POLÍTICA DE PROTECCIÓN Y SEGURIDAD DIGITAL

1. INTRODUCCIÓN

La Unidad de Búsqueda de Personas dadas por Desaparecidas en el Contexto y en Razón del Conflicto Armado en adelante (UBPD), como entidad de carácter humanitario y extrajudicial funda su mandato en el principio de construcción de confianza, el cual tiene como finalidad garantizar a todas las familias, aportantes, personas y organizaciones que buscan, que la información suministrada a la entidad será tratada bajo el marco de la protección, seguridad y confidencialidad de la información, garantizando que se protegerán sus datos y no serán revelados con el fin de mantener a salvo su integridad y seguridad.

La UBPD partiendo de su carácter humanitario y extrajudicial, así como de su mandato, tiene la responsabilidad de definir políticas, lineamientos, directrices, entre otros instrumentos, que permitan el especial cuidado de la información que está bajo su tutela; en ese sentido, es preciso mencionar que a partir de la adopción de la *Política General de Protección, Seguridad y Confidencialidad de la Información* se fijó la base para conocer los riesgos y las medidas que se deben adoptar, para promover y mantener la seguridad de la información, entre ellas, la mencionada en la "*Línea de Acción N° 2: Seguridad Digital*", mediante el cual la entidad, plantea la necesidad de construir una Política de Protección y Seguridad Digital, que se desarrolla en el presente documento.

Así mismo, es de mencionar que la UBPD hace uso de herramientas y servicios que ofrecen las tecnologías de la información y las comunicaciones, con el fin de facilitar y soportar el flujo de información interna y externa, la comunicación electrónica entre sus servidores y servidoras, contratistas, personal delegado, entidades públicas, sociedad civil y ciudadanía, y, de manera general, en el ejercicio de las diferentes actividades de su quehacer.

El creciente uso de las tecnologías de la información y comunicaciones ha venido acompañado de un progresivo incremento en las acciones, que, al margen de la Ley, suceden en los medios digitales y las cuales pueden poner en situación de riesgo o vulnerabilidad a comunidades, organizaciones públicas y privadas, personas, no solo en lo que concierne a su patrimonio, sino, en su buen nombre, privacidad e incluso integridad física.

Con base en lo expuesto, esa necesidad de diseñar e implementar una Política de Protección y Seguridad Digital, se ve orientada a prevenir, mitigar[1] y gestionar los riesgos y amenazas asociados al uso de los entornos digitales, en pro del aprovechamiento de las tecnologías de la información y comunicaciones como herramienta estratégica para el cumplimiento del especifico mandato institucional.

2. PROBLEMÁTICA

El creciente uso de las plataformas tecnológicas a nivel mundial para conectarse, comunicarse, procesar, intercambiar y almacenar información hace que se incrementen las amenazas cibernéticas y que estás aprovechen las vulnerabilidades de las entidades y las personas para realizar ataques y de este modo, obtener, secuestrar, modificar o destruir la información obedeciendo a fines políticos, financieros, entre otros. En consecuencia, se desarrollan convenios, tratados u otro tipo de acuerdos que permitan la colaboración entre países para construir un entorno digital seguro, una regulación homogénea y mecanismos de prevención y de reacción ante los ciberataques.

[1] Mitigar minimizar el impacto de los riesgos que puedan afectar la seguridad digital de la UBPD

Colombia no es ajeno a este escenario, en los últimos años ha registrado un crecimiento importante en el uso de la tecnología para ejecutar actividades laborales, educativas, culturales, económicas, entre otras, tanto en el sector público como en el sector privado. Lo anterior, ha ocasionado que se incrementen las amenazas en seguridad digital y el número de ciberataques que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información. Una de las vulnerabilidades identificadas por el Estado Colombiano es que los ciudadanos y las entidades públicas no cuentan con las medidas adecuadas y suficientes de seguridad digital[2]. Es por esto, que en Colombia se han establecido espacios que permitan construir políticas, estrategias e iniciativas orientadas al desarrollo, fortalecimiento y generación de capacidades de los diferentes entornos digitales seguros como mecanismo para generar confianza, gestionar adecuadamente las amenazas del entorno digital y mitigar los riesgos asociados a estas.

La UBPD tiene mayor responsabilidad y exposición a las amenazas cibernéticas, no solo por ser una entidad pública que, para el cumplimiento de su mandato realiza la obtención, creación, modificación, almacenamiento, intercambio y disposición final de la información proveniente de entidades del estado, organizaciones de la sociedad civil, defensores de derechos humanos y víctimas o actores del conflicto armado, y los demás que correspondan. La gestión de esta información es soportada con herramientas digitales, las cuales requieren ser protegidas ante las amenazas y riesgos asociados al uso de nuevas tecnologías.

Con base en lo expuesto, es necesario controlar, fortalecer y mejorar el esquema actual de la infraestructura tecnológica, sistemas de información, herramientas digitales, servicios de almacenamiento en la nube, servidores, equipos de cómputo e infraestructura de red y comunicaciones, para obtener un nivel adecuado de seguridad digital que permita proteger la información de las amenazas latentes y facilite el seguimiento, monitoreo y control de los lineamientos establecidos en la Política General de Seguridad, Protección y Confidencialidad de la Información de la UBPD.

2. OBJETIVO GENERAL

Definir los lineamientos y líneas de acción a implementar en la UBPD, con el fin de prevenir y mitigar los riesgos y amenazas inherentes al uso de entornos digitales, como lo son; los sistemas de información, infraestructura, canales de comunicaciones, medios de almacenamiento, y en general, servicios tecnológicos, dispuestos por la Oficina de Tecnologías de la Información y Comunicaciones para soportar la gestión de la UBPD.

3. ÁMBITO Y ALCANCE

La Política de Protección y Seguridad Digital aplicará a todos los mecanismos, dispositivos, sistemas de información, servicios, comunicaciones e infraestructura tecnológica dispuestos por la Oficina de Tecnologías de la Información y las Comunicaciones para soportar la operación de la UBPD, así como, a quienes hagan uso de éstos. La Política de Protección y Seguridad Digital es de estricta observancia por los (las) servidores (as), contratistas o personal delegado de la UBPD, durante todas sus actividades diarias que impliquen la gestión de información, haciendo uso de Tecnologías de la Información y Comunicaciones - TICs. En tal sentido, esta política tiene como marco general la Política General de Seguridad, Protección y Confidencialidad de la Información, abarcando todas las fases de la gestión de información: recolección, transporte, almacenamiento, custodia, preservación, conservación o intercambio.

[2] Adaptado del CONPES 3995

4. MARCO NORMATIVO

El marco normativo que soporta la política de protección y seguridad digital se fundamenta en lo establecido en la normatividad que se relaciona a continuación, de la cual se toman como referencia, entre otros, los componentes aplicables a seguridad digital para el establecimiento de la política de protección y seguridad digital; así mismo, atendiendo a la naturaleza especial y autonomía de la UBPD, es importante resaltar, que algunas normas no son de obligatoria implementación por parte de la Entidad, toda vez que su ámbito de aplicación no cobija a la UBPD, sin embargo, se han identificado las que por su contenido son compatibles con nuestro carácter y la misión, para incluirlas como una buena práctica e implementarlas para el fortalecimiento de la seguridad digital en la entidad.

a) Acto Legislativo 1 de 2017

b) Decreto Ley 589 de 2017

c) Decreto 1393 de 2018, Artículo 7, **Funciones de la Oficina de Tecnologías de la Información y las Comunicaciones, a través del cual se ordena el** desarrollo de estrategias para garantizar la seguridad; Así mismo, definir, actualizar e implementar, el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) en concordancia con la Arquitectura Empresarial y los lineamientos de la Estrategia de Gobierno en Línea (GEL).

d) Resolución N° 537 de 2020, mediante la cual se crea el Comité de Seguridad de la Información. Este comité se crea, debido a que la confidencialidad es el eje fundamental sobre el cual se enmarcan las acciones humanitarias de la UBPD y que de no contar con herramientas que propendan por mantener dicha confidencialidad, se podrían configurar algunos riesgos como no mantener la seguridad, protección y reserva de la información suministrada por los aportantes, las víctimas, las ONGs, entre otros, así como de la información generada o producida por la UBPD.
De este modo, el comité se encarga de evaluar y analizar las necesidades que tiene la entidad en torno a la seguridad de la información y por ende verifica los documentos que buscan fortalecer la seguridad de la información.

e) Resolución N° 588 de 2020, mediante la cual se establece la estructura y roles del sistema de seguridad de la información (SSI).

f) Los Lineamientos de Política para Ciberseguridad y Ciberdefensa establecidos en el Conpes 3701 de 2011, el cual establece las estrategias para enfrentar los riesgos, las amenazas, las vulnerabilidades y los incidentes cibernéticos que pueden infringir la seguridad de las entidades del Estado, así como, el fortalecimiento de las capacidades en seguridad digital, el marco de gobernanza en seguridad digital y la adopción de modelos, estándares y marcos de trabajo de seguridad digital como lo establece el Conpes 3995 Política Nacional de Confianza y Seguridad Digital con el fin de desarrollar la confianza digital a través de la mejora la seguridad digital, serán considerados como marcos de referencia, los cuales atendiendo la autonomía de la UBPD pueden adoptarse siempre y cuando sean acordes con la misionalidad de la entidad.

g) La implementación de medidas de seguridad digital en la infraestructura de la UBPD tomando como referencia las normas emanadas por el NIST (National Institute of Standards and Technology) inherentes a la seguridad de la infraestructura tecnológica la cual nos permite tener una guías ampliamente probadas y estructuradas.

h) Las normas agrupadas dentro de los estándares ISO 27000, ISO 27001, ISO 27002, entre otros establecen la referencia para la implementación de un Sistema de Gestión de Seguridad de la Información en especial el Anexo A de la ISO 27001 donde indica los objetivos de control y controles a nivel de seguridad digital que deben ser implementados para asegurar la información.

i) Estos estándares y buenas prácticas serán la guía en la implementación de controles de seguridad digital y serán considerados de acuerdo con la necesidad específica de la UBPD.

j) Adicionalmente esta política, desarrolla 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*, en particular sobre los lineamientos específicos de seguridad digital, según lo definido en la *Línea de Acción N° 2: Seguridad Digital*, cuyo objetivo reza: *"Establecer lineamientos para la seguridad de la información gestionados a través de la plataforma tecnológica, los servicios tecnológicos y de comunicación de la UBPD"*

5. ELEMENTOS DE LA POLÍTICA

5.1. DECLARACIÓN DE LA POLÍTICA

En cumplimiento de lo establecido en la GSI-PC-001_V1 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, en su línea de acción No 2 Seguridad Digital, cuyo objetivo es "Establecer lineamientos para la seguridad de la información gestionados a través de la plataforma tecnológica, los servicios tecnológicos y de comunicación de la UBPD" y con el fin de desarrollar los lineamientos allí expuestos y otros considerados fundamentales para garantizar la seguridad digital de la UBPD se establece esta política.

Esta política a su vez, se desarrollará mediante la ejecución de estrategias, planes y proyectos que conlleven a implementar o fortalecer los controles de seguridad digital que permitan dar cumplimiento a los principios y líneas de acción establecidas en la misma.

La UBPD, en atención a su naturaleza especial, carácter humanitario y extrajudicial y su deber de construir confianza, utiliza las tecnologías de la información y comunicaciones, en pro de una gestión eficiente y segura, se compromete a afrontar las amenazas y vulnerabilidades inherentes a los entornos digitales, a través de lineamientos y líneas de acción orientadas a proteger y asegurar la información que produce y a la que tiene acceso en el desarrollo de su misión.

Los servidores y servidoras, contratistas y personal delegado de la UBPD acatan y aplican los lineamientos y las líneas de acción de la política de Protección y Seguridad Digital, y los demás que se deriven de ella, para garantizar ambientes digitales seguros; para ello, la UBPD se compromete a incentivar una cultura de uso y apropiación responsable y segura de las Tecnologías de la Información y Comunicaciones.

5.2. PRINCIPIOS

La Política de Protección y Seguridad Digital, se construye y se desarrolla en armonía con los principios que hacen parte de la Política General de Protección, Seguridad y Confidencialidad de la Información; en ese sentido, la UBPD ha creado unos principios específicos que orientaran la gestión adecuada de la seguridad digital, los cuales se enuncian a continuación:

CONCORDANCIA: la UBPD diseña e implementa las soluciones y servicios digitales de conformidad con los principios definidos y establecidos en la Política General de Seguridad, Protección y Confidencialidad de la Información, así como, en las normas que son de aplicación obligatoria por parte de la UBPD, como entidad pública, con el fin de garantizar el uso eficiente y seguro de las TICs.

ACCESO RESTRINGIDO: La Oficina de Tecnologías de la Información y Comunicaciones establece los permisos necesarios para el acceso a los sistemas de información, infraestructura, comunicaciones o servicios tecnológicos para que las servidoras y servidores, contratistas o personal delegado de la UBPD realicen sus actividades. Estos permisos obedecen a características de mínimo acceso, con el fin de evitar el uso indebido de la información confidencial de la UBPD.

MONITOREO PROACTIVO: la UBPD a través de la Oficina de Tecnologías de la Información y Comunicaciones realiza el monitoreo proactivo de los entornos digitales, utilizando herramientas de monitoreo especializadas a fin de detectar, mitigar y controlar el uso adecuado y seguro de los mismos, así como, la transferencia o intercambio de información, sin acceder al contenido propiamente dicho.

AUTENTICIDAD: La Oficina de Tecnologías de la Información y Comunicaciones establece mecanismos y controles que permiten validar la identificación de los servidores y servidoras, contratistas y personal delegado de la UBPD que acceden a los sistemas de información, infraestructura, comunicaciones o servicios tecnológicos a fin de evitar la suplantación de identidades.

TRAZABILIDAD: La Oficina de Tecnologías de la Información y Comunicaciones establece mecanismos que permiten registrar e identificar las acciones realizadas por los servidores y servidoras, contratistas, personal delegado de la UBPD y en especial los usuarios administradores en los sistemas de información, infraestructura, comunicaciones o servicios tecnológicos que se requieran.

NO REPUDIO: La Oficina de Tecnologías de la Información y Comunicaciones establece mecanismos en los servicios tecnológicos, que así lo requieren, para comprobar la identidad de las personas que intervienen en el uso de medios de comunicación para el intercambio de información.

5.3. LÍNEAS DE ACCIÓN DE LA POLÍTICA DE PROTECCIÓN Y SEGURIDAD DIGITAL

Atendiendo a lo planteado en la problemática, los principios y los objetivos definidos en esta política, la UBPD establece los siguientes lineamientos y líneas de acción que permitan materializar esta política.

Así mismo, es necesario mencionar, que si bien, las líneas de acción que a continuación se presentan buscan direccionar el modo de actuar frente al uso de elementos digitales por parte de los servidores, servidoras, contratistas y personal delegado de la UBPD, y que dichos elementos pueden ser aquellos que brinde la entidad o los que son de uso personal por parte de los funcionarios(as), la UBPD se encuentra bajo el estricto deber de garantizar que el acceso a las herramientas digitales, se hará respetando la normatividad nacional e internacional vigente y bajo los límites que establece.

Línea de Acción N° 1: Uso de dispositivos móviles
Objetivo
Mitigar los riesgos y garantizar la protección y seguridad digital de los dispositivos móviles institucionales o personales autorizados para acceder a los servicios tecnológicos dispuestos por la Oficina de Tecnologías de la Información y Comunicaciones de la UBPD.
Lineamientos
A. Los (as) servidores y servidoras, contratistas y personal delegado de la UBPD, que tengan asignados dispositivos móviles institucionales, deben permitir la instalación y configuración del software que se establezca como necesario para proteger los dispositivos móviles y así mitigar pérdidas o fugas de información. B. El uso de dispositivos móviles personales de los(as) servidores y servidoras, contratistas y personal delegado de la UBPD, debe ser solicitado por el Jefe o la Jefa de la dependencia con la justificación de uso. Esta solicitud se debe realizar por medio de los canales establecidos y deberá contar con la aprobación de la Oficina de Tecnologías de la Información y Comunicaciones. C. La instalación, configuración, mantenimiento preventivo y correctivo, de los dispositivos móviles, propiedad de la UBPD, estará a cargo de la Oficina de Tecnologías de la Información y Comunicaciones quién atenderá las solicitudes o programará los mantenimientos a través de la mesa de servicio. D. La instalación de software y cambios de configuración en los dispositivos móviles de propiedad de la UBPD debe ser autorizada y coordinada por la Oficina de Tecnologías de la Información y Comunicaciones. E. Cuando el dispositivo móvil de propiedad de la UBPD o los que sean autorizados para acceder a la información, o los sistemas de información sean perdidos, hurtados o se considere que se ha comprometido la seguridad de éste, se debe notificar a la mesa de servicios de manera inmediata directamente o por intermedio del Jefe de la dependencia, para proceder a retirar los accesos y realizar el borrado de la información de ser posible y comunicar al (la) Oficial de Seguridad de la Información. F. Los dispositivos móviles propiedad de la UBPD y que sean asignados a sus servidores y servidoras, contratistas y personal delegado deben cumplir como mínimo con las siguientes condiciones de seguridad: a. Control de acceso al usuario mediante contraseña o reconocimiento de huella. b. Tener instalada y actualizada la herramienta de antivirus que defina la Oficina de Tecnologías de la Información y Comunicaciones. G. Los dispositivos móviles que no sean propiedad de la UBPD y que estén autorizados para acceder a la información, los sistemas de información o los servicios, deben contar como mínimo con las siguientes condiciones de seguridad: a. Control de acceso al usuario mediante contraseña o reconocimiento de huella. b. Tener instalada y actualizada una herramienta de antivirus. c. Perfil independiente para el tratamiento de la información de la UBPD. H. Permitir a la UBPD utilizar mecanismos para la ubicación, cifrado, bloqueo, borrado remoto y el retiro de acceso a los sistemas de información o información cuando el dispositivo haya sido robado, extraviado o esté comprometida su seguridad.
Responsables
● Oficina de Tecnologías de la Información y Comunicaciones ● Servidoras, servidores y contratistas.

Línea de Acción N° 2: Pantallas Bloqueadas
Objetivo
Evitar el acceso a computadores de escritorio y portátiles, por personas no autorizadas, en el momento en que se encuentren desatendidos.
Lineamientos
A. El bloqueo automático de la pantalla y la ejecución del protector de pantalla en los equipos de la UBPD después de un tiempo determinado de inactividad será implementado como control preventivo de intrusión no autorizada a los equipos. La implementación de estos mecanismos preventivos estará a cargo de la Oficina de Tecnologías de la Información y Comunicaciones. B. El personal (servidor y servidoras públicas, contratistas o personal delegado), que tiene asignado para su trabajo computadores de escritorio y/o portátiles debe bloquear o apagar, cuando se ausente de su puesto de trabajo o al finalizar la jornada laboral. C. El escritorio de los computadores no se debe utilizar para almacenar ningún tipo de archivo, excepto los accesos que se configuren desde la Mesa de Servicio. D. Todos los equipos de cómputo y dispositivos de impresión y digitalización deben apagarse cuando no estén en uso.
Responsables
● Oficina de Tecnologías de la Información y Comunicaciones ● Servidoras, servidores y contratistas.

Línea de Acción N° 3: Controles de Acceso
Objetivo
Asegurar el acceso controlado y lógico a los sistemas de información, plataforma tecnológica, servicios de red e instalaciones de procesamiento de información que administra la Oficina de Tecnologías de la Información y Comunicaciones.
Lineamientos
A. Los controles y permisos para el acceso a la información, sistemas de información, plataforma tecnológica y servicios de red serán establecidos de acuerdo con la clasificación de la información, las funciones u obligaciones de los servidores y servidoras públicos, contratistas y personal delegado, según corresponda, las necesidades y requerimientos de cada una de las áreas de la UBPD de Búsqueda de Personas dadas por Desaparecidas y las líneas de acción orientados a garantizar la protección y seguridad de la Información. B. Es responsabilidad de los líderes de procesos realizar el análisis de las necesidades y restricciones requeridas por sus servidores y servidoras públicas, contratistas y personal delegado para solicitar la asignación de accesos lógicos a la Dirección Técnica de Información, Planeación y Localización para la Búsqueda.

C. Los accesos a la información en formato digital, sistemas de información, plataforma tecnológica y servicios de red serán gestionados mediante la asignación de un usuario único para cada servidor o servidora pública, contratistas o personal delegado de acuerdo con su perfil y los accesos necesarios para el cumplimiento de sus funciones u obligaciones, este usuario es intransferible y es responsabilidad del servidor o servidora pública, contratistas o personal delegado las acciones que se ejecuten con éste.

D. Los accesos lógicos, asignados a los servidores y servidoras públicas, contratistas y personal delegado deben ser desactivados una vez se terminen los vínculos contractuales con la UBPD , por solicitud del supervisor del contrato, director, subdirector, jefe o por la Dirección Técnica de Información, Planeación y Localización para la Búsqueda. La desactivación se debe realizar a más tardar al siguiente día hábil después de la terminación del vínculo laboral, contractual o de la recepción de la solicitud.

E. El acceso a las instalaciones de procesamiento de información responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones debe ser restringido y contar con los controles suficientes que permitan mitigar el acceso no autorizado, la fuga de información o la salida no autorizada de activos de información.

F. Las actividades de tipo remoto que se realicen fuera de las instalaciones de la UBPD deben contar con la debida autorización y coordinación de la Oficina de Tecnologías de la Información y las Comunicaciones y también deberán ser informados al (la) Oficial de Seguridad de la Información. Para los accesos autorizados o de administración de configuración se deberá establecer el periodo de tiempo de conexión y se deberá realizar mediante las herramientas definidas por la Oficina de Tecnologías de la Información y las Comunicaciones las cuales deben permitir el registro de las actividades realizadas durante el tiempo de conexión remota.

G. La conexión de dispositivos de infraestructura a la red de la UBPD debe ser coordinada con la Oficina de Tecnologías de la Información y las Comunicaciones a través de la herramienta de mesa de servicio.

H. La creación, modificación, des-habilitación o retiro de usuarios en los sistemas de información o servicios de red se realiza de acuerdo con el o los procedimientos definidos en la Oficina de Tecnologías de la Información y las Comunicaciones.

I. Ante cualquier sospecha de que el usuario asignado para el ingreso a cualquiera de las herramientas tecnológicas o sistemas de información de la entidad ha sido utilizado de manera inadecuada, debe informarse inmediatamente a la Oficina de Tecnologías de la Información y Comunicaciones, registrando un caso en la mesa de servicios. El caso será asignado al Experto Técnico responsable de Seguridad Digital quién se encargará de informar al jefe del área y a el (a) Oficial de Seguridad de la Información.

J. La Oficina de Tecnologías de la Información y Comunicaciones, podrá utilizar mecanismos de doble factor de autenticación (Ej: envío de un código al teléfono celular) para los servicios o sistemas de información donde sea requerido un mayor nivel de protección en el acceso.

K. Todos los servicios digitales deben manejar un código o contraseña de acceso para los servidores y servidoras, contratistas y personal delegado de la UBPD.

Responsables
● Líderes de Proceso ● Oficina de Tecnologías de la Información y Comunicaciones ● Servidoras, servidores y contratistas.

Línea de Acción N° 4: Controles de Uso de Internet
Objetivo
Controlar el uso adecuado del internet y servicios relacionados mitigando los riesgos asociados al uso de este. A. El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas propias de la función desarrollada en cada una de las dependencias de la UBPD. B. La Oficina de Tecnologías de la Información y las Comunicaciones implementará las restricciones necesarias, de acuerdo con los perfiles de uso que se establezcan entre la Oficina de Tecnologías de la Información y Comunicaciones, el (la) Oficial de Seguridad de la Información y la Dirección Técnica de Información, Planeación y Localización para la Búsqueda. Lo anterior, con el fin de mitigar los riesgos inherentes al uso de internet, que incrementan los riesgos y vulnerabilidades de la información. C. Los usos diferentes a los necesarios para el cumplimiento de las funciones de la entidad son de entera responsabilidad de los servidores y servidoras, contratistas y personal delegado de la UBPD al que se le asigna la cuenta de acceso al servicio y el uso no adecuado se considera una violación a la política de protección y seguridad digital. La Oficina de Tecnologías de la Información y Comunicaciones debe implementar los mecanismos necesarios que soporten el uso seguro de internet haciendo uso de herramientas especializadas, que permitan analizar y registrar de manera detallada el tráfico desde y hacia la entidad, si así se requiere, esto sin vulnerar el derecho a la intimidad y privacidad de los servidores y servidoras, contratistas y personal delegado. D. Los servidores y servidoras, contratistas y personal delegado no podrán utilizar el servicio de internet para el envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones, o que esté protegida por derechos de autor, el uso del servicio para actividades comerciales particulares, el acceso a sitios de entretenimiento online, el acceso a sitios Web considerados como ilegales por la normatividad colombiana, incluidos en la Ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia. E. La Oficina de Tecnologías de la Información y las Comunicaciones definirá el navegador que será utilizado por los servidores y servidoras y contratistas en los computadores de la entidad, así como, los controles que permitan garantizar una utilización segura del servicio.
Responsables
● Líderes de Proceso ● Oficina de Tecnologías de la Información y Comunicaciones ● Servidoras, servidores y contratistas.

Línea de Acción N° 5: Control Copias de Seguridad
Objetivo
Establecer los lineamientos generales para la realización, almacenamiento y recuperación de las copias de seguridad de la información de la UBPD.

Lineamientos
A. La Oficina de Tecnologías de Información en coordinación con los propietarios de la información define los activos de información y prioridad para efectuar respaldos, teniendo en cuenta entre otros: a. Sistemas Operativos b. Máquinas Virtuales c. Configuración de equipos activos d. Aplicativos e. Bases de datos f. Repositorios Compartidos g. Datos de usuario h. Correos electrónicos B. La periodicidad de ejecución de las copias de respaldo se establece con base en el activo, el tipo de backup, el tipo de activo a respaldar, el tamaño, el tiempo objetivo de recuperación y punto objetivo de recuperación. Estos deben quedar especificados en el procedimiento de copias de respaldo. C. Se debe establecer un plan para realizar restauraciones periódicas de la data o parte de ella, con el fin de verificar la posibilidad de restauración a partir de las copias de respaldo.
Responsables
● Líderes de Proceso o Jefes de Área ● Oficina de Tecnologías de la Información y Comunicaciones ● Servidoras, servidores y contratistas.

Línea de Acción N° 6: Desarrollo Seguro
Objetivo
Establecer los lineamientos que permitan garantizar el diseño y la implementación de la seguridad en todas las fases del ciclo de vida en el desarrollo de software y sistemas de información.
Lineamientos
A. Todos los (las)servidores, servidoras y contratistas que realicen actividades del ciclo de vida de desarrollo de software, deben tener entrenamiento básico en seguridad de la información y privacidad, y deben conocer las políticas de protección, seguridad y confidencialidad de la información de la UBPD . B. La especificación de los requisitos de seguridad de la información para nuevos desarrollos de software y sistemas de información se deben realizar en la etapa de levantamiento de requerimientos, estos serán identificados de acuerdo a los protocolos, guías o líneas de acción establecidos en la Política General de Seguridad, Protección y Confidencialidad de la Información y en esta Política.

C. Los requerimientos de seguridad de la información identificados, deben considerar los posibles riesgos, a fin de establecer los mecanismos de seguridad digital, que apliquen para el caso de: software a la medida, software de terceros o desarrollos propios.

D. Durante el desarrollo del código y para los software o sistemas de información que sean aplicables y se haya identificado en la especificación de requisitos, se deben establecer revisiones de código estático, permitiendo tener un mejor nivel de seguridad, evidenciando tempranamente problemas del software o sistema de información.

E. Los contratos establecidos para el desarrollo de software por parte de contratistas de la UBPD o contratados con terceros deben especificar los acuerdos sobre propiedad, entrega y custodia del código fuente y sus respectivas versiones, documentación técnica y de uso del software o sistema de información, derechos de propiedad intelectual, soportes del desarrollo de las actividades establecidas en la presente política.

F. El software desarrollado por servidoras o servidores de la UBPD , en el ejercicio de sus funciones, se entiende propiedad de la UBPD y éste deberá ser documentado, almacenado y controlado de acuerdo a los procedimientos establecidos en el Proceso de Gestión de Tecnologías de la Información y Comunicaciones.

G. Una vez concluido el desarrollo del software o sistema de información se deben ejecutar pruebas de seguridad que permitan establecer el cumplimiento de los requisitos de seguridad identificados, la eficacia de los controles implementados para los posibles riesgos, y la búsqueda de posibles vulnerabilidades.

Responsables

- Oficina de Tecnologías de la Información y Comunicaciones
- Servidoras, servidores y contratistas.

Línea de Acción N° 7: Relación con Proveedores y terceros

Objetivo

Establecer las medidas de seguridad para los activos de información de la UBPD a los que pueden acceder los proveedores, a través de la adopción de controles que minimicen la violación de la confidencialidad, integridad y disponibilidad.

Lineamientos

A. Dentro de los acuerdos, contratos o convenios firmados entre la UBPD y los proveedores se deben definir claramente los requerimientos de seguridad y protección digital.

B. La Oficina de Tecnologías de la Información y las Comunicaciones es responsable de incluir en los contratos, condiciones en las cuales se establezcan y acuerden los requisitos de seguridad de protección y seguridad digital relacionadas con el bien o servicio a contratar.

C. Para el otorgamiento a un proveedor, del acceso a los activos de información de la UBPD, se debe tener en cuenta el nivel de clasificación del activo de información al cual se concederá el acceso, administración, uso o tratamiento para establecer los controles de seguridad apropiados; esto, previo a la firma del Acuerdo de Confidencialidad y demás requisitos que considere la Política General de Seguridad, Protección y Confidencialidad de la Información.

D. Los proveedores deben conocer y cumplir las políticas, procedimientos, líneas de acción y demás directrices relacionadas a la protección y seguridad digital de la UBPD que sea inherente a la actividad que va a realizar.

Responsables

- Oficina de Tecnologías de la Información y Comunicaciones
- Proveedores y terceros

Línea de Acción N° 8: Protección y Seguridad Digital para el Intercambio de Información

Objetivo

Establecer las medidas necesarias y suficientes que garanticen el intercambio de información de forma segura a través de entornos tecnológicos.

Lineamientos

A. La Oficina de Tecnologías de la Información y las Comunicaciones establece los estándares tecnológicos de los canales o medios autorizados para el intercambio de información en formato electrónico.

B. La Oficina de Tecnologías de la Información y las Comunicaciones diseña e implementa los controles necesarios para proteger el intercambio de información a través de los servicios digitales (correo, vpn, USB y discos cifrados) contra interceptación, copiado, modificación, enrutado y destrucción.

C. La Oficina de Tecnologías de la Información y las Comunicaciones diseña e implementa los controles necesarios en el servicio de correo electrónico para proteger la información comunicada por este medio.

D. La Oficina de Tecnologías de la Información y las Comunicaciones establece las herramientas para el uso de técnicas criptográficas, en canales de comunicación, servidores, sistemas de información, dispositivos de almacenamiento externo.

E. Los acuerdos de intercambio de información con otras entidades, organizaciones o sociedad civil, que sean gestionados por las diferentes áreas de la UBPD, deberán incorporar en el acuerdo, los estándares tecnológicos establecidos para el intercambio seguro de información.

Responsables

- Oficina de Tecnologías de la Información y Comunicaciones
- Área responsable de gestionar el Convenio o Acuerdo
- Proveedores y terceros

Línea de Acción N° 9: Servicios en la Nube
Objetivo
Establecer las medidas de seguridad digital para los sistemas de información, servicios e infraestructura, de los que hace uso la UBPD , que se encuentren alojados en plataformas de computación en la nube.
Lineamientos
A. Para seleccionar el uso de servicios en la nube, se deben identificar y valorar los riesgos asociados a dicho servicio, según la información a gestionarse y clasificación de los activos de información de la UBPD. B. Establecer las responsabilidades tanto del proveedor del servicio como de la Oficina de Tecnologías de la Información y las Comunicaciones y del área o proceso que hacen uso del servicio, cuando sea necesario. C. El acceso y uso de los servicios, información o sistemas de información en la nube debe ser acorde a las políticas de protección y seguridad digital. D. La Oficina de Tecnologías de la Información y las Comunicaciones es responsable de establecer los medios de acceso, los dispositivos que tienen acceso, las ubicaciones desde las cuales se puede acceder a los servicios en la nube.
Responsables
● Oficina de Tecnologías de la Información y Comunicaciones ● Líderes de Proceso o Jefes de Área. ● Proveedores y terceros

Línea de Acción N° 10: Uso de Dispositivos de Almacenamiento Externos
Objetivo
Establecer las medidas de protección de los computadores y medios de almacenamiento externos (Memorias USB, Discos duros, Unidades de CD, Memorias MicroSD, entre otros), institucionales o personales autorizados en el desarrollo de las funciones de las diferentes áreas de la UBPD.
Lineamientos
A. Los servidores y servidoras públicas, contratistas y personal delegado de la UBPD para hacer uso de medios de almacenamiento externos (asignados por la entidad o externos) en los computadores portátiles o de escritorio dispuestos por la Oficina de Tecnologías de la Información y Comunicaciones, deben aplicar las líneas de acción, mecanismos, estándares y controles establecidos en los protocolos, guías o líneas de acción enfocados a proteger y asegurar los computadores portátiles o de escritorio. B. El uso de dispositivos de almacenamiento externo personales de los(as) servidores y servidoras, contratistas y personal delegado de la UBPD, debe ser solicitado por el Jefe o la Jefa de la dependencia con la justificación de uso. Esta solicitud debe realizarse por medio de los canales establecidos, deberá contar con la aprobación de la Oficina de Tecnologías de la Información y Comunicaciones.

C. Los servidores y servidoras públicos, contratistas y personal delegado de la UBPD, que tengan asignados dispositivos de almacenamiento externo o de uso personal que han sido utilizados en equipos de cómputo fuera de la entidad, deben informar y permitir el análisis con herramientas de prevención dispuestas por la Oficina de Tecnologías de la Información y Comunicaciones para identificar posibles amenazas y así reducir daños, pérdidas o fugas de información o a la infraestructura tecnológica de la UBPD.

D. La instalación, configuración y activación de dispositivos de almacenamiento externo (asignados o personales), estará a cargo de la Oficina de Tecnologías de la Información y Comunicaciones, previa autorización del jefe de la dependencia, las solicitudes se atenderán a través de la mesa de servicio y se comunicara (al) o (la) Oficial de Seguridad de la Información.

E. Los (as) jefes (as) de las dependencias de la entidad analizarán y viabilizarán los permisos que deban ser asignados a los servidores y servidoras públicos, contratistas y personal delegado de la UBPD para el cumplimiento de las actividades asociadas a cada dependencia.
F. La Oficina de Tecnologías de la Información y Comunicaciones implementará las restricciones o mecanismos necesarios para llevar trazabilidad y control de los medios de almacenamiento externos (asignados o personales) conectados a los computadores portátiles o de escritorio propiedad de la UBPD, de acuerdo a los perfiles establecidos y los protocolos, guías o líneas de acción, lo cual se comunicará y pondrá en conocimiento del o (la) Oficial de Seguridad de la Información.

G. Los servidores y servidoras públicas, contratistas y personal delegado de la UBPD, deben velar porque los medios de almacenamiento externos propiedad de la UBPD sean utilizados y conectados únicamente en los equipos autorizados por la entidad.

Responsables

- Oficina de Tecnologías de la Información y Comunicaciones
- Líderes de Proceso o Jefes de Área.
- Servidoras, servidores y contratistas

Línea de Acción N° 11: Uso de Correo Electrónico

Objetivo

Establecer las medidas para el uso seguro del servicio de correo electrónico.

Lineamientos

A. El servicio de correo electrónico debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la UBPD. Los usos diferentes a los necesarios para el cumplimiento de las funciones de la entidad se consideran una violación a la política de protección y seguridad digital por parte de los servidores y servidoras, contratistas o del personal delegado de la UBPD al que se le asigna la cuenta de correo electrónico.

B. El envío de correos masivos está limitado a cuentas de correo asignadas por la Oficina de Tecnologías de la Información y las Comunicaciones para esta labor.

C. El servicio de correo electrónico oficial de la UBPD es el establecido por la Oficina de Tecnologías de la Información y las Comunicaciones. Los servidores y servidoras, contratistas y personal delegado de la UBPD, que utilicen otras cuentas de correo para la gestión de sus labores en la UBPD, reconoce y acepta que los incidentes de seguridad de la información generados por el uso de servicios de cuentas de correo electrónico no autorizadas, serán de su entera responsabilidad y serán considerados una violación a la política de protección y seguridad digital

D. La Oficina de Tecnologías de la Información y las Comunicaciones podrá restringir el acceso a plataformas de correo distintas a la plataforma oficial de correo de la UBPD, a fin de mitigar los riesgos de fuga o pérdida de información y descarga de software malicioso.
E. La Oficina de Tecnologías de la Información y las Comunicaciones se reserva el derecho de filtrar, de manera automática, los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán analizados por las herramientas de protección definidas para tal fin.

F. La configuración de acceso a la cuenta de correo desde medios distintos a los asignados por la UBPD debe ser autorizada y coordinada con Oficina de Tecnologías de la Información y las Comunicaciones.

G. No se debe usar el servicio de correo electrónico de la UBPD para el envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, que promuevan la discriminación sobre la base de raza, color, pertenencia étnica, origen nacional o social, género, edad, estado marital, orientación sexual, religión o discapacidad, opiniones políticas o de otra índole, posición económica, nacimiento o cualquier otra condición social, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales o cualquier contenido que represente riesgos para la seguridad de la información.

Responsables

- Oficina de Tecnologías de la Información y Comunicaciones
- Líderes de Proceso o Jefes de Área.
- Servidoras, servidores y contratistas

Línea de Acción N° 12: cultura de uso seguro de los entornos digitales

Objetivo

Establecer e implementar estrategias de sensibilización en seguridad digital para los (as) servidores y servidoras públicas, contratistas y personal delegado de la UBPD.

Lineamientos
A. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) diseña y desarrolla anualmente el Plan de Sensibilización y Concientización donde se establecen los temas que se deben comunicar, los temas de sensibilización, los responsables, herramientas, público objetivo y el cronograma para la ejecución de estas actividades, con el fin de realizar la divulgación de los lineamientos, procesos, procedimientos y controles que se establezcan y el fomento del comportamiento responsable y seguro en los entornos digitales. B. Los servidores, servidoras, contratistas y delegados de la UBPD deben participar activamente en las distintas actividades establecidas en el Plan de Sensibilización y Concientización de Seguridad Digital, con el fin de mantenerse informado y fortalecer los conocimientos y habilidades para responder ante posibles amenazas digitales.
Responsables
● Oficina de Tecnologías de la Información y Comunicaciones ● Líderes de Proceso o Jefes de Área. ● Servidoras, servidores y contratistas

Línea de Acción N° 13: Respuesta a Incidentes de Seguridad Digital
Objetivo
Gestionar adecuadamente los incidentes de seguridad digital que se puedan presentar en la UBDP.
Lineamientos
A. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) realiza Análisis de vulnerabilidades y pruebas de seguridad orientadas a los Sistemas de Información, Infraestructura y Servicios, así como pruebas de Ingeniería Social a Personas, con el fin de establecer brechas de seguridad que permitan la materialización de los riesgos de seguridad digital. B. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) informa a la Dirección General, al (la) Oficial de Seguridad de la Información y/o al Comité de Seguridad de la Información, las vulnerabilidades, riesgos o incidentes de seguridad que se hayan presentado o se estén presentando, que impidan la continuidad de los servicios tecnológicos y/o la confidencialidad o integridad de la información afectando la operación normal de la Entidad De acuerdo al nivel de criticidad resultante de la valoración del incidente. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) realiza la gestión permanente de los accesos lógicos de los usuarios asignados a los servidores y servidoras, contratistas y personal delegado, realizando la habilitación o desactivación de acuerdo al tiempo que tiene un vínculo con la UBPD, con el fin de prevenir el mantener activos a usuarios que ya no tienen vínculo con la UBPD. C. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) administra proactiva y correctivamente los entornos digitales, con el fin de proteger y asegurar los sistemas de información, herramientas, hardware y software dispuestos para la operación segura de la UBPD.

D. La Oficina de Tecnologías de la Información y las Comunicaciones realiza la aplicación de medidas o controles de seguridad digital requeridos por la Dirección General en pro del cumplimiento misional de la UBPD, así como, del Comité de Seguridad de la Información.

E. Los servidores, servidoras, contratistas y delegados de la UBPD deben reportar los eventos o incidentes de seguridad de la información, que se hayan presentado haciendo uso de medios digitales, de forma inmediata a su identificación o sospecha.

Responsables

- Oficina de Tecnologías de la Información y Comunicaciones
- Líderes de Proceso o Jefes de Área.
- Servidoras, servidores y contratistas

Línea de Acción N° 14: Fortalecimiento de la Infraestructura de Seguridad Digital

Objetivo

Implementar herramientas tecnológicas que permitan gestionar controles preventivos y detectivos para mitigar los riesgos de seguridad digital.

Lineamientos

A. La OTIC evalúa la necesidad de adquirir, implementar o actualizar las herramientas que permitan gestionar de manera adecuada los controles de seguridad digital.

B. Los (as) servidores y servidoras, contratistas y personal delegado deben usar las herramientas de seguridad digital implementadas o autorizadas por la OTIC.

C. La OTIC diseña e implementa el Plan de Recuperación de Desastres orientado al restablecimiento de los sistemas, servicios, comunicaciones e infraestructura tecnológica de la UBPD, que le permitan continuar con su funcionamiento en caso de presentarse un incidente que amerite su ejecución.

Responsables

- Oficina de Tecnologías de la Información y Comunicaciones
- Líderes de Proceso o Jefes de Área.
- Servidoras, servidores y contratistas

Línea de Acción N° 15: Control para el Trabajo Remoto Seguro

Objetivo

Establecer las medidas mínimas de seguridad digital para realizar el trabajo remoto.

Lineamientos
A. Los (as) servidores, servidoras, contratistas y personal delegado deben cumplir con todos los lineamientos y líneas de acción establecidas en esta política aun cuando se esté realizando trabajo remoto. B. Cuando sea posible la conexión remota a los Sistemas de Información de la UBPD debe realizarse mediante VPN. C. Los computadores o dispositivos móviles personales usados para realizar trabajo remoto deben contar con antivirus activado y actualizado, Sistema Operativo actualizado y licenciamiento del software instalado. D. Los computadores o dispositivos móviles personales deben usar un perfil de usuario diferente al utilizado para las actividades personales. E. En los computadores o dispositivos móviles usados para realizar trabajo remoto no se debe realizar guardado de usuarios y contraseñas para conexión a los sistemas de información, correo electrónico, almacenamiento en nube entre otros.
Responsables
● Oficina de Tecnologías de la Información y Comunicaciones ● Servidoras, servidores y contratistas

Línea de Acción N° 16: Seguimiento y Evaluación al Cumplimiento de la Política de Seguridad Digital
Objetivo
Establecer los mecanismos de seguimiento y monitoreo de la eficacia en la implementación y ejecución de controles derivados de los lineamientos y líneas de acción de esta política.
Lineamientos
A. La Oficina de Tecnologías de la Información y las Comunicaciones y el (la) Oficial de Seguridad de la Información realizarán el seguimiento a la implementación de esta política, al menos, una vez al año. Esto con el fin de analizar y considerar las distintas dinámicas que se presenten en la entidad, a su vez coordinará en caso de requerirse su actualización. B. El Comité de Seguridad de la Información realizará seguimiento o requerirá informes del estado de implementación de la política. C. La evaluación del cumplimiento de las acciones propuestas en la política se realizará mediante: a. Seguimiento de efectividad de los controles. b. Resultado de metas de indicadores c. Seguimiento al Modelo de seguridad digital y al plan anual de seguridad digital d. Seguimiento a las estrategias de sensibilización y concientización. e. Revisión y resultados de la revisión por la dirección. f. Seguimiento a resultados de auditorías internas y/o externas.

Responsables
● Oficina de Tecnologías de la Información y Comunicaciones ● Oficial de Seguridad de la Información ● Comité de Seguridad de la Información ● Directivos y Jefes de Oficina ● Oficina Asesora de Planeación ● Oficina de Control Interno

5.4. MANEJO DE DESVIACIONES Y EXCEPCIONES

Las desviaciones y excepciones que sean necesarias en la Gestión de Protección y Seguridad Digital, serán manejadas teniendo en cuenta niveles aceptables de racionalidad, proporcionalidad y necesidad en el tratamiento de la información tanto a nivel interno como la que se obtenga o transfiera con otras entidades; así mismo se entiende que su manejo no podrá ejecutarse sobrepasando la normatividad que regula la materia, ni los principios y directrices establecidas en la Política General de Protección, Seguridad y Confidencialidad de la Información.

Las excepciones a las políticas, procedimientos y controles en la Gestión de Protección y Seguridad Digital deben ser evaluadas por la Oficina de Tecnologías de la Información y Comunicaciones y el (la) Oficial de Seguridad de la Información, teniendo en cuenta:

a. El evento que genera la excepción.

b. Los posibles riesgos que puedan presentarse con la excepción.

c. El posible impacto que pueda generar la excepción.

d. Las acciones para el manejo de la excepción.

De ser necesario, por el impacto que pueda generar en la operación de la UBPD, continuidad de los servicios, y en términos generales en el cumplimiento de la misionalidad, la situación de excepcionalidad deberá ser informada y escalada al Comité de Seguridad de la Información.

6. GLOSARIO

ACTIVO DE INFORMACIÓN: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la entidad.

AMENAZA: Posible causa de un incidente no deseado, que puede producir daño a un sistema u organización.

CIFRADO: Acciones para convertir datos de un formato legible a un formato ilegible, que solo se pueden leer o procesar si se tiene la clave para descifrarlo.

CONTROL: Conjunto de acciones preventivas y correctivas, documentos, políticas, procedimientos o medidas técnicas que permitan gestionar y mitigar el riesgo identificado, las cuales deben ser medibles en cuanto a su eficacia. salvaguarda.

DESVIACIONES Y EXCEPCIONES: Son aquellos casos en los cuales se debe operar de manera distinta a los lineamientos establecidos en la política, sin sobrepasar los límites que establece la norma que regula la materia y sin que se ponga en riesgo la confidencialidad de la información.

DISPOSITIVO O MEDIO DE ALMACENAMIENTO: Activos que se utilizan para almacenar información tales como archivos, carpetas, discos externos, dispositivos USB, entre otros.

DISPOSITIVO MÓVIL: Equipo portátil con capacidad de almacenamiento, procesamiento y conexión a redes, desde el cual se realiza tratamiento de información.

GESTIÓN DE RIESGOS: Son las actividades coordinadas para identificar, analizar y tratar la probabilidad de materialización de un riesgo, el impacto que tendría para la entidad, los controles existentes y las medidas ADICIONALES PARA MITIGARLO.

INCIDENTE DE SEGURIDAD DIGITAL: Un evento o serie de eventos de Seguridad Digital no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información o seguridad digital.

TERCERO: hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.

MITIGAR: Acciones ejecutadas o controles implementados con el fin de disminuir la probabilidad de materialización de un riesgo o el impacto que puede llegar a producir si se materializa el riesgo.

VPN: (Virtual Private Network) - Red Privada Virtual es una conexión a internet de forma segura que permite acceder a los Sistemas de Información, servicios e infraestructura tecnológica de la UBPD sin estar conectado a la red física de la Entidad.

7. VIGENCIA

La presente política rige a partir de su comunicación.

Proyectó:
Victoria Díaz - Jefe Oficina de Tecnologías de la Información y Comunicaciones
Cristian Zanguña - Experto Oficina de Tecnologías de la Información y Comunicaciones
Juan Aponte - Contratista - Oficina de Tecnologías de la Información y Comunicaciones

Revisó:
Nancy Cruz - Jefe Oficina Asesora Jurídica.
Carolina Grajales - Experto Técnico Oficina Asesora Jurídica.
Diana Rincón – Analista Técnico Oficina Asesora Jurídica.
Revisó: Miembros del Comité de Seguridad de la Información en la sesión No. 7 del día 23 de diciembre de 2020.
Aprobó: Luz Marina Monzón Cifuentes –Directora General– Comité de Seguridad de la Información en la sesión No. 7 del día 23 de diciembre de 2020.