

TIC-MN01

**MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**TABLA DE CONTENIDO**

1 INTRODUCCIÓN 3

2 MARCO LEGAL 3

3 OBJETIVO 5

4 ALCANCE 5

5 TÉRMINOS Y DEFINICIONES 5

6 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 9

7 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 9

8 POLÍTICAS OPERACIONALES 11

1. **INTRODUCCIÓN**

La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, y pertenecen al habilitador transversal de Seguridad y Privacidad de la Política de Gobierno Digital.

El Modelo de Seguridad y Privacidad debe estar acorde con las buenas prácticas de seguridad y debe ser actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, de la Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá está determinado por las necesidades objetivas, los requisitos de seguridad, los procesos, el tamaño y la estructura de la Entidad, con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos personales.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de la Unidad Administrativa Especial Cuerpo de Bomberos de Bogotá se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital aumentando la confianza en la ciudadanía.

1. **MARCO LEGAL**

Constitución Política de Colombia: Artículo 15 (Derecho a la intimidad y buen nombre), artículo 20 (Derecho de información) y artículo 74 (Acceso a documentos públicos).

Ley 44 de 1993 *“por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.” (Derechos de autor)*

Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."

Ley 594 de 2000 *“Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.*

Ley Estatutaria 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009. Ley por medio de la cual se crea y se protege el bien jurídico de la información y los datos personales. Así mismo, se tipifican conductas penales como daño informático, violación de datos personales, acceso abusivo a sistema informático, interceptación de datos informáticos, hurto por medios informáticos, entre otras.

Ley estatutaria 1581 de 2012 (Por la cual se dictan disposiciones generales para la protección de datos personales.).

Decreto Reglamentario 1377 de 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"

Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Decreto 886 de 2014 “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.”

Decreto Único Reglamentario 1074 de 2015 (Compilatorio en ley de Protección de Datos Personales)

Decreto 103 de 2015: “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 (Ley de Transparencia y acceso a la información pública) y se dictan otras disposiciones.”

Decreto 1081 de 2015, Título 1, Este Título tiene por objeto reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública.

CONPES como el 3701 de 2011 *“Lineamientos de política para ciberseguridad y ciberdefensa”*

CONPES 3834 del 2016 *“Política Nacional de Seguridad Digital”*

Demás normas y/o jurisprudencia que complementen, modifiquen o deroguen sustituyan las anteriores

1. **OBJETIVO**

Definir los lineamientos de seguridad y privacidad de la información para mitigar y controlar los riesgos relacionados con confidencialidad, integridad y disponibilidad, mediante la implementación del modelo de seguridad y privacidad de la información acorde a las guías de buenas prácticas y requerimientos legales vigentes.

1. **ALCANCE**

Establecer las políticas específicas de seguridad y privacidad de la información que permitan reducir amenazas y vulnerabilidades de los activos de información de la **Unidad Administrativa Especial Cuerpo Oficial Bomberos de Bogotá**, enfocadas en afianzar los principios de confidencialidad, disponibilidad e integridad de la información, con el fin de contribuir a la continuidad del negocio y gestionar los riesgos asociados.

Las Políticas de seguridad de la Información cubren los aspectos de seguridad y privacidad de la información basados en riesgos de integridad, disponibilidad y confidencialidad; Relacionados con cualquier activo de información, lo cual conlleva a disponer de guías y controles que deben ser cumplidos por directivos, servidores, contratistas y terceros, que laboren o tengan relación con la **Unidad Administrativa Especial Cuerpo Oficial Bomberos de Bogotá**, para alcanzar un adecuado nivel de protección en cuanto a confidencialidad, integridad y disponibilidad de la información.

Este documento debe ser conocido por USUARIOS los servidores y contratistas de la **Unidad Administrativa Especial Cuerpo Oficial Bomberos de Bogotá**. Así mismo, se exige su cumplimiento en los procesos de contratación de la entidad, y su conocimiento es requisito antes de realizar cualquier proceso de contratación a terceros encargados de información.

1. **TÉRMINOS Y DEFINICIONES**

**Activo:** Recurso del sistema de información o cualquier elemento que tenga valor para la entidad.

**Activo de Información:** Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la entidad. Ej. Bases de datos, sistemas operacionales, redes, sistemas de información y comunicaciones, documentos impresos, fichas, formularios, recursos humanos, etc.

**Administrador del Sistema:** Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está dirigida por la Oficina Asesora de Planeación.

**Análisis de riesgos:** Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias

**Ataque Cibernético:** Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado, por lo general con intenciones insanas y perjudiciales.

**Auditor Interno:** Persona encargada de auditar la entidad en nombre de ella misma.

**Brecha de Seguridad:** deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

**Centro de Datos:** También conocido como Centro de Procesamiento de Datos, o Data Center es una instalación que se encarga del procesamiento de datos e información de manera sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesarios para cumplir con dicha tarea.

**Confidencialidad:** Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.

**Control:** Mecanismo para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

**Control correctivo:** Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.

**Control preventivo:** Conjunto de acciones tomadas para eliminar la(s) causa(s) de una conformidad potencial u otra situación potencial no deseable.

**Contraseña:** Es una forma de autenticación privada, compuesta por un conjunto de números, letras y caracteres, que permiten al usuario tener acceso a un computador, a un archivo y/o a un programa.

**Custodio de los activos de información:** Es una parte designada de la entidad, un cargo, proceso, encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

**Disponibilidad:** Es la garantía de poder acceder a los activos de la información cuando sea necesario, por personal autorizado.

**Evento de Seguridad de La información:** Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

**Incidente de Seguridad de la información:** Es la identificación de la ocurrencia de un hecho que está relacionado con los activos de información, que indica una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

**Infraestructura de Procesamiento de Información:** Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

**Firewall:** Dispositivo que permite bloquear o filtrar el acceso en redes de comunicación.

**Hacker:** Persona dedicada a realizar entradas no autorizadas a los sistemas, por medio de redes de comunicación como Internet, con el objeto de encontrar vulnerabilidades en los sistemas.

**Host:** Término usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios de ella. Los usuarios deben utilizar hosts para tener acceso a la red.

**Información sensible**: Información de carácter personal que puede generar descremación

**Integridad:** La propiedad de salvaguardar la exactitud y completitud de los activos de información.

**Internet:** Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

**Intranet:** Red privada dentro de una empresa, que utiliza el mismo software y protocolos servidores en la Internet global, pero que es de uso interno.

**LAN:** (Local Área Network). (Red de Área Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

**Malware:** Código malicioso o cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.

**Política:** Son instrucciones obligatorias que regulan la forma en la entidad previene, protege y administra los riesgos de diferentes daños.

**Programas Utilitarios:** Software que resuelve problemas relacionados con la administración de sistemas de información. Existen programas utilitarios que ayudan a resolver gran cantidad de problemas.

**Red:** Se tiene una red cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

**Responsable de los activos de información:** Es la parte designada de la entidad, un cargo o proceso, para garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifique adecuadamente, de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables.

**Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

**Seguridad:** Mecanismos de control que evita el uso no autorizado de recursos.

**Seguridad de la Información:** Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información.

**Servidor:** Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

**Sistema Operativo:** Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora, servidor o dispositivo móvil.

**Terceros:** Se entiende por tercero a toda persona, jurídica o natural ajena a la UAECOB, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

**Usuario:** Cualquier persona, entidad, cargo, proceso o sistema automatizado que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Entidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información

**Virus:** Software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así programas ejecutables, sin la autorización ni el conocimiento del usuario.

1. **POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**

En el cumplimiento de sus funciones institucionales de proteger la vida, el ambiente y el patrimonio de la población de Bogotá D.C., mediante la atención y gestión del riesgo en incendios, rescates, incidentes con materiales peligrosos y otras emergencias, de manera segura, eficiente, con sentido de responsabilidad social, fundamentadas en la excelencia institucional del talento humano, la **Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá**, implementará las medidas que estén a su alcance para salvaguardar la integridad, la disponibilidad, la confidencialidad y privacidad de la información necesaria para el cumplimiento de su misión, gestionando los riesgos de manera integral con criterios de efectividad, eficiencia y transparencia en todos sus procesos y el fortalecimiento de sus capacidades en materia de seguridad de la información.

En este sentido, se declara como prioritario y de la más alta relevancia la seguridad y privacidad de la información en la ejecución de las labores de la Unidad Administrativa Especial Cuerpo Oficial Bomberos de Bogotá, mediante la protección de los activos de información, la infraestructura crítica y de soporte, con el fin de garantizar la continuidad de negocio y sus servicios relacionados; contribuyendo por tanto al cumplimiento de su misión y los objetivos estratégicos institucionales.

1. **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

La organización de la seguridad de la información se basa en las responsabilidades básicas que pueden ser clasificadas de acuerdo con las siguientes estructuras:

**7.1. Estructura orgánica**

Está basada en las responsabilidades generales en relación con el organigrama de la entidad.



**7.2. Estructura con relación a los sistemas de información.**

Está basada en los perfiles específicos con relación a los sistemas de información automatizados y se dividen en:

| **PERFILES** | **RESPONSABILIDADES** |
| --- | --- |
| Dueño del sistema | Define y acepta los requerimientos para el desarrollo y mantenimiento de los sistemas automatizados de información. Autoriza los accesos a la información. |
| Usuario | Servidor o contratista que utiliza los sistemas automatizados. |
| Desarrollador de Sistemas | Servidor, contratista o tercero encargado para desarrollarlo de acuerdo al requerimiento. |
| Operadores/Mantenimiento de Sistemas | Servidor, contratista o tercero encargado de operar, dar mantenimiento al sistema automatizado.  Gestionar los accesos. |
| Custodio de la información | Servidor, contratista o tercero responsable por la custodia de los datos físicos de la entidad.  Asistir en la administración de bases de datos.  Guiar a los dueños de datos, desarrolladores y usuarios finales en el diseño, creación, mantenimiento, manipulación e integración de bases de datos. |
| Auditor Interno | Servidor o contratista encargado de verificar la implementación de políticas y procedimientos en relación con la seguridad de la información. |

1. **POLÍTICAS OPERACIONALES**

La siguiente estructura de matriz para el desarrollo de políticas operacionales en la UAE Cuerpo Oficial de bomberos, es basada en la norma ISO 27001 del 2013 donde se identifican dominios, subdominio y temática, desdoblado de manera posterior en la dependencia/ rol (que participa) en donde se señala la persona o dependencia responsable de dar cumplimiento a la obligación o prohibición que sobre el tema se debe desarrollar en la entidad.

| **DOMINIO** | **SUBDOMINIO** | **TEMÁTICA** | **DEPENDENCIA**  **/ROL**  **(QUE**  **PARTICIPA)** | **ES OBLIGACIÓN** | **ESTÁ PROHIBIDO** | **ESTÁ PERMITIDO** |
| --- | --- | --- | --- | --- | --- | --- |
| DISPOSITIVOS MÓVILES  Y TELETRABAJO | Dispositivos móviles y teletrabajo | Dispositivos móviles | Usuario | Configurar de manera segura los dispositivos móviles de la entidad y realizar el borrado seguro cuando se requiera | El uso de dispositivos móviles personales en el data center a personal no autorizado | El uso de dispositivos móviles personales dentro de la entidad |
| Envío de información por dispositivos móviles | Usuarios | Enviar información sensible como fotografías y videos de actividades de la entidad únicamente por medios oficiales | El envío de información sensible de la entidad como fotografías y videos de actividades, por medio de dispositivos personales |  |
| Seguridad para teletrabajo o trabajo remoto | Oficina  Asesora de  Planeación | Definir los requerimientos técnicos para mitigar los riesgos informáticos en conexiones seguras y propender por la disponibilidad, confidencialidad e integridad . |  |  |
| Oficina  Asesora de  Planeación | Configurar las herramientas para el acceso remoto a la información en los equipos designados para el desempeño de las funciones. |  |  |
| Accesos para teletrabajo | Oficina  Asesora De  Planeación | Autorizar el acceso únicamente a la información, servicios y sistemas de información necesarios para la realización de las actividades a cargo del funcionario o contratista. |  |  |
| Director, Subdirectores, Jefes de Oficina y Jefes de Oficinas Asesoras | Solicitar a la Oficina Asesora de Planeación el acceso a los sistemas de información para teletrabajo o trabajo remoto de los servidores o contratistas que lo requieran. |  |  |
| Oficina Asesora de Planeación | Implementar métodos de verificación de identidad de usuarios para la realización de teletrabajo o trabajo remoto |  |  |
| Usuarios |  | Utilizar los equipos de la entidad únicamente para actividades laborales de la entidad.  En caso de que los equipos sean personales, toda la información del desempeño de las funciones debe ser almacenada en drive |  |
| SEGURIDAD DE LOS RECURSOS HUMANOS | Antes de asumir el empleo | Verificación de datos | Dependencias | Verificar los datos en los procesos de selección de personal para contratistas mediante el uso de listas de chequeo establecidas dentro de la entidad. |  |  |
| Conocer las Polìticas de Seguridad y Privacidad de la información | Usuarios | Conocer el Manual de Políticas de Seguridad y Privacidad de la Información y sus actualizaciones. |  |  |
| Durante la ejecución del empleo | Recursos | Dirección | Disponer los recursos para la inducción del modelo de seguridad y privacidad de la información. |  |  |
| Conocimiento | Usuarios | Aplicar los lineamientos establecidos por el modelo de seguridad y privacidad de la información en el desarrollo de sus labores. |  |  |
| Control del recurso humano | Usuarios | Firmar el acuerdo de confidencialidad frente a lo establecido en el modelo de seguridad y privacidad de la información de la entidad. |  |  |
| Terminación y cambio de empleo | Novedades | Usuarios | Realizar la devolución de activos de información como: archivos, documentos, credenciales de acceso a instalaciones, contraseñas de acceso a sistemas o servicios, equipos informáticos o software a cargo del servidor cuando se produzca desvinculación o cambio de funciones. |  |  |
| Finalización del contrato | Usuarios | Mantener las responsabilidades frente a la confidencialidad de la información de la entidad en caso de desvinculación del funcionario o contratista |  |  |
| Ausencias Temporales | responsable de La Dependencia | Notificar por medio de la mesa de ayuda acerca de la necesidad de bloquear provisionalmente los accesos a cargo del funcionario, contratista o tercero durante la vigencia de su ausencia temporal. |  |  |
| Novedades Laborales | Responsable de La Dependencia | Notificar por medio de la mesa de ayuda acerca de la necesidad de bloquear provisionalmente los accesos a cargo del funcionario, Cuando se produzca ausencia temporal o vacaciones. |  |  |
| GESTIÓN DE ACTIVOS | Responsabilidad por los activos | Activos de Información | Oficina Asesora De Planeación | Definir la arquitectura para los repositorios de información por parte de cada dependencia .  Identificar los sistemas de información automatizados y sus repositorios  Realizar el inventario de activos de información identificando los propietarios.  Identificar los riesgos y proponer los controles asociados a los activos de información. |  |  |
| Usuarios | Comunicar al responsable de sistematizar los activos de información los repositorios que trate, las modificaciones, actualizaciones y eliminaciones que se realicen sobre estos repositorios. | Eliminar información oficial de la entidad sin autorización. |  |
| Clasificación de la información | Clasificación de la información | Subdirección De Gestión Corporativa | Clasificar la información física como: Información pública, Información pública clasificada e información pública reservada, de acuerdo al Artículo 6 Ley 1712 del 2014. |  |  |
| Oficina asesora De Planeación | Clasificar La información automatizada como: Información pública, Información pública clasificada e información pública reservada, de acuerdo al Artículo 6 Ley 1712 del 2014.  Definir los lineamientos necesarios para realizar el etiquetado de la información digital. |  |  |
| Manejo de medios | Medios Removibles | Oficina Asesora de Planeación | Definir los lineamientos para el manejo de medios removibles. |  |  |
| Usuarios |  | Usar medios removibles en los equipos de la entidad. |  |
| Oficina Asesora De Planeación | Eliminar los medios de almacenamiento de manera segura una vez terminen su ciclo de vida. |  |  |
| CONTROL DE ACCESO | Requisitos del negocio para control de acceso | Accesos para sistemas de información | Usuarios | Hacer todo lo posible por mantener la seguridad de los accesos en cada uno de los sistemas de información, usuarios y contraseñas, tarjetas de acceso, llaves, etc. |  |  |
| Director, Subdirectores, Jefes De Oficina Y Jefes De Oficina Asesora | Autorizar accesos únicamente a la información de carácter confidencial o reservado necesaria para el desempeño de las actividades asignadas al usuario. |  |  |
| Usuarios | Velar por la seguridad del usuario y contraseña asignados son personales e intransferibles  Gestionar contraseñas seguras y renovarlas de manera mensual. |  |  |
| Gestión de acceso de usuarios | Procedimiento de gestión de usuarios | Oficina Asesora de Planeación | Definir el procedimiento de gestión de usuarios para los sistemas de información de la entidad  Definir la estructura de seguridad para la asignación de usuarios con accesos privilegiados.  Definir el sistema de monitoreo y seguimiento de la gestión de usuarios para identificar que los usuarios activos sean los autorizados. |  |  |
| Subdirección de Gestión Humana | Integrar dentro del proceso de gestión del talento humano los lineamientos para gestión de usuarios. |  |  |
| Responsabilidades de los usuarios | Responsabilidades de los usuarios | Oficina Asesora de Planeación | Capacitar a todo el personal con acceso a la información de la entidad en seguridad de la información. |  |  |
| Oficina Asesora jurídica | Firmar acuerdos de confidencialidad con las personas con acceso a la información reservada y clasificada. |  |  |
| Control de acceso a sistemas y aplicaciones | Seguridad en la gestión de usuarios | Director, Subdirectores, Jefes de Oficina Y Jefes de Oficina Asesora | Identificar los diferentes repositorios de información e identificar los diferentes niveles de acceso. |  |  |
| Oficina Asesora de Planeación | Definir el programa de monitoreo y control para los diferentes niveles de acceso a la información.  Definir los lineamientos para las contraseñas seguras que deben incluir tener más de 8 caracteres alfanuméricos, que incluya mayúsculas y minúsculas y también caracteres especiales, ser renovadas de manera mensual y no puede incluir el nombre propio ni del usuario.  Custodiar los códigos fuente, definir las personas con acceso y controlar el versionamiento |  |  |
| CRIPTOGRAFÍA | Controles criptográficos | Criptografía | Director, Subdirectores, Jefes De Oficina Y Jefes De Oficina Asesora | Definir los repositorios de información que deben ser encriptados |  |  |
| Oficina Asesora De Planeación | Definir la estructura de las llaves donde sea necesario establecer el control criptográfico y establecer el ciclo de vida de las llaves. |  |  |
| SEGURIDAD FÍSICA Y DEL ENTORNO | Áreas seguras | Definición de áreas seguras | Subdirección de Gestión Corporativa | Definir las áreas seguras de zonas de tratamiento y almacenamiento de información física y virtual teniendo en cuenta los aspectos identificados por Seguridad y Salud y el trabajo |  |  |
| Gestión del riesgo físico | Subdirección De Gestión Corporativa | Implementar controles de seguridad para el acceso a zonas seguras y definir mecanismos de monitoreo para el seguimiento de acceso a terceros. |  |  |
| Acceso a áreas seguras | Oficina Asesora De Planeación | Definir los lineamientos de acceso a las instalaciones de la entidad, así como al centro de datos  Establecer los lineamientos para trabajo en áreas seguras |  |  |
| Subdirección De Gestión Corporativa | Definir los lineamientos para de acceso en los diferentes puntos de ingreso a la entidad |  |  |
| Equipos | Ubicación de equipos | Usuarios | Generar bloqueo automático después de tres minutos y no pueden retirarse ni ingresar equipos de la entidad sin autorización. |  |  |
| Conexiones | Oficina Asesora de Planeación | Definir los controles de seguridad contra fallas eléctricas.  Rotular todas las conexiones de redes y redes eléctricas de manera que permita identificar los enlaces de las conexiones |  |  |
| Usuarios | Mantener los equipos de cómputo de la entidad conectados a redes reguladas con supresores de picos para evitar riesgos eléctricos y daños en los equipos. |  |  |
| Inventario de equipos | Usuarios | Utilizar los equipos asignados a la entidad. | Retirar equipos de la entidad sin autorización. |  |
| Oficina Asesora de Planeación | Mantener actualizado el inventario de equipos de la entidad identificando los equipos que se encuentren fuera y los que se encuentren defectuosos.  Realizar proceso de borrado seguro cuando se entreguen equipos alquilados o cuando se vayan a reutilizar equipos.  Configurar los equipos utilizados en la entidad para bloqueo automático cuando se presente inactividad mayor a tres minutos. |  |  |
| Usuarios | Almacenar la información institucional en el drive asignado. | Almacenar información institucional en los equipos ya que puede ser borrados en cualquier momento. |  |
| SEGURIDAD DE LAS OPERACIONES | Procedimientos operacionales y responsabilidades | Oficina Asesora de Planeación | Definir los lineamientos en relación con seguridad de la información digital de la entidad en procedimientos, instructivos y guías.  Al modificar los procedimientos y las actividades relacionadas con la seguridad de la información registrar los cambios para conocer la trazabilidad.  Elaborar el Plan Estratégico de Tecnologías de la Información y la Comunicación proyectando los requerimientos en capacidad tecnológica y de comunicaciones. |  |  |
| Protección contra códigos maliciosos | Instalación de antivirus | Oficina Asesora de Planeación | Implementar antivirus en todos los equipos de la entidad para detectar y prevenir acciones frente a códigos maliciosos |  |  |
| Copias de respaldo | Estructuración de copias de respaldo | Oficina Asesora de Planeación | Definir la metodología de realización de las copias de respaldo de la información teniendo en cuenta repositorios, periodicidad y pruebas. |  |  |
| Implementación de copias de respaldo | Oficina Asesora de Planeación | Realizar copias de respaldo incrementales y las pruebas pertinentes para la implementación en caso de presentarse un incidente relacionado con la disponibilidad de la información. |  |  |
| Registro y seguimiento | Reporte de antivirus | Oficina Asesora de Planeación | Realizar un informe mensual con los reportes del antivirus y evidenciar los eventos que desencadenaron acciones preventivas y correctivas. |  |  |
| Integridad de logs | Oficina Asesora de Planeación | Asegurar la integridad de los registros de los eventos del antivirus definiendo lineamientos y los custodios de la información.  Definir los accesos a las diferentes plataformas de consulta de registro de eventos.  Definir responsables de la extracción de los eventos y responsable del análisis de la información. |  |  |
| Sincronización de equipos | Oficina Asesora de Planeación | Sincronizar todos los equipos de la entidad con la hora Oficial de Colombia de acuerdo con lo establecido en el numeral 14 del artículo 6 del Decreto número 4175 de 2011. |  |  |
| Control de software operacional | Instalación de software | Oficina Asesora de Planeación | Realizar la instalación de los sistemas operativos de los equipos. |  |  |
| Usuarios |  | Instalar sistemas operativos, ningún usuario tiene privilegios para instalación de software. |  |
| Gestión de la vulnerabilidad técnica | Identificación de vulnerabilidades | Oficina Asesora de Planeación | Realizar por lo menos una vez al año un análisis de vulnerabilidades para identificar amenazas frente a los sistemas de información |  |  |
| Consideraciones sobre auditorías de sistemas de información | Auditoria de equipos | Oficina Asesora de Planeación | Definir un plan de auditoria de los sistemas operativos que incluya la identificación de los equipos, licencias instaladas y versiones. |  |  |
| SEGURIDAD DE LAS COMUNICACIONES | Gestión de la seguridad de las redes | Estructuración de redes | Oficina Asesora de Planeación | Segmentar la red por servicios con el fin de garantizar la funcionalidad de la red y la Seguridad de la Información. |  |  |
| Disponibilidad de red | Oficina Asesora de Planeación | Monitorear los recursos de red con el fin de proteger la información en los sistemas y aplicaciones velando por la disponibilidad de la información. |  |  |
| Monitoreo de red | Oficina Asesora de Planeación | Velar porque los recursos de los servicios de red de la entidad sean operados y administrados en condiciones controladas y seguras, que permita identificar vulnerabilidades de manera preventiva. |  |  |
| Transferencia de información | Envío de información institucional | Usuarios | Verificar el contenido y el destinatario de la trasferencia de información.  Solamente utilizar los canales de comunicación institucionales.  En caso de transferencia de información con un proveedor se deben tener acuerdos de confidencialidad. | El envío de información institucional por medio de canales personales como son vía correo electrónico o WhatsApp |  |
| Director, Subdirectores, Jefes De Oficina Y Jefes De Oficina Asesora | Remitir la información Institucional a las entidades y organismos de control. |  |  |
| Control de terceros | Terceros | Firmar un acuerdo de confidencialidad antes de acceder a la información. |  |  |
| Canales de comunicación | Oficina Asesora de Planeación | Establecer las condiciones de seguridad para envío de información y adquirir herramientas de mensajería electrónica segura. |  |  |
| Adquisición, desarrollo y mantenimiento de sistemas | Requisitos de seguridad de los sistemas de información | Evaluación de riesgos para nuevos sistemas de información | Oficina Asesora de Planeación | Evaluar los riesgos de seguridad de la información cada vez que se vayan a implementar nuevos sistemas de información. |  |  |
| Redes públicas | Oficina Asesora de Planeación | Configurar redes públicas separadas de las redes de la entidad. |  |  |
| Requisitos de seguridad en las comunicaciones | Usuarios | Evitar la transmisión incompleta de información, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada de información y la duplicación o reproducción de mensajes no autorizados. | Instalar o configurar redes públicas por su cuenta en las instalaciones de la entidad. |  |
| Seguridad en los procesos de desarrollo y de soporte | Definir reglas de buenas prácticas para el desarrollo de software | Oficina Asesora de Planeación | Establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la entidad de acuerdo a las buenas prácticas de desarrollo de software y deben quedar debidamente documentadas.  Definir los lineamientos que permitan mantener la trazabilidad de control de cambios en el desarrollo de sistemas de información. |  |  |
| Cambios en la implementación de las aplicaciones | Oficina Asesora de Planeación | Probar las aplicaciones críticas en ambientes modificados antes de realizar cambios en las plataformas de operación. | Evitar las modificaciones a los paquetes de software de acuerdo a las buenas prácticas de desarrollo de software |  |
| Seguridad en el desarrollo | Oficina Asesora de Planeación | Establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas en cada una de sus etapas.  Supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.  Realizar pruebas de funcionalidad de la seguridad de los sistemas de información relacionados con la integración con otras aplicaciones, los niveles de acceso, el uso de contraseñas administrativas.  Evidenciar brechas de seguridad tomar las medidas pertinentes para el desarrollo seguro.  Realizar pruebas a las actualizaciones, nuevas versiones o nuevos sistemas de información antes de ser puesto en producción. |  | Hacer desarrollos y pruebas en ambientes de operación. |
| Datos de prueba | Datos de prueba | Oficina Asesora de Planeación | Asegurar que los sistemas de información que necesiten datos de prueba no contengan información oficial de la entidad ni datos personales sensibles. |  |  |
| RELACIONES CON LOS PROVEEDORES | Seguridad de la información en las relaciones con los proveedores | Seguridad para el personal de terceros | Terceros | Conocer, aceptar y cumplir con el manual de políticas de seguridad y privacidad de la información |  |  |
| Oficina Asesora de Planeación | Establecer los acuerdos de nivel de servicio con cada uno de los proveedores definiendo los accesos a la información, los controles para los posibles riesgos.  Revisar que los acuerdos de confidencialidad con terceros para que contemplen el seguimiento de seguridad en la cadena de suministro. |  |  |
| Gestión de la prestación de servicios de proveedores | Seguimiento de terceros | Oficina Asesora de Planeación | Elaborar un plan de auditoria con los proveedores con acceso a la información.  Realizar seguimiento de los acuerdos de confidencialidad de acuerdo con lo establecido en el manual de políticas de seguridad y privacidad de la información. |  |  |
| Gestión de incidentes de seguridad de la información | Gestión de incidentes y mejoras en la seguridad de la información | Procedimiento de gestión de incidentes | Oficina Asesora de Planeación | Definir el procedimiento de gestión de incidentes estableciendo roles y responsabilidades en cuanto a identificación, reporte, investigación, gestión y definición de acciones correctivas y preventivas.  Evaluar el impacto del incidente de seguridad de la información e identificar si el incidente afecto confidencialidad, integridad o disponibilidad e identificar la cantidad y el tipo de información en riesgo.  Implementar acciones preventivas que permitan reducir la frecuencia o el impacto para que no se repita el incidente o que en caso de repetirse se mitigue el impacto.  Realizar informe de gestión de los incidentes de seguridad reportados incluyendo las pruebas y establecer los mecanismos para garantizar la integridad de los soportes. |  |  |
| Usuarios | Reportar por medio de la mesa de ayuda cualquier incidente relacionado con seguridad de la información en cuanto a confidencialidad, integridad o disponibilidad. |  |  |
| ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO | Continuidad de seguridad de la información | Definición de plan de continuidad de negocio | Subdirección de Gestión del Riesgo  Oficina Asesora De Planeación | Determinar los requisitos de información necesarios para el plan de continuidad de negocio.  Definir el plan de continuidad de negocio donde se establezca, documente, implemente y mantengan los lineamientos y controles para asegurar el nivel de continuidad requerido. |  |  |
| Pruebas | Oficina Asesora de Planeación  Subdirección de Gestión del Riesgo | Realizar pruebas anuales al plan de continuidad de negocio definir los tiempos de recuperación, revisión de los lineamientos y modificar el plan en los aspectos por mejorar. |  |  |
| Redundancias | Redundancias | Oficina Asesora de Planeación | Definir los recursos necesarios para implementar redundancia en los sistemas de información. |  |  |
| CUMPLIMIENTO | Cumplimiento de requisitos legales y contractuales | Matriz legal | Oficina Asesora jurídica | Establecer la matriz requerimientos legales en materia de gestión de la información a nivel de la entidad. |  |  |
| Subdirección de Gestión Corporativa  Oficina Asesora de Planeación | Definir el plan para el cumplimiento de la matriz legal en gestión de la información.  Definir los repositorios de información crítica que deben ser custodiados por parte de la entidad.  Establecer los lineamientos para mitigar los riesgos relacionados con la seguridad de la información. |  |  |
| Oficina Asesora de Planeación | Formular e implementar el Programa Integral de Protección de Datos Personales. |  |  |
| Revisiones de seguridad de la información | Definición del programa de auditoria | Dirección | Programar anualmente una auditoría externa para verificar el cumplimiento del modelo de seguridad y privacidad de la información. |  |  |
| Auditoria interna | Oficina Asesora de Planeación | Verificar que los lineamientos relacionados con la seguridad de la información sean acordes con este manual y que se encuentre implementado cumpliendo con los requerimientos legales. |  |  |
| Oficina Asesora de Planeación | Realizar semestralmente auditorías internas a los lineamientos relacionados con seguridad de la información. |  |  |