INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMATICO - IDIGER

Resolución Número 549

(Septiembre 21 de 2017)

"Por la cual se adopta el Manual de Políticas de Seguridad de la Información del Instituto Distrital de Gestión de Riesgos y Cambio Climático"

EL DIRECTOR GENERAL DEL INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMATICO - IDIGER
En uso de sus facultades legales y estatutarias, en especial las conferidas el numeral 11 del artículo 7° del Decreto Distrital 173 de 2014 y,

CONSIDERANDO:

Que el artículo 209 de la Constitución Política de Colombia establece que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad.

Que mediante Acuerdo Distrital 122 de 2004, se adoptó el Sistema de Gestión de Calidad creado por la Ley 872 de 2003 *"como una herramienta de gestión sistemática y transparente para dirigir y evaluar el desempeño institucional, en términos de calidad y satisfacción social en la prestación de los servicios a cargo de las entidades y agentes obligados, herramienta que estará enmarcada en los planes estratégicos y de desarrollo de las entidades."*

Que la elaboración del Manual de Políticas de Seguridad y Privacidad de Información para IDGER, hace parte del Modelo de Seguridad y Privacidad de la Infor-

mación de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

Que el Manual de Políticas de Seguridad y Privacidad de Información, cuenta con herramientas que incluyen normas, protocolos y controles a los activos de información, permitiendo hacer una adecuada gestión del riesgo y fortaleciendo la Entidad ante posibles amenazas que afecten la continuidad del negocio, para lo cual se definen los límites del alcance y la declaración de aplicabilidad de acuerdo a la Norma ISO 27001:2013.

Que las leyes números 1266 del 31de diciembre de 2008 "Por lo cual se dictan disposiciones generales del habeas data y se regula el manejo de la información", 1273 del 05 de enero de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones", y 1581 del 17de octubre de 2012 "Por la cual se dictan disposiciones generales para la protección datos personales", y, el Decreto 1377 de 2013 reglamentario de la Ley 1581, así como el Decreto 1078 de 2015 Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones, rigen el tema de la información tanto de las entidades estatales como de las entidades privadas, en lo que les compete...

Que en mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°. Adoptar el Manual de Políticas de Seguridad de la Información del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER, el cual hace parte integral de la presente resolución.

PARÁGRAFO ÚNICO. Los cambios de versión y/o actualizaciones de este Manual se realizarán de conformidad con el control de documentos y registros que se lleva a cabo para el sistema integrado de gestión – SIG de la Entidad, previo concepto favorable del Comité de TIC

ARTÍCULO 2°. La presente Resolución rige a partir de la fecha de su publicación

Dada en Bogotá, D. C., a los veintiún (21) días del mes de septiembre de dos mil diecisiete (2017).

PUBLÍQUESE Y CÚMPLASE.

RICHARD VARGAS HERNÁNDEZ
Director General

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
AMBIENTE
Instituto Distrital de Gestión de Riesgos y Cambio Climático

Manual de Políticas de Seguridad de la Información

ADM-MA-05
Versión 1

Dependencia

Oficina TIC, Dirección General

Objetivo

Establecer dentro del Sistema de Gestión de Seguridad de la Información – SGSI, las políticas, medidas de seguridad y mecanismos de control que permitan proteger, asegurar y garantizar la confidencialidad, autenticidad, integridad, disponibilidad y confiabilidad de los activos de información del IDIGER, alineadas a los objetivos estratégicos de la entidad.

Alcance

Las Políticas de Seguridad de la Información del IDIGER presentadas por este manual, se aplica a todos los activos de información de la entidad, durante su ciclo de vida, incluyendo creación, distribución, trasmisión, almacenamiento y eliminación; Están orientadas a proteger los activos de información en todos los ambientes en los cuales reside y a asegurar que estén sometidos a controles equivalentes para su protección.

Las Políticas de Seguridad de la información son aplicables a la administración de:
La información: Datos almacenados en cualquier medio magnético y físico.
El software: Sistemas operacionales, programas, productos y aplicaciones
El hardware: Equipos de cómputo, telecomunicaciones y redes.
Las Personas: Usuarios y Administradores de la información, ya sean los empleados, contratistas y terceros que prestan servicios a la entidad.
Procesos: Las Políticas y Normas de Seguridad de la información cubren todas las operaciones y funciones que se apoyen en sistemas de información

01/08/2017

1. Introducción

El IDIGER, en cumplimiento de la Política Nacional de Seguridad digital del Ministerio de Tecnologías de la Información y las Comunicaciones contenida en el documento CONPES 3854 aprobada el 11 de abril de 2016, y como un estándar del Distrito y mejores prácticas, define el esquema para garantizar la seguridad y calidad de la información que maneja a través de su canal y medio de distribución de productos y servicios para clientes y usuarios; para ello ha elaborado en este documento de manual de políticas de seguridad de la información, a fin de que sean aplicables por todo el personal de planta y contratistas, que acceden a activos de información de la Entidad, quienes tendrán conocimiento de la importancia de la información y servicios críticos, los riesgos y nuevas amenazas a que están expuestos.

Estas políticas serán divulgadas formalmente a todos los funcionarios y se establecerá mecanismos de seguimiento y control, sobre el conocimiento y aplicación de las mismas.

El Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETIC establece una guía de acción clara y precisa para la administración de las Tecnologías de Información y Comunicaciones del IDIGER, mediante la formulación de estrategias y proyectos que garantizan el apoyo al cumplimiento de sus objetivos y funciones, en línea con el Plan de Desarrollo de la ciudad: mejorar de manera continua sus procesos; con este fin, se gestiona y se mide cada parámetro, lo que permite determinar cuándo una variación puede afectar la producción o los servicios que brindan.

Las políticas incluidas en este Manual se constituyen como parte fundamental para el cumplimiento de la misión y visión del IDIGER y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La Seguridad de la Información es una prioridad para IDIGER y por tanto es responsabilidad de todos velar por que no se realicen actividades que vayan en contra del fundamento de cada una de estas políticas.

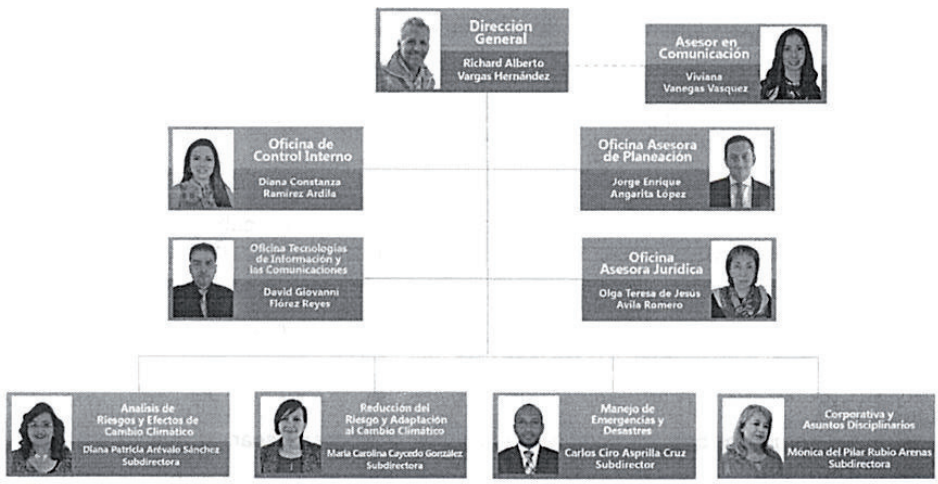
2. Objetivos Específicos

Dar a conocer las Políticas y procedimientos de Seguridad de la información, las cuales serán de obligatorio cumplimiento en el desarrollo de las actividades de los empleados, contratistas y terceros que prestan servicios a la entidad. , así mismo, operaciones de cómputo, Telecomunicaciones, Redes y desarrollo de Sistemas de Información de IDIGER.
Determinar los mecanismos de protección necesarios que garanticen el funcionamiento óptimo de los recursos informáticos de la organización.
Establecer las labores de seguridad y vigilancia de las diferentes dependencias del IDIGER.
Establecer las medidas de seguridad para los terceros que tienen algún tipo de convenio con el manejo y/o administración de los activos de información de la organización.
Divulgar y capacitar a los funcionarios del IDIGER, sobre el presente manual de acuerdo a sus funciones y responsabilidades.

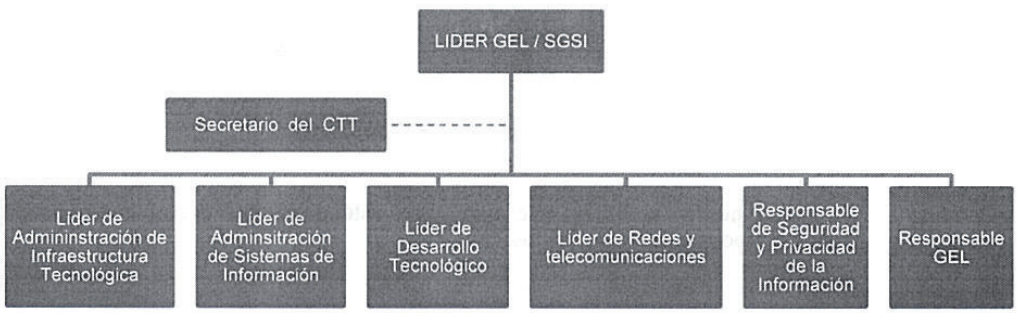
3. Consideraciones

3.1. Estructura Organizacional

A continuación se presenta la Estructura Organizacional del IDIGER definida de acuerdo a lo convenido en la Resolución 112 de 2016.



3.2. Estructura Comité Técnico TIC - CTT



3.3. Marco Conceptual

La seguridad de Información se refiere al establecimiento de las medidas organizacionales, técnicas y sociales, necesarias para proteger los activos de información: hacking informático, divulgación, duplicación, intercepción, modificación, destrucción, pérdida, supresiones, daños, deterioros, robo, mal uso, interrupción de sistemas, etc., que se pueda producir en forma intencional o accidental.

3.3.1 Terminología y Definiciones de Criterios de Seguridad de la Información

Activo de información
Es todo aquel recurso tangible o intangible que tenga VALOR o IMPORTANCIA para la organización, de acuerdo a la tipificación definida.

Adaptabilidad
Condición que permite identificar y rastrear toda operación llevada a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados.

Archivos
Conjunto de datos o instrucciones que se almacenan en el Disco Duro y/o cualquier otro medio de almacenamiento con un nombre que los identifica.

Autenticidad
Consiste en garantizar que las personas, entidades o procesos sean lo que dicen ser ante un activo de información.

Autorización
Es el otorgamiento de permiso a una persona, entidad o proceso, para acceder a un activo de información.

Autorización
Proceso o procedimiento oficial, por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información o activos físicos.

Backup
Copia que resguarda la información para protegerla de posibles riesgos.

Confidencialidad
Consiste en garantizar que el activo de información no esté disponible o sea divulgado por personas, entidades o procesos NO autorizados.

Confiabilidad
La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

Contraseña (Password)
Clave para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc. Esta clave debe ser personal e intransferible y no se debe anotar en documentos físicos de fácil acceso.

Cuenta de Usuario
Identificador que utiliza un Sistema de Información en la autenticación de un usuario.

Cuenta de Correo
Servicio en línea que provee un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico en Internet.

Disponibilidad
Consiste en garantizar que el activo de información este accesible y utilizable en el momento oportuno que se requiera bajo la demanda de personas, entidades o procesos.

Eficiencia
Criterio de calidad en que el procesamiento y suministro de la información, que debe contar con la capacidad de lograr ese efecto con el mínimo de recursos posibles o en el menor tiempo posible.

Equipos de cómputo
Dispositivo electrónico que se emplea para procesar datos. También pueden ser considerados como equipos de cómputo los equipos que prestan servicios de almacenamiento y procesamiento desde la nube.

Hardware
Partes físicas de un sistema de procesamiento de datos,

Incidente
Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política

Información
Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Integridad
Consiste en asegurar o salvaguardar que el activo de información cuente con las propiedades de: exactitud, precisión, consistencia, confiablidad y totalidad.

Log
Archivo que registra movimientos y actividades de un determinado programa, utilizado como mecanismo de control y estadística.

Medios de almacenamiento externo
Medio utilizado para el almacenamiento de información, que puede conectarse o introducirse y retirarse del Hardware por varias interfaces como puertos USB, unidad de cinta, unidades de disco, etc.

No-Repudiación
Consiste en asegurar que el activo de información NO sea negado bajo un evento o transacción demandado por personas, entidades o procesos.

Parche de Seguridad
Conjunto de instrucciones de corrección para un software en especial, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento en su código original.

Periféricos
Dispositivo electrónico físico que se conecta o acopla a una computadora, pero no forma parte del núcleo básico

Recursos informáticos
Software y hardware.

Red
Nombre dado al conjunto de equipos de cómputo y de telecomunicaciones, interconectados entre sí al interior de la organización, para permitir a los usuarios acceso a los recursos tecnológicos.

Software
Es el conjunto de instrucciones mediante las cuales el Hardware puede realizarlas tareas ordenadas por el usuario. Está integrado por los programas, sistemas operativos y utilidades.

Software ilegal
Es el Software que se adquiere y se instala sin el consentimiento de la empresa que lo desarrolla o sin licencia de uso.

Trazabilidad
Asegurar que en todo momento se podrá determinar quién accedió a qué activo de información (servicio, datos, etc.), qué hizo y en qué momento lo hizo.

3.3.2 Terminología y Definiciones Para el Estudio de los Riesgos y Controles a la Seguridad de la Información

Análisis del riesgo
Se basa en la revisión y evaluación sistemática de la información para identificar las fuentes y estimación del riesgo a través de las causas de las posibles amenazas y probables de eventos no deseados y los daños y consecuencias que éstas puedan producir. La medición y evaluación continua de amenazas, impacto y vulnerabilidades sobre los activos de información que permitan la minimización de la ocurrencia de dichos riesgos de seguridad, esto se realiza a través del PHVA.

Amenaza
Es la indicación de un potencial evento no deseado que afecte negativamente la confidencialidad, integridad, disponibilidad o confiabilidad de los activos de información y que expone de alguna manera la entidad. Para cada amenaza se medirá la criticidad de la Probabilidad de ocurrencia de la misma, bajo los siguientes criterios:

Cuantitativo	Cualitativo	Descripción
1	Muy Baja	No afecta las operaciones del negocio, genera riesgos a todo nivel insignificantes.
2	Baja	No afecta las operaciones del negocio, genera riesgos a todo nivel inusuales.
3	Media	Afecta imperceptiblemente las operaciones del negocio, genera riesgos a todo nivel con cierta frecuencia.
4	Alta	Afecta considerablemente las operaciones del negocio y genera riesgos a todo nivel iterativamente.
5	Muy Alta	Afecta significativamente las operaciones del negocio y genera pérdidas, riesgos financieros u operaciones importantes.

Autenticación fuerte
Esquema de autenticación mediante el cual el sujeto que se identifica debe utilizar por lo menos dos de tres posibles factores. Los factores pueden ser algo que se tiene, tal como una tarjeta de proximidad; algo que se sabe, como una clave personal (contraseña); algo que se es, es decir, una característica única inherente a la persona, como la huella digital.

Cifrado fuerte
Técnicas de codificación para protección de la información que utilizan algoritmos de robustez reconocidos internacionalmente, brindando los niveles de seguridad ofrecidos.

Control
Una forma para manejar el riesgo, en la cual se incluyen políticas, procedimientos, estructuras organizacionales y elementos tecnológicos, que pueden ser de carácter administrativo, técnico, procedimental o legal.

Continuidad
Es la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Gestión del riesgo
Actividades coordinadas para dirigir y controlar los activos de información de la organización con respecto al riesgo, para cada uno de sus procesos, subprocesos o áreas funcionales. La importancia de la administración del riesgo se basa en la:

- Necesidad de cumplir con un número creciente de disposiciones regulatorias.
- Necesidad de responder rápida y efectivamente a los cambios y riesgos del entorno de los negocios.
- Necesidad de asegurar la sustentabilidad de los negocios en el tiempo.
- Mejora continua a través de controles que disminuyan las vulnerabilidades, fallas, consecuencias ante la probabilidad de impacto.

Incidente de seguridad de la información
Se considera un Incidente de seguridad de la Información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Propietario activo de información
Área o persona que tiene la responsabilidad de clasificar y definir el grado de seguridad que se debe aplicar a un activo de información, autorizar el acceso y velar por que se implementen controles que disminuyan el riesgo por pérdida de la integridad, confidencialidad y disponibilidad del mismo.

Riesgo
Es la posibilidad que una amenaza explote o penetre una vulnerabilidad de un activo de información, impactando a este activo de información y/o activos asociados, viéndose afectando del mismo modo los objetivos del negocio

Vulnerabilidad

Es una característica propia de debilidad en términos de seguridad asociada a un activo de información que puede hacer que una amenaza se haga efectiva.

Para cada vulnerabilidad se debe medir la criticidad de la probabilidad de ocurrencia de la misma, bajo los siguientes criterios.

Cuantitativo	Cualitativo	Descripción
1	Muy Baja	No afecta las operaciones del negocio, genera riesgos a todo nivel insignificantes.
2	Baja	No afecta las operaciones del negocio, genera riesgos a todo nivel inusuales.
3	Media	Afecta imperceptiblemente las operaciones del negocio, genera riesgos a todo nivel con cierta frecuencia.
4	Alta	Afecta considerablemente las operaciones del negocio y genera riesgos a todo nivel iterativamente.
5	Muy Alta	Afecta significativamente las operaciones del negocio y genera pérdidas, riesgos financieros u operaciones importantes.

Se deberá realizar un análisis de vulnerabilidades internas y externas por lo menos una vez al año a toda la infraestructura tecnológica.

3.4. Clasificación de información

IDIGER, define el esquema de clasificación de la información, con el fin de mantener actualizado el inventario y la tasación de los activos de información más relevantes, ya que no toda la información tiene el mismo nivel de importancia. Para clasificar un activo de información se evaluarán los criterios de seguridad más importantes de acuerdo con su nivel de confidencialidad, integridad, disponibilidad y no repudio, siguiendo la reglamentación establecida por la legislación Colombiana vigente.

3.4.1 Identificación Fuentes de la información:

La identificación se puede realizar mediante entrevistas, formularios o cuestionarios. Si las fuentes de información no han sido identificadas, se pueden catalogar como fuentes de información los encargados o líderes de área, los administradores de sistemas de información o de equipos de tecnología y el personal en general.

Para clasificar los niveles de información, es necesaria la rotulación, para definir las metas de protección de los datos.

La clasificación que adopta el IDIGER es:

<table>
<tr><td colspan="2">Información Pública Reservada</td></tr>
<tr><td rowspan="2">Información Pública Clasificada</td><td>Semi-privada</td></tr>
<tr><td>Privada</td></tr>
<tr><td colspan="2">Información Pública</td></tr>
</table>

De acuerdo a la ley 1712 de 2014, toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no puede ser reservada o limitada sino por disposición constitucional o legal.

La información que se recibe de otras áreas debe:

- Mantener el nivel de clasificación otorgado por la entidad que la originó.
- Se manejará de acuerdo con los esquemas de seguridad definidos por la legislación o por el nivel de clasificación que tiene.
- La información que ha sido clasificada en un nivel superior de protección, puede ser reclasificada en un nivel inferior de protección solo por el funcionario o área que la originó.

No toda la información tiene el mismo nivel de importancia para la organización, consecuentemente la clasificación de la información en categorías es necesaria para identificar los criterios fundamentales para la determinación del valor relativo de la misma y el conjunto de controles apropiados y requeridos para preservar su valor.

En las actividades de clasificación de información deben participar activamente los propietarios, usuarios finales y custodios de la misma, ya que solo el propietario puede determinar el nivel de clasificación que debe recibir.

Dentro de las múltiples razones por las cuales se debe realizar la clasificación de la información contenida en los activos, están:

- Cumplimiento regulatorio.
- Eficiencia en costos frente a la implementación de complejas soluciones de tecnología.
- Compromiso real y demostrado de los usuarios para la protección de la información.
- Mejoramiento de los procesos de auditoría interna, ya que le permite a los auditores evidenciar las medidas de control que se aplican y a los responsables de la información les define con claridad las responsabilidades a cumplir.

Información reservada: La jurisprudencia de la Corte Constitucional, en Sentencia T-729 de 2002, hace referencia a la información reservada de la siguiente manera:

> *"La información reservada, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.*
> *Para la Corte, esta tipología es útil al menos por dos razones: la primera, porque contribuye a la delimitación entre la información que se puede publicar en desarrollo del derecho constitucional a la información, y aquella que constitucionalmente está prohibido publicar como consecuencia de los derechos a la intimidad y al habeas data y ley 1581 de 2012 protección de datos, La segunda, porque contribuye a la delimitación e identificación tanto de las personas como de las autoridades que se encuentran legitimadas para acceder o divulgar dicha información. "*

Ejemplo de ella es la información genética y los datos sensibles (aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como aquellos que revelan el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, a organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garantice los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, la vida sexual y los datos biométricos - Art. 5, ley 1581 de 2012).

Información privada: La jurisprudencia de la Corte Constitucional, en Sentencia T-729 de 2002, hace referencia a la información privada, así:

> *"La información privada, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio."*

Esta información, que es sensible dentro de la ICN, puede causar pérdidas serias a la organización, pérdida de confianza en la organización, daños a terceros y afectación de las relaciones con terceros. Esta clasificación incluye información altamente confidencial y personal. Sólo estaría disponible a un grupo específico debido a su función o rol; si esta información se filtra fuera de la organización causará pérdida de imagen o perdida financiera. La pérdida de CONFIDENCIALIDAD compromete legal o administrativamente a la organización. El acceso a esta información debe ser restringida sobre el principio de "Necesidad de ser conocida". En caso de requerirse la divulgación de la información a una tercera parte se requiere la aprobación del propietario y se recomienda la firma de un acuerdo de confidencialidad.

Es el caso de los libros de los comerciantes, los documentos privados, las historias clínicas y los llamados datos sensibles a los que se hizo referencia anteriormente.

Información semiprivada: La jurisprudencia de la Corte Constitucional, en Sentencia T-729 de 2002, en relación a la información semi-privada, afirma:

> *"La información semi-privada, será aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas."*

Esta información es sensible si está fuera de las instalaciones de la organización y puede impactar los niveles de servicio, desempeño o generar pérdidas económicas a las personas o la entidad. Esta clasificación incluye información personal, registros financieros y bancarios o detalles relacionados con la operación de la ICN. La información sólo está disponible a los funcionarios y contratistas debidamente autorizados; y sólo es suministrada si su conocimiento es necesario para el desarrollo de una función o tarea asignada a la persona.

Si esta información se filtra fuera de la organización, puede tipificar negligencia administrativa o financiera. La divulgación de esta información no causa daños serios a la entidad y el acceso a la misma se puede proporcionar a todos los funcionarios, contratistas y demás colaboradores. Ejemplo: datos personales, circulares, políticas, materiales de entrenamiento, datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas.

Información Pública: La jurisprudencia de la Corte Constitucional, en Sentencia T-729 de 2002, respecto de la información pública, se refiere en los siguientes términos:

> *"La información pública, calificada como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. Por vía de ejemplo, pueden contarse los*

actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; igualmente serán públicos, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno."

Esta información es creada en el curso normal de la función misional de la entidad y tiene poca probabilidad de causar daño. La información pública incluye la información que debe ser publicada por mandato legislativo o para dar cumplimiento a una política de divulgación de información. La información pública está disponible al ciudadano, funcionarios, contratistas, subcontratistas y demás personal.

La no disponibilidad de esta información no causa ningún daño a la organización. Si esta información se filtra fuera de la organización no hay ninguna perdida.

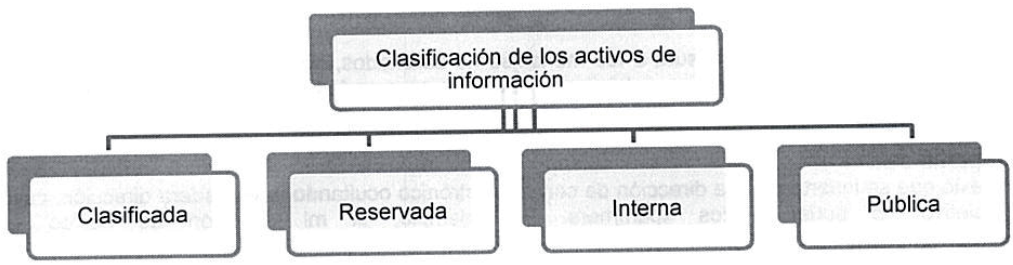
Por otra parte, el artículo 3° del Decreto 1377 del 27 de junio de 2013, define el Dato Público de la siguiente manera:

"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 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".

Información pública reservada: De acuerdo a la ley 1712, citada, se define como " (…) aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley".

Información pública clasificada: La ley 1712 la define como *"(…) aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado 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 consagrados en el artículo 18 de esta ley".*

Para efecto de presente manual, el IDIGER manejará la siguiente clasificación, teniendo en cuenta el grado de confidencialidad.



Confidencial.
Es toda aquella información de los clientes, empleados y contratistas que implique el número de cuenta, saldos, datos personales como el número de identificación, nombre (s) y apellidos (s), Se considera información confidencial: Plan Estratégico de la Compañía, Carpetas de los empleados (Recursos Humanos), Información de Clientes, registros financieros de la entidad, nomina entre otros

Reservada
Es toda la información interna crítica, con alto nivel de riesgo, la cual es de manejo exclusivo de personas designadas dentro de la Entidad, Se considera información restringida: los informes de auditoría, actas de comités, información sobre planeación o información sensible que se encuentre en medio magnético, bases de datos, archivos e impresiones que contenga Información confidencial o restringida que a juicio del dueño de información tenga esta calidad.

- Interna: información que se puede compartir con toda la Entidad.
- Pública: Información que además de compartirse con la Entidad podría ser de uso de los clientes o proveedores, ejemplo folletos, información expuesta en página Web etc.

3.5 Tipos de Ataques y Atacantes

Hoax (correos falsos).
Es un mensaje de correo electrónico con contenido falso o engañoso. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante, a que parece provenir de una fuente seria y fiable o porque el mismo mensaje pide ser reenviado.

Phishing (Pesca).
Es el acto de pescar usuarios mediante señuelos y de este modo obtener información financiera y contraseñas para intentar adquirir información confidencial de forma fraudulenta.

Spoofing (suplantación de identidad).
Es una técnica que consiste en hacer creer al receptor de un mensaje de correo electrónico, que quien remite el mensaje es alguien de confianza. El verdadero emisor queda suplantado por una dirección real, que ofrece garantías al receptor, que abrirá ingenuamente el mensaje sin conocer los verdaderos motivos (ocultos).

Spammers.
Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido; habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.

Spamblock.
Texto que se inserta en una dirección de correo electrónico ocultando la verdadera dirección, cuyo objetivo es burlar a los spammers. Por ejemplo, si mi dirección de correo es grupo@compañiaf.com.co, mediante esta técnica se puede transformar en grupo@rcompañiaf.com.co.

Crimeware.
Es un software diseñado específicamente para cometer delitos financieros en entornos en línea, técnicas mediante la ingeniería social u otras técnicas genéricas de fraude en línea. El objetivo es robar identidades en línea para acceder a los datos financieros de un usuario, con el fin de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el crimeware.

Malware (Software malicioso).
Tipo de software que tiene como objetivo infiltrarse o dañar un Pc sin consentimiento de su dueño.

Virus.
Es un software que se copia por sí mismo, infecta un Pc, se propaga dentro de todo los archivos, luego se copia de Pc a Pc; estos virus se adhieren en archivos específicos (de arranque, script, macros o ejecutables); el fin de este software es alterar o corromper el funcionamiento normal de un Pc.

Spyware.
Es un software cuyo objetivo es mandar información a un tercero de toda las páginas visitadas; el fin es espiar y recabar información de las páginas a las cuales fueron visitadas (incluyen claves de cuenta, correos, etc.) para luego en lo posterior, enviar o saturar de publicidades. La recolección de esta información es mediante un canal falso, produciendo un consumo de ancho de banda de internet y a su vez poniendo lento el computador.

Gusano.
Es un software cuyo único cometido radica en pasar de Pc en Pc a través de redes informáticas en forma automática sin la intervención de ningún usuario; estos normalmente buscan traspasar los agujeros de seguridad para infectar toda la red a su alcance.

Adware.
Se trata de un software que permite publicidad no deseada vía Internet y que generalmente se instala sin nuestro consentimiento.

Scareware (Software de miedo).
Es un software que engaña a un usuario para descargar un programa haciendo creer que está infectado de virus; es un método de estafa para hacer comprar un software utilizando prácticas comerciales poco éticas.

Caballo de Troya.
Es un software inocente que contiene códigos escondidos que permiten la modificación no autorizada y la explotación o destrucción de la información. Los troyanos se distribuyen por Internet, juegos, protectores de pantalla y crack de programas.

Botnet.
Son redes de computadoras infectadas, también llamadas "zombies", que pueden ser controladas a la vez por un individuo y realizan distintos ataques (envío masivo de spam o para lanzar ataques DDos). El fin de este ataque puede ser de extorsión, impedir su correcto funcionamiento, etc.

Rogue software.
Software que hace creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso; esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.

Hijacking.
Es una técnica ilegal que tiene por objetivo el adueñarse o robar (TCP/IP, página web, dominio, navegadores, módems, temas de foros, sesiones de terminal, servicios etc.) mediante una conexión de red.

Carding.
Uso ilegítimo de las tarjetas de crédito ajenas, generar números de tarjetas de crédito y cualquier otra actividad ilegal relacionada con las mismas.

Trashing.
Se trata de buscar en la basura (física o informática) información que pueda ser útil para realizar fraudes, copias, suplantaciones, etc.

Graffiti.
Modificación que un hacker hace de la página web de un servidor para evidenciar la falta de protección de un sistema.

Defacement.
Hace referencia a la deformación o cambio de manera intencionada a una página web, ya sea por venganza, diversión o burla; esto se debe a algún error de programación de la página por algún bug en el propio servidor o por una mala administración de este.

Phreaking.
Son individuos que orientan sus estudios u ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas y sistemas que componen una red telefónica, electrónica aplicada a sistemas telefónicos.

Cracker.
Son individuos que se dedican a desproteger programas, como evitar tener que pagar las licencias de los mismos, comprar una copia y usarla en 20 puestos simultáneamente.

Hacker.
Persona que es capaz de eludir los sistemas de seguridad de un computador para acceder a la información que contiene ya sea con fines maléficos o benéficos.

Hacktivista.
Persona especialista que se moviliza con conocimientos informáticos contra la mundialización, las multinacionales y en defensa de los internautas.

Ankle-Biter (packet-monkeys, script kiddies o crashers)
Son personas que indagan por la red ya sea por diversión o pasa tiempo para realizar ataques sólo para divertirse, sin importar quién los recibe.

Rootkit
Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

3.6. Normatividad

El marco que regula la seguridad de la información está conformado por las siguientes normas técnicas y jurídicas, a saber:

3.6.1. Técnica

Norma Internacional ISO 27000 y 27001, con sus respectivas actualizaciones liberadas, que se ha configurado como un estándar de facto a la hora de auditar los aspectos relacionados con la seguridad de la información en las organizaciones.

3.6.2. Jurídica

3.6.2.1. Nacional.

Ley 527 de 1999. Art. 10, referencia la fuerza probatoria de los mensajes de datos para las pruebas de evidencias.
Art. 11, presenta los criterios probatorios de los mensajes de datos. "confiabilidad en la forma que se generó la evidencia", "confiabilidad en la forma en que se conservó la evidencia" y la "confiabilidad en la forma en cómo se identificó al autor".

Ley 1266 de 2008 Hábeas Data.

Ley 1273 del 2009, "De la protección de la información y de los datos".

Ley 1581 de 2012 Protección de Datos.

Decreto Nacional 2573 de 2014, establece los lineamientos generales de la Estrategia de Gobierno en línea, reglamenta parcialmente la Ley 1341 de 2009 y dicta otras disposiciones.

3.6.2.2. Distrital

Acuerdo 20 de 1989, Artíuclo18 Parágrafo 3, autoriza la creación y reglamentación de la Comisión Distrital de Sistemas, como organismo rector de las políticas a nivel de sistematización para todas las Entidades del Distrito Especial, incluyendo al Centro Distrital de Sistematización y de Servicios Técnicos "SISE".

Acuerdo 409 de 2009, modifica la integración de la Comisión Distrital de Sistemas, Concejo de Bogotá.

Acuerdo 57 de 2002, dicta normas generales para la implementación del Sistema Distrital de Información -SDI-, organiza la Comisión Distrital de Sistemas y dicta otras disposiciones.

Decreto Distrital 680 de 2001, modifica la Comisión Distrital de Sistemas –CDS.

Decreto Distrital 619 de 2007, establece la Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital y dicta otras disposiciones.

Decreto Distrital 296 de 2008, asigna funciones relacionadas con el Comité de Gobierno en Línea a la Comisión Distrital de Sistemas y dicta otras disposiciones en la materia.

Decreto Distrital 316 de 2008, modifica parcialmente el artículo 3° del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.

Resolución 305 de 2008, expide 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 378 de 2008, adopta la guía para el diseño y desarrollo de sitios web de las entidades y organismos del distrito capital.

Resolución IDIGER 360 de 2015, establece dentro Comité del Sistema Integrado de Gestión, el Comité Anti trámite, Gobierno en Línea y Seguridad de la Información y le señala funciones en materia de Información.

Resolución 318 de 2017, modifica y adiciona la resolución 360 de 2015. .....

Directiva 05 del 12 de 2005, Secretaría General- Alcaldía Mayor, Por medio de la cual se adoptan las políticas generales de tecnología de información y comunicaciones aplicables al Distrito Capital.

Circular 82 de 2002 Secretaria General- Alcaldía Distrital - SISTEMA DISTRITAL DE INFORMACION.

3.6.2.3. Jurisprudencia.

Sentencia No. C-662 de junio 8 de 2000, da el mismo valor de peso a la evidencia digital frente a otros medios probatorios existentes.

3.7 Obligatoriedad

El Manual de Políticas de Seguridad de la Información es de obligatorio cumplimiento para todos los funcionarios, contratistas, o terceras personas que tengan acceso a los activos de información del IDIGER.

Todos los usuarios están obligados a continuar protegiendo la información y cumplir las políticas de seguridad de la información después de terminar su relación con la Entidad de acuerdo con la cláusula de confidencialidad pactada en el contrato de trabajo.

Si un usuario viola las disposiciones de las políticas de seguridad de la información, por negligencia o intencionalmente, el IDIGER, se reserva el derecho de aplicar las medidas pertinentes.

Entre otros se podrá solicitar el inicio de proceso disciplinario al funcionario o funcionarios que hayan violado las políticas y procedimientos de seguridad de la información.

Debido a la propia evolución de la tecnología, a las amenazas de seguridad y a las nuevas aportaciones legales en esta materia, IDIGER, se reserva el derecho a modificar estas políticas cuando sea necesario. Los cambios realizados en estas políticas serán divulgados a los usuarios y proveedores que les aplique, utilizando los medios que se consideren pertinentes, para garantizar la publicidad de los mismos.

3.8 Administración de la política

Para la Administración de las Políticas de Seguridad de la información, IDIGER, tiene las siguientes instancias:

Comité Anti trámites, Gobierno el Línea y Seguridad de la Información, establecido en el artículo 19 de la Resolución 360 de 2015, acto administrativo modificado y adicionado Resolución 138 de 2017.

Comité Técnico de TIC- CTT, que permitirá gestionar y hacer seguimiento a la política de seguridad y privacidad de la información.

3.8.1 Labores esenciales de la administración del Sistema Gestión de Seguridad de la Información SGSI

Las labores que se enuncian a continuación, serán responsabilidad del oficial de seguridad de la información, que para efecto del presente manual será el Líder de apoyo estratégico de la Oficina de Tecnologías de información y las comunicaciones

- Coordinar y ejecutar todas las actividades necesarias para adaptar, aprobar e implementar las políticas de seguridad de información del IDIGER, dentro del marco de la regulación.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Revisar y proponer cambios, ajustes y modificaciones al Manual de Políticas de Seguridad de la Información.
- Establecer y definir los procesos administrativos necesarios para el fortalecimiento de las políticas de seguridad de información en IDIGER.
- Identificar y analizar toda situación de riesgo inherente a los activos de información, para implementar los controles necesarios para minimizar su impacto.
- Actualizar y mantener los reglamentos de la política de seguridad de la información de acuerdo a las necesidades cambiantes del IDIGER.
- Informar al comité GEL a través de la secretaría técnica, cualquier cambio o ajuste que se requiera para el fortalecimiento de la política de seguridad.
- Programar en forma periódica el seguimiento al cumplimiento de las normas y procedimientos e informar al Jefe Oficina Tecnologías de la Información y las Comunicaciones de los resultados correspondientes.
- Propender por la capacitación de los usuarios en el conocimiento y aplicación de este manual.
- Evaluar y analizar las solicitudes que se realicen por las diferentes áreas de la entidad que puedan vulnerar y/o afectar la seguridad de la información. Igualmente se pronunciara respecto de cualquier modificación que se introduzca en los procedimientos operativos que puedan poner en riesgo la seguridad de la información.
- Coordinar el proceso de administración de continuidad de las operaciones de la entidad.
- Evaluar y aprobar los mecanismos de seguridad física de las oficinas, áreas de acceso, áreas de trabajo y áreas de las diferentes sedes con que cuenta la entidad a fin de establecer la seguridad de activos de información del IDIGER.

3.8.2 Labores de Seguridad

Las labores de seguridad, estarán en cabeza del responsable de la seguridad de la información de IDIGER del grupo de trabajo de la Oficina de Tecnologías de información y las comunicaciones.

- Administrar y garantizar el acceso a nivel de red, hardware, software y bases de datos (Mini-CD, CD-A, CD-ROM, CD-R, CD-RW, CD+G, VCD, MMCD, USB u otros mediosxon de almacenamiento) o documentos impresos, mediante la coordinación del área de Infraestructura de la oficina TIC y la de Gestión Documental de la Subdirección Corporativa y Asuntos Disciplinarios.
- Clasificar la información y categorizarla según su importancia para toma de decisiones; bajo la responsabilidad del propietario de la información.
- Proporcionar o asignar lugares adecuados para el almacenamiento de la información aislándola de cualquier riesgo que pueda entorpecer su confidencialidad, integridad y disponibilidad, en coordinación con el grupo de Infraestructura de la oficina TIC y Gestión Documental de la Subdirección Corporativa y Asuntos Disciplinarios, según el tipo de información.
- Administrar y garantizar que las copias de seguridad (Backup) de los sistemas de información tengan un adecuado manejo según su valor y el tiempo que estime la Ley. Implementar controles definidos para los sistemas de información que custodia, incluyendo investigación e implementación de actualizaciones de seguridad, en coordinación con el área de seguridad. Según el tipo de información, las responsabilidades estarán distribuidas en el área de infraestructura de la oficina TIC y/o Gestión Documental de la Subdirección Corporativa y Asuntos Disciplinarios.
- Desarrollar procedimientos de autorización y autenticación.
- Monitorear permanente el cumplimiento del procedimiento del resguardo de información según el medio donde esté almacenada. En coordinación con el área de Gestión Documental de la Subdirección corporativa y Asuntos Disciplinarios

3.8.3 Labores Esenciales de los Administradores de la Información

- Identificar y clasificar la información por subdirección, oficina y área según su uso, teniendo en cuenta el perfil, el rol y privilegios de acceso del usuario.
- Establecer los métodos y técnicas para clasificar la información según el grado de sensibilidad o de criticidad.
- Cumplir con las políticas y normas de seguridad establecidas para los recursos de cómputo asignados a su cargo de acuerdo a los parámetros establecidos por IDIGER.
- Velar porque se utilicen los activos de información solamente por personal autorizado y para los fines establecidos por IDIGER en cada área.
- Definir y autorizar el uso de los datos haciendo referencia específica de: a quien, por cuanto tiempo, bajo que restricciones de acceso y porque medio (teléfono, vía remoto, acceso a base de datos, etc.).
- Informar al oficial de seguridad de la información para que administre bajo su responsabilidad los niveles de acceso al software de aplicación y datos, cumpliendo con las condiciones establecidas por el presente manual de seguridad de la información.
- Mantener actualizado los ingresos, suspensión, traslado o retiro de funcionarios, en coordinación con el área de Talento Humano, con el objeto que el estado del usuario se mantenga actualizado o inhabilitado en los sistemas de información.
- Programar con la Subdirección Corporativa y Asuntos Disciplinarios actividades de capacitación y entrenamiento continuo en el manejo y administración de los sistemas de aplicación utilizados para el procesamiento de los datos del IDIGER.

- Definir y mantener actualizada las especificaciones de todos los procedimientos correspondientes del área, bajo su responsabilidad en coordinación con la Oficina Asesora de Planeación.
- Sugerir al comité GEL, los cambios que sean necesarios con el fin de asegurar la confidencialidad e integridad de la información de la Entidad de acuerdo a la normatividad.
- Aplicar pruebas de Seguridad de la información, para verificar y garantizar las modificaciones realizadas a los sistemas que soportan la operación de IDIGER.
- Todo cambio a los sistemas de información debe estar probado y autorizado por el CTT y por el comité GEL antes de ser instalado y puesto en producción de forma definitiva.
- Informar al Jefe de la Oficina TIC sobre las deficiencias de control que detecte en su área automatizada.
- Participar en forma activa en la definición e identificación de los requerimientos funcionales y de control, necesarios para el desarrollo de los nuevos sistemas de información.
- Definir los controles específicos para el área, en lo referente al manejo de los datos que se generen para su procesamiento o se reciban de él para garantizar su calidad y razonabilidad.
- Definir los mecanismos de seguridad física requeridos en la oficina o área de trabajo al personal de seguridad de la información, necesarios+ para la custodia de los activos de información.
- Reportar al jefe de la Oficina TIC a través de correo incidentes de seguridad presentados en la oficina o área de trabajo.

3.8.4 Deberes de los funcionarios y contratistas en relación con la información

Los funcionarios y contratistas del IDIGER, en relación con la información que se les entregue o a la que accedan para el desempeño de sus funciones o el cumplimiento de sus obligaciones contractuales, según el caso, así como los terceros usuarios de ella, tendrán los siguientes deberes:

- No revelar ni transmitir información reservada o sensible, sin la autorización previa y escrita, del dueño de la información.
- Custodiar el identificador de usuario y contraseña de cada sistema de información a su cargo y no revelarlos a persona alguna, bajo ningún concepto.
- Asumir toda actividad relacionada con el uso de su acceso autorizado.
- No utilizar ningún identificador y contraseña de otro usuario, aunque disponga de la autorización del propietario.
- Garantizar que el(los) equipo(s) quede(n) protegido(s) del acceso a personal no autorizado, cuando queden desatendidos (abandono temporal del activo de información).
- Tener acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones o el cumplimiento de sus obligaciones contractuales.
- Acogerse a la política de escritorio limpio, esto quiere decir, que por ningún motivo o circunstancia dejará el computador desbloqueado, al alcance visual o el acceso físico, ni ningún documento que tenga información valiosa sobre el escritorio mientras atiende a personas, o se retire temporal o definitivamente del escritorio de trabajo.

3.9 Inventario de activos de información

Para la captura y diligenciamiento del inventario de activos de información, IDIGER, definió las especificaciones descritas en este numeral.

- El inventario de los activos de información físicos (hardware), deben contar con la placa de inventario que lo identifica como activo fijo de la entidad, antes de empezar a operar y es responsabilidad del área de almacén de la subdirección corporativa y asuntos disciplinarios que se cumpla esta política.
- El inventario de la información almacenada en documento físico es responsabilidad del área de Gestión Documental.
- El inventario de los activos de información digitales (software, bases de datos y archivos digitales), es responsabilidad de la oficina TIC
- Se deben identificar claramente los activos donde se soporta y procesa la información, de la misma forma que clasificarlos según su importancia y riesgo.

3.9.1 Tipos de activos de información

La tipificación de los activos de información es de interés para el estudio y criterio de identificación de amenazas potenciales y salvaguardas (controles) apropiadas a la naturaleza del activo. La relación que sigue a continuación clasifica los activos de información dentro de un nivel de jerarquía, a saber:

Tipos de Activos de Información			
Nombre	**Cód.**	**Descripción**	**Grupo**
Servicios	S	Servicios prestados por Terceros (persona natural o jurídica) que prestan una labor determinada a la entidad. Servicios de tecnología de información y comunicaciones requeridos para el desempeño de la entidad.	Contratos. Servicios Públicos. Correo Electrónico. Página Web. De Red. (TCP/IP, UDP, FTP, TELNET, HTTP, SMTP, SSL).
Datos/Información	D	Elementos de información que solos o agrupados de alguna forma representan el conocimiento que se tiene de algo. Son los que permiten a la entidad prestar sus servicios.	Datos o Registros de los Usuarios/Ciudadanos. Estudios, conceptos, lecturas, informes. Datos de Interés Comercial o Administrativos. Código Fuente (Programas). Código Ejecutable (Programas). Datos de Configuración (Servidor, PBX, Equipos de Comunicaciones, Etc.). Registros.

Tipos de Activos de Información			
Nombre	**Cód.**	**Descripción**	**Grupo**
Software	**SW**	Se refiere a tareas que han sido automatizadas para almacenar, proteger, gestionar, procesar, analizar, transmitir y transformar los datos, permitiendo la explotación de la información para la prestación de los servicios.	Aplicaciones en Producción. Aplicaciones en Desarrollo. Sistemas de Gestión de Bases de Datos. Ofimática (Word, Excel, PowerPoint, etc.) Programas de Uso General. Sistemas Operativos. Navegador Web (Explorer, etc.). Sistemas de seguridad
Hardware	**HW**	Se refiere a los bienes materiales físicos destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo repositorios de los datos, aplicaciones informáticas o responsables del procesado o la transmisión de datos.	Servidores en General, Equipos de Cómputo o Comunicaciones. Equipos Personales (Escritorio, Agenda Electrónica, Token). Dispositivos de Red (Firewall, Modems, Router, switch, bridge, Access point). Portátil. Periféricos (Impresoras, Escáneres, Dispositivos Criptográficos, videobean) Teléfonos / Fax Conmutado Estaciones Hidrometeorológicas, radares, sensores entre otros.
Redes de Comunicaciones	**COM**	Se refiere a los medios de transporte que llevan datos de un sitio a otro a través de canales de comunicación.	Red de Datos (cableado estructurado). Red de Voz (Telefónica). Red Inalámbrica. Red Local (LAN). Red Privada Virtual (VPN). Internet. ADSL. Antenas, torres Radar. Radio modem
Soportes de Información	**SI**	Se consideran dispositivos físicos que permiten almacenar información de forma permanente o al menos durante largos periodos de tiempo.	Carpetas Físicas o Electrónicas. Discos Duros. Discos Removibles. Cintas de Grabación. Dispositivos USB. DVD / CD-ROM. Tarjetas de Memoria. Tarjetas Inteligentes. Microfilmaciones. Material Impreso (Manuales, Documentación en General). Documentación Electrónica (Informes, Manuales).
Equipamiento Auxiliar	**AUX**	Se refieren a otros equipos físicos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.	Fuentes de Alimentación. UPS. Plantas Eléctricas. Cableado de Voz y Datos. Mobiliario Tecnológico (Madera, Metálico). Sellos. Suministros Esenciales.

Tipos de Activos de Información			
Nombre	**Cód.**	**Descripción**	**Grupo**
Instalaciones	I	Se refiere a los lugares o sitios donde se hospedan los sistemas de información y comunicaciones	Centro de procesamiento de datos (CPD). Edificio. Local. Plataformas Móviles. Rack de Comunicación.
Personal	P	Se refiere a las personas relacionadas con los sistemas de información.	Usuarios (externos e internos). Administradores.

3.10. Seguridad por parte contratistas.

Todo aquel que contrate con el IDIGER, ya se trate de personas naturales o jurídicas que tengan acceso a información confidencial o sensible que posea la entidad, deberán cumplir, como mínimo, con los siguientes requerimientos:

- Permitir que en el contrato a suscribir se consignen los siguientes aspectos:
  - El acuerdo de nivel de servicio (ANS).
  - Alcance y nivel de operación de la información a que tenga acceso.
  - Acuerdos de confidencialidad sobre la información manejada y sobre las actividades a desarrollar (aplicar si corresponde).
  - Restricciones sobre el software empleado.
  - Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma una vez finalizados el servicio.
  - Planes de continuidad y contingencia.

- Definir con los administradores de la información para mayor efectividad, confidencialidad y veracidad, las copias de seguridad (Back-up) de servidores, computadores, portátiles y demás dispositivos móviles.

- Exigir, en el evento de contratos, que subcontratistas, dispongan de planes de contingencia y continuidad debidamente documentados.

- Establecer por parte del contratista, procedimientos que permitan identificar físicamente, de manera inequívoca, los terceros contratados.

- Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados.

3.11 Políticas de Uso

3.11.1 Política de uso de correo electrónico

Todos los mensajes enviados por medio de correo electrónico pertenecen a IDIGER, el cual se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.

Queda terminantemente prohibido a los usuarios el envío de mensajes masivos a través de correo electrónico; este tipo de mensajes sólo puede ser enviado por usuarios debidamente autorizados. Los usuarios autorizados son: El Director general, el jefe de oficina TIC, el sub-director corporativo, el Administrador de las cuentas de correo electrónico – Coordinador infraestructura TIC-, y, quien sea autorizado previamente por escrito al efecto, en casos especiales por el Director General o por el Jefe de la Oficina TIC.

Es responsabilidad del Usuario enmarcar todos los mensajes que envíe a través de correo electrónico dentro de las normas mínimas de respeto y protocolo electrónico, sin incluir contenidos hostiles que molesten a los receptores del mismo, tales como comentarios sobre sexo, raza, religión o preferencias sexuales, tendencia política entre otras que generen algún tipo de discriminación; así mismo, es responsabilidad del usuario reportar al Jefe de área la recepción de este tipo de mensajes, quien a su vez deberá reportarla al área que corresponda, con copia a la Oficina TIC en caso de comprometer la seguridad de la información de la entidad.

Es responsabilidad del Usuario evitar que su cuenta de correo electrónico sea utilizada por terceros.

Es responsabilidad del Usuario evitar que la información confidencial y/o sensible sea transmitida por medio de su cuenta de correo electrónico, salvo autorización previa y escrita del dueño de la información y del Director de la entidad, un subdirector o un jefe de oficina, en cuyo caso los archivos deben viajar en forma Segura (encriptados).

Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

Es responsabilidad del Usuario eliminar periódicamente de sus dispositivos de almacenamiento los mensajes que ya no necesite. Con esto se reducen los riesgos de que otros usuarios puedan acceder a esa información; y además, se libera espacio en disco.

3.11.1.1. Se considera uso inapropiado de la cuenta de correo electrónico, lo siguiente:

- Enviar mensajes desde la cuenta de correo electrónico de un usuario con firma de otro.
- Intentar acceder y/o accesar sin autorización a otra cuenta de correo electrónico.
- Transmitir mensajes de correo con información sensible o confidencial sin autorización expresa del propietario de la información.
- Participar en cadenas de mensajes que congestionen la red.

3.11.1.2 Política de medios de almacenamiento extraíbles

Los medios electrónicos que contengan información confidencial o sensible están sujetos a las siguientes directrices de almacenamiento:

- La información confidencial y sensible nunca debe copiarse en medios removibles sin una autorización previa de la Dirección General o la Sub Dirección Corporativa, siempre y cuando se cuente para su manipulación con autorización previa y escrita, del dueño de la información.
- Los medios electrónicos que contengan datos confidenciales o sensibles deben ser físicamente retenidos, almacenados o archivados únicamente dentro de entornos de oficina seguros.
- Todos los medios electrónicos que contengan información confidencial y sensible deben etiquetarse claramente como tal.
- Todos los medios deben enviarse o entregarse por medio de un mensajero confiable u otro método de entrega que pueda rastrearse de modo preciso.
- Es responsabilidad de los usuarios Administradores o Custodios de centros de almacenamiento de información (impreso o electrónico), mantener un registro de Inventario de Medios. Todos los medios impresos y electrónicos almacenados que contengan información confidencial o sensible deben ser inventariados por lo menos anualmente.
- La documentación en papel u otros medios que contengan información confidencial y sensible que haya cumplido su período de retención, serán desechados mediante un proceso que garantice la destrucción apropiada de dichos elementos, por el responsable del manejo de la información documental.

3.11.1.3 Política de seguridad física

Todos los sitios donde se encuentren sistemas de procesamiento informático o de almacenamiento, así como el acceso a las diferentes oficinas, deben de ser protegidos contra accesos no autorizados, utilizando procedimientos o tecnologías de autenticación, monitoreo y registro.

3.11.1.4 Política de seguridad aplicable a logs

Es responsabilidad de la oficina TIC asegurar que se generen logs para toda la plataforma tecnológica, especialmente para los equipos y aplicaciones calificados como críticos, dichos logs deben ser custodiados en forma segura para evitar su modificación.

Es responsabilidad de la oficina TIC, que los logs generados sean monitoreados regularmente para detección temprana de posibles fallas en los equipos y aplicaciones o vulnerabilidades de seguridad.

3.11.1.5 Política de seguridad aplicable VPN

Todos los usuarios que tengan acceso por medio de VPN a la red interna de IDIGER, deben estar debidamente autorizados y documentados.

Es responsabilidad de los usuarios que utilizan los servicios de VPN asegurar que otras personas no autorizadas accedan a las redes internas de IDIGER.

Los gateways para el uso de VPN, serán implementados y administrados por la oficina TIC de IDIGER,

Al usar tecnologías de VPN con equipos ajenos a la entidad, los usuarios entienden y aceptan que sus máquinas son una extensión de la red de IDIGER, y por esta razón deben cumplir con las mismas políticas y regulaciones que aplican para las máquinas propiedad de IDIGER, como por ejemplo la política de hoja de vida de los equipos limpios de virus y programas no licenciados.

3.12 Control de Cambios

Es responsabilidad de todos los funcionarios de IDIGER, realizar el respectivo proceso de control de cambios, cada vez que soliciten la implementación de un nuevo sistema, modificación a uno existente o la implementación de cualquier cambio tecnológico, que afecte la infraestructura de TI, seguridad de la información, Bases de Datos, Software, hardware, sistemas o aplicaciones del IDIGER directa o indirectamente.

Para la realización de cualquier modificación se debe consultar con el Comité Técnico de TIC, para evaluar la viabilidad del mismo y generar la aprobación o no. Cada cambio se debe documentar en las diferentes plataformas donde corresponda (intranet, log de BD, NAS), o la que corresponda, para mantener la trazabilidad del cambio y posterior control.

3.12.1 Objetivos principales del Control de Cambios:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas
- Colaborar y apoyar el trabajo de Auditoría Informática interna/externa
- Definir, implantar y ejecutar mecanismos y controles para comprobar el grado de cumplimiento de los servicios informáticos.
- Realizar en los diferentes sistemas y entornos informáticos el control de las diferentes actividades que se realizan

3.12.2 Clasificación de los controles de cambios:

- Controles Preventivos: para la producción de errores o hechos fraudulentos, como por ejemplo el software de seguridad que evita el acceso a personal no autorizado.
- Controles para Detección: para descubrir a posteriori errores o fraudes que no haya sido posible evitar con controles preventivos.
- Controles Correctivos: para asegurar que se subsanen todos los errores identificados mediante los controles detectivos.

3.12.3 Lineamientos para solicitar cambios

3.12.3.1 Definición del formulario a utilizar para solicitar cambios.

Este formulario debe contener información suficiente para determinar, entre otros:

- Por qué se necesita el cambio (el elemento no funciona tal y como debe hacerlo, le falta alguna característica, etc.)
- Qué hay que cambiar
- Quién lo solicita

- Descripción del problema lo suficientemente detallada como para que se pueda recomendar una solución.
- Otros: que se pueden ver afectados por el cambio.
- Aprobación del cambio.
- Cómo se solucionó el problema, etc.
- Fecha y hora en que ocurrió,
- Descripción del incidente,
- Efectos que ha producido,
- De qué forma se puede duplicar el incidente, si es que se ha podido duplicar, volcado de datos, referencia al tipo de prueba que se estaba efectuando.

La aprobación o rechazo de las solicitudes de cambio, se harán con fundamento en la información en el contenido.

Algunos criterios que serán tenidos en cuenta para tomar la decisión de aprobar o rechazar las solicitudes de cambio serán:

- Valor agregado que aporta el cambio a la entidad.
- Tamaño
- Complejidad
- Impacto sobre el rendimiento del producto (uso de memoria y CPU)
- Recursos disponibles para efectuar el cambio (humanos y materiales)
- Relación con otros cambios ya aprobados y en progreso
- Tiempo estimado para completar el cambio
- Relación con las políticas de la empresa (satisfacción del cliente, competitividad, etc.)
- Existencia de alternativas, etc.
- Descripción,
- Severidad,
- Urgencia o prioridad
- Causa del problema (omisiones en el análisis, error en la documentación de entrada, falta de experiencia,...)
- Solución al problema
- Módulos afectados,
- Persona que lo notificó,
- Persona responsable,
- Fechas de notificación, resolución, etc.
- Fase/etapa en la que se originó el problema
- Fase/etapa en la que se detectó el problema

3.12.3.2 Presentación de la solicitud

La solicitud con el formulario diligenciado debe ser enviada y autorizada por el sub director o jefe de oficina, al jefe de TIC para ser evaluada y posterior trámite ante el comité CTT.

2.12.3.3 Responsabilidades el CTT frente a las solicitudes de cambios:

- Definir los mecanismos para solicitar cambios sobre los Elementos de Configuración.
- Definir los mecanismos para analizar y evaluar el impacto de las solicitudes de cambio.
- Definir los mecanismos para aprobar o rechazar las solicitudes de cambio.
- Definir los mecanismos para controlar la realización de los cambios aprobados.
- Construir una bitácora para realizar seguimiento y control a los cambios.

3.13 Acceso al Rack de Comunicaciones.

- Los rack de comunicaciones deben estar instalados en un lugar seguro, bajo llave y su acceso físico debe contar con la aprobación del jefe de la oficina TIC o el líder del grupo de administración tecnológica e infraestructura.
- La ubicación debe contar con un ambiente de temperatura y ventilación adecuado, las tomas eléctricas deben estar debidamente organizados (ver NTC 2050).
- El rack de comunicaciones de las oficinas deben estar bajo la custodia y responsabilidad del jefe de la oficina TIC o el líder del grupo de administración tecnológica e infraestructura y está prohibido acceder a él sin la debida autorización.
- El cableado de voz y datos del rack de comunicaciones debe estar rotulado e identificado.

3.14 Centro de procesamiento de datos (CPD)/Data Center principal

- El CPD principal deberá permanecer cerrado y su ingreso o salida deberá ser a través de un sistema de autenticación biométrica (huella dactilar) y/o con tarjeta de proximidad.
- Todo ingreso y salida de personas al CPD principal, debe ser registrada en una bitácora o planilla que identifique la fecha de ingreso, hora de ingreso, nombre completo de la persona que visita el CPD principal, motivo de la visita, visto bueno de la persona que autoriza el ingreso, fecha de salida, hora de salida y las tareas realizadas entre otras, como medida de control y seguimiento a las actividades realizadas en esta área.
- Se realizaran pruebas del plan de contingencia de acuerdo a la necesidad del negocio, midiendo su efectividad y evidenciando las mejoras de BCP mínimo dos veces por año.

3.14.2 Ambiente de producción, desarrollo y de pruebas.

- El IDIGER debe contar con los tres ambientes diferenciados claramente en cuanto a servidores de aplicaciones y BD.
- Se debe proteger cada uno de los computadores, dispositivos de red y de comunicaciones que se consideren críticos por intervenir directamente en el ambiente de producción, del acceso físico de personal no autorizado, para garantizar la confidencialidad, disponibilidad e integridad de la información.
- Los accesos al ambiente de producción deben ser restringidos por segregación de funciones y permisos de administrador de cada ambiente.

3.15. Seguridad del equipamiento de recursos tecnológicos

3.15.1 Computadores portátiles.

Sobre los equipo portátiles de propiedad del IDIGER, funcionarios y contratistas no pueden realizar ningún cambio, alteración física de algún componente de los equipos de tecnología

Los equipos portátiles entregados a funcionarios para sus labores cotidianas, cumplirán las normas de seguridad física y lógica y los funcionarios asignados tendrán la responsabilidad de verificar su cumplimiento.

Los portátiles de propiedad de los funcionarios del IDIGER, deben contar con guaya de seguridad instalada, mientras se encuentren en la oficina o lugar de trabajo, con el fin de prevenir el robo de los mismos.

Las computadoras asignadas a funcionarios y contratistas para el cumplimiento de sus funciones o de sus obligaciones contractuales, que se usan por fuera de la entidad deben serlo de manera segura y puntual, no pueden ser utilizados en actividades distintas a las antes indicadas y en consecuencia no pueden ser dejados expuestos a la utilización por parte de terceros, a fin de evitar fuga de información confidencial o sensible.

Si la conexión a internet se realiza desde otro lugar que no sea la red inalámbrica o alámbrica de la entidad, se debe realizar la conexión desde un lugar seguro (red inalámbrica con seguro WPA, WPA2, etc.).

Las computadoras portátiles se deben llevar como equipaje de mano en maletín adecuado.
Realizar el back-up permanente de toda la información, para en caso de pérdida o robo del computador portátil. En el evento, que se maneja información confidencial sensible, cifrar el disco duro.

Contar con actualización constante del antivirus para evitar contagio y propagación del mismo en IDIGER.

3.15.2 Equipos de Cómputo o de Escritorio

- Está prohibido a los funcionarios y contratistas a quienes se suministre equipos de cómputo de propiedad del IDIGER, realizar cualquier cambio, alteración física de algún componente de los equipos de tecnología.
- Se debe atender las recomendaciones del fabricante del equipo, referente a la protección física y ambiental del mismo, p.ej. contra la exposición de campos electromagnéticos muy fuertes.
- Se debe realizar periódicamente pruebas de operación de las UPS, previamente programadas y en un horario que no afecte la disponibilidad de los recursos de información de IDIGER. Estas pruebas deben ser documentadas como medida de control y seguimiento.
  Se debe realizar mantenimiento trimestral y/o semestral a las plantas eléctricas instaladas en IDIGER. Esta actividad se debe programar de manera coordinada entre la Oficina TIC y Subdirección Corporativa. Al final de cada mantenimiento la empresa contratada al efecto, debe entregar un informe de la labor realizada.

3.16. Gestión de la Continuidad del Negocio

Para mantener la continuidad de los procesos operativos y funcionales del IDIGER, la Entidad cuenta con un Centro de Procesamiento de Datos Alterno.

Para garantizar la continuidad del negocio, se definen las siguientes políticas de seguridad:

- Se cuenta con una planeación y dedicación en recursos financieros, humanos y tecnológicos rigurosa para el plan de continuidad del negocio de la organización, con el fin de garantizar el éxito del plan.
- El plan de continuidad del negocio debe tener contemplado la seguridad de la información para cada evento que se pueda presentar.
- Se deben documentar los planes de continuidad del negocio, tratando los requerimientos de seguridad de la información con la estrategia acordada para la continuidad del mismo.
- El plan de continuidad del negocio debe estar actualizado y revisado periódicamente. Es responsabilidad de la oficina de TIC, mantener el plan de continuidad de IDIGER en el ámbito tecnológico.

3.16.1. Plan de Continuidad (BCP)

El IDIGER elaborara y expedirá el Plan de Continuidad, en el cual tendrá en cuenta el numeral anterior.

3.16.2 Evento Catastrófico

Se debe velar para que la entidad, continúe funcionando a través del Centro de Procesamiento de Datos Alterno. En caso de presentarse un desastre natural (inundación, incendio, huracán, tornado, terremoto, tormenta invernal o tormenta solar de gran magnitud y severidad que afecte de manera importante la infraestructura tecnológica de la Entidad.)

3.16.3 Evento Humano

- Se debe crear un plan de concientización y compromiso de todos los funcionarios y contratistas del IDIGER, sobre la importancia del plan de continuidad del negocio para garantizar su éxito.
- Se debe tener identificado el uncionario clave para la toma de decisiones, así como el personal operativo que se requiera para iniciar y llevar a cabo los esfuerzos de recuperación.
- El recurso humano involucrado al plan de continuidad debe estar suficientemente familiarizado con sus roles y responsabilidades, para minimizar fallas humanas durante la realización del plan.
- Se debe documentar la información de todo el personal que estaría a cargo de la ejecución del plan de continuidad, para agilizar las notificaciones en caso de un desastre.
- El listado del personal de recuperación de desastre, de emergencia y operativo, debe contener mínimo la siguiente información: nombres, función a desempeñar, números de teléfono y direcciones Información similar se debe tener de proveedores, de compañías de seguros, de contactos para el retiro de copias de respaldo, entre otros.

3.16.4 Recuperación de Desastre de Tecnología de Información (TI).

El IDIGER, debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de información críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios, entre otros.
Los servidores y estaciones de trabajo se deben equipar con unidades suplementarias de energía eléctrica (UPS), supresores de picos de corrientes y en lo posible, eliminadores de corriente estática.
A todo equipo de cómputo, comunicación y de soporte debe realizársele un mantenimiento preventivo y periódico, para reducir el riesgo a fallas.
Se deben implementar al menos dos servidores de aplicaciones, con distribución de cargas para las oficinas.
Se deben contar con canales de comunicación alternos de alta disponibilidad y garantizados por el proveedor de comunicaciones de IDIGER.
Los sistemas de información (equipos, comunicaciones, periféricos, software, entre otros) que hacen parte del plan de continuidad, deben ser probados regularmente con el fin de asegurar que el mismo sea efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse al comité TIC y a la alta dirección.

3.16.5 Evento de Operaciones

- El plan de continuidad del negocio debe identificar y documentar las operaciones críticas de la organización de acuerdo a los procesos prioritarios. (BIA)
- Se deben inventariar los medios de respaldo, informes, manuales, y cualquier otra documentación requeridos para atender el plan de continuidad del negocio en eventos o fallas operativas, referenciando el proceso que soportará.
- Por falla en los sistemas de información de la organización (Oficinas y Dirección General), las operaciones diligenciadas manualmente sobre las plantillas o documentos soportados para atender el plan de continuidad, debe estar fechados y autorizados por el funcionario responsable de la misma, para garantizar la validez de la información y su posterior ingreso al sistema de información.

3.16.6 Pólizas y Seguros de Protección de los Activos de información

Se debe adquirir y mantener las pólizas de seguros de protección de activos informáticos contra todo riesgo como parte del plan de continuidad del negocio.

El manual de continuidad del negocio debe contemplar como mínimo lo siguiente:

- Planeación de un BCP.
- Análisis de riesgos (RIA).
- Análisis de Impactos (BIA).
- Desarrollo de estrategias.
- Desarrollo de un BCP.
- Sensibilización y capacitación.
- Prueba y ejercicio.
- Mantenimiento y actualización.
- Planes de evacuación y manejo de crisis.

4. Control de Cambios.

Versión	Fecha	Descripción de la Modificación	Aprobado por
1	1/08/2017	Creación Manual de Seguridad de la Información	Jefe Oficina TIC

5. Aprobación.

Elaborado por	Validado por	Aprobado por
Jaime Guerrero Clavijo **Profesional Oficina TIC**	Jonnathan Andrés Lara H. **Profesional de Planeación** Carlos Alberto Sosa Romero **Profesional Oficina TIC**	Jorge E. Angarita L. Jorge Enrique Angarita López **Jefe Oficina Asesora de Planeación** David Giovanny Flórez Reyes **Jefe Oficina TIC**

Nota: Para una mayor información referente a este documento comunicarse con la dependencia responsable.

Anexo 1. Glosario

Término	Definición
Activos:	Información importante que desea proteger frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta fundamental para la organización es lo que se denomina activo.
Autenticación:	Proceso mediante el cual el usuario se identifica como uno de los entes a los que se les ha otorgado derechos para ingresar al entorno computacional al que intenta ingresar. Este proceso establece la legitimidad del usuario.
Autorización:	Proceso por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información; el proceso determina cuáles actividades son permitidas, por ejemplo, manejo de datos o ejecución de programas
Confidencialidad:	Protección de la información para que nadie pueda leerla o copiarla, sin autorización del dueño.
Crítico:	Estado en el cual la pérdida de capacidad de procesamiento pueda llegar a tener consecuencias negativas significativas, desde los siguientes puntos de vista: continuidad del negocio, operacional y de integridad del personal.
Contraseña:	Contraseña, password o clave de acceso es una combinación de letras, números y signos, que conoce y debe teclear el usuario para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc.
Cuenta de Usuario:	Es el identificador que utiliza un Sistema de Información en la autenticación de un usuario.
Custodios de la información:	Se denominan así al personal o departamento que proporciona servicios informáticos de todo tipo en cualquier área de IDIGER, Los custodios no necesitan conocer la información para la realización de su trabajo, solamente procesarla, gestionar su almacenamiento y hacerla accesible.
Disponibilidad:	Asegurar que la información y los servicios del negocio de la organización estén disponibles permanentemente y sean oportunos para los propósitos requeridos.
Administrador de la información :	Es la persona responsable de una aplicación que utiliza sistemas de información para proporcionar servicios que apoyan una o varias unidades de negocio. Es el responsable por velar que se implementen controles que disminuyan el riesgo de la información a su cargo. Es también la persona que tiene la potestad de autorizar el acceso a la información
Firewall:	Es un filtro o cortafuegos (hardware o software) que controla todas las comunicaciones que pasan de una red a otra y en función de lo que sean permite o deniega su paso.
Recursos Tecnológicos:	Elementos de tecnología que pueden ser hardware y/o software, tales como equipos de cómputo, servidores, impresoras, teléfonos, faxes, programas y/o aplicativos de software, dispositivos USB, entre otros.
Terceros:	Se entiende por tercero toda persona jurídica o natural, que no tiene vínculo laboral con la entidad, como contratistas que provean bienes o servicios a la Entidad.
Usuario de la información:	Es aquella persona que tiene acceso a información perteneciente a la entidad
Información Confidencial:	Es la información privada en poder del Estado cuyo acceso público se prohíbe por mandato constitucional o legal en razón de un interés personal jurídicamente protegido. Es decir, la información referente a la intimidad personal y familiar, al honor y propia imagen, así como archivos médicos cuya divulgación constituiría una invasión a la privacidad de la persona. A esta información solo tendrán acceso las personas que son dueñas de ella. Dentro de la información confidencial están los datos personales la cual es la información privada de una persona, como por ejemplo su nacionalidad, domicilio, patrimonio, dirección electrónica, número de teléfono o cualquier otra parecida.

Término	Definición
Información Reservada:	Es la información pública cuyo acceso se restringe de manera expresa, según lo estipula la LAIP, en razón de un interés general durante un periodo determinado y por causas justificadas. Por ejemplo, los planes militares secretos, las negociaciones internacionales o cualquier tipo de negociación o discusión que se tenga, mientras no se adopte una decisión definitiva. O toda aquella información que esté relacionada con la investigación o persecución de actos ilícitos o que genere una ventaja indebida en perjuicio de un tercero. Si la información que solicitas es reservada, puedes solicitar una versión pública. Esta es un documento en el cual se tacharán todos los datos que no puedes ver y te permitirá acceder al resto de información pública.
Información Privada:	Información de uso exclusivo de una persona o de la entidad o que administra el IDIGER.
Información Sensible:	Información que por su naturaleza, debe mantenerse bajo medidas de seguridad que garanticen el acceso solo al personal autorizado y para el propósito definido. La información de IDIGER, en medio magnético, bases de datos, archivos – e impresa, que maneje Información Reservada, Confidencial o Privada es clasificada como Sensible.
Información, Clasificación de Datos:	La información de IDIGER, se clasifica en 3 categorías, confidencial, Interna y Publica.
Información Interna:	Documentos de trabajo que circulan entre las áreas encargadas del mismo, que no tienen el carácter de reservados ni sensible.
Información Pública:	Es aquella que se ha hecho disponible para la distribución pública a través de los canales Autorizados de las empresa IDIGER, Son ejemplos, los boletines de servicios, folletos y anuncios.
Integridad de datos:	Proteger y garantizar la exactitud e integridad de la información en el momento de su ingreso a los sistemas y la identificación de cualquier alteración de la información.
Evidencia Digital:	Es un tipo de evidencia física que puede tomar muchas formas como son: • Registros de aplicaciones, • sistema operacional, • comunicaciones (logs de transacciones, logs de seguridad, logs de intentos de login fallidos, etc.) • Imágenes o graficas • Documentos en todos los formatos • Correo electrónico y faxes • Información financiera y de transacciones • Archivos de cache, cookies • Archivos eliminados • Archivos de intercambio
Nivel de seguridad estándar:	Nivel de seguridad que restringe a los usuarios la ejecución de algunos comandos o el acceso a algunos archivos basados en permisos y en niveles de acceso. Este nivel de seguridad requiere de auditoría del sistema. Esto incluye la creación de un registro de auditoría para cada evento que ocurre en el sistema.
Riesgo Informático:	Es una combinación de la posibilidad de que una amenaza contra un activo de información ocurra aprovechando una vulnerabilidad y/o falla en un control, y la severidad del impacto adverso resultante. Reduciendo la amenaza o la vulnerabilidad reduce el riesgo.
Sensitiva:	Información que por su naturaleza, debe mantenerse bajo medidas de seguridad que garanticen el acceso solo al personal autorizado y para el propósito definido.
Sistema:	Este término utilizado sin otra palabra que lo adjetive designa un conjunto de hardware y software específico.

Término	Definición
Software:	Creación intelectual que comprende los programas, los procedimientos, las reglas y cualquier documentación asociada pertinente a la operación de un sistema de procesamiento de datos.
Usuario:	Persona que usa un sistema o aplicativo. Credencial con contraseña asignada a aquella persona, empleados de IDIGER y personal de empresas que prestan servicios al mismo para poder acceder a cualquier sistema de información. Es personal e intransferible.
Usuario de la información:	Es aquella persona, funcionario, contratista o tercero, que en razón de sus funciones u obligaciones contractual o necesidad personal, hace uso de la información que posee el IDIGER Para adquirir perfil como usuario es necesaria previa autorización por el Dueño del Sistema, ya sea de modo individualizado o de forma general (información disponible para todo el personal de un área y de IDIGER.)
Vulnerabilidad:	Debilidad de un sistema, que da posibilidad de realizar alguna acción que afecte negativamente a éste.