad de la Información SSI de la Entidad, y las Políticas de seguridad de la información y las Políticas de Seguridad Digital, que respondan a temas técnicos y administrativos propios de las entidades públicas, y a su vez protocolos de protección de información, para cumplir a cabalidad con su mandato y salvaguardar su carácter humanitario y extrajudicial. Frente a los temas objeto del desarrollo misional, la UBPD se rige por las necesidades en el manejo de la información contenidas en el Acto Legislativo 1 de 2017, el Acuerdo de Paz, el Decreto Ley 589 de 2017 y los decretos reglamentarios que lo desarrollan.

Con el fin de garantizar la efectividad del trabajo humanitario y extrajudicial de búsqueda, toda la información que reciba, recaude o produzca, en el desarrollo de sus actividades misionales de búsqueda, es de carácter confidencial, por lo tanto, con el fin de garantizar lo anterior, se establecen las siguientes Políticas de Seguridad de la Información, las cuales aplican para todos los activos de información y específicamente para los de tipo información sin importar el formato (digital, electrónico y físico) y el lugar donde se encuentre.

Las Políticas de Seguridad de la Información y las Políticas de Seguridad Digital establecen las pautas que debe seguir cualquier “servidor, contratista o personal delegado”[9] de la UBPD cuando genere, acceda, almacene, transporte o intercambie información que contribuya a la implementación de acciones humanitarias para la búsqueda, esta información, contenida en documentos, independientemente de su soporte , puede

[9] En lo posible utilizar la expresión “formato físico o electrónico” Así el formato físico hace referencia al soporte papel y el formato electrónico o formato no tradicional se refiere a los documentos especiales en formato electrónico: audios, vídeos, correos electrónicos, bases de datos, contenidos en redes sociales, entre otros.

referirse tanto a personas, hechos, lugares, como a contextos de regiones, actores o periodos que permitan la caracterización del conflicto armado y las modalidades, prácticas y tipologías de desaparición. También, incluye pautas para el registro de datos que contribuyan a la búsqueda de personas dadas por desaparecidas que sean puestos en conocimiento de la UBPD por medio de distintos canales como derechos de petición, llamadas telefónicas, redes sociales, contactos directos o espacios de socialización.

La UBPD comprometida con el tratamiento seguro de la información adopta los mecanismos tecnológicos necesarios que le permitan prevenir, identificar, controlar y mitigar los riesgos asociados a los sistemas de información, infraestructura, comunicaciones o servicios digitales.

El uso de los componentes digitales por parte de los servidores, contratistas y personal delegado de la UBPD como herramientas para la ejecución de sus funciones y facilitador de la comunicación interna y externa, pone a la Entidad en un ámbito donde hay exposición a diferentes riesgos que afectan la integridad, confidencialidad y disponibilidad de la información, es por esto por lo que la UBPD también establece lineamientos de Seguridad Digital.

Las Políticas de Seguridad de la Información y las Políticas de Seguridad Digital aplicarán a los activos de información de la UBPD, a nivel central y en sus equipos territoriales en todos los procesos misionales, estratégicos, apoyo y de evaluación y control. Los lineamientos descritos en cada política deben ser cumplidos por parte de los servidores, contratistas y personal delegado de la Entidad.

7.1 POLÍTICA GENERAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

La UBPD reconoce la importancia de identificar y proteger sus activos de información, garantizando su confidencialidad, integridad y disponibilidad, desde un enfoque de seguridad de la información y seguridad digital, ya que a partir de la necesidad de proteger la información sin importar el formato en el que se encuentre se definen las políticas de seguridad de la información y teniendo en cuenta que la mayor parte de la información se encuentra en formato digital y que esta soportada, almacenada, procesada y transportada a través de las plataformas tecnológicas, se definen las políticas de seguridad digital, comprometiéndose a establecer, implementar, mantener y mejorar continuamente el Sistema de Seguridad de la Información – SSI.

7.2 OBJETIVOS

7.2.1 Objetivo General

Definir y establecer los lineamientos en seguridad de la información y seguridad digital, que permitan garantizar la confidencialidad, integridad y disponibilidad de la información, conservando, salvaguardando y protegiendo la información producida y recibida en los procesos de la Entidad.

7.2.2 Objetivos Específicos

- Servir de apoyo a la Entidad frente al cumplimiento de la visión y misión de esta.
- Documentar los lineamientos que permitan dar una directriz sobre los controles de seguridad a implementar en la Entidad con el fin de proteger los activos de información.
- Definir las acciones necesarias para antes, durante y después de la implementación de las políticas de seguridad de la información y seguridad digital.
- Fortalecer la cultura en seguridad de la información, por parte de los servidores, contratistas y personal delegado de la Entidad.
- Generar las bases para definir procedimientos, guías, indicadores, y en general toda la documentación necesaria para el establecimiento del Sistema de Seguridad de la Información.

7.3 APLICABILIDAD Y VIGENCIA

Las políticas de seguridad de la información y de seguridad digital entran en vigencia a partir del momento en que es firmada y aprobada por parte del (la) directora (a) General de la UBPD y su posterior publicación. Los lineamientos que se encuentran definidos en cada política son de obligatorio cumplimiento por parte de los servidores (ras), contratistas y personal delegado de la UBPD.

7.4 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Como parte fundamental del Sistema de Seguridad de la Información, se definieron una serie de lineamientos que con su implementación le permiten a la Entidad garantizar unos óptimos niveles frente a la confidencialidad, integridad y disponibilidad de la información. Estos lineamientos específicos están detallados en el plan de trabajo para la implementación del Sistema de Seguridad de la Información.

7.5 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DIGITAL

El creciente uso del entorno digital para desarrollar actividades propias de la Entidad, generan incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados continuamente. El no hacerlo, puede llevar a la materialización de los riesgos asociados a ataques cibernéticos.

Por lo anterior, las políticas de seguridad digital de la UBPD definen los lineamientos y mecanismos para garantizar la confidencialidad, integridad y disponibilidad para los activos digitales. Estos lineamientos específicos están detallados en el plan de trabajo Seguridad Digital.

7.6 METODOLOGÍA PARA ACTUALIZACIÓN DE LAS POLÍTICAS

Con el fin de tener las herramientas necesarias para garantizar el mantenimiento de las políticas de seguridad de la información y de seguridad digital, se define la siguiente metodología que detalla las fases relacionadas con la revisión, ajustes, aprobación y socialización de las políticas en la Entidad.

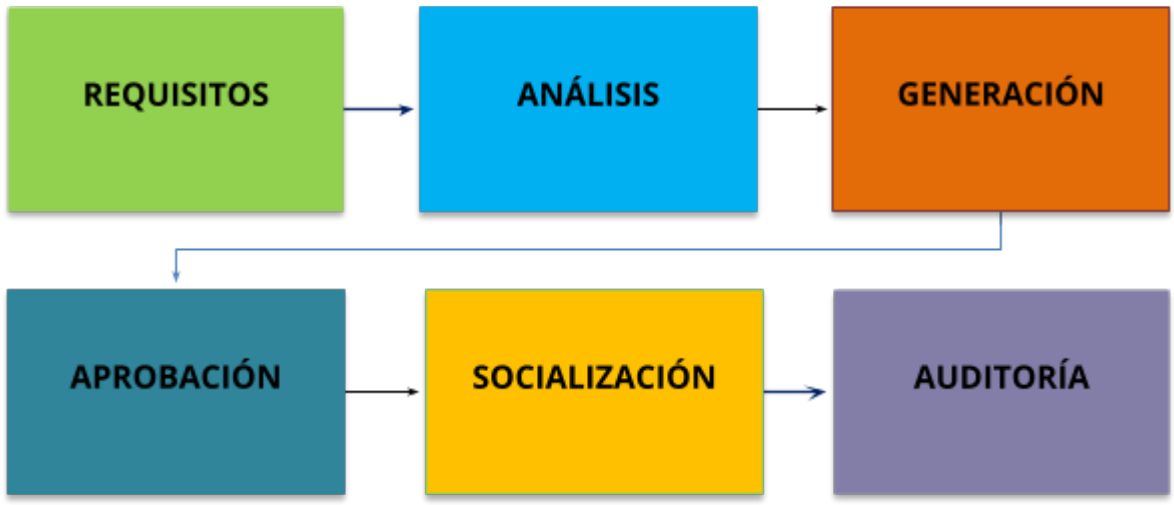


Ilustración 6 Fases Metodología para actualización de las políticas Fuente: Elaboración UT MYQ-ALINA TECH

7.7 REQUISITOS

Las políticas de seguridad de la información y de seguridad digital deben ser revisadas detalladamente cada año por el Oficial de Seguridad de la Información y experto técnico de la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, quienes llevarán al Comité de Seguridad de la Información las actualizaciones para ponerlas a consideración, y posteriormente ser aprobadas por la Directora General, o antes en el caso de que se lleguen a presentar nuevos requisitos o requerimientos internos o externos que ameriten la necesidad de revisión de las políticas. Esta revisión puede conllevar a la creación, modificación, o eliminación de alguna(s) política(s) de seguridad.

De acuerdo con lo mencionado anteriormente, los casos que ameritan la revisión y si es necesario el ajuste de las políticas son los siguientes:

- Cambios en la estructura organizacional de la Entidad.
- Cambios en el mapa de procesos de la Entidad.
- Surgimiento de normatividad institucional o nacional que esté relacionada con el propósito de la Entidad o con seguridad de la información y seguridad digital aplicable a la UBPD.
- Identificación de riesgos de seguridad que estén relacionados con los lineamientos establecidos en la Entidad.
- Avances tecnológicos que afecten a la Entidad.

7.8 ANÁLISIS

Se deberá realizar el análisis del(los) factor(es) que impulsan la revisión de las políticas, y dependiendo del factor, consultar con el (las) área(s) de la Entidad que correspondan, para realizar con el apoyo del Oficial de Seguridad de la Información, el análisis de riesgos de seguridad de la información y seguridad digital donde se identifique el impacto y la prioridad en la atención al nuevo requerimiento.

Si el nuevo requerimiento surge por un cambio de normatividad, se debe realizar la revisión con la Oficina Asesora Jurídica - OAJ para determinar la aplicabilidad de esta norma, ley, decreto, circular, resolución, o cualquier otra que deba ser validada por esta oficina, identificando la obligatoriedad, beneficios y riesgos de la implementación o por el contrario su omisión.

Dentro de este análisis es importante revisar los eventos e incidentes de seguridad, indicadores de seguridad, auditorías y pruebas de seguridad, con el fin de determinar la necesidad de ajustar las políticas de seguridad,

y que respondan a las necesidades del Sistema de Seguridad de la Información, generando una mejora y madurez continua de este.

7.9 GENERACIÓN

Se deberá realizar el análisis del(los) factor(es) que impulsan la revisión de las políticas, y dependiendo del factor, consultar con el (las) área(s) de la Entidad que correspondan, para realizar con el apoyo del Oficial de Seguridad de la Información, el análisis de riesgos de seguridad de la información y seguridad digital donde se identifique el impacto y la prioridad en la atención al nuevo requerimiento.

Si el nuevo requerimiento surge por un cambio de normatividad, se debe realizar la revisión con la Oficina Asesora Jurídica - OAJ para determinar la aplicabilidad de esta norma, ley, decreto, circular, resolución, o cualquier otra que deba ser validada por esta oficina, identificando la obligatoriedad, beneficios y riesgos de la implementación o por el contrario su omisión.

Dentro de este análisis es importante revisar los eventos e incidentes de seguridad, indicadores de seguridad, auditorías y pruebas de seguridad, con el fin de determinar la necesidad de ajustar las políticas de seguridad, y que respondan a las necesidades del Sistema de Seguridad de la Información, generando una mejora y madurez continua de este.

7.10 APROBACIÓN

Posterior a que se documente la nueva versión de las políticas, el Oficial de Seguridad de la Información deberá presentar el documento de las Políticas de Seguridad de la Información, y el experto técnico de la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC Digital el documento de las Políticas de Seguridad Digital, al Comité de Seguridad de la Información para socializarlo (s) y realizar las aclaraciones correspondientes. Si el Comité solicita algún ajuste, el Oficial de Seguridad de la Información, y el Líder y Arquitecto de Seguridad Digital procederán a realizarlo y presentarlo en el siguiente Comité, si la nueva política se requiere aprobar de manera prioritaria, se deberá convocar un Comité extraordinario para revisión y análisis del (los) documento (s) y la correspondiente aprobación y firma por parte del (la) Director (a) General de la UBPD.

7.11 SOCIALIZACIÓN

Con el fin de fomentar la cultura en seguridad y para que todos los servidores, contratistas y personal delegado tengan conocimiento de los lineamientos aprobados frente a la seguridad de la información y seguridad digital, se deben diseñar e implementar estrategias como campañas de sensibilización, talleres,

capacitaciones, material POP (Point Of Purchase- siglas en inglés) Punto de compra, entre otras, las cuales servirán para que todo el personal conozca en detalle los lineamientos y así mismo se comprometan con dar cumplimiento de ellos. Las estrategias de comunicación deben ser acordadas y desarrolladas entre el Oficial de Seguridad de la Información, la Oficina Asesora de Comunicaciones y Pedagogía, y la Subdirección de Gestión Humana, es de anotar, que estas sensibilización o concientización de los temas de seguridad se deben realizar de manera permanente, y alineada con la estrategia de concientización.

7.12GENERACIÓN

Luego de su socialización y publicación se deben implementar las políticas teniendo en cuenta las acciones previas a la implementación establecidas en cada de las Políticas de seguridad de la información y las Políticas de seguridad Digital, con el fin de comenzar a contar con los registros correspondientes que evidencien su implementación y las oportunidades de mejora correspondientes.

7.13AUDITORÍA

Con el fin de validar la correcta implementación de los lineamientos de seguridad, se deben realizar auditorías sobre el cumplimiento de estos lineamientos. Estas auditorías deben ser lideradas por la Oficina de Control Interno y de los auditores capacitados en la norma ISO/IEC 27001:2013 con el acompañamiento del Oficial de Seguridad de la Información.

Posterior a las auditorías, la Oficina de Control Interno deberá socializar los resultados ante el Comité de Seguridad de la Información y los representantes de las áreas auditadas, sobre las oportunidades de mejora que surjan se deben establecer planes de acción, con responsables y fechas, sobre los cuales la Oficina de Control Interno deberá hacer el respectivo seguimiento y periódicamente informar al Oficial de Seguridad de la Información los correspondientes avances.

7.14RECOMENDACIONES

- Socializar a todos los servidores, contratistas y personal delegado, las políticas de seguridad de la información y seguridad digital, con el fin de que sean conocidas, entendidas y se comprometan formalmente con su cumplimiento. Para esta actividad se recomienda ejecutar campañas de socialización, no solamente a nivel formal, sino utilizando esquemas como los planteados en el P57 – Ejecución de actividades de Gestión del cambio, que incluye la generación de piezas gráficas, reuniones y espacios a partir de los cuales se pueda brindar esa información.

- Sensibilizar a los servidores, contratistas y personal delegado, sobre la importancia y necesidad del cumplimiento de los lineamientos de las Políticas de Seguridad de la Información y Seguridad Digital. Para esta actividad se recomienda ejecutar campañas de sensibilización, que pueden realizarse tomando como referencia las campañas diseñadas en el marco del proyecto en el P57 – Ejecución de actividades de Gestión del cambio, y que apoyan de manera importante la apropiación de los conceptos por parte de los integrantes de la UBPD.
- Destinar los medios, logística y recursos necesarios para la correcta implementación de las Políticas de Seguridad de la Información y Seguridad Digital.
- Aplicar la Metodología para Actualización de las políticas de seguridad de la información y seguridad digital, por lo menos una vez al año.

8. MATRIZ RACI DE ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una gestión completa de los diferentes componentes del Sistema de Seguridad de la Información, se debe definir una estructura organizacional relacionada con Seguridad de la Información y Seguridad Digital, es por esto por lo que a continuación, se describen los roles propuestos y sus respectivas responsabilidades. Es de anotar, que no necesariamente corresponde a los cargos establecidos en la Entidad, por lo que un servidor puede asumir responsabilidades de más de uno de estos roles, dependiendo de los recursos con los que cuente la UBPD, es de anotar, que con relación al Gobierno de TI se definieron roles como Jefe de la OTIC, Experto Técnico designado como Líder y Arquitecto de Seguridad Digital, y el Administrador de Seguridad Digital, para los cuales se especifican las responsabilidades de seguridad digital más adelante.

Para el desarrollo de esta propuesta se tuvo en cuenta el Decreto No. 1393 de 2018 “Por el cual se establece la estructura interna de la UBPD y se determinan las funciones de sus dependencias” y el Decreto Ley No. 589 de 2017 “Por el cual se organiza la UBPD”, así mismo, se tuvo presente la Resolución N° 588 del 8 de junio de 2020.

Un grupo que tiene una especial importancia, dentro de la organización de la seguridad de la Información y Seguridad Digital, es el Grupo GRIES (Grupo de Respuesta a Incidentes y Eventos de Seguridad de la Información y Seguridad Digital), el cual ofrece un enfoque estructurado y planificado para la gestión de los incidentes de seguridad de la información y seguridad digital, su objetivo principal es evitar o contener el impacto de los incidentes para reducir los costos directos e indirectos que puedan causar la materialización de algún incidente de seguridad, la descripción de su operación se encuentra detallada dentro del Manual del Equipo GRIES.

A continuación, se relacionan cada uno de los roles con las responsabilidades en seguridad de la información y/o seguridad digital, los cuales se mapean en el "Anexo - Matriz de Roles y Responsabilidades RACI", en la cual para cada una de las responsabilidades se asigna el rol responsable teniendo en cuenta la siguiente tabla de Tipos de Responsabilidades.

TIPOS DE RESPONSABILIDADES	
R	Responsabile (Responsable): Es quien realiza el trabajo para lograr la tarea o actividad. Normalmente hay un único rol con la designación de un tipo de participación de responsable, aunque se pueden delegar otros para ayudar en el trabajo requerido, sin embargo, se recomienda en lo posible dejar un solo Responsable y así evitar que la responsabilidad se diluya.
A	Accountable (Aprobador): Es la autoridad o cargo de aprobación final. Este es el responsable en última instancia de la finalización correcta y exhaustiva de la entrega, tarea o actividad En otras palabras, un aprobador debe firmar (aprobar) el trabajo que proporciona el Responsable. Debe haber un solo aprobador especificado para cada tarea o responsabilidad.
C	Consulted (Consultado): Aquellos cuyas opiniones o información que pueda entregar se buscan para aportar al desarrollo de la tarea o actividad; y con quien hay comunicación bidireccional. Puede haber varios Consultados por cada tarea, actividad o responsabilidad.
I	Informed (Informado): Aquellos que se mantienen actualizados sobre el progreso, a menudo solo al completar la tarea, actividad o responsabilidad; y con quien solo hay comunicación unidireccional. Puede haber varios informados por cada tarea, actividad o responsabilidad.

Tabla 1 Tipos de responsabilidades Fuente: UT MYQ- ALINA TECH

8.1 DIRECTOR (RA) GENERAL

Dirige, administra y coordina la formulación de planes, programas, proyectos y protocolos para la búsqueda de las personas dadas por desaparecidas en el contexto y en razón del conflicto armado, entre otras. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Aprobar los principios rectores, estrategias, lineamientos y orientaciones del Sistema de Seguridad de la Información.
- Aprobar las políticas, directivas, circulares, instrucciones, planes y protocolos de seguridad de la información.
- Convocar, cuando lo estime necesario, y presidir el Comité de Seguridad de la Información.

8.2 SECRETARIA GENERAL

Coordina las acciones necesarias para el cumplimiento de las políticas, normas y las disposiciones que regulen los procedimientos y trámites de carácter administrativo, financiero, gestión documental, notificaciones, de talento humano y contratación pública de la UBPD, entre otras. Respecto a seguridad de la información, se encuentra, además, la siguiente responsabilidad:

- Adelantar los procesos disciplinarios contra los servidores de la Entidad, para emprender acciones legales que surjan a partir de una violación a las políticas de seguridad de la información y seguridad digital.
- Garantizar que estén formalizados los acuerdos de confidencialidad con cada uno de los contratistas de la Entidad.

8.3 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN RESOLUCIÓN 537 DE 2020

El Comité de Seguridad de la Información tiene como objetivo establecer, evaluar y realizar seguimiento a las necesidades, lineamientos, directrices, protocolos, políticas, entre otros, a alto nivel en materia de seguridad de la información y seguridad digital, apoyados en el Sistema de Seguridad de la Información de la Entidad, con el fin de mantenerlo y mejorarlo continuamente.

Con el propósito de dar las pautas necesarias para que la información gestionada por la UBPD en ejercicio de sus funciones cumpla con los criterios de reserva y confidencialidad, el Comité de Seguridad de la Información de la UBPD, tendrá dentro de sus funciones:

- Asesorar a la Dirección General en la toma de decisiones y acciones a emprender que contribuyan a la confidencialidad, reserva legal, seguridad, protección e integridad de la información de la UBPD.
- Generar estrategias para que los servidores, contratistas y personal delegado de la Entidad, se enfoquen en 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.
- Generar, revisar, asesorar y proponer la creación, modificación o eliminación de objetivos, indicadores, directrices, protocolos, modelos y políticas, entre otros, de seguridad de la información y seguridad digital a nivel institucional para aprobación de la (el) Directora (r) General que permitan asegurar y proteger adecuadamente los activos de información de la UBPD, garantizando el cumplimiento de los principios establecidos en la Política de Seguridad de la Información y en la Política de Seguridad Digital.

- Estudiar el estado general de la seguridad de la información y seguridad digital de la UBPD en cumplimiento de su objeto misional, suministrada por los responsables de seguridad de la información y seguridad digital en cada área o dependencia, los cuales deberán entregar periódicamente (cada tres (3) meses) un informe, con el fin de identificar debilidades y buenas prácticas que permitan generar actividades de mejora y de esta manera fortalecer el Sistema de Seguridad de la Información.
- Revisar, analizar y recomendar las acciones que considere adecuadas frente a los incidentes de seguridad de la información y seguridad digital que llegaren a presentarse en el manejo de la información que no sean competencia de otras dependencias o autoridades.
- Revisar y asesorar a la Dirección General en la definición de los roles y responsabilidades del Sistema de Seguridad de la Información.
- Evaluar los cambios externos o internos que puedan afectar al Sistema de Seguridad de la Información, con el fin de emitir las recomendaciones o indicaciones correspondientes.
- Realizar seguimiento de las no conformidades, acciones correctivas y planes de tratamiento de riesgos asociados al Sistema de Seguridad de la Información.
- Apoyar e Impulsar el desarrollo de proyectos, planes y actividades relacionados con Seguridad de la Información y Seguridad Digital.
- Realizar seguimiento del resultado de los indicadores que se definan para monitorear y mejorar la gestión del Sistema de Seguridad de la Información, con el fin de emitir recomendaciones o lineamientos para mejorarlo de manera continua.
- Las demás funciones inherentes a la naturaleza del Comité.

Conformación: El Comité de Seguridad de la Información de la UBPD está integrado por:

- La (el) Directora (r) General, quien lo presidirá.
- La (el) Secretaria (o) General.
- La (el) Subdirectora (r) General Técnico (a) y Territorial, quien presidirá el Comité en ausencia de la (el) Directora (r) General.
- La (el) Jefe (a) Oficina de Tecnologías de la Información y las Comunicaciones.
- La (el) Jefe (a) de la Oficina Asesora Jurídica.
- El (la) Director (a) Técnico (a) de Información, Planeación y Localización para la Búsqueda.
- El (la) Subdirector (a) de Gestión de la Información para la Búsqueda.
- El (la) Oficial de Seguridad de la Información.
- La (el) Jefe (a) Oficina de Control Interno.

8.4 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Responsable del diseño, desarrollo, implementación, mantenimiento y verificación del correcto funcionamiento del Sistema de Seguridad de la Información. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Coordinar las actividades de seguridad de la información.
- Revisar los aspectos relacionados con la seguridad de la información en los proyectos de políticas, directivas, circulares, instrucciones, planes y protocolos relativos a la gestión documental, archivos, u otras materias.
- Mantener informada, de forma regular y periódica, a él (la) Director (a) General, sobre los aspectos más relevantes relacionados con seguridad de la información.
- Informar de inmediato a él (la) Director (a) General sobre cualquier incidente de impacto alto o situación que afecte la seguridad de la información.
- Informar de inmediato a él (la) Director (a) General, la Secretaria General y a los responsables del Nivel Operativo, sobre los temas concernientes a violaciones de políticas, directivas, circulares, instrucciones, planes y protocolos de seguridad de la información por parte de servidores, contratistas y personal delegado de la UBPD.
- Promover y supervisar la implementación de las políticas, directivas, circulares, instrucciones, planes y protocolos relacionados con seguridad de la información, por parte de los servidores, contratistas y personal delegado de la UBPD.
- Dirigir, coordinar o supervisar a alto nivel (según el caso) las medidas y respuestas frente a ataques, y escenarios de riesgos de seguridad de la información.
- Liderar y coordinar en conjunto con la Subdirección de Gestión Humana y con los Oficiales de Seguridad de la Información Operativos, las actividades de capacitación y sensibilización en materia de seguridad de la información, dirigidas a los miembros de la UBPD.
- Apoyo en la definición y gestión de los indicadores de seguridad de la información y seguridad digital en la Entidad.
- Gestionar recursos ante la alta dirección para los programas de capacitación y formación en temas de Seguridad de la Información.
- Presentar ante el Comité de Seguridad de la Información las actualizaciones realizadas a las Políticas de Seguridad de la Información.
- Generar informes y comunicarlos a él (la) Director (a) General en cuanto al cumplimiento de las políticas de seguridad de la información.

8.5 OFICIALES DE SEGURIDAD DE LA INFORMACIÓN OPERATIVOS

Responsables del apoyo operativo en cada una de las áreas de la Entidad, respecto a la implementación, mantenimiento y verificación del correcto funcionamiento del Sistema de Seguridad de la Información. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Apoyar en la implementación de las políticas, directivas, circulares, instrucciones, planes y protocolos de seguridad de la información en su respectiva dependencia de la UBPD, y además supervisar el respectivo cumplimiento.
- Apoyar en la identificación, clasificación y valoración de los activos de información relacionados en los procesos de cada una de sus dependencias.
- Apoyar en la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información y seguridad digital relacionados en los procesos de cada una de sus dependencias.
- Informar de inmediato a Control Interno Disciplinario y al Oficial de Seguridad de la Información, sobre:
    - cualquier incidente de seguridad o situación que afecte la seguridad de la información.
    - violaciones en las políticas, directrices, circulares, instrucciones, planes y protocolos de seguridad de la información por parte de servidores públicos, contratistas o personal delegado de la UBPD de su respectiva dependencia.
- Coordinar o implementar, según el caso y bajo las instrucciones del Oficial de Seguridad de la Información, las acciones, medidas o planes de continuidad del negocio para la seguridad de la información.
- Garantizar que al interior de las dependencias se cumpla y participen de manera activa en la implementación del Plan de Recuperación de Desastres.

8.6 SUBDIRECTOR (A) DE GESTIÓN HUMANA

Responsable de la estrategia en gestión humana para la prevención, el autocuidado y el apoyo a los servidores, facilitando los mecanismos necesarios para la creación de una cultura organizacional. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Apoyar a el (la) Oficial de Seguridad de la Información y a la Oficina de Comunicaciones y Pedagogía, en el diseño, desarrollo e implementación del Programa de Capacitación y Sensibilización en Seguridad de la Información.
- Incluir en los procesos de inducción dirigidos a servidores, contratistas y personal delegado, los diferentes lineamientos en seguridad de la información y seguridad digital.

- Reportar de manera oportuna a la Oficina de Tecnologías de la Información y las Comunicaciones las novedades de personal, tales como ingreso, retiro, renuncia, licencias y cambio de áreas y cargos de los servidores de la Entidad.
- Incluir en el manual de funciones, las responsabilidades de seguridad de la información para los distintos cargos en la Entidad.
- Garantizar que estén formalizados los acuerdos de confidencialidad con cada uno de los servidores y servidoras públicas de la Entidad.
- Gestionar los recursos que se requieran para el desarrollo de planes de capacitación y sensibilización en Seguridad de la Información y Seguridad Digital.

8.7 SUBDIRECTOR (A) GENERAL TÉCNICO (A) Y TERRITORIAL

Coordina, articula y hace el seguimiento a las direcciones técnicas y a los equipos territoriales de la UBPD; dirige la implementación del Plan Nacional y los planes Regionales de búsqueda bajo las directrices de la Dirección General, entre otras. Respecto a seguridad de la información, se encuentra, además, la siguiente responsabilidad:

- impartir lineamientos para que, en la gestión territorial a cargo de la UBPD, se apliquen los protocolos institucionales que aseguren la protección y confidencialidad de la información obtenida para la búsqueda, el contacto y protección de personas y organizaciones que aporten información para la búsqueda, en desarrollo del carácter extrajudicial de la UBPD[10].
- Hacer seguimiento a la observancia y advertir sobre los riesgos en materia de protección de la Información[11].
- Estar atento a los cambios del contexto interno y externo que puedan afectar los equipos territoriales, con el fin de participar en la definición de los controles de seguridad de la información, y apoyar la oportuna y correcta gestión de los riesgos que puedan afectar el entorno de la Territorial.

8.8 DIRECTOR (A) TÉCNICO DE INFORMACIÓN, PLANEACIÓN Y LOCALIZACIÓN PARA LA BÚSQUEDA

Coordina las acciones técnicas, investigativas, de gestión y análisis de la información requeridas para la planeación de la búsqueda y localización de las personas dadas por desaparecidas, así como la elaboración

[10] Tomado de Resolución 588 del 8 de junio de 2020 “Por medio de la cual se establece la estructura y roles del sistema de seguridad de la información (SSI) de la UBPD.”
[11] Ibídem

del plan nacional y los planes regionales de búsqueda, entre otras. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Elaborar los proyectos de protocolos, circulares e instructivos para garantizar la integridad, protección, confidencialidad y reserva de la información obtenida para la búsqueda, y el contacto y protección de personas y organizaciones que aporten información para la búsqueda.
- Coordinar concertadamente con el Oficial de Seguridad de la Información, las acciones, medidas o planes de contingencia para la seguridad de la información.

8.9 SUBDIRECTOR (A) DE GESTIÓN DE INFORMACIÓN PARA LA BÚSQUEDA

Recolecta, organiza, procesa y protege la información necesaria para establecer el universo de las personas dadas por desaparecidas en el contexto y en razón del conflicto armado, el registro nacional de lugares de disposición y para la planeación de la búsqueda, entre otras. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Implementar los lineamientos y directrices en materia de confidencialidad, reserva legal, seguridad, protección e integridad de la información.
- Implementar concertadamente con el (la) Oficial de Seguridad de la Información y la Dirección Técnica de Información, Planeación y Localización para la Búsqueda, las acciones, medidas o planes de contingencia para la seguridad de la información.

8.10 JEFE (a) DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Define, actualiza e implementa el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI); diseña e implementa los lineamientos y procesos de arquitectura tecnológica de la UBPD, entre otras. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Desarrollar estrategias para garantizar la seguridad digital de la UBPD.
- 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.
- Coordinar las actividades de seguridad digital.
- Revisar y diseñar los proyectos de políticas, directivas, circulares, instrucciones, planes y protocolos de seguridad digital de la UBPD, para aprobación por parte de la Dirección General.
- Mantener informados, de forma regular y periódica, a él (la) Director (a) General y a él (la) Oficial de Seguridad de la Información, sobre los aspectos más relevantes relacionados con la seguridad digital.

- Informar de inmediato a él (la) Director (a) General y a él (la) Oficial de Seguridad de la Información sobre cualquier incidente de impacto alto de seguridad o situación que afecte la seguridad digital y la operación de la Entidad.
- Liderar y coordinar en conjunto con la Subdirección de Gestión Humana las actividades de capacitación en materia de seguridad digital, dirigidas a los miembros de la UBPD.

8.11 COORDINADOR (A) DE LA SEDE TERRITORIAL

Coordina y lidera las actividades desarrolladas en la correspondiente sede Territorial, y en cuanto a sus responsabilidades asociadas a Seguridad de la Información, están:

- Garantizar niveles adecuados de acceso a la información que se gestiona en la Territorial, a través de la asignación granular de permisos de acuerdo con las funciones de los diferentes cargos establecidos en la territorial.
- Garantizar que la información de datos personales recolectada por la Territorial tiene adecuados y suficientes controles para proteger la información restringida o privada, y, además, cumplir con la normatividad vigente aplicable.
- Garantizar que se usen los mecanismos definidos por la Oficina de Tecnologías de la Información y las Comunicaciones, para transmitir o compartir información desde la Territorial, los cuales deben estar alineados con las políticas y demás lineamientos de seguridad digital y seguridad de la información.
- Reportar oportunamente las novedades (retiros, licencias, vacaciones) del personal (servidores, contratistas, o personal delegado) de la Territorial, a la Mesa de Servicio de la Oficina de Tecnologías de la Información y las Comunicaciones, para proceder con los ajustes a nivel de acceso que corresponda, de acuerdo con las políticas y demás lineamientos de seguridad digital y seguridad de la información.
- Velar por el cumplimiento de los lineamientos de seguridad de la información y de seguridad digital en el entorno de la Territorial.
- Monitorear que se estén cumpliendo los lineamientos de protección establecidos por el Asesor de Prevención y Protección para los (las) servidores (as), contratistas, y personal delegado, propendiendo por la vida e integridad de las personas que participan en el desarrollo de las actividades de la Territorial.
- Revisar y acordar con las Organizaciones y aportantes que se encuentran en la Territorial, los mecanismos de seguridad a través de los cuales se va a compartir o recibir la información que estas organizaciones o de aportantes de información que no hacen parte de estas Organizaciones puedan aportar, brindándole garantías sobre la protección de la información que la UBPD va a recibir.

- Recolectar y analizar información sobre el contexto de riesgo y amenazas en el territorio que sustenten la estrategia de prevención en la protección y seguridad de las tareas del equipo y la participación de las víctimas, sus familias, organizaciones y quienes ofrezcan información para la búsqueda[12].

8.12ASESOR (A) DE PREVENCIÓN Y PROTECCIÓN

Asesorar y emitir recomendaciones para la protección física de los tipos de activos de información, tales como: personas e instalaciones de la Entidad. Respecto a seguridad de la información, se encuentran las siguientes responsabilidades, entre otras:

- Definir los protocolos de seguridad para intervinientes, organizaciones, familiares, víctimas y demás personal que participan en la búsqueda de personas dadas por desaparecidas.
- Generar análisis de seguridad teniendo en cuenta el contexto de las zonas a las cuales se van a generar las comisiones, emitiendo las recomendaciones correspondientes.
- Emitir recomendaciones y asesorar a la Secretaria General y a la Subdirección Administrativa y Financiera en términos de seguridad física para contratar servicios de transporte, servicios de seguridad privada y de posibles sedes para la Entidad.
- Realizar el estudio de confiabilidad y emitir las recomendaciones de vinculación de servidores y contratistas.
- Verificación de experiencias laborales generales y específicas y validación de la consistencia de las certificaciones.
- Definir y emitir protocolos de seguridad para los servidores y contratistas que participan en las comisiones.
- Emitir conceptos de los posibles riesgos que pueden afectar a las comisiones.
- Realizar seguimiento de los comisionados, evaluar su participación y generar el reporte correspondiente.
- Definir las zonas o lugares en los cuales no es posible ingresar a desarrollar las actividades para la comisión.
- Definir los protocolos para protegerse contra las minas antipersona.
- Informar a él (la) Oficial de Seguridad de la Información, cualquier novedad desde el punto de vista de seguridad física, que se presente con los activos de información.

[12] Tomado de la Cartilla de los Equipos Territoriales

- Mantener estrecha comunicación con él (la) Oficial de seguridad de la información, para informar los incidentes presentados y relacionados con seguridad física que afecten los activos de información de la Entidad.

8.13LÍDER Y ARQUITECTO DE SEGURIDAD DIGITAL (experto técnico 4)

Diseña la arquitectura de seguridad digital en la Entidad, tiene el conocimiento técnico y de gestión para la implementación del componente de seguridad digital, además, las siguientes responsabilidades:

- Evaluar los riesgos en cuanto a la Seguridad digital en aplicativos, productos, sistemas operativos, herramientas y redes, y generar las recomendaciones correspondientes.
- Entender los requerimientos de Seguridad digital del negocio y especificarlos en términos de tecnología de información.
- Definir los eventos a ser auditados en materia de Seguridad digital, así como su monitoreo permanente para detectar anomalías o acciones no autorizadas y poder tomar acciones de manera oportuna.
- Generar los lineamientos de administración de los elementos de seguridad digital de la Entidad.
- Diseñar e implementar las políticas de seguridad digital de la UBPD.
- Realizar la evaluación y diagnóstico de la situación que podría impactar en las operaciones de la UBPD, con el fin de coordinar e implementar los planes de recuperación de desastres tecnológicos (DRP) de la Entidad.
- Dirigir, coordinar o supervisar (según el caso) las medidas y respuestas frente a ataques, amenazas y escenarios de riesgos de seguridad digital.
- Liderar la definición de la arquitectura de seguridad digital para la Entidad.
- Gestionar la implementación de los controles tecnológicos de seguridad digital.
- Evaluar la efectividad de las políticas, directivas, circulares, instrucciones, planes y protocolos de seguridad digital.
- Coordinar y apoyar al Administrador de Seguridad Digital en la ejecución de las pruebas de vulnerabilidades y ethical hacking.
- Diseñar estrategias de seguridad digital para preservar la confidencialidad, disponibilidad e integridad de la información.
- Gestionar los incidentes de seguridad digital con el fin de garantizar un completo y oportuno manejo de estos.
- Estar en permanente comunicación con el Oficial de Seguridad de la Información para tratar y acordar diferentes temas en torno a la Seguridad Digital.

8.14LÍDER DEL EQUIPO GRIES

Liderará el equipo que gestionará los incidentes de seguridad de la información y seguridad digital, quien tiene las siguientes responsabilidades:

- Coordina las actividades técnicas del equipo de GRIES indicando las diferentes tareas que se deben ejecutar durante la contención y recuperación del incidente.
- Realizar el análisis forense de los diferentes incidentes que se presenten en la UBPD.

8.15ADMINISTRADOR (A) EN SEGURIDAD DIGITAL (experto técnico 4)

Es el encargado de gestionar los dispositivos de seguridad digital, al igual que apoyar al Líder y Arquitecto de Seguridad Digital en el análisis frente a este tipo de infraestructura, además, tiene las siguientes responsabilidades:

- Administrar los diferentes dispositivos de la plataforma de seguridad digital propiedad de la Entidad y coadministrar los equipos o soluciones de seguridad digital que se encuentren en servicios de outsourcing.
- Gestionar y monitorear los eventos e incidentes de seguridad digital.
- Revisar los controles implementados en seguridad digital.
- Ejecutar las pruebas de vulnerabilidades y ethical hacking, en conjunto con el Líder y Arquitecto de Seguridad Digital.
- Validar y gestionar todos los requerimientos que tengan relación con Seguridad digital.
- Analizar en conjunto con el Líder y Arquitecto de Seguridad Digital y con él (la) Oficial de Seguridad de la Información, el impacto tecnológico de la implementación de mecanismos de Seguridad de la Información en la Entidad.
- Probar los diferentes parches de seguridad en ambientes controlados, garantizando que no van a tener un impacto negativo en la plataforma tecnológica en producción.
- Supervisar que los parches de seguridad en la plataforma tecnológica de la Entidad se encuentren implementados de manera oportuna.
- Garantizar que se implemente adecuadamente el acceso a las diferentes plataformas o sistemas de información, basado en los perfiles definidos y aprobados en la Entidad.
- Realizar análisis de seguridad de software comercial o libre solicitados por los usuarios.

8.16 ADMINISTRADOR (A) DE LA BASE DE DATOS BASES DE DATOS EN INGLES DATA BASE ADMINISTRATOR DBA

Administra la plataforma y gestiona las bases de datos de la Entidad, con el fin de mantenerlas actualizadas, depuradas, organizadas, además, tiene las siguientes responsabilidades:

- Garantizar la integridad de la información de las bases de datos.
- Garantizar la adecuada, completa y oportuna gestión de los usuarios de bases de datos.
- Implementar mecanismos de cifrado para mantener la confidencialidad de las bases de datos que contengan información restringida o privada.
- Gestionar la capacidad de almacenamiento de las bases de datos.
- Gestionar los cambios realizados sobre las bases de datos.
- Garantizar las copias de respaldo de las bases de datos.
- Mantener actualizados los parches de seguridad de las bases de datos.
- Mantener esquemas de alta disponibilidad de las bases de datos.
- Realizar aseguramiento (hardening) de las bases de datos.
- Garantizar el registro de los logs con el fin de mantener la trazabilidad de las acciones realizadas sobre las bases de datos.
- Proponer cambios en la base de datos que respondan a las necesidades cambiantes de la UBPD.

8.17 JEFE (A) DE LA OFICINA ASESORA JURÍDICA

Asesora en la definición de políticas, objetivos y estrategias relacionadas con la gestión jurídica de los procesos de la UBPD, entre otras. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Verificar que el Sistema de Seguridad de la Información de la Entidad cuente con el sustento legal que permita su formalización, aplicación y obligatorio cumplimiento previa publicación y difusión.
- Atender y resolver las consultas que el Comité de Seguridad de la Información o el Oficial de Seguridad de la Información pudieran hacer en cuanto a la implementación, actualización y formalización del Sistema de Seguridad de la Información de la Entidad.
- Asesorar a la Entidad en la aplicación de las normas legales locales y/o internacionales en cuanto a seguridad de la información y seguridad digital.
- Informar oportunamente a él (la) Oficial de Seguridad de la Información cuando se presenten cambios en la legislación relacionada con seguridad de la información, que afecten al Sistema de Seguridad de la Información de la Entidad.

8.18JEFE (A) DE LA OFICINA ASESORA DE COMUNICACIONES Y PEDAGOGÍA

Diseña e implementa estrategias pedagógicas y comunicativas para el reconocimiento social de la importancia de la búsqueda de las personas dadas por desaparecidas y para facilitar la comprensión y participación de los familiares en las fases del proceso de búsqueda, entre otras. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Apoyar a él (la) Oficial de Seguridad de la Información, en la generación de las comunicaciones relacionadas con las actividades de capacitación y sensibilización en materia de seguridad de la información, dirigidas a servidores (ras), contratistas y personal delegado de la Entidad.
- Elaborar en conjunto con el (la) Oficial de Seguridad de la Información las comunicaciones de eventos de interrupción de la Entidad, y emitirlas hacia los servidores (ras), contratistas y personal delegado, durante y después de la crisis.
- Proporcionar los mecanismos para la transmisión de los contenidos de seguridad de la Información.
- Apoyar en el desarrollo de piezas gráficas y de video para la transmisión de mensajes de seguridad de la Información.

8.19JEFE (A) DE LA OFICINA DE CONTROL INTERNO

Planea, dirige y organiza la verificación y evaluación del Sistema de Control Interno de la UBPD; constata que los controles definidos para los procesos y actividades de la UBPD se cumplan, entre otras. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Diseñar un programa de auditoría en seguridad de la información y en seguridad digital para la Entidad, el cual debe ser actualizado y ejecutado por lo menos una vez al año.
- Mantener informado permanentemente al Oficial de Seguridad de la Información acerca del estado de las auditorías realizadas en seguridad de la información, dando cuenta de los hallazgos, no conformidades y oportunidades de mejora.

8.20JEFE (A) DE LA OFICINA ASESORA DE PLANEACIÓN

Asesora a las demás dependencias en la formulación, ejecución, seguimiento y evaluación de planes, programas y proyectos de la UBPD. Entre sus responsabilidades de seguridad de la información, están:

- Revisar que las estrategias que incluyen iniciativas, proyectos o programas en seguridad de la información, estén alineadas con el plan estratégico de la Entidad.
- Hacer seguimiento a la implementación de los indicadores de seguridad de la información y seguridad digital desarrollados por el (la) Oficial de Seguridad de la Información en la Entidad dentro del Plan de acción.
- Seguimiento, evaluación y control detallado a los planes de tratamiento de riesgos de seguridad digital.

8.21 COORDINADOR (A) DE MESA DE SERVICIO (NIVEL CENTRAL O TERRITORIAL)

Lidera la coordinación del personal y de las actividades desarrolladas desde la Mesa de Servicio en la sede territorial que tiene a cargo, además, frente a seguridad de la información tiene las siguientes responsabilidades:

- Reportar y asignar los diferentes requerimientos, eventos o incidentes de seguridad, a los responsables de seguridad de la información o seguridad digital, según corresponda.
- Recategorizar un caso que debe clasificarse como un incidente de seguridad de la información o seguridad digital, y determinar su nivel de criticidad.
- Habilitar y deshabilitar cuentas en el Directorio Activo de acuerdo con los requerimientos enviados.
- Crear unidades organizacionales (OU) en el Directorio Activo de acuerdo con los requerimientos enviados.
- Asignar los usuarios con los mínimos permisos necesarios para el desarrollo de sus funciones en las diferentes unidades organizacionales (OU) y grupos de distribución de GSUITE de acuerdo con las solicitudes de los propietarios de los activos de tipo información.

8.22 AGENTE DE SOPORTE EN SITIO

Atiende y apoya en los tiempos requeridos los tickets en las distintas dependencias de la Entidad además frente a seguridad de la información, tiene las siguientes responsabilidades:

- Identificar y reportar requerimientos de seguridad a los Analistas de Mesa de Servicio.
- Identificar y reportar a través de la herramienta de la Mesa de Servicio posibles incidentes o eventos de seguridad de la información y seguridad digital, y reportarlos oportunamente al Coordinador de la Mesa de Servicio.

- Divulgar y recordar a los usuarios finales las buenas prácticas y controles de seguridad que deben tener en cuenta para la debida protección de la información de la Entidad.
- Ejecutar periódicamente o a demanda escaneos de antivirus en los equipos de cómputo.
- Ejecutar actualizaciones de software en los equipos de cómputo.

8.23 ANALISTA DE MESA DE SERVICIO

Es el encargado de recibir los casos reportados a la Mesa de Servicio por parte de los distintos servidores de la Entidad, asignar los tickets correspondientes, además frente a seguridad de información, tiene las siguientes responsabilidades:

- Recibir los requerimientos de seguridad de la información y seguridad digital, para realizar el correspondiente registro en la herramienta de la Mesa de Servicio, y el escalamiento a los Coordinadores de Mesa de Servicio.
- Revisar la completitud de las solicitudes o requerimientos relacionadas con seguridad de la información o seguridad digital.
- Escalar posibles incidentes o eventos de seguridad de la información y seguridad digital al Coordinar de Mesa de Servicio.
- Validar solicitudes de software frente a la lista blanca o negra de software.

8.24 COORDINADOR (A) GESTIÓN GLOBAL

Consolidar e informar el estado de relacionados con seguridad de la información y seguridad digital, relacionados con seguimiento de la renovación de licenciamiento y suscripciones de los equipos y software sobre los cuales son responsables de su administración, además, tiene las siguientes responsabilidades:

- Generar reportes periódicos de los incidentes, requerimientos, solicitudes que a nivel de seguridad de la información o seguridad digital se hayan presentado, tanto en la Mesa de Servicio como en el NOC.
- Determinar y garantizar una correcta integración de los servicios de las diferentes gestiones de TI, que tengan relación con aspectos de seguridad de la información y seguridad digital.
- Realizar Gestión y Seguimiento de la renovación de licenciamiento y suscripciones a nombre de la UBPD.
- Garantizar que el software autorizado instalado en los equipos de los usuarios se mantenga actualizado con las últimas versiones, parches y actualizaciones entregadas y publicadas por los proveedores y/o fabricantes previa autorización de la UBPD.

- Realizar diagnósticos mensuales con el fin de identificar software instalados en las máquinas de los usuarios que no estén autorizados por la oficina TIC.

8.25 GESTOR DE REDES Y MONITOREO (COORDINADOR DEL NOC)

Verifica que los lineamientos establecidos para los equipos de red y de monitoreo, estén debidamente aplicados en la infraestructura, además frente a seguridad digital, tiene las siguientes responsabilidades:

- Validar que el aprovisionamiento de los equipos de comunicaciones y servidores a cargo de su administración, cuenten con las correctas configuraciones de seguridad.
- Analizar y aprobar solicitudes relacionadas con configuraciones de equipos de telecomunicaciones y seguridad perimetral a cargo de su administración.

8.26 ANALISTA DE ASEGURAMIENTO

Aplica o implementa los lineamientos de configuración, aseguramiento, revisión de logs, a actualizaciones y garantiza la correcta gestión y mantenimiento en los equipos de seguridad a cargo de su administración, además, tiene las siguientes responsabilidades:

- Mantener aplicados los parches de seguridad en los equipos o soluciones de seguridad digital a cargo de su administración.
- Realizar y mantener el aseguramiento (hardening) de los equipos o soluciones de seguridad digital a cargo de su administración.
- Configurar y parametrizar los diferentes equipos o soluciones de seguridad digital a cargo de su administración.
- Revisión permanente de las consolas de administración y logs de eventos de los diferentes equipos o soluciones de seguridad a cargo de su administración.
- Generar y mantener actualizados los estándares o guías de aseguramiento de la plataforma tecnológica a cargo de su administración.
- Realizar auditorías a la plataforma tecnológica con el fin de validar la completa y correcta aplicación de los estándares o guías de aseguramiento, y reportar lo evidenciado al Gestor de Redes y Monitoreo.
- Apoyar al Analista de Red y Analista de Infraestructura sobre los temas de seguridad digital en los cuales ellos requieran asesoría.
- Realizar copias de respaldo de los equipos o soluciones de seguridad digital a cargo de su administración.

- Configurar equipos de seguridad informática a cargo de su administración.

8.27 ANALISTA DE RED (Experto técnico 4)

Implementar las configuraciones y actualizaciones correctas en los equipos de telecomunicaciones, además, frente a seguridad digital tiene las siguientes responsabilidades:

- Mantener aplicados los parches de seguridad en los equipos de telecomunicaciones a cargo de su administración.
- Realizar y mantener el aseguramiento (hardening) de los equipos de telecomunicaciones a cargo de su administración.
- Revisión permanente de las consolas de administración y logs de eventos de los equipos de telecomunicaciones a cargo de su administración.
- Configurar los equipos de telecomunicaciones a cargo de su administración.
- Realizar copias de respaldo de los equipos de telecomunicaciones a cargo de su administración.

8.28 ANALISTA DE INFRAESTRUCTURA (Experto técnico 4)

Encargado de las actualizaciones de seguridad en la infraestructura tecnológica, puntualmente, tiene siguientes responsabilidades:

- Mantener aplicados los parches de seguridad en la infraestructura tecnológica a cargo de su administración.
- Realizar y mantener el aseguramiento (hardening) de los equipos de la infraestructura tecnológica a cargo de su administración.
- Revisión permanente de las consolas de administración y logs de eventos de la infraestructura tecnológica a cargo de su administración.

8.29 ADMINISTRADOR DE INFRAESTRUCTURA (EXPERTO TÉCNICO 4, Y ANALISTA TÉCNICO 2)

Gestiona la infraestructura tecnológica de la Entidad, y da apoyo en el desarrollo de la atención de los incidentes de seguridad, además, tiene las siguientes responsabilidades:

- Validar y reportar posibles incidentes de seguridad digital que se detecten en la plataforma tecnológica al Coordinador de Mesa de Servicio.

- Analizar en conjunto con el Líder y Arquitecto de Seguridad Digital y con el Administrador en Seguridad Digital, los incidentes de seguridad digital de la plataforma tecnológica.
- Monitorear permanentemente los niveles de disponibilidad y procesamiento de los diferentes componentes de la plataforma tecnológica.

8.30 SERVIDORES DESIGNADOS COMO SUPERVISORES DE CONTRATO

Es responsable de monitorear y controlar que los contratistas bajo su supervisión cumplan con las políticas, directrices, reglamento y demás lineamientos de seguridad de la información. Respecto a seguridad de la información, se encuentran, además, las siguientes responsabilidades:

- Revisar que los contratistas cumplan con los acuerdos establecidos en cuanto a Seguridad de la Información.
- Identificar riesgos de seguridad de la información asociados a los bienes o servicios provistos por el proveedor dentro del marco del contrato, definir planes y realizar el seguimiento correspondiente.
- Reportar de manera oportuna a la Oficina de Tecnologías de la Información y las Comunicaciones las novedades administrativas de los contratistas, para realizar los ajustes que correspondan en cuanto a modificación o eliminación de permisos sobre la plataforma tecnológica de la Entidad.

8.31 USUARIOS

Los usuarios son todos los servidores, contratistas y personal delegado de la UBPD que tenga relación con los activos de información de la Entidad, los cuales son responsables de poner en práctica las directrices, políticas, procedimientos y demás lineamientos de seguridad de la información. Respecto a seguridad de la información, se encuentran las siguientes responsabilidades, entre otras:

- Identificar las debilidades de seguridad y posibles riesgos de seguridad de la información sobre los activos de información a los cuales tengan acceso o conocimiento, e informarlo a los propietarios de los activos de información y al Oficial de Seguridad de la Información, de acuerdo a como esté definido en el procedimiento de gestión de incidentes de seguridad digital, y el procedimiento de gestión de incidentes de seguridad de la información.
- Conocer, entender y dar cumplimiento a las directrices, políticas, procedimientos y demás lineamientos de seguridad de la información y seguridad digital de la Entidad.
- Participar en las campañas de sensibilización y las capacitaciones en seguridad de la información de la Entidad.

- Reportar de manera oportuna los eventos o incidentes que afecten la seguridad digital y la seguridad de la información, de acuerdo a como esté definido en el procedimiento de gestión de incidentes de seguridad digital, y el procedimiento de gestión de incidentes de seguridad de la información.

9. INDICADORES DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Para evaluar el cumplimiento de los objetivos del Sistema de Seguridad de la Información, se deben estar monitoreando de acuerdo con frecuencia definida para cada indicador de las actividades que apoyan el Sistema, lo cual implica la generación de unos indicadores para medir la seguridad de la información y seguridad digital.

Por lo anterior, se han desarrollado un conjunto de indicadores enfocados a medir el desempeño y la eficacia del Sistema de Seguridad de la Información, para garantizar la integridad, disponibilidad y confidencialidad de la información, con el fin de apoyar la mejora continua del Sistema, mediante reportes que faciliten la toma de decisiones frente a riesgos, incidentes y mejoras en políticas, lineamientos y controles de seguridad.

En la medida que el Sistema de Seguridad de Información SSI, vaya madurando y mejorando se debe aplicar la siguiente metodología para establecer nuevos indicadores o modificar los existentes, así:

- Determinar cuáles indicadores se han venido cumpliendo en el término de 6 meses, los cuales se podrían ajustar en la meta o replantearlo.
- A partir de los incidentes de seguridad, de los resultados de las pruebas de auditoria y de las pruebas de seguridad, poder establecer nuevos indicadores sobre temas que se deseen medir y monitorear ya que ameritan una mejora, teniendo en cuenta la situación del momento.
- Para poder definir nuevos indicadores tener presente que se debe contar con información confiable y oportuna de las fuentes de información.
- Los nuevos indicadores deben buscar apalancar el cumplimiento de los objetivos del SSI y a su vez los objetivos estratégicos de la Entidad.
- La definición de los indicadores debe permitir analizar el impacto de los temas que se están evaluando y su mejora o deterioro en el tiempo para poder tomar acciones oportunas.

Para evaluar el Sistema de Seguridad de la Información, se definieron una serie de indicadores que permiten medir, controlar y comprobar, entre otros temas los siguientes:

- La calidad de los controles, directrices y planes de tratamiento implementados.
- Evaluar la conciencia y aplicación de las prácticas de seguridad exigidas por la Entidad[13].

[13] La cultura se basa en la concientización, aprendizaje y aplicabilidad permanente de buenas prácticas en temas de seguridad.

- Justificar la aplicación de nuevos controles y herramientas o programas de formación adicional.
- Los beneficios de la implementación de controles en seguridad de la información.

Dichos indicadores se generaron teniendo en cuenta los criterios SMART como se indica a continuación:

- “S” Specific, quiere decir que el objetivo debe ser algo concreto y entre más nivel de detalle mejor.
- “M” Measurable, deben ser medibles para que de acuerdo con su evaluación periódica, se puedan ir mejorando.
- “A” Actionable, proponer planes de mejoramiento de mediciones del indicador factibles de alcanzar.
- “R” Relevant, las acciones que se tomen para el mejoramiento de la medición de los indicadores deben generar beneficios relevantes.
- “T” Timely, las acciones para mejorar las mediciones de los indicadores deben ser realizables de manera oportuna.

Con base en lo anterior, los siguientes son los indicadores del Sistema de Seguridad de la Información propuestos, basados en los aspectos más relevantes que se considere ir midiendo para poder evaluar el desempeño del Sistema de Seguridad de la Información SSI, con el fin de generar la mejora continua correspondiente, los cuales se encuentran desarrollados en las plantillas **“DPE-FT-013 V1_Indicador 0X_Nombre Indicador_V1.xlsx”** anexas correspondientes a cada indicador, en donde se encuentra el detalle de su metodología de cálculo, fuentes de información, fórmulas, metas, seguimiento, entre otros campos, así:

Número del Indicador	Nombre del Indicador	Descripción General
1	Sensibilización y capacitación en Seguridad de la Información y Seguridad Digital	El indicador mide el nivel de conocimiento que tienen los servidores, contratistas y personal delegado en cuanto a la seguridad de la información y seguridad digital, adquirido a través de las diferentes campañas de sensibilización realizadas dentro de la Entidad.
2	Cierre de Brechas Pruebas de Vulnerabilidades de Seguridad	El indicador mide el cierre de brechas encontradas a partir de las pruebas de vulnerabilidades de seguridad realizadas, con el fin de evitar que se presenten posibles incidentes de seguridad en la plataforma tecnológica de la Entidad.

3	Mantenimiento de Infraestructura Tecnológica	El indicador mide el total de mantenimientos preventivos realizados y que han sido programados a la infraestructura tecnológica.
4	Pruebas de Ingeniería Social	El indicador mide el nivel de respuesta que tienen servidores, contratistas y personal delegado ante ataques diseñados para identificar debilidades en cuanto al conocimiento en seguridad en el personal, con el fin de verificar el cumplimiento de las políticas de seguridad de la información y seguridad digital.
5	Incidentes de Seguridad atendidos oportunamente	El indicador mide el nivel de respuesta con el que cuenta la Entidad para atender los incidentes de seguridad de la información y seguridad digital dentro de los tiempos establecidos dependiendo la categorización de los incidentes.
6	Riesgos de Seguridad con Planes de Acción ejecutados	El indicador mide la capacidad con la que cuenta la Entidad para ejecutar los planes de acción definidos para el tratamiento de los riesgos de seguridad dentro de los tiempos establecidos.
7	Pruebas de Restauración de Backups exitosas	El indicador mide la capacidad con la que cuenta la Entidad para generar copias de respaldo de la información con las que se pueda restaurar la información después de una eventual pérdida de datos.
8	Conocimiento y Aplicación de Políticas de Seguridad de la Información y Seguridad Digital	El indicador mide el nivel de conocimiento que tienen los servidores, contratistas y personal delegado en cuanto a las políticas de seguridad de la información y seguridad digital, y la aplicabilidad de éstas dentro de sus funciones.
9	Equipos con Antivirus Instalado y Actualizado	El indicador mide la cantidad de equipos de cómputo de la Entidad protegidos contra códigos maliciosos, al validar que cuentan con el antivirus

		adquirido por la Entidad y actualizado, con el fin de evitar posibles incidentes de seguridad de la información y seguridad digital.
10	Cambios en Plataforma Tecnológica con Análisis de Seguridad	El indicador mide que los cambios implementados en la plataforma tecnológica cuenten con los análisis de seguridad correspondientes a partir de las solicitudes de cambios generadas, con el fin de reducir la posibilidad de que se presenten incidentes de seguridad digital, que afecten la disponibilidad de los equipos tecnológicos de la Entidad.
11	Áreas Seguras con controles de acceso físico adecuados.	El indicador mide que todas las áreas seguras cuenten con los controles de acceso implementados de acuerdo con las necesidades en cada área.
12	Sistemas de Información Seguros	El indicador mide la cantidad de sistemas de información que cuenten con protocolos seguros, tanto para la transferencia de información como para el proceso de autenticación.
13	Permisos en Sistemas de Información	El indicador mide que los sistemas de información, recursos y servicios tecnológicos de la Entidad cuenten con los accesos y permisos autorizados mínimos necesarios para el desarrollo de las funciones.

Tabla 2 Indicadores del SSI Fuente UT MYQ-ALINA TECH

10. METODOLOGÍA DE SEGUIMIENTO AL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

FASES DEL SEGUIMIENTO AL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN:

La Entidad con el fin de generar oportunidades de mejora al Sistema de Seguridad de la Información – SSI, realizará el seguimiento de acuerdo con las fases que se presentan en la siguiente ilustración y que se describe posteriormente:

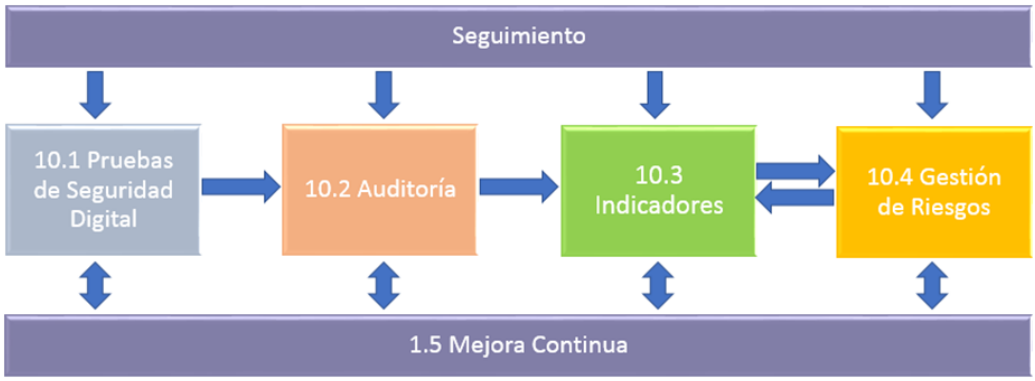


Ilustración 7 Fases del seguimiento al SSI Fuente: UT MYQ-ALINA TECH

Seguimiento: Se estableció la presente metodología con el fin de poder hacer un seguimiento transversal al Sistema de Seguridad de la Información, para lo cual se requiere desarrollar una serie de actividades como las que se indican a continuación y que más adelante se detallan, así:

- El resultado de las pruebas de seguridad digital ejecutadas.
- Las auditorías al Sistema de Seguridad de la Información.
- Los indicadores de seguridad y la gestión de riesgos, y a partir de las salidas de cada uno de ellos, contribuir a mejorar continuamente el Sistema de Seguridad de la Información.

Es de anotar, que de acuerdo a como se establezcan las pruebas de seguridad, los checklist de las auditorías, y el diseño de los indicadores, también se podrá medir la efectividad de los controles.

De acuerdo a las anteriores actividades, a continuación, se detallan algunas relaciones entre ellas, así:

- Los Informes de pruebas de vulnerabilidades y ethical hacking son insumo para las auditorías realizadas al Sistema de Seguridad de la Información.
- Los Informes de las evaluaciones de las Auditorías realizadas para medir la eficacia del SSI sirven de fuente para el indicador “Conocimiento y Aplicación de Políticas de Seguridad de la Información y Seguridad Digital”.
- El Informe del resultado del indicador “Cobertura de Riesgos de Seguridad con Planes de Tratamiento” sirve como insumo para el seguimiento de la gestión de riesgos, y a su vez la matriz

"GTI-MR-001 Mapa de Riesgos Seguridad" y el informe con el total de riesgos de seguridad que se encuentran identificados y que cuentan con un plan de tratamiento, como insumos para la evaluación del indicador.

- Y en cuanto a la mejora continua por parte del Comité de Seguridad de la Información se realiza seguimiento a los 4 temas:

    - Pruebas de seguridad digital.
    - Auditoría
    - Indicadores.
    - Gestión de riesgos.

A continuación, se encuentra el detalle del seguimiento que se debe realizar a cada uno de los temas así:

10.1 PRUEBAS DE SEGURIDAD DIGITAL

A partir de las pruebas de vulnerabilidades y ethical hacking realizadas por el Administrador en Seguridad Digital (experto técnico 4), éste generará un informe ejecutivo el cual debe contener las vulnerabilidades que no han sido cerradas, detallando una categorización teniendo en cuenta el impacto que puede generar el no cerrarlas, y las observaciones, y es enviado al Líder y Arquitecto de Seguridad Digital para que en conjunto con el Administrador en Seguridad Digital y él (la)Oficial de Seguridad de la Información lo socialicen en el Comité de Seguridad de la Información, con el fin de que se evalúe dicho análisis y poder generar las oportunidades de mejora correspondientes.

10.2 AUDITORÍA

Tomando como referencia el Plan de Auditoría Interna del Sistema de Seguridad de la Información, y a partir de los seguimientos realizados por parte de la Oficina de Control Interno a las acciones correctivas planteadas por cada uno de los responsables de los procesos auditados dentro de las auditorías, y registradas dentro del formato **"SEC-FT-002 PLAN DE MEJORAMIENTO"**, de acuerdo a lo indicado en el procedimiento **"SEC-PR-001 Formulación, Seguimiento y Evaluación de Planes de Mejoramiento"**, el Jefe de la Oficina de Control Interno enviará el reporte mensual correspondiente a dichos seguimientos a el (la) Oficial de Seguridad de la Información, quien identificará cuáles acciones correctivas dentro de las fechas programadas no han sido ejecutadas, con el fin de realizar un análisis del impacto que genera el no implementarlas, e informa al Comité de Seguridad de la Información, para que se realice el seguimiento correspondiente.

10.3 INDICADORES

En las plantillas de indicadores de seguridad **"DPE-FT-013 V1_Indicador XX_nombre indicador_V1.xlsx"**, el responsable de cada indicador del proceso de Gestión de Seguridad de la Información deberá realizar el monitoreo correspondiente a cada indicador de seguridad, y a partir de esta revisión, el Oficial de Seguridad de la Información cada trimestre debe generar un reporte total de los monitoreos realizados, dentro de un informe ejecutivo el cual debe contener:

- Resultado del avance dentro del semestre por cada uno de los indicadores:

Número del Indicador	**Nombre del Indicador**	**Fórmula**	**% de Avance**	**Cumple con la Meta SI/NO**	**Observaciones metas no alcanzadas**
01	*Nombre_Indicador*	*(Variable1/Variable2) x 100*	*X%*	*Indicar si cumple o no cumple con la meta*	*Relacionar las situaciones que generaron el incumplimiento de la meta*
n…					

Tabla 3 Resultado de avance de los indicadores Fuente: UT MYQ-ALINA TECH

Después de generar el informe ejecutivo, a él (la) Oficial de Seguridad de la Información presenta ante el Comité de Seguridad de la Información lo evidenciado, con el fin de evaluar las observaciones y se generen las oportunidades de mejora correspondientes.

10.4 GESTIÓN DE RIESGOS

Dentro de la gestión de riesgos de seguridad de la información y seguridad digital ejecutada a través de la "Metodología de Gestión de Riesgos de Seguridad de la Información y Seguridad Digital", se realiza el seguimiento a cada uno de los riesgos identificados, dentro del cual el Oficial de Seguridad de la Información

asigna un responsable para dicho seguimiento, quien documenta lo evidenciado dentro de las revisiones realizadas a los planes de tratamiento en la herramienta adquirida por la UBPD para tal fin.

Después de obtener este seguimiento por cada riesgo, el (la) Oficial de Seguridad de la Información debe generar un reporte mensual del total de los seguimientos realizados, dentro de un informe ejecutivo el cual debe contener:

- Consolidado del total de riesgos identificados por proceso:

Proceso	Total de riesgos de seguridad de la información	Total de riesgos de seguridad digital
Proceso 1	*cantidad n…*	*cantidad n…*
Proceso 2		
Proceso n…		

Tabla 4 Consolidado del total de riesgos Fuente: UT MYQ-ALINA TECH

El porcentaje de la cantidad de riesgos por zona de riesgo (bajo, moderado, alto, extremo), lo cual se toma del Mapa de Riesgos de la Entidad:

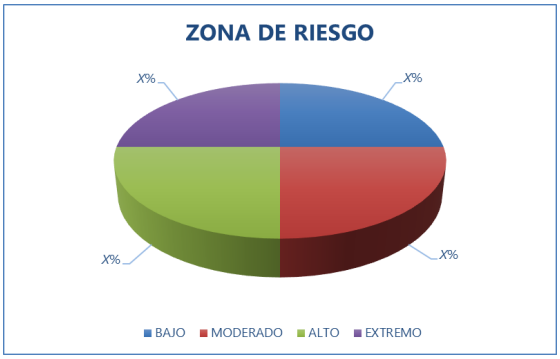


Ilustración 8 Porcentaje de riesgos por zona Fuente: UT MYQ – ALINA TECH

- Riesgos en los que no se implementaron los planes de acción dentro de los tiempos establecidos de acuerdo a lo definido en la Metodología de Gestión de Riesgos de Seguridad de la Información y Seguridad Digital:

Proceso	Riesgo	Zona de riesgo	Acción a tomar	Responsable	Observaciones por las cuales no se implementó el plan
Proceso 1	*Nombre del riesgo*	*Zona bajo, moderado, alto o extremo en el cual se encuentra el riesgo residual*	*Plan de acción para tratar el riesgo definido en el mapa de riesgos.*	*Responsable (s) de ejecutar la acción.*	*Detallar los motivos por los cuales no se ejecutó el plan.*
Proceso 2					
Proceso n…					

Tabla 5 Planes de acción de riesgos no implementados Fuente: UT MYQ – ALINA TECH

- Conclusiones.

Después de generar el informe ejecutivo anual , a él (la) Oficial de Seguridad de la Información presenta ante el Comité de Seguridad de la Información lo evidenciado, con el fin de evaluar el cumplimiento de las acciones ejecutadas y la efectividad de los controles, así mismo, en caso de que se determinen causas de atrasos en ejecución de planes de tratamiento, se deben proponer oportunidades de mejora correspondientes.

10.5 MEJORA CONTINUA

Con el fin de contribuir a la mejora continua del Sistema de Seguridad de la Información, a partir de los informes generados por el Oficial de Seguridad de la Información de los seguimientos realizados a la gestión de riesgos, análisis de indicadores, informes de auditorías y pruebas de seguridad digital, el Comité de Seguridad de la Información revisará la gestión de los temas, para identificar oportunidades de mejora y así cada uno de los responsable poder tomar las medidas necesarias acordes a:

- Gestión de riesgos: Implementar los planes de acción que no fueron ejecutados dentro de los tiempos establecidos o redefinirlos ya que puede que no hayan sido los correctos, así mismo, se debe realizar una nueva evaluación de riesgos sobre los cuales se implementaron, con el fin de validar si su riesgo residual disminuyó hasta el nivel aceptable de riesgo.
- Indicadores: Mitigar desviaciones en cuanto a las metas planteadas para el cumplimiento de cada indicador.

- Auditorías: Revisar la eficacia de las medidas correctivas definidas para remediar las no conformidades identificadas en las auditorías realizadas al Sistema de Seguridad de la Información.
- Pruebas de seguridad digital: Implementar los planes de remediación para las brechas que no fueron cerradas de acuerdo con el plan de cierre de brechas.

Las actividades necesarias para realizar el seguimiento del cumplimiento de los lineamientos y controles del Sistema de Seguridad de la Información – SSI, como son las pruebas de seguridad digital, gestión de riesgos de seguridad, indicadores y auditorías, se establecen en el **"GSI-PR-001 Procedimiento Seguimiento SSI "**.

10.6 RECOMENDACIONES DEL SEGUIMIENTO

- Garantizar que se cumpla con la periodicidad definida en la que se realizarán las actividades puntuales respecto al seguimiento del SSI.
- Generar los registros correspondientes a los seguimientos realizados para cada uno de los temas a evaluar.
- Informar oportunamente al Comité de Seguridad de la Información el resultado del seguimiento del SSI, con el fin de que se tomen las decisiones adecuadas para contribuir a la mejora continua del SSI.

De otro lado, con el fin de garantizar el seguimiento y control desde la definición de las necesidades para las diferentes herramientas o sistemas de información, a adquirir o desarrollar, para su implementación en la Entidad, se deben realizar una serie de actividades, así:

- Garantizar que las nuevas herramientas cumplan con las políticas de seguridad de la información y seguridad digital, cuando se evalúen los requerimientos no funcionales.
- Realizar un análisis de riesgo cuando se va a adquirir, desarrollar o implementar un nuevo sistema de información o herramienta.
- Ejecutar pruebas de seguridad en los sistemas de información en un ambiente controlado para este tipo de actividades, antes de realizar el paso al ambiente de producción.
- Realizar los cambios de acuerdo con lo definido en el procedimiento "GTI-PR-002 Gestión de cambios" para el ciclo de vida de desarrollo de software.
- Definir y evaluar los requerimientos de disponibilidad y los Acuerdos de Nivel de Servicio - ANS requeridos que suplan las necesidades de la Entidad.
- Definir e implementar lo correspondiente a:
    - Esquemas de autenticación y autorización.
    - Roles y responsabilidades.
    - Backups y logs de auditoría.

11. PLAN DE AUDITORÍA INTERNA DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

11.1 OBJETIVO

Identificar el estado del Sistema de Seguridad de la Información de la Unidad de Búsqueda de Personas Dadas por Desaparecidas, mediante la ejecución de una auditoría interna tomando como referencia la norma ISO 27001:2013, ISO 19011:2018, COBIT 2019 e ISO 27032.

11.2 ALCANCE

Para la ejecución de la auditoría interna al Sistema de Seguridad de la Información (SSI) se debe tener en cuenta la información documentada y formalizada que hace parte del SSI, y los registros correspondientes que evidencien su implementación y ejecución.

Debería ejecutarse una auditoría interna anual al Sistema de Seguridad de la Información, primero desde el punto de vista documental, y luego de la aplicabilidad y efectividad de los controles, y en cuanto a la disponibilidad y garantizar el mantenimiento de las operaciones de la entidad es necesario auditar los planes, desarrollo y pruebas del BCP y DRP, esta debe ejecutarse según lo definido en el programa de auditoria, la aplicabilidad de los controles pertinentes al SSI de la UBPD y sobre los cuales se debe enmarcar la auditoria para definir su alcance, se encuentra en el P33 Análisis y Aplicabilidad de Dominios, Objetivos de Control y Controles.

Se propone que en una primera auditoría al SSI a ser ejecutada, se incluyan los procesos misionales, y los procesos de apoyo, estratégicos y de evaluación que tengan relación con el diseño e implementación de los controles de seguridad, los cuales se indican a continuación:

- Procesos Misionales:
    - Participación en las acciones humanitarias y extrajudiciales para la búsqueda.
    - Planificación de acciones humanitarias y extrajudiciales para la búsqueda.
    - Implementación de acciones humanitarias y extrajudiciales para la búsqueda.

- Procesos de Apoyo (procesos que están relacionados de forma directa con el SSI):

- Gestión humana.
- Gestión contractual.

- Procesos Estratégicos (procesos que están relacionados de forma directa con el SSI):

  - Gestión de seguridad de la información.
  - Gestión de TIC.
  - Gestión jurídica.
- Procesos de Evaluación (procesos que están relacionados de forma directa con el SSI):

  - Seguimiento evaluación y control.
  - Control Interno Disciplinario.

11.3 CRITERIO DE AUDITORÍA

Para la evaluación al Sistema de Seguridad de la Información, el equipo auditor tomará como criterio principalmente la norma ISO/IEC 27001:2013, la cual contiene los siguientes numerales y dominios:

- Numerales:

  - Contexto de la Organización
  - Liderazgo
  - Planificación
  - Soporte
  - Operación
  - Evaluación del desempeño
  - Mejora

- Dominios

  - Políticas de Seguridad
  - Organización de Seguridad de la información
  - Seguridad de los recursos humanos
  - Gestión de los activos
  - Control de acceso
  - Criptografía
  - Seguridad física y del entorno

- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Relaciones con los proveedores
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio
- Cumplimiento

Adicionalmente, con el fin de realizar una completa evaluación al Sistema de Seguridad de la Información, dentro de la lista de verificación **soporte o Lista de verificación para auditorías internas SSI**, en la hoja "Instructivo Diligenciamiento", se encuentra la descripción de los campos a diligenciar, y en la hoja "Lista Verificación" se relacionaron a los numerales de la norma ISO/IEC 27001:2013 y a los controles de su Anexo A, las siguientes normas y marco de trabajo, teniendo en cuenta algunos temas particulares de cada uno así:

a) **COBIT 2019:** Guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI). De acuerdo con su estructura, el framework se compone de una serie de objetivos de gobierno y gestión, los cuales se agrupan en cinco dominios, de los cuales se tuvo en cuenta los siguientes objetivos de gobierno y gestión:

- Dominio "Evaluar, Dirigir y Monitorizar (EDM)":
  - Objetivo de Gobierno: "EDM03: Asegurar la optimización del riesgo".
- Dominio "Alinear, Planificar y Organizar (APO)":
  - Objetivo de gestión: "APO07: Gestionar los recursos humanos".
    - Práctica de gestión: "APO07.01: Adquirir y mantener una dotación de personal suficiente y adecuada".
    - Práctica de gestión: "APO07.03: Mantener las habilidades y competencias del personal".
  - Objetivo de gestión: "APO12: Gestionar el riesgo".
  - Objetivo de gestión: "APO13: Gestionar la seguridad".
    - Práctica de gestión: "APO13.01: Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)".
    - Práctica de gestión: "APO13.02: Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad"
    - Práctica de gestión: "APO13.03: Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)"

- Objetivo de gestión: “APO14: Gestionar los datos”.
    - Práctica de gestión: “APO14.01: Definir y comunicar la estrategia y los roles y responsabilidades de la gestión de datos de la organización”.
    - Práctica de gestión: “APO14.07: Definir la estrategia de depuración de datos”.
    - Práctica de gestión: “APO14.08: Gestionar el ciclo de vida de los activos de datos”.
    - Práctica de gestión: “APO14.09: Soportar el archivo y retención de datos”.

- Dominio “Construir, Adquirir e Implementar (BAI)”:
    - Objetivo de gestión: “BAI06: Gestionar los cambios de TI”.
    - Objetivo de gestión: “BAI07: Gestionar la aceptación y la transición de los cambios de TI”.
    - Objetivo de gestión: “BAI09: Gestionar los activos”.
    - Objetivo de gestión: “BAI11: Gestionar los proyectos”.
- Dominio “Entregar, Dar Servicio y Soporte (DSS)”:
    - Objetivo de gestión: “DSS05: Gestionar los servicios de seguridad”.
        - Práctica de gestión: “DSS05.01: Proteger contra software malicioso”.
        - Práctica de gestión: “DSS05.02: Gestionar la seguridad de la conectividad y de la red”.
        - Práctica de gestión: “DSS05.03: Gestionar la seguridad de endpoint”.
        - Práctica de gestión: “DSS05.04: Gestionar la identidad del usuario y el acceso lógico”.
        - Práctica de gestión: “DSS05.05: Gestionar el acceso físico a los activos de I&T”.
        - Práctica de gestión: “DSS05.06: Gestionar documentos sensibles y dispositivos de salida”.

b) **ISO/IEC 31000:2018:** Es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones. Esta norma fue publicada por la Organización Internacional de Normalización (ISO) y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades. De esta norma se tuvo en cuenta los siguientes numerales:

- 6.2 Comunicación y consulta.
- 6.3 Alcance, contexto y criterios.
- 6.4 Evaluación del riesgo.
- 6.5 Tratamiento del riesgo.
- 6.6 Seguimiento y revisión.
- 6.7 Registro e informe.

c) **ISO/IEC 27032:2012:** Es un estándar de ciberseguridad publicado por la Organización Internacional de Normalización (ISO), la cual ofrece unas líneas generales de orientación para fortalecer el estado de la Ciberseguridad en una entidad, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con: la Seguridad en la Redes, Seguridad en Internet, Seguridad de la información y la Seguridad de las Aplicaciones. De esta norma se tuvo en cuenta los siguientes numerales:

- Activos en el ciberespacio.
- 9.1. Amenazas.
- Roles de las partes interesadas en ciberseguridad.
- 11.2 Evaluación y tratamiento de riesgos.
- 12.2 Control de nivel de aplicación.
- 12.3 Protección de servidores.
- 12.4 Controles de usuario final.
- 12.5 Controles frente a ataques de ingeniería social.
- 13.2 Políticas.
- 13.4 Personas y Organizaciones.

d) **ISO/IEC 22301:2012:** Es una norma que proporciona un marco de referencia para gestionar la continuidad del negocio en una organización, disminuyendo la posibilidad de ocurrencia de un incidente disruptivo y, en caso de producirse, poder estar preparado para responder en forma adecuada y, de esa forma, reducir drásticamente el daño potencial de ese incidente. De esta norma se tuvo en cuenta los siguientes numerales:

- 5.3 Política.
- 5.4 Roles organizacionales, responsabilidades y autoridades.
- 8.2 Análisis de Impacto del Negocio y Evaluación del Riesgo.
- 8.4.4 Planes de Continuidad del negocio.
- 8.4.5 Recuperación.

11.4. TIPIFICACIÓN

11.4.4.1 Tipo de Auditoría

De acuerdo con el **"Estatuto de Auditoría Interna"** de la UBPD en su numeral **"6.1 Tipo de auditoría: Aseguramiento"**, se ejecutará la auditoría de primera parte, o auditoría interna realizada por la misma Entidad, por lo que se deberá contar con el personal capacitado para realizar dichas auditorías, y que sean independientes a los procesos a auditar, por lo que los auditores internos de acuerdo al numeral **"5.6 Auditores Internos"** de dicho estatuto, deberán suscribir la declaración de independencia, utilizando el formato **"SEC-FT-005 Declaración de Independencia"**.

11.4.2 Método de Auditoría

Realizar las auditorías en sitio con interacción de los auditados, generando las visitas de acuerdo a lo acordado con cada uno de los líderes de los procesos en días completos, y el total de días dependerá del total de procesos a auditar. Se debe realizar las siguientes actividades:

- Entrevistas.
- Completar la lista de verificación "SEC-FT-0XX Lista de verificación para auditorías internas SSI" en compañía y con la participación del auditado.
- Revisar documentos con la participación del auditado.
- Realizar muestreos.

11.5 EQUIPO AUDITOR

De acuerdo con el "Estatuto de Auditoría Interna" de la UBPD, el jefe de la Oficina de Control Interno selecciona a los auditores internos teniendo en cuenta el perfil de los servidores públicos de la Entidad en cuanto a su educación, formación, experiencia y habilidades, teniendo en cuenta que dentro del equipo auditor, se pueden incluir especialistas técnicos de apoyo en caso de que se requiera. Para elegir el equipo auditor al Sistema de Seguridad de la Información, se debe tener en cuenta lo siguiente:

- Conocimientos básicos:
    - Conocimiento en las versiones vigentes de las normas ISO 27001:2013 e ISO 27007:2020.
    - Conocimientos en la norma ISO 27002:2013.
    - Conocimientos en la norma ISO 19011:2018.

- Estudios:

    - Carrera profesional en Sistemas, Electrónica o afines.
    - Auditor Interno o Auditor Líder certificado en la versión vigente de la norma ISO 27001.
    - Los auditores del Sistema de Seguridad de la Información deben tener conocimientos y habilidades en tecnologías de la información y seguridad de la información, demostrados, por ejemplo, mediante certificaciones relevantes. La experiencia laboral de los auditores del Sistema de Seguridad de la Información también debe contribuir al desarrollo de sus conocimientos y habilidades.
    - Los auditores deben tener conocimiento en el Sistema de Seguridad de la Información de la Entidad, y conocer las particularidades de ésta en cuanto a su misionalidad.

- Experiencia:

    - Experiencia mínima de 4 años en el campo laboral.
    - Experiencia mínima de 2 años auditando sistemas de gestión de seguridad de la información.
    - Haber realizado mínimo una auditoría con monitoreo o de práctica.

11.6 METODOLOGÍA

A continuación, se describen las fases para realizar la auditoría interna al Sistema de Seguridad de la Información basado en el ciclo PHVA:

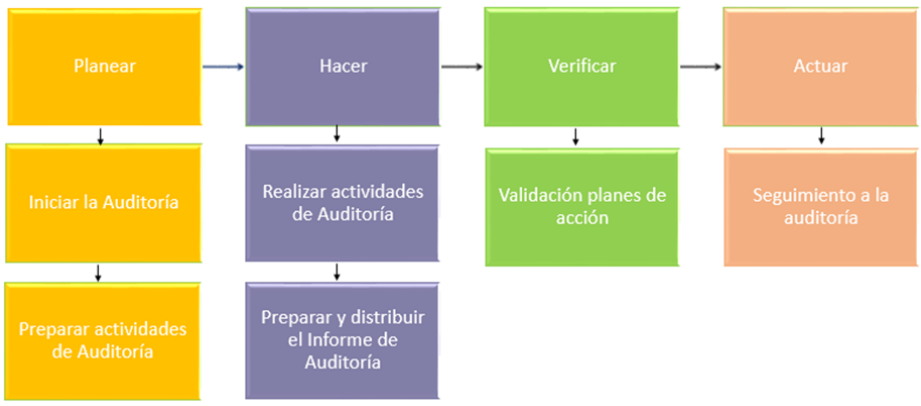


Ilustración 9 Metodología Plan de Auditoría Interna Fuente: Elaboración UT MYQ – ALINA TECH

11.6.1 Planear

a) Iniciar la Auditoría

Teniendo en cuenta el alcance de la auditoría, el auditor líder responsable de la auditoría debe identificar los responsables de cada uno de los procesos para que se genere una comunicación de la realización de la auditoría al Sistema de Seguridad de la Información, informando el objetivo, alcance y métodos de auditoría, así como los auditores quienes ejecutarán la auditoría. Adicionalmente, se deben acordar las fechas de la auditoría con el auditado, e informarle las responsabilidades que este tiene de acuerdo con el **"Estatuto de Auditoría"** en el ítem **"5.7 Auditados"**.

b) Preparar Actividades de Auditoría

Para la realización de la auditoría se deben registrar las actividades a ejecutar en el formato **"SEC-FT-013 Plan de Trabajo de Auditoría"**. Adicionalmente, se deben solicitar al auditado la documentación y registros correspondientes al Sistema de Seguridad de la Información, los cuales se encuentran listados en el formato **"Documentos y Registros del SSI"**, dicho formato cuenta con una hoja **"Instructivo Diligenciamiento"**, en la que se encuentra la descripción de los campos a diligenciar. Lo anterior con el fin de adelantar las actividades relacionadas a la documentación del Sistema de Seguridad de la Información.

Teniendo preparado el plan de auditoría, en el cual se incluye: el objetivo, alcance, criterio de evaluación, tipo de auditoría, método de auditoría, equipo auditor, fechas de ejecución de la auditoría, lugar y tiempo establecido para la ejecución de la auditoría, el Auditor Líder debe enviarlo al Oficial de Seguridad de la Información para que, en conjunto con los responsables de los procesos auditados, se genere una revisión y aprobación del plan.

Luego el Auditor Líder debe preparar los papeles de trabajo, revisando el checklist soporte o lista de **verificación para auditorías internas SSI"**, informes de entes externos, plan anual de seguridad y planes de sensibilización, con el fin de verificar que los convocados a las entrevistas sean los suficientes para poder responder a todas las preguntas listadas en la lista de verificación, y las demás que se consideren pertinentes.

Las entradas para el desarrollo de la auditoría son:

- Documentación relacionada a los procesos auditados.
- Documentación y registros del Sistema de Seguridad de la Información.
- SEC-FT-013 V1Plan de trabajo de auditoría.

11.6.2 Hacer

a) Realizar actividades de auditoría

Para comenzar con la ejecución de la auditoría, el Auditor Líder debe convocar a la reunión de apertura, en la que los auditados indicarán si se encuentran de acuerdo con el Plan de Auditoría, para asegurar que todas las actividades planteadas pueden llevarse a cabo.

Durante la ejecución de la auditoría, el equipo auditor debe ir realizando la revisión de documentos y registros proporcionados por los auditados, para que se identifique si son conformes al criterio de evaluación.

A partir de las entrevistas realizadas, y la revisión de toda la documentación y registros recolectados, se totalizan los hallazgos identificados, y evaluación de los controles de seguridad de la información y seguridad digital, con el fin de para que identificar si se documenten las conformidades, no conformidades y observaciones. Por último, se deben generar las conclusiones de acuerdo con los hallazgos.

En el momento que se tenga el resultado de la auditoría, el Auditor Líder debe convocar a la reunión de cierre para presentar los hallazgos y conclusiones de la auditoría.

b) Preparar y distribuir el informe de auditoría

Cuando se tenga el registro de toda la información, el Auditor Líder generará el informe de la auditoría, incluyendo dentro de este:

- Objetivo de la auditoría.
- Alcance.
- Criterio de Auditoría.
- Equipo Auditor.
- Fechas y lugares de las entrevistas.
- Hallazgos de Auditoría.
- Conclusiones.

11.6.3 Verificar

a) Validación planes de acción

El responsable de cada proceso de acuerdo con el informe de auditoría debe generar las acciones correctivas correspondientes a remediar las no conformidades encontradas. Esto previo acuerdo en la reunión de apertura de auditoria.

Las salidas de la auditoría ejecutada son:

- Checklist soporte de **verificación para auditorías internas SSI"** totalmente diligenciado.
- Soporte de Informe de Auditoría.
- Soporte de Informe de acciones correctivas de cada proceso auditado.

11.6.4 Actuar

a) Seguimiento a la Auditoría

El responsable de cada proceso auditado debe informar al equipo auditor sobre los avances realizados en la implementación de las acciones correctivas. El equipo auditor debe verificar si las acciones fueron completadas de acuerdo con las fechas establecidas para su ejecución.

12. DISEÑO DEL CICLO DE VIDA DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de ir mejorando y madurando el Sistema de Seguridad de la Información, se establece un ciclo de vida de este sistema basado en el PHVA, así:

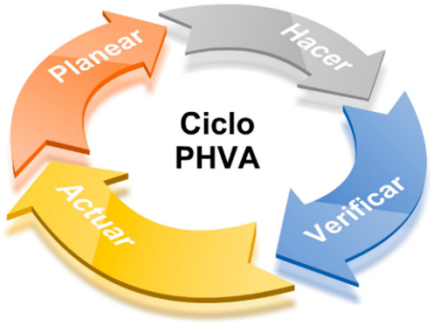


Ilustración 10 Ciclo PHVA del Sistema de Seguridad de la Información Fuente: UT MYQ – ALINA TECH

- **PLANEAR:** Establecer las políticas, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información y la seguridad digital con el fin de entregar resultados acordes con las misión, visión, objetivos y planes estratégicos de la Entidad.

- **HACER:** Implementar y operar las políticas, los controles, procesos y procedimientos del Sistema de Seguridad de la Información.
- **VERIFICAR:** Evaluar, y en donde sea aplicable, medir el desempeño del proceso de Gestión de Seguridad de la Información contra la política y los objetivos de seguridad y la experiencia práctica y reportar los resultados a la alta dirección para su revisión.
- **ACTUAR:** Emprender acciones correctivas y preventivas con base en los resultados de la fase de verificación para lograr la mejora continua.

Ilustración 11 Actividades del SSI realizadas en el PHVA Fuente: UT MYQ – ALINA TECH

A continuación, se especifican las fases del ciclo de vida del Sistema de Seguridad de la Información, las cuales se ven de manera más detallada (Proveedor, Entrada, Actividad, Descripción, Responsable, Registro, Control, Salida y Usuario) en la "GSI-CR-001 Caracterización Gestión de Seguridad de la Información", así:

- PLANEAR:
    - Determinar las necesidades de Seguridad de la Información de la Entidad
    - Establecer el Plan Estratégico de Seguridad (PESI)
    - Formular la planeación estratégica de Gestión de Seguridad de la Información
    - Elaborar, revisar y/o actualizar la documentación relacionada al proceso de Gestión de Seguridad de la Información
    - Identificar y/o actualizar activos de información
    - Identificar y valorar los riesgos de Seguridad y generar los planes de tratamiento
    - Gestionar los recursos humanos, técnicos y administrativos necesarios para la ejecución de los planes de tratamiento de riesgos
    - Gestionar los recursos financieros necesarios para la ejecución de los planes de capacitación y sensibilización

- HACER:
    - Ejecutar el Plan de Acción, y el Plan Estratégico de Seguridad de la Información (PESI)
    - Implementar la documentación asociada al proceso
    - Ejecutar el Plan de Sensibilización y Capacitación de Seguridad
    - Ejecutar los planes de tratamiento de los riesgos de seguridad

- VERIFICAR:
    - Ejecutar el Plan de Auditoría del Sistema de Seguridad de la Información
    - Realizar las pruebas de seguridad digital
    - Evaluar las variables de los indicadores de seguridad
    - Realizar el seguimiento a los planes de tratamiento de los riesgos de seguridad
    - Analizar informes de seguimiento a: pruebas de seguridad, indicadores, auditorías y riesgos

- ACTUAR:
    - Implementar las acciones de acuerdo con las oportunidades de mejora

13. GLOSARIO

- **Aceptación del riesgo:** Decisión informada de tomar un riesgo particular. [Norma ISO 27000:2018].
- **Apetito del riesgo:** Magnitud y tipo de riesgo que una entidad está dispuesta a buscar o retener. [Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4, octubre de 2018].
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización. [Norma ISO 27000:2018].
- **Análisis de riesgo:** proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [Norma ISO 31000:2018].
- **Confidencialidad:** Característica que asegura la intimidad y el secreto de la información que se genera en el proceso de atención entre el servidor público y el ciudadano. [Comité Internacional de la Cruz Roja - CICR. Las personas desaparecidas, guía para los parlamentos. Octubre de 2016].
- **Consecuencia:** Resultado de un evento que afecta los objetivos. [Norma ISO 31000:2018].
- **Control:** Medida que mantiene y/o modifica el riesgo. [Norma ISO 31000:2018].

- **Controles detectivos:** Diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.
- **Controles preventivos:** Diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a pedido por una entidad autorizada. [Norma ISO 27000:2018].
- **Evaluación del riesgo:** proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable. [Norma ISO 27000:2018].
- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias. [Norma ISO 27000:2018].
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar la organización con relación al riesgo. [Norma NTC-ISO 31000:2018].
- **Identificación del riesgo:** Proceso de encontrar, reconocer y describir riesgos. [Norma ISO 27000:2018].
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo. [Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4, octubre de 2018].
- **Integridad:** Propiedad de precisión e integridad. [Norma ISO 27000:2018].
- **Oficial de Seguridad de la Información Operativo:** Es la persona que ejerce el rol de Líder de Proceso, y es el encargado de implementar y supervisar el cumplimiento de las políticas, lineamientos, directivas, circulares, instrucciones, planes y protocolos de seguridad de la información por parte de los servidores públicos, contratistas o personal delegado de la UBPD de su respectiva dependencia.
- **Probabilidad de ocurrencia:** Posibilidad de que ocurra algo. [Norma NTC-ISO 31000:2018].
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. [Norma NTC-ISO 31000:2018].
- **Riesgo de seguridad de la información:** son todos los eventos o situaciones que atentan contra la integridad, disponibilidad y confidencialidad de la información, en cualquier parte del flujo de la información de la UBPD.
- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. [Guía para la

administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, Versión 4, octubre de 2018].

- **Tratamiento del riesgo:** Proceso para modificar el riesgo. [Norma ISO 27000:2018].
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas. [Norma ISO 27000:2018].

14. BIBLIOGRAFÍA / CIBERGRAFÍA

- Ministerio de Tecnologías de la Información y las Comunicaciones, Guía para la Gestión y Clasificación de Activos de Información, http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf
- Norma Técnica Colombiana NTC-ISO/IEC 27001:2013, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- Guía Técnica Colombiana GTC-ISO/IEC 27002:2013, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas,
- https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316352?_com_liferay_document_library_web_portlet_DLPortlet_INSTANCE_bGsp2IjUBdeu_redirect=https%3A%2F%2Fwww.funcionpublica.gov.co%2Fweb%2Feva%2Fbiblioteca-virtual%2F-%2Fdocument_library%2FbGsp2IjUBdeu%2Fview%2F34316316
- Guía de Orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, Territoriales y Sector Público,
- https://www.urnadecristal.gov.co/sites/default/files/Guia%20para%20la%20orientacio%CC%81n%20de%20la%20GRSD%20en%20el%20Gobierno%20Nacional%20Entes%20Territoriales%20y%20Sector%20Publico..pdf
- Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP),
- https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Riesgos+de+gesti%C3%B3n%2C+corrupci%C3%B3n+y+seguridad+digital+-+Versi%C3%B3n+4+-+Octubre+de+2018.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?download=true
- Decreto N° 1393 del 2 de agosto del 2018 “Por el cual se establece la estructura interna de la Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado (UBPD) y se determinan las funciones de sus dependencias”.
- Decreto Ley N° 589 del 5 de abril del 2017 “Por el cual se organiza la Unidad de Búsqueda de Personas dadas por desaparecidas en el contexto y en razón del conflicto armado”.

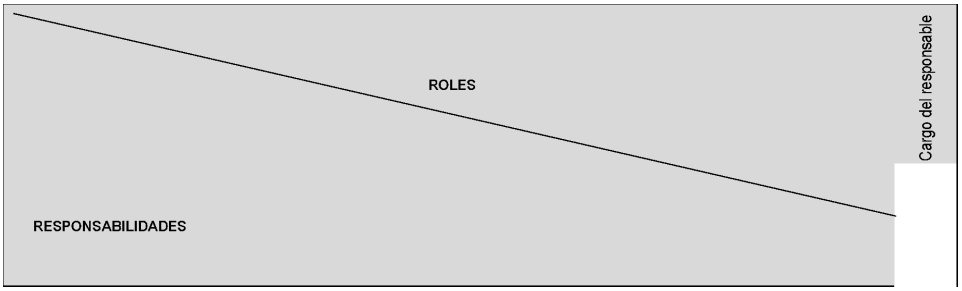
- Resolución N° 537 del 11 de mayo de 2020 “Por medio de la cual se conforma el Comité de Seguridad de la Información de la Unidad de Búsqueda de Personas Desaparecidas en el Contexto y en Razón del Conflicto Armado – UBPD”.
- Resolución N° 588 del 8 de junio de 2020 “Por medio de la cual se establece la estructura y roles del sistema de seguridad de la información (SSI) de la Unidad de Búsqueda de Personas Desaparecidas en el Contexto y en Razón del Conflicto Armado – UBPD”.
- Resolución 1140 de 2021 “Por medio de la cual se adopta la Política de protección y seguridad Digital de la Unidad de Búsqueda de Personas Dadas por Desaparecidas en el Contexto y en Razón del Conflicto Armado-UBPD.
- Resolución 1141 de 2021 “Por medio de la cual se adopta la Política General de Seguridad, Protección y Confidencialidad de la Información de la Unidad de Búsqueda de Personas Dadas por Desaparecidas en el Contexto y en Razón del Conflicto Armado-UBPD.

15. ANEXOS

- Anexo 1. Proceso de Gestión de Seguridad de la Información
    - GSI-CR-001 Caracterización Gestión de Seguridad de la Información

- Anexo 2. Políticas específicas de Seguridad
    - GSI-PC-001 _V1 Política General de Seguridad, Protección y Confidencialidad de la información
    - GSI-PC-002_V1 Política de protección y seguridad digital

- Anexo 3. Procedimientos de Seguridad
    - GSI-PR-001 Procedimiento de Seguimiento al Sistema de Seguridad de la Información
    - GSI-PR-002 Procedimiento de Trabajo en Áreas Seguras
    - GSI-PR-004 Procedimiento de Gestión de Activos de Información
    - GSI-PR-005 Procedimiento de Etiquetado de Información
    - GSI-PR-003 Procedimiento Incidentes de Seguridad Info
    - GTI-PR-002 Procedimiento de Gestión de Cambios
    - GTI-PR-007 Procedimiento de Gestión de Eventos e Incidentes de Seguridad Digital
    - GSI-GU-001 Procedimiento de Gestión de Incidentes de Seguridad de la Información
    -
- Anexo 4. Roles y Responsabilidades - RACI
    - Matriz de Roles y Responsabilidades RACI



- Anexo 5. Indicadores de Seguridad
    - DPE-FT-013 V1_Indicador 01_Campañas Sensibilizacion
    - DPE-FT-013 V1_Indicador 02_Pruebas Vulnerabilidades
    - DPE-FT-013 V1_Indicador 03_Mantenimiento Infraestructura tecnológica
    - DPE-FT-013 V1_Indicador 04_Ingenieria Social
    - DPE-FT-013 V1_Indicador 05_Incidentes de seguridad
    - DPE-FT-013 V1_Indicador 06_Riesgos de Seguridad
    - DPE-FT-013 V1_Indicador 07_Pruebas Restauración de Backups
    - DPE-FT-013 V1_Indicador 08_Politicas de Seguridad
    - DPE-FT-013 V1_Indicador 09_Equipos Antivirus
    - DPE-FT-013 V1_Indicador 10_Gestión de Cambios
    - DPE-FT-013 V1_Indicador 11_Controles Áreas Seguras
    - DPE-FT-013 V1_Indicador 12_Sistemas de Información Seguros
    - DPE-FT-013 V1_Indicador 13_Permisos en Sistemas de Información

- Anexo 6. Seguimiento al SSI
    - GSI-PR-001 Procedimiento Seguimiento SSI