Firma de Autorizaciones		
Elaboró	**Revisó**	**Aprobó**
Técnico Operativo Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación	Dirección General IDEP

Control de cambios	
Fecha	**Descripción**
Noviembre de 2018	Creación del documento
Febrero de 2019	Se incluye fecha de aprobación de la política.
Mayo 2019	Se actualiza el alcance y la política de seguridad y privacidad de la información y se incluye como herramienta para su implementación la firma del compromiso de cumplimiento de las políticas TIC del IDEP.
Noviembre 2021	Se reestructura la Política de seguridad y privacidad de la información y se incluye el manejo de la información según las TRD.
Junio 2023	Se actualiza la Política de seguridad y privacidad de la información por el cambio de sede.

1. OBJETIVO GENERAL

El objetivo de este documento es establecer las políticas en seguridad de la información del IDEP, con el fin de regular la gestión de la seguridad de la información, para la debida protección de los derechos de los usuarios, visitantes, ciudadanos y demás personas que suministran sus datos personales a la Entidad por los diferentes canales de atención y medios de recolección de Información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y de sus activos relacionados.

2. OBJETIVOS ESPECÍFICOS

- Establecer y velar por el cumplimiento de los principios mínimos generales definidos en las normas vigentes para preservar y mantener la seguridad y privacidad de la información.

- Identificar y mitigar los riesgos en seguridad y gobierno digital para la entidad, así como minimizar los posibles impactos a los servicios que pudieran ser afectados por incidentes, fallas o vulnerabilidades.

- Proteger los activos de la información institucional, mediante la clasificación de controles de acuerdo con los lineamientos de la norma ISO 27002:2013.

3. ALCANCE

Las políticas de seguridad de la información aplican para todos los procesos del Instituto que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que laboren o tengan relación con el IDEP y la ciudadanía en general.

Igualmente, aplica a todas las bases de datos y archivos de información personal que se encuentren en poder de la Entidad, y que haya sido contemplada por la Ley 1581 de 2012.

4. MARCO LEGAL

- Ley 57 de 1985. Publicidad de los actos y documentos oficiales.
- Ley 527 de 1999. Ley de Comercio Electrónico y Firmas Digitales.
- Ley 594 de 2000. Ley General de Archivos.
- Ley 734 de 2002. Código Único Disciplinario.
- Ley 790 de 2002. Programa de Reforma de la Administración Pública.

- Ley 906 de 2004 Código de Procedimiento Penal.
- Ley 1266 de 2008. Ley de Habeas Data.
- Ley 1273 de 2009. Ley de Delitos Informáticos.
- Ley Estatutaria 1581 de 2012. Protección de datos personales.
- Ley estatutaria 1618 de 2013. Ejercicio pleno de las personas con discapacidad.
- Ley 1712 de 2014. Ley de Transparencia y el Derecho de Acceso a la Información Pública Nacional.
- Decreto 3816 de 2003. Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.
- Decreto 296 de 2008. Comité de Gobierno en Línea a la Comisión Distrital de Sistemas.
- Decreto Nacional 1151 de 2008. Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia.
- Decreto 235 de 2010. Intercambio de información entre entidades para el cumplimiento de funciones públicas.
- Decreto 2364 de 2012. Firma electrónica.
- Decreto 2609 de 2012. Gestión documental (Compilado en el 1080 de 2015, Capítulo III).
- Decreto 2573 de 2014. Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia.
- Decreto 1078 de 2015. Decreto Único Sectorial - Lineamientos generales de la Estrategia de Gobierno en Línea.
- Decreto 103 de 2015. Reglamentación parcial de la Ley 1712 de 2014.
- Acuerdo 279 de 2007 Consejo de Bogotá. Lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital.
- Acuerdo 006 del 15 de octubre de 2014 del Archivo General de la Nación.
- Acuerdo 003 de 2015, Gestión de documentos electrónicos como resultado del uso de medios electrónicos. Archivo General de la Nación.
- Resolución 305 de 2008, de la Comisión Distrital de Sistemas CDS “Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre”.
- Resolución 3564 de 2015 Reglamentaciones asociadas a la Ley de Transparencia y Acceso a la Información Pública. Ministerio de Tecnologías de la Información y las Comunicaciones.
- Directiva 005 de 2005 de la Alcaldía mayor de Bogotá, “Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital”.
- Directiva 011 de 2012 de la Alcaldía Mayor de Bogotá. Promoción y uso de software libre en el Distrito Capital.

- Directiva 002 de 2000. Plan de Acción de la estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las Comunicaciones.
- 4.32. Circular No. 058 de 2009 de la Procuraduría General de la Nación Cumplimiento Decreto 1151 de 2008.
- Circular 10 de 2015, Secretaría General de la Alcaldía Mayor de Bogotá. Metodología para la estandarización de la elaboración y consolidación de informes por entidad u organismo y por sector.
- Circular No. 007 de 2015, Secretaría General de la Alcaldía Mayor de Bogotá. Lineamientos generales para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información.
- Circular No. 001 de 2016, Secretaría General de la Alcaldía Mayor de Bogotá. Consideraciones Circular 001-2016. Entrega de las claves de Ingreso a los sistemas de información por parte de los funcionarios que dejan el cargo.
- Circular 16 2016, Conpes 3854. Ministerio de Tecnologías de la Información y las Comunicaciones. Política nacional de seguridad nacional.
- Circular 17 2016. Medición índice Gobierno en línea.
- Circular 005 de 2012 emitida por el Archivo General de la Nación. Recomendaciones para llevar a cabo procesos de digitalización y comunicaciones oficiales electrónicas en el marco de la iniciativa cero papel.
- Conpes 3248 de 2003 Renovación de la Administración Pública. Ministerio de Tecnologías de la Información y las Comunicaciones.
- Conpes 2790 de 1995 Gestión Pública orientada a resultados. Departamento Nacional de Planeación.
- Conpes 3072 de 2000 Agenda de Conectividad. Ministerio de Tecnologías de la Información y las Comunicaciones.
- Conpes 3854 de 2016, Ministerio de Tecnologías de la Información y las Comunicaciones. Política Nacional de Seguridad Digital.
- Norma NTC-ISO/IEC 27001 de 2013, Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información SGSI. ICONTEC.

5. DEFINICIONES

Acceso: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas del IDEP en un momento dado.

Acceso físico: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio de la entidad.

Acceso lógico: En general, el acceso lógico es un acceso en red, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información.

Activo de Información: Es todo aquello que en la entidad es considerado importante o de alta validez para la misma, ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

Activo de seguridad de la información: Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes como bases de datos, hardware, software, información física o digital, fichas diligenciadas, ítems, edificios, personas etc.) que tenga valor para la organización.

Amenaza: Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Antivirus: Programa especializado en la detección y, si es posible, en el bloqueo y/o eliminación de virus informáticos.

Autenticación: Servicio que permite verificar la identidad de un ciudadano para acceder a trámites y servicios que requieran, a través de medios electrónicos.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Backup: Copia de seguridad de los datos, de tal forma que se pueda restaurar un sistema después de una pérdida de información. Se puede realizar en medios magnéticos, servidores externos y almacenar en un lugar seguro.

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.
Conexión remota: Operación de conectarse a una red o computadora desde un punto remoto, ajeno a esa red, usando la conectividad de redes de Internet y consiguiendo las mismas prestaciones y funciones que si se tratase de una conexión local.
Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
Dato personal: Cualquier información vinculada o que pueda asociarse a una ó varias personas naturales determinadas o determinables.

Carpetas Compartidas: es básicamente igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.

Cifrar: Es el proceso para volver ilegible información considerada importante. Se trata de una medida de seguridad usada para almacenar o transferir información delicada que no debería ser accesible a terceros. La información una vez cifrada sólo puede leerse aplicándole una clave.

Copias de respaldo: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Criptografía: La criptografía es una técnica o conjunto de métodos cuya función es transformar un determinado mensaje o información en otro totalmente distinto ilegible para aquellas personas que no estén autorizadas a leerlo.

Dato: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

Dato público: Es el dato que no sea, semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así come los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por si misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Escritorio limpio: Protección de los papeles y dispositivos removibles de almacenamiento de información, almacenados y manipulados en estaciones de trabajo, de accesos no autorizados, perdida y/o daño de la información.

Estación de trabajo: Área dispuesta por el IDEP para que cada colaborador pueda llevar a cabo sus actividades. Tales como oficinas, escritorios entre otros.

File Server: Es un servidor de archivos que almacena y distribuye diferentes tipos de archivos

informáticos confidenciales o críticos del IDEP.

Guía o Manual: Son esencialmente, recomendaciones que deben considerarse al implementar la política.

Hardware: Es un término genérico para todos los componentes físicos.

Incidente: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Datos relacionados que tienen valor para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada (ISO/IEC 27001:2013)

Información pública: Es toda información que el IDEP genere, obtenga, adquiera, o controle; corresponde a datos que son de acceso público y que por lo tanto no tienen requerimientos frente a la Confidencialidad. Está en esta clasificación la información denominada como "Pública" en la Ley 1712 de 2014 y como "dato público" en el decreto 1377 de 2013.

Información pública clasificada: Es aquella información que estando en poder o custodia del IDEP, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados. Esta corresponde a toda aquella información cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:

A. El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.
B. El derecho de toda persona a la vida, la salud o la seguridad.
C. Los secretos comerciales, industriales y profesionales.

También corresponden a esta categoría los datos que son catalogados como "dato semiprivado o privado" de acuerdo al decreto 1377 de 2013; además de los datos de uso interno de la entidad y que no deben ser conocidos por el público en general. Están en esta clasificación todos los documentos manejados en la operación diaria pero que no tengan el carácter de reservado con base en la ley 1712 de 2014.

Información pública reservada: Es aquella información que estando en poder o custodia del IDEP es exceptuada de acceso a la ciudadanía por daño a intereses públicos. Esta corresponde a aquella información cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional:

A. La defensa y seguridad nacional;

B. La seguridad pública;
C. Las relaciones internacionales;
D. La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso;
E. El debido proceso y la igualdad de las partes en los procesos judiciales;
F. La administración efectiva de la justicia;
G. Los derechos de la infancia y la adolescencia;
H. La estabilidad macroeconómica y financiera del país;
I. La salud pública.

También corresponde a información de carácter reservado los datos catalogados como sensibles por el decreto 1377 de 2013.

Internet: Es una red de computadoras que se encuentran interconectadas a nivel mundial para compartir información. Se trata de una red de equipos de cálculo que se relacionan entre sí a través de la utilización de un lenguaje universal.

Lugar seguro: es aquel que protege el activo de información de acceso de personas no autorizadas, que su contenido no sea alterado y que el activo pueda ser recuperado por las personas autorizadas de manera oportuna (algunos ejemplos: cajón seguro con llave, oficina con llave, etc.)

Log: es un registro oficial de eventos durante un rango de tiempo en particular. Se usa para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

Mejor Práctica: Una regla de seguridad específica o una solución que es aceptada y establecida para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.

Mesa de Ayuda: es el único Centro de Atención al Usuario en donde se presta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servicios TICs en el IDEP.

MSPI: Es el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información – MINTIC.

Nombre del responsable de la producción de la información (propietario): nombre del área, dependencia o unidad interna, o al nombre de la entidad externa que creó la información. Es el responsable del activo, quien debe velar por el cumplimiento de los requerimientos establecidos frente a las propiedades de disponibilidad, confidencialidad e integridad.

Página Web: Una página web es el nombre de un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces y muchas otras cosas, adaptada para la World Wide Web y que puede ser accedida mediante un navegador.

Plan de contingencia: Es un conjunto de procedimientos alternativos a la operatividad normal de cada entidad. Su finalidad es la de permitir el funcionamiento de ésta, aun cuando alguna de sus funciones deje de hacerlo a causa de algún incidente tanto interno como externo a la organización.

Plataforma informática: Es el conjunto de hardware (servidores de bases de datos, servidores de aplicaciones, máquinas de respaldo, equipos de conectividad, etc.), software (framework, aplicaciones empresariales, módulos especializados, servicios, etc.), estándares internacionales, metodologías, servicios entre otros con los que cuenta una organización.

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Programas utilitarios: Hacen referencia a software diseñado para realizar una función determinada. El término utilitario se refiere normalmente al software que resuelve problemas relacionados con la administración del sistema. Algunos ejemplos de software utilitario son: aplicaciones para cifrado y descifrado de archivos, aplicaciones para compresión de archivos, software antivirus, navegadores (Google Chrome, Mozilla Firefox, entre otros) editores de texto, administradores de tareas, aplicaciones para realizar copias de respaldo, entre otros.

Proxy: En una red informática, es un servidor, programa o dispositivo, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C), y este Interviene en la navegación por la web, con distintos fines: seguridad, rendimiento, anonimato entre otros.

Procedimiento: Definen cómo las políticas, estándares, mejores prácticas y guías, serán llevados a cabo en una situación dada.

Responsable de activo de información: Es el nombre del responsable de la información ó custodio: Que corresponde al nombre del área, dependencia o unidad encargada de la custodia, tratamiento y/o control de la información para efectos de permitir su acceso. Es el responsable de administrar y hacer efectivos los controles que el propietario del activo defina con base al análisis de riesgos.

Propietario de activo de información: Es el nombre del responsable de la producción de la información (propietario): Que corresponde al nombre del área, dependencia o unidad interna, o al nombre de la entidad externa que creó la información. Es el responsable del activo, quien debe velar por el cumplimiento de los requerimientos establecidos frente a las propiedades de disponibilidad, confidencialidad e integridad.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Spam: Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

Tercero: Cualquier persona natural o jurídica externa al instituto y que presta algún tipo de servicio o realiza alguna labor para el IDEP.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

URL (localizador de recursos uniforme): Es un identificador de recursos uniforme (Uniform Resource Identifier, URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo. Están formados por una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que designa recursos en una red.

VPN: (Red privada virtual) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. CONDICIONES DE PRIVACIDAD Y TRATAMIENTO DE LOS DATOS PERSONALES.

El usuario, visitante, ciudadano y toda persona que proporciona sus datos personales a la Entidad por cualquier medio, acepta que el ingreso y suministro de su información personal lo hace voluntariamente y ante la necesidad de presentar requerimientos específicos a la Entidad para realizar un trámite, presentar una queja o reclamo, acceder a los mecanismos de interacción que ofrecen los Sitios y/o Aplicativos Web, o para ingresar a las instalaciones dé la misma. Lo que significa que la Entidad podrá recoger tales datos personales.

Los datos personales que recolecta, almacena, usa, circula o suprime, la Entidad en sus bases de datos se utilizarán única y exclusivamente para el desarrollo de sus funciones legales, y no serán cedidos a terceros sin conocimiento del titular de la información.

Asimismo, la Entidad podrá recolectar Información para mejorar la calidad del servicio y generar datos estadísticos en relación con el uso de los Sitios y/o Aplicativos Web, como consecuencia de la navegación y/o registro en los mismos, como el software o- hardware del computador del cual accede el usuario, la dirección IP, tipo de navegador usado para ingresar, nombre del dominio y tiempo de uso.

Teniendo en cuenta que, al ingresar a las instalaciones de la Entidad por asuntos de seguridad, se solicitan datos sensibles a los visitantes, el tratamiento de los mismos solo se llevará a cabo cuando medie autorización expresa por parte del titular para tal fin, la cual no será obligatoria.

El almacenamiento y usó de la información personal se regirá por lo dispuesto en la Ley 1581 de 2012, el Decreto 1377 de 2013, y las demás normas que los modifiquen, adicionen o complementen, teniendo en cuenta el derecho que tienen todas las personas de conocer, actualizar y rectificar la información que la Entidad registre en las bases de datos o archivos susceptibles de tratamiento.

7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección General del IDEP, entendiendo la importancia de una adecuada gestión de la información, se compromete con la implementación de prácticas orientadas a preservar la protección de los activos de información de la Entidad con el fin de minimizar los riesgos por pérdida de confidencialidad, disponibilidad o integridad de la información.

Teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones Según los lineamientos de seguridad de la información estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus funcionarios y contratistas.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios y contratistas del IDEP.
- Garantizar la continuidad del negocio frente a incidentes.
- El IDEP ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen las 12 políticas de seguridad que soportan los lineamientos de seguridad de la información del IDEP:
• El IDEP ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas o terceros.

• El IDEP protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

• El IDEP protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• El IDEP protegerá su información de las amenazas originadas por parte del personal.

• El IDEP protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• El IDEP controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• El IDEP implementará control de acceso a la información, sistemas y recursos de red.

• El IDEP garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• El IDEP garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• El IDEP garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

• El IDEP garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

7.1. CONTROL DE ACCESO

El control de acceso se hace por 2 medios:

7.1.1. Acceso físico

- El acceso al Centro de Datos (Data Center) se hará usando el sistema de reconocimiento de huellas (Biométrico).
- Este acceso queda restringido a las personas que, según su perfil, requieran acceder al centro de datos dado que allá están los servidores, equipos de comunicación, equipos de red al igual que el sistema de control de la alarma de incendios, el sistema de la alarma de la casa y los tableros eléctricos.

7.1.2. Acceso lógico

- Medio lógico a la Red LAN del Instituto a través del registro del funcionario y/o contratista en el Dominio (Directorio Activo) e igualmente el acceso remoto a través de conexión VPN en el Firewall.
- Con el acceso lógico se habilita los permisos a los diferentes activos de

información al que el usuario tenga derecho y para los contratistas los permisos que haya solicitado el supervisor de contrato.

Para la entrega de claves el funcionario y/o contratista debe firmar el formato FT-GT-12-20 Compromiso de cumplimiento de las políticas TIC del IDEP para tal fin y las cuentas se crean según el instructivo IN-GT-12-01 Instructivo para la asignación de usuarios.

Los usuarios deben cumplir con todos los puntos del Compromiso de cumplimiento de las políticas TIC del IDEP.

A través de Talento Humano, se establece el procedimiento de teletrabajo manteniendo los aspectos relacionados con la seguridad y privacidad de la información, dirigido a los tele-trabajadores y aspirantes a esta modalidad en la entidad.

7.2. SEGURIDAD EN LA OPERACIÓN

El Instituto cuenta con herramientas de seguridad como un Firewall y un Antivirus para la protección de la red LAN.

Se socializa a través del correo electrónico los boletines de la CSIRT, los casos de información fraudulenta enviados por correo, sms, chats y se envían campañas de seguridad (Notiseguridad) para informar tips de seguridad.

Se encuentra restringido el acceso de equipos diferentes a los institucionales a la red LAN del IDEP y en caso de requerir acceso debe solicitar la autorización respectiva.

El acceso a la red WiFi del Instituto solo permite navegación y tiene restringido acceso a la red LAN.

Los funcionarios y contratistas deben garantizar que sus equipos de cómputo personales (con los que establece conexión VPN y/o conexión remota) cuenten con sistema operativo licenciado y antivirus para garantizar que la información y productos del IDEP estén salvaguardados ante cualquier amenaza.

Está prohibido instalar software del que no está autorizado por el Instituto y en caso de ser necesario deben pedir autorización para el mismo.

No descargue software ilegal ni ejecute programas maliciosos o espías, o intente hacer daño y/o modificar los sistemas de información o equipos conectados a la red del IDEP.

Los funcionarios y contratistas deben cambiar la contraseña de red cada vez que el sistema lo solicite, cumpliendo los siguientes parámetros: longitud mínima de ocho (8) caracteres combinando letras (Al menos una letra mayúscula), números y símbolos, No usar nombres, apellidos, números de documento de identidad ni la palabra IDEP (En todas sus variaciones), no usar claves que haya usado anteriormente.

Las cuentas de usuario y contraseñas son de uso personal, no comparta las claves de acceso que le fueron entregadas. Todas las operaciones que se realicen con su usuario y contraseña están bajo su responsabilidad.

Para el almacenamiento de la información institucional, debe seguir el IN-GT-12-02 Instructivo para el almacenamiento de la información en carpetas compartidas.

7.3. GESTIÓN DE LA INFORMACIÓN

El IDEP cuenta con las Tablas de Retención Documental, las cuales indican el tipo de clasificación (series, subseries y documentos contenidos) y servirá para subir la información final a la carpeta compartida para este fin y se apoya en el IN-GD-07-04 Instructivo para el almacenamiento de información en carpetas compartidas.

7.4. REALIZACIÓN DE BACKUPS

Los backups se realizan de manera continua según la periodicidad del mismo y que está definido en el manual para la gestión de back up del IDEP.

Las copias de respaldo se guardarán únicamente con el objetivo de restaurar información cuando por situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o por requerimientos legales, sea necesario recuperarla.

8. DOCUMENTOS ASOCIADOS

La presente política de Seguridad y Privacidad de la Información, el IDEP cuenta y se apoya con los siguientes instrumentos que están disponibles en el sitio web del Instituto:

- **Proceso gestión tecnológica:** El objetivo de este proceso es proveer y mantener los recursos de Tecnología de Información y Comunicación necesarios para el funcionamiento del IDEP.
- **PRO-GT-12-05 Procedimiento para el mantenimiento de infraestructura tecnológica:** Este procedimiento indica la forma como el IDEP realiza el mantenimiento de su infraestructura tecnológica y mantiene actualizada la base de datos de los activos de

información de información tipo software, hardware y servicios.

- **PRO-GT-12-08 Procedimiento formulación y seguimiento al PETIC:** El objetivo de este procedimiento es mantener actualizado el PETIC, el cual está dirigido al soporte de los objetivos, planes y estrategias del IDEP en tecnologías de información y comunicación TICs, permitiendo dar continuidad al proceso de actualización y modernización de la gestión.

- **PRO-GT-12-10 Procedimiento mesa de servicios:** El objetivo de este procedimiento es registrar y gestionar las solicitudes de soporte técnico a usuarios y de la infraestructura y servicios de tecnología.

- **IN-GT-12-01 Instructivo para la asignación de usuarios**: Este documento establece los parámetros para la creación de cuenta de usuario en los diferentes medios de procesamiento de información y finaliza con la desactivación de las mismas al momento de desvinculación del funcionario o contratista del Instituto.

- **IN-GT-12-05 Instructivo para cambio de contraseña de ingreso a los sistemas de información del IDEP**: Este documento va dirigido al usuario final de los sistemas de información Goobi y Humano y el objetivo principal es indicar al usuario final la manera en que debe realizar el cambio de contraseña para el ingreso al sistema.

- **FT-GT-12-16 Formato para el control de BackUps y revisión de servidores:** Este documento establece los parámetros para el control de BackUps y revisión de servidores del IDEP.

- **PL-GT-12-01 Plan estratégico de tecnologías de la información y comunicaciones PETIC:** Este documento presenta el contexto general de las tecnologías de la información y comunicaciones al interior del IDEP, identificar las necesidades tecnológicas, identifica las herramientas que permiten el aprovechamiento de los recursos tecnológicos y de inversión, describe las estrategias y proyectos que se ejecutarán en el IDEP en la vigencia, en cumplimiento de sus funciones misionales y de visión propuestos en el Plan Estratégico Institucional.

- **PL-GT-12-02 Plan de Contingencia Tecnológica IDEP:** Este documento presenta el plan que permite garantizar el funcionamiento de la tecnología informática y la recuperación en el menor tiempo posible ante una falla que interrumpa la prestación de los servicios alterando la correcta operación de la entidad.

- **Diagrama de Infraestructura Tecnológica:** Este documento es un diagrama básico de la infraestructura informática del hardware del IDEP.

- **Política de privacidad y tratamiento de datos:** Este documento establece las políticas en seguridad de la información, para la debida protección de los derechos de los usuarios, visitantes, ciudadanos y demás personas que suministran sus datos personales al IDEP

por los diferentes canales de atención y medios de recolección de información. La política fue adoptada mediante Resolución No. 040 de 2017.

- **Manual interno de políticas y procedimientos de protección de datos personales:** El objetivo de este documento es garantizar el adecuado cumplimiento de la Ley 1581 de 2012 y en especial, la atención de consultas y reclamos. Asimismo, dar cumplimiento al Artículo 13 del Decreto 1377 de 2013, en el cual se establece la obligatoriedad por parte de los responsables del tratamiento de datos, de desarrollar sus políticas para el manejo de los datos personales y velar porque los encargados del tratamiento den cabal cumplimiento a las mismas y al Decreto 886 de 2014, que regula lo relacionado al Registro Nacional de Bases de Datos.

- **PL-GT-12-04 Plan seguridad de la información:** Este documento contiene las actividades que el IDEP se compromete a ejecutar en la vigencia, en lo que corresponde a políticas de seguridad de la información, organización de la seguridad de la información, gestión de activos y control de acceso.

- **PL-GT-12-05 Plan tratamiento de riesgos de seguridad de la información:** Este documento contiene las actividades que el IDEP se compromete a ejecutar en la vigencia, en lo que corresponde al tratamiento de riesgos de seguridad de información de acuerdo con el Modelo de seguridad y privacidad de la información.

- **FT-GT-12-20 Compromiso de cumplimiento de las políticas TIC del IDEP:** Este documento los funcionarios y contratistas evidencian mediante su firma su compromiso con el cumplimiento de las normas definidas por el IDEP para minimizar los riesgos de seguridad de la información y optimizar el uso de los recursos tecnológicos del Instituto.

- **MN-GT-12-08 Manual para la gestión de back up del IDEP:** Documento para apoyar el proceso de gestión tecnológica del IDEP, en el momento de realizar los backups de la base de datos, servidores, sistemas de información, página web y micrositios, dominio, firewall, biométrico, antivirus y carpetas institucionales del instituto.