DIRECCIÓN NACIONAL DE BOMBEROS DE COLOMBIA

GESTIÓN DE TECNOLOGÍA E INFORMATICA

MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL DNBC DIRECCIÓN NACIONAL BOMBEROS COLOMBIA

INTRODUCCIÓN

La Dirección Nacional de Bomberos de Colombia, en adelante DNBC, reconoce la importancia de la información que gestiona y es consciente de las amenazas que enfrenta la información y de las consecuencias a las que se expone cuando no cuenta con medidas de seguridad y protección adecuadas. Por tal motivo la DNBC toma una visión general de los riesgos de seguridad digital, donde se podrán establecer controles y medidas efectivas, viables y transversales con el propósito de realizar el aseguramiento de la disponibilidad, integridad y confidencialidad tanto de la información del negocio como de los datos de los servidores públicos, contratistas y partes interesadas, para lo cual la DNBC enfocará sus esfuerzos en realizar una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos de seguridad digital que puedan afectar la información de la entidad, con el propósito de implementar medidas y controles efectivos que permitan estar preparados ante situaciones en las que se vea comprometida tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Su objetivo es el de establecer los principios orientadores en seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información de la DNBC, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI. La seguridad de la información es para la DNBC, una labor prioritaria que anima a todos a velar por el cumplimiento de las políticas establecidas en el presente documento.

La finalidad de implementar esta política no es otra más que garantizar que los riesgos en la seguridad y privacidad en la información sean conocidos, para poder ser gestionados y tratados de manera adecuada para la entidad, permitiendo una mayor eficiencia en cada proceso que se realiza. Esta estrategia liderada por el ministerio de las TICs tiene como finalidad, garantizar el aprovechamiento de las tecnologías de la información y las comunicaciones, buscando en todo momento un manejo de la información más transparente y eficiente. Así mismo la entidad está acatando la normatividad regional y nacional, dada por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC sostiene que en la entidad se debe contar con una "Política general de seguridad y privacidad en la información".

1 TABLA DE CONTENIDO

1. OBJETIVO

Establecer las políticas y/o lineamientos con el fin de fortalecer la gestión la adecuada gestión de la seguridad y privacidad de la información en la Dirección Nacional de Bomberos de Colombia, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio y por el cumplimiento de la normatividad vigente aplicable.

1.1. Objetivos Específicos

a) Dar a conocer en toda la entidad e implementar la estrategia de privacidad y seguridad de la información.

b) Crear una cultura de seguridad de la información entre los funcionarios, contratistas y terceros de la DNBC, mediante el desarrollo de planes de sensibilización y capacitación, como medida preventiva para la protección de la información y sus activos.

c) Asegurar la confidencialidad, integridad y disponibilidad de los activos de información a través de la implementación de un proceso de gestión de riesgos de seguridad de la información, acompañados en todo momento con el proceso de Inspección, Vigilancia y Control.

d) Proteger los recursos de TI (humanos, físicos, financieros, técnicos, etc.) para asegurar la continuidad de la prestación del servicio.

e) Garantizar la continuidad de las operaciones de la DNBC mediante la gestión de los incidentes de seguridad de la información.

f) Implementar y ajustar el modelo de seguridad y privacidad de la información-MSPI para proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizados.

g) Ejecutar las acciones que contribuyan al mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, teniendo en cuenta los planes de mejora definidos para tal fin.

2. ALCANCE

Las políticas y/o lineamientos contenidos en el presente manual son aplicables a todos los procesos estratégicos, misionales, de apoyo, y de evaluación y de control, definidos en el Mapa de Procesos de la dirección, Tablas de Retención Documental – TRD, documentos de apoyo y demás información que administre, proteja y preserve, así como cualquier entidad que gestione información en nombre de la DNBC a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional.

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de la Dirección Nacional de Bomberos de Colombia, aplica a todos los niveles funcionales y organizacionales de la Dirección, a todos sus funcionarios, contratistas y proveedores, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la Dirección Nacional de Bomberos de Colombia, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.

3. DEFINICIONES

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones [ISO 27000:2013] y las definiciones de acuerdo a la Resolución 1519 de 2020: ANEXO 3. CONDICIONES MÍNIMAS TÉCNICAS Y DE SEGURIDAD DIGITAL.

- ACTIVO DE INFORMACIÓN: conocimiento o información que tiene valor para la organización.
- ACTIVO CRÍTICO: Son aquellos elementos o componentes que hacen parte de la infraestructura critica.
- ADMINISTRACIÓN DE RIESGOS: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo en forma periódica.
- ALTA DIRECCIÓN: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad. Es la máxima autoridad en el sistema.
- AMENAZA: causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
- ANÁLISIS DE IMPACTO AL NEGOCIO: Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.
- AUTENTICACIÓN: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- AUTENTICIDAD: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- CENTRO DE CABLEADO: El centro de cableado es el lugar donde se ubican los recursos de comunicación de Tecnología de información, como Switch, Patch Panel, UPS, Router, Cableado de voz y de datos.
- CIBERACTIVO CRÍTICO: Ciberactivo que es crítico para la operación de un activo crítico.
- CIBERACTIVO: Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.
- CIBERSEGURIDAD: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- CIFRADO: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- COMITÉ DIRECTIVO: Es el instrumento gerencial adoptado por la Alta Dirección para fortalecer la gestión institucional y consolidar la efectividad organizacional, a través de la aplicación de criterios y mecanismos de monitoreo y evaluación de las facultades conferidas a dichas entidades públicas, permitiendo la toma de decisiones oportunas en pro del cumplimiento de su misión, visión y objetivos institucionales.
- CONFIABILIDAD DE LA INFORMACIÓN: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- CONTROL: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- CONTROL CORRECTIVO: Aquellos que permiten, después de ser detectado el evento no deseado, el restablecimiento de la actividad.

- CONTROL DETECTIVO: Control que está diseñado para identificar un evento o resultado no previsto después de que se haya producido.
- CONTROL DISUASORIO: Control que reduce la posibilidad de materialización de una amenaza, por ejemplo, por medio de avisos disuasorios.
- CONTROL PREVENTIVO: Control que está diseñado para evitar un evento no deseado en el momento en que se produce.
- CÓDIGO MALICIOSO: Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto
- replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.
- DATACENTER: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.
- DATO PERSONAL: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados.
- DATO PERSONAL PÚBLICO: Toda información personal que es de conocimiento libre y abierto para el público en general.
- DATO PERSONAL PRIVADO: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.
- DATO SEMIPRIVADO: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general. (Ej. Datos financieros, crediticios).
- DATOS SENSIBLES: es el dato que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (artículo 5° Ley 1581 de 2012)
- DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
- DISPOSITIVOS MÓVILES: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.
- DMZ: Sigla en inglés de DeMilitarized Zone hace referencia a un segmento de la red que se ubica entre la red interna de una organización y la red externa o internet.
- EQUIPOS ACTIVOS DE RED: Son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos.
- EVALUACIÓN DE RIESGOS: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.
- EVENTO: Ocurrencia o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000:2009]. Un evento puede tener una o más consecuencias, o puede tener diferentes causas; puede consistir en algo no ocurrido, y puede ser referido algunas veces como un "incidente" o "accidente".
- EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 27000:2009].

- FIABILIDAD: Se define como la probabilidad de que un bien funcione adecuadamente durante un período determinado bajo condiciones operativas específicas (por ejemplo, condiciones de presión, temperatura o velocidad).
- IMPACTO: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- INCIDENTE DE SEGURIDAD: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- INFORMACIÓN: Datos relacionados que tienen significado para la entidad
- INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos
- LEGALIDAD: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.
- MEDIO REMOVIBLE: Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son Memorias USB, Discos duros extraíbles, DVD y CD.
- MESA DE SERVICIOS: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas,
- incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Proceso de Gestión de Tecnología Informática recolecta las necesidades que tienen las dependencias en cuanto a los recursos tecnológicos.
- NO REPUDIO: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.
- OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: Es la persona que cumple la función de supervisar el cumplimiento de la Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran
- PARTES INTERESADAS: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- PANELES DE CONEXIÓN (PATCH PANEL): Elemento encargado para la organización de conexiones en la red.
- PLAN DE CONTINUIDAD DE NEGOCIO: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
- PLAN DE TRATAMIENTO DE RIESGOS: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma
- PRIVACIDAD DE LA INFORMACIÓN: El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- PROPIETARIO DEL RIESGO: Persona o proceso con responsabilidad y autoridad para gestionar un riesgo.
- PROTECCIÓN A LA DUPLICACIÓN: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- RIESGO: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- SISTEMA DE INFORMACIÓN: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información

según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso de la Dirección Nacional de Bomberos de Colombia.

- TECNOLOGÍAS DE LA INFORMACIÓN: Es el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de la información.
- TEST DE PENETRACIÓN: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.
- HARDENING: En el contexto de seguridad digital, hardening o endurecimiento, implica eliminar todas las configuraciones por defecto, reduciendo las vulnerabilidades y asegurando los sistemas e infraestructuras digitales.
- POLÍTICAS DE ORIGEN DE LAS CABECERAS: Serie de reglas que garantizan la seguridad de las cabeceras del protocolo HTTP.
- TOKEN DE CSRF: Código único de seguridad enviado en forma remota para validar la identidad del usuario.
- COLCERT: Grupo de Respuesta a Emergencias Cibernéticas del Ministerio de Defensa Nacional.
- CSIRT – GOBIERNO: Grupo de Respuestas a Incidentes de Seguridad Informática del Gobierno Nacional.
- TERCEROS: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad. Usuarios externos a la Dirección Nacional de Bomberos de Colombia que en algún momento pueden llegar a interactuar por las tareas propias de su trabajo. Entre estos se pueden considerar a los clientes y entes de vigilancia, control y/o certificación.
- Script. Es un conjunto de comandos que se usa para la configuración del código fuente.
- COOKIES: Archivo creado por los sitios web en donde se almacenan datos sobre la navegación del usuario.
- PLUGINS: Herramientas o aplicaciones de software que realizan funciones específicas, añadiendo en un software principal.
- VPN: De las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.
- VULNERABILIDAD: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
- DEFACEMENT: Denominación en inglés que hace referencia al tipo de ataque cibernético, bajo el cual, se desconfiguran los contenidos del sitio o portal web, incluso poniéndoles "otra cara" mediante colores, imágenes o contenidos no originales.
- ESCAPE DE VARIABLES EN EL CÓDIGO: Proceso de validación para confirmar que los datos ingresados en una variable correspondan con las entradas o caracteres válidos asignados por defecto en su configuración.
- FIRMAS FACSÍMIL: Es una reproducción electrónica (fotografía o escaneo) de una firma manuscrita.

4. NORMATIVIDAD

4.1. La Dirección Nacional de Bomberos de Colombia referencia las siguientes normas y modelos para la gestión de la seguridad y privacidad de la información, en la Entidad:
4.2. Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
4.3. Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
4.4. Ley 527 de 1999. Por 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.
4.5. Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
4.6. Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas

4.7. Ley 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.
4.8. Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
4.9. Ley 1273 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 Tecnología de la información y las comunicaciones, entre otras disposiciones.
4.10. Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnología de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
4.11. Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
4.12. Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
4.13. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
4.14. Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
4.15. Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
4.16. Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
4.17. Ley 1978 de 2019. Por la cual se moderniza el sector de las Tecnología de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un
4.18. regulador único y se dictan otras disposiciones.
4.19. Ley 1955 de 2019. por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
4.20. Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
4.21. Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
4.22. Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
4.23. Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
4.24. Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
4.25. Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
4.26. Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnología de la Información y las Comunicaciones.
4.27. Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
4.28. Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

4.29. Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico

4.30. Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
4.31. Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnología de la Información y las Comunicaciones.
4.32. Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
4.33. Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
4.34. Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
4.35. CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
4.36. CONPES 3854 de 2016. Política Nacional de Seguridad digital.
4.37. CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.

5. POLÍTICAS

La Dirección Nacional de Bomberos de Colombia, determina la información como un activo más importante para su funcionamiento y el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma. Esta puede ser de naturaleza legal, estratégica, financiera, operativa y en algunos casos corresponder a datos personales de empleados públicos, colaboradores, contratistas y grupos de interés. Igualmente, es consciente de las amenazas que enfrenta dicho activo y de las consecuencias a las que se expone la Entidad cuando ésta no cuenta con las medidas de seguridad adecuadas.

En ese sentido en el presente Manual, se hace necesario propender por la seguridad y privacidad de la información en la Dirección Nacional de Bomberos de Colombia, teniendo presente que la vulneración se encuentra en cualquier estado de su ciclo de vida (creación, procesamiento, almacenamiento, transmisión, utilización o destrucción), puede llegar a tener impactos a nivel legal, operacional, de imagen y/o reputacional en el cumplimiento de la misión y los objetivos estratégicos de la Dirección Nacional de Bomberos de Colombia.

Teniendo en cuenta lo anterior, el presente Manual establece los principios orientadores de seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información de la Dirección Nacional de Bomberos de Colombia, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, encaminados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI.

La Dirección Nacional de Bomberos de Colombia, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la Información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas

colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.

5.1 LINEAMIENTOS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.1.1 ORGANIZACIÓN INTERNA

Propósito: Establecer e implementar directrices y lineamientos de gestión y operación de seguridad y privacidad de la información en la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. Los activos de información deberán estar bajo la responsabilidad del Líder del Proceso para evitar conflicto y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información de la Dirección Nacional de Bomberos de Colombia.
b. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, debe mantener y documentar los contactos con autoridades (Policía Nacional, INTERPOL, Bomberos, Defensa Civil, Grupos de atención de desastres, etc.) u otros especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información que requiera de asesoría externa, siempre que esta sea informada por el líder del proceso afectado.
c. La Dirección Nacional de Bomberos de Colombia a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y demás personal que este determine debe mantener contacto con grupos de interés especializados en seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos en pro a la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información de la Dirección Nacional de Bomberos de Colombia.

5.1.2 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

Propósito: Establecer e implementar directrices y lineamientos de seguridad de la información en la gestión de proyectos en la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

El proceso de Gestión de Análisis y Mejora Continua o quien haga sus veces con el apoyo del Oficial de Seguridad y Privacidad de la información o a quien este delegue de acuerdo con la especificidad técnica, deberán definir e incluir en la metodología de gestión de proyectos de la Dirección Nacional de Bomberos de Colombia, y en todas sus fases, los aspectos relacionados con la seguridad y Privacidad de la Información. Para este fin se tendrán en cuenta los siguientes aspectos:

a. Durante la ejecución del proyecto se debe certificar el cumplimiento de los lineamientos de la política de seguridad y privacidad de la información, seguridad digital, continuidad de la operación de los servicios y la política de tratamiento de datos personales de la Dirección Nacional de Bomberos de Colombia que apliquen al objeto del proyecto.

b. Se debe realizar seguimiento y revisión periódica de los lineamientos correspondientes a seguridad y privacidad de la información enmarcado en la normativa interna de la Dirección Nacional de Bomberos de Colombia vigente en virtud de la ejecución del proyecto.

c. Al inicio del proyecto se debe definir el tiempo que la información será utilizada, los periodos de conservación y la accesibilidad.

d. Incluir los aspectos de seguridad y privacidad de la información y los datos personales en el análisis de riesgos previo al proyecto. Teniendo en cuenta los datos personales recolectados, se deben gestionar al inicio del proyecto las autorizaciones de tratamiento.

e. Si el proyecto involucra terceros se debe suscribir un documento de compromiso de confidencialidad, en el cual el responsable del proyecto deberá solicitar la entrega una vez se firme el contrato.

f. Si el proyecto incluye el desarrollo de sistemas de información, se deben establecer buenas prácticas de desarrollo seguro al inicio del proyecto.

g. Los terceros que participan en los proyectos deben divulgar periódicamente al interior de los equipos de trabajo las políticas de seguridad y privacidad de la información, y de tratamiento de datos personales adoptadas por la Dirección Nacional de Bomberos de Colombia.

h. Si el proyecto involucra terceros se debe prever un plan de recuperación y contingencia al inicio del proyecto, ante los eventos que puedan afectar el cumplimiento de la ejecución del proyecto de acuerdo con su objeto.

i. Se debe contemplar que en el momento que se presente un incidente de seguridad y privacidad de la información, este sea reportado al responsable del proyecto.

j. El Proceso de Gestión de Análisis y Mejora Continua o quien haga sus veces y el Oficial de Seguridad y Privacidad de la información o a quien este delegue de acuerdo con la especificidad técnica, deberán apoyar cuando se requiera en la evaluación de los riesgos de seguridad y privacidad de la información en una fase inicial del proyecto para identificar los controles necesarios, de acuerdo con el tipo de proyecto.

k. El líder del Sistema de gestión de Seguridad y privacidad de la información de manera autónoma debe revisar o auditar el cumplimiento e implementación de los requerimientos y consideraciones en materia de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la metodología de gestión de proyectos de la entidad. En el caso que se necesite incluir y/o reprogramar un ciclo de auditoría interna al Sistema de Seguridad de la Información en el Programa Anual de Auditoría Interna, al inicio de cada vigencia, el Líder del Sistema deberá hacer la solicitud mediante memorando o correo electrónico a la Asesora de Control Interno con copia al Director General, para que se coordine su programación y sea aprobado en el Comité Institucional de Coordinación de Control Interno.

5.1.3 DISPOSITIVOS MÓVILES

Propósito: Establecer e implementar directrices y lineamientos para la operación de dispositivos móviles que gestionen información propia de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. EL Proceso de Gestión de Tecnología e Informática, debe establecer la documentación necesaria que brinde a las dependencias la orientación con respecto a la autorización, configuración y uso de los dispositivos móviles de propiedad de empleados públicos, contratistas o terceros que requieran tener acceso a la información a través de los servicios tecnológicos de la Dirección Nacional de Bomberos de Colombia.

b. El proceso de Gestión de Tecnología e Informática debe implementar las medidas necesarias de seguridad y privacidad, para propender por la protección de la información gestionada mediante aplicaciones y sistemas de información.

c. El proceso de Gestión de Tecnología e Informática debe establecer los mecanismos técnicos u operativos en aras de garantizar que los computadores portátiles personales, cuenten con software licenciados y antivirus actualizado.

d. Los computadores portátiles de propiedad de los colaboradores no deberán estar incluidos en el dominio @dnbc.gov.co o cualquiera que funcione dentro de la Dirección Nacional de Bomberos de Colombia, para conectarse a los servicios de la red de datos deberán realizar solicitud a la mesa de servicios y cumplir con los lineamientos referentes a seguridad de la información.

e. El proceso de Gestión de Tecnología e Informática debe proporcionar a los dispositivos móviles, las herramientas Ofimáticas, Antivirus y de almacenamiento en nube licenciadas por la Dirección Nacional de Bomberos de Colombia.

f. El proceso de Gestión de Tecnología e Informática para la modalidad de Teletrabajo debe definir y proveer las herramientas tecnológicas para teletrabajar. Estableciendo las condiciones de seguridad y privacidad de la información, de acuerdo con las directrices internas y las enmarcadas en el Libro Blanco del Teletrabajo o cualquiera que la adicione, modifique o complemente.

g. El proceso de Gestión del Talento Humano debe mantener actualizado la documentación de teletrabajo y trabajo en casa y en especial los aspectos relacionados con la seguridad y privacidad de la información.

h. El proceso de Gestión del Talento Humano debe establecer los mecanismos necesarios para sensibilizar a los teletrabajadores y aspirantes a teletrabajo en temas de seguridad y privacidad de la información.

i. Para la modalidad de Teletrabajo, proceso de Gestión de Tecnología e Informática, debe establecer mecanismos de monitoreo sobre las conexiones y los servicios tecnológicos a los que el teletrabajador tiene acceso.

5.2 LINEAMIENTOS DE SEGURIDAD DE LOS RECURSOS HUMANOS

5.2.1 ANTES DE ASUMIR EL EMPLEO

Propósito: Establecer e implementar directrices y lineamientos para asegurar que el personal a contratar cumpla con las políticas de seguridad y privacidad de la Información de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión del Talento Humano debe definir formalmente un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación de la Dirección Nacional de Bomberos de Colombia y los que dicte la Función Pública.

b. El proceso de Gestión Contractual debe definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con lo que dicta la Ley y la reglamentación vigente.

c. Los procedimientos de selección de personal de empleados públicos y contratistas de prestación de servicios deben contener la autorización para el tratamiento de los datos personales acorde con la Política de tratamiento de datos personales de la Dirección Nacional de Bomberos de Colombia y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.

d. El proceso de Gestión Contractual y el proceso de Gestión del Talento Humano deben establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.

e. Todo empleado público o contratista debe firmar un documento o compromiso de confidencialidad y no divulgación de la información con la Dirección Nacional de Bomberos de Colombia, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.

f. El proceso de Gestión del Talento Humano debe incluir dentro del manual de funciones las responsabilidades con respecto al cumplimiento de las políticas de seguridad y privacidad de la información, así como todos los lineamientos en el marco del Sistema de Gestión de Seguridad de la Información.

g. El proceso de Gestión Contractual debe incluir en el pliego de condiciones y estudios previos, así como en la minuta contractual, las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad de la información que dicte la Dirección Nacional de Bomberos de Colombia.

h. El proceso de Gestión del Talento Humano, y el proceso de Gestión Contractual deben dar a conocer durante la inducción las responsabilidades u obligaciones en materia de la seguridad y privacidad de la información y aclarar que estas se extienden más allá de los límites de la Dirección Nacional de Bomberos de Colombia y del horario normal de trabajo o de ejecución del objeto contractual.

5.2.2 DURANTE LA EJECUCIÓN DEL EMPLEO

Propósito: Establecer los lineamientos sobre las responsabilidades de los colaboradores de la Dirección Nacional de Bomberos de Colombia con la seguridad de la información, de acuerdo con las políticas y procedimientos establecidos.

Lineamientos:

a. Una vez formalizado el proceso de vinculación, el jefe inmediato, supervisor o el delegado de la dependencia para tal fin, debe solicitar el paquete de herramientas colaborativas de TI (Microsoft Office, Navegadores de internet, reproductores de video y audio, programas de diseño gráfico, etc.). Esto de acuerdo con la necesidad del usuario y la apertura del inventario y demás servicios que requiera el colaborador para la ejecución de sus funciones u obligaciones contractuales.

b. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces en conjunto con el proceso de Gestión de Comunicaciones diseñarán e implementarán un Plan de

cambio y cultura organizacional en apropiación del SGSI, el cual se debe ejecutar durante la vigencia al interior de la Dirección Nacional de Bomberos de Colombia.

c. El proceso de Gestión del Talento Humano o el supervisor del contrato deben propender que los colaboradores de la Dirección Nacional de Bomberos de Colombia y usuarios de terceras partes que desempeñen funciones reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.

d. El proceso de Gestión del Talento Humano en conjunto con el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, deben socializar lo relacionado con seguridad y privacidad de la información y seguridad digital.

e. En lo pertinente al incumplimiento y desacato de las políticas de la seguridad de la información, se aplicará lo establecido en los mecanismos documentales destinados para tal fin, por los entes de control interno de la Dirección Nacional de Bomberos de Colombia, enmarcados en la Ley 1952 de 2019 y la Ley 2094 de 2021 para empleados públicos y Ley 1474 de 2011 para contratistas, sus decretos reglamentarios o cualquiera que la modifique, adicione, derogue o subrogue.

5.2.3 TERMINACIÓN Y CAMBIO DE EMPLEO

Propósito: Establecer los lineamientos sobre las responsabilidades de los colaboradores de la Dirección Nacional de Bomberos de Colombia con la seguridad de la información que permanecen válidos después de la terminación o cambio de empleo.

Lineamientos:

a. El jefe inmediato o a quien este delegue debe recoger y custodiar la información propia de la Dirección Nacional de Bomberos de Colombia, que se encuentra en gestión del empleado público, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones.

b. El supervisor del contrato o a quien éste delegue debe recoger y custodiar la información de la Dirección Nacional de Bomberos de Colombia bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.

c. El proceso de Gestión de Tecnología e Informática debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.

d. El proceso de Gestión del Talento y el proceso de Gestión Contractual o a quienes se deleguen deberán informar al procesos de Gestión de Tecnología Informática a través de la Mesa de Servicios, cualquier novedad de desvinculación administrativa, laboral o contractual del colaborador; una vez notificada la novedad al proceso de Gestión de Tecnología Informática se deberá proceder a la inactivación de los accesos del colaborador, teniendo en cuenta los siguientes parámetros: Si el buzón pertenece a una cuenta de correo genérica (ejemplo atencionciudadano@dnbc.gov.co), a este se le deberá cambiar la contraseña inmediatamente y asignar nuevo responsable para evitar accesos no autorizados.

e. En caso de que el buzón sea objeto de investigación por parte de las autoridades competentes, se les entregará en cadena de custodia una copia del buzón garantizando su integridad. Se deben inactivar los accesos biométricos o de tarjetas de proximidad de los sistemas de control de acceso.

f. Para el buzón de correo electrónico se creará una copia de respaldo una vez se dé por terminada la vinculación con la Dirección Nacional de Bomberos de Colombia.

g. Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; solo se podrán restablecer buzones en ambientes offline y no se podrán emitir correos ni notificaciones desde estos buzones.

h. Se deben inactivar todos los accesos a los sistemas de información de la Dirección Nacional de Bomberos de Colombia.

i. Se debe solicitar la devolución del carné o cualquier distintivo de autenticación o prenda de vestir, que lo acredita como colaborador de la Dirección Nacional de Bomberos de Colombia.

j. Cuando un empleado público o contratista cesa en sus funciones o culmina la ejecución de contrato con la Dirección Nacional de Bomberos de Colombia, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa del Director de la Dirección Nacional de Bomberos de Colombia, por orden judicial, por solicitud del proceso de Gestión de Asuntos Disciplinarios o quien haga sus veces, como parte de un proceso de investigación.

k. Cuando un empleado público del proceso de Gestión de Tecnología e Informática cambia de funciones o dependencia y su vínculo laboral sigue vigente, se podrá generar una copia de su buzón institucional. El proceso de Gestión de Tecnología e Informática deberá crear un nuevo usuario de directorio activo para que el empleado público pueda asumir su nuevo rol.

5.3 LINEAMIENTOS DE SEGURIDAD PARA LA GESTIÓN DE ACTIVOS

5.3.1 RESPONSABILIDAD POR LOS ACTIVOS

Propósito: Establecer lineamientos para la identificación y valoración de los activos de información de la Entidad, y definir las responsabilidades para su protección.

Lineamientos:

a. El proceso de Gestión Documental de la Dirección Nacional de Bomberos de Colombia, con el acompañamiento permanente del Oficial de Seguridad y Privacidad de la información o a quien este delegue, deben diseñar una metodología para la identificación, clasificación, valoración y buen uso de los activos de información.

b. Todas las dependencias de la Dirección Nacional de Bomberos de Colombia deben contar con un inventario de sus activos de información y se debe evidenciar a través de los instrumentos dispuestos.

c. El proceso de Gestión Documental de la Dirección Nacional de Bomberos de Colombia con acompañamiento del Oficial de Seguridad y Privacidad de la información o quien este

delegue y el proceso de Planeación Estratégica, deben consolidar los inventarios reportados por los procesos en un instrumento único que contenga todos los activos de información de la Dirección Nacional de Bomberos de Colombia.

d. El proceso de Planeación Estratégica debe extraer del inventario de activos de información de la Dirección Nacional de Bomberos de Colombia lo requerido para el reporte del índice de transparencia, de acuerdo con lo establecido en los instrumentos de gestión de la información adoptados por la Dirección Nacional de Bomberos de Colombia; para la publicación es necesario que cuente con la validación de la Dirección Jurídica en el marco de la clasificación de la información (Pública, Clasificada y Reservada).

e. El proceso de Gestión de Tecnología e Informática debe identificar los ciberactivos (activos de seguridad digital) críticos con base en los activos definidos en el análisis de impacto en el negocio (BIA). Estos ciberactivos son aquellos que contienen, trasmiten o procesan información de los servicios esenciales de la Dirección Nacional de Bomberos de Colombia.

f. Las firmas de documentos oficiales y que se constituye como activos de información de acuerdo con la tabla de retención documental o acto administrativo deben reposar en original o con firma digital del sistema de gestión documental, en ningún caso se debe utilizar firmas facsímil, digitalizadas o escaneadas, salvo en aquellos que se autorice por Resolución expedida por la Dirección Nacional de Bomberos de Colombia, indicando para qué fin y por qué medios podrá ser utilizada.

g. Los empleados públicos y contratistas de la Dirección Nacional de Bomberos de Colombia deben hacer entrega de los activos bajo su responsabilidad de acuerdo con el formato de Paz y Salvo de los procesos de Gestión del Talento Humano y Gestión Contractual.

5.3.2 CLASIFICACIÓN DE LA INFORMACIÓN

Propósito: Establecer lineamientos para la protección de la información de la Entidad, de acuerdo con su criticidad.

Lineamientos:

a. La metodología de clasificación de información de la Dirección Nacional de Bomberos de Colombia que trata la Resolución de Seguridad y Privacidad de la Información, seguridad digital y continuidad de la operación de los servicios, hará parte integral de la metodología para la identificación, clasificación, valoración y buen uso de los activos de información, que trata el lineamiento de Clasificación de la Información.

b. El proceso de Gestión Documental de la Dirección Nacional de Bomberos de Colombia en conjunto con el Oficial de Seguridad y Privacidad de la información o a quien este delegue deben diseñar la documentación pertinente para el rotulado de la información física y digital de acuerdo con lo establecido en la normatividad sobre información pública y protección de datos personales.

c. Las Tablas de Retención Documental (TRD) deben indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas.

d. El Proceso de Gestión de Tecnología e Informática, debe cumplir con los requerimientos de uso, manipulación y conservación de los medios tecnológicos para el

almacenamiento de información dadas por el fabricante, con el fin de mantener la disponibilidad e integridad de la información.

e. Los colaboradores deben aplicar la clasificación de la información de la Dirección Nacional de Bomberos de Colombia, de acuerdo con las TRD, el inventario de activos de información y la documentación pertinente para el rotulado de la información.

f. Cada Propietario del activo de Información debe velar por el cumplimiento de su clasificación de acuerdo con lo establecido en la documentación pertinente para el rotulado de la información.

g. Para el intercambio de información se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

5.3.3 MANEJO DE MEDIOS

Propósito: Establecer lineamientos para evitar la divulgación, modificación, retiro o destrucción de la información almacenada en los medios de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e Informática, en acompañamiento del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces deben establecer la documentación necesaria para el uso correcto y control de medios removibles.

b. El proceso de Gestión de Tecnología e Informática en acompañamiento del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces deben proveer a los usuarios de la Dirección Nacional de Bomberos de Colombia, los métodos de cifrado de la información, así como administrar el software o herramienta utilizado para tal fin, y poner a disposición la guía para el usuario.

c. Todo medio removible deberá ser escaneado mediante el antivirus suministrado por Proceso de Gestión de Tecnología Informática el proceso de Gestión de Tecnología e informática cada vez que se conecte a un equipo de la Dirección Nacional de Bomberos de Colombia.

d. Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío de este.

e. Se prohíbe el uso de medios removibles que contengan información reservada o clasificada de la Dirección Nacional de Bomberos de Colombia en dispositivos de acceso al público.

f. La Subdirección Administrativa y Financiera de la Dirección Nacional de Bomberos de Colombia, debe crear o actualizar si fuere necesario el procedimiento o documento donde se establezca la disposición final de residuos de aparatos eléctricos y electrónicos (RAEE).

g. Se deberán emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los medios de propiedad de la Dirección Nacional de Bomberos de Colombia o en servicio de alquiler que serán reutilizados o eliminados y dejar evidencias

de la actividad, con el fin de controlar que la información de la Dirección Nacional de Bomberos de Colombia contenida en estos medios no se pueda recuperar. Esta solicitud deberá ser mediante requerimiento a la Mesa de Servicios, con aprobación del jefe inmediato o supervisor de contrato.

h. Cuando se requiera transferir un medio de almacenamiento de información de la Dirección Nacional de Bomberos de Colombia a otras entidades se deben establecer un acuerdo entre las partes. Dichos acuerdos deben dirigirse a la transferencia segura de información de interés entre de la Dirección Nacional de Bomberos de Colombia, y las partes.

i. Cuando en la Dirección Nacional de Bomberos de Colombia se requiera transferir un medio de almacenamiento se debe tener en cuenta el registro de contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y el recibido.

j. Los colaboradores y terceras partes que interactúen en procesos de intercambio de información al exterior de la Dirección Nacional de Bomberos de Colombia deben cumplir los lineamientos, recomendaciones o estrategias establecidas por el proceso de Gestión de Tecnología Informática con el fin de garantizar su recuperación en caso de desastre.

k. El transporte para los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información de la Dirección Nacional de Bomberos de Colombia.

5.4 LINEAMIENTOS DE SEGURIDAD PARA EL CONTROL DE ACCESO

5.4.1 REQUISITOS PARA EL CONTROL DE ACCESO

Propósito: Establecer e implementar directrices y lineamientos para controlar el acceso a la información y las instalaciones de procesamiento de información de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe suministrar a los usuarios las credenciales para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados; las credenciales de acceso son de uso personal e intransferible.

b. La conexión remota a servicios específicos de infraestructura tecnológica a los cuales se acceden a través de la red de área local de la Dirección Nacional de Bomberos de Colombia debe establecerse a través de una conexión VPN, la cual deberá ser aprobada, registrada y monitoreada por la Proceso de Gestión de Tecnología Informática; además, se debe mantener una relación de las VPN con su respectiva solicitud de creación.

c. El proceso de Gestión de Tecnología e informática debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servicios.

d. El proceso de Gestión de Tecnología e informática debe establecer para el control de acceso a los datos, información y servicios el principio del menor privilegio y la necesidad de conocer, lo que implica que no se otorgará acceso a menos que sea explícitamente autorizado.

e. El proceso de Gestión de Tecnología e informática debe verificar periódicamente los controles de acceso para los usuarios de la Dirección Nacional de Bomberos de Colombia y los provistos a terceras partes, con el fin de revisar que dichos usuarios tengan los permisos únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

f. El proceso de Gestión de Tecnología e informática debe revisar que los equipos personales de los colaboradores que se conecten a las redes de datos de la Dirección Nacional de Bomberos de Colombia cumplan con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.

g. El Gestión de Tecnología e informática, debe controlar la utilización de conexiones a través de proxys anónimos o técnicas similares, a fin de minimizar los riesgos de seguridad digital de estas técnicas.

5.4.2 GESTIÓN DE ACCESO DE USUARIOS

Propósito: Establecer e implementar directrices y lineamientos para prevenir el acceso no autorizado a sistemas y servicios de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El Proceso de Gestión de Tecnología e informática, debe definir mecanismos para documentar el registro y la inhabilitación de usuarios para el acceso a los recursos de Tecnología de la Información de la Dirección Nacional de Bomberos de Colombia, teniendo en cuenta que las identificaciones de los usuarios deberán ser únicas.

b. El proceso de Gestión de Tecnología e informática debe definir un estándar para la identificación de usuarios, teniendo en cuenta los siguientes parámetros:

- Usar la primera letra del primer nombre más el apellido, en caso de homónimos se utiliza, la primera letra del primer nombre más la primera letra del segundo nombre más el apellido, de persistir la situación, se deberá utilizar la primera letra del primer nombre más el apellido, seguido de la primera letra del segundo apellido; si todas las opciones anteriores se encuentra en uso, se utilizará la primera letra del primer nombre más la primera letra del segundo nombre más el primer apellido más la primera letra del segundo apellido. El nombre para mostrar debe ser los nombres y apellidos completos. El usuario de correo electrónico debe ser igual al usuario de red, es decir, debe existir interoperabilidad entre el servicio de correo y el directorio activo (DA). El proceso de Gestión de Tecnología e informática solo otorgará a los usuarios accesos solicitados y autorizados por el jefe inmediato o supervisor del contrato. Las cuentas de usuario por defecto de los sistemas operativos o aplicaciones tales como: "root", "adm", "admin", "administrador", "SQLAdmin", "administrator" y "system", entre otros, deben ser deshabilitadas siempre que no sean de uso obligatorio para el funcionamiento del servicio, de ser así, las credenciales de acceso deben ser asignadas, controladas, monitoreadas y vigiladas por los administradores de los

servicios del proceso de Gestión de Tecnología Informática, éstas deben cumplir con los parámetros definidos para el uso de contraseñas.

c. Solo se debe otorgar los privilegios para la administración de recursos tecnológicos, servicios de red, sistema operativo y sistemas de información únicamente a aquellos colaboradores que cumplan dichas funciones, deben ser cuentas únicas asociadas al usuario de dominio del colaborador; en caso de requerirse usuarios de acceso genérico, éstos deben ser entregados al colaborador de manera formal por parte del jefe inmediato o supervisor del contrato; en caso de cambiar el titular de la cuenta genérica la contraseña de acceso debe ser modificada me manera inmediata.

d. Los usuarios administradores de recursos tecnológicos, servicios de red, sistema operativo y sistemas de información, entre otros, tienen la responsabilidad de entregar para la custodia según procedimiento establecido por el proceso de Gestión de Tecnología Informática todas las cuentas y claves administradoras bajo su responsabilidad.

e. Se deben restringir las conexiones remotas para la administración de la plataforma tecnológica; únicamente se deberá permitir el acceso a los colaboradores autorizados por El proceso de Gestión de Tecnología e informática.

f. El proceso de Gestión de Tecnología e informática debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos.

g. El proceso de Gestión de Tecnología e informática de la Información debe mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos.

h. La contraseña para la autenticación se debe suministrar a los usuarios de manera segura, y el sistema debe solicitar el cambio inmediato de la misma al ingresar.

i. Se debe establecer mecanismos para verificar la identidad de un usuario antes de reemplazar la información secreta para la autenticación o proporcionar una nueva o temporal.

j. El proceso de Gestión de Tecnología e informática debe generar reportes de uso de cada uno de los sistemas de información o recursos tecnológicos con el fin de identificar la periodicidad de uso de los usuarios, en caso de identificar inactividad mayor o igual a 15 días hábiles se bloqueará el usuario y se debe realizar validación con el área a la que pertenece para determinar si se procede a la deshabilitación definitiva o temporal por novedad.

k. El proceso de Gestión de Tecnología e informática debe revisar los derechos de acceso de los usuarios administradores por lo menos cada seis meses, técnicamente dos veces al año.

l. Para realizar el ajuste o retiro de los derechos de acceso se debe tener en cuenta lo establecido en el control de terminación y cambio de empleo de este documento.

m. El proceso de Gestión de Tecnología e informática debe establecer mecanismos para verificar y documentar el monitoreo a las actividades realizadas por los usuarios con accesos privilegiados por lo menos una vez al año.

n. El proceso de Gestión de Tecnología e informática debe establecer mecanismos para documentar la creación, asignación y custodia de contraseñas de los usuarios superadministradores de las herramientas de administración que se crean para configurar los servicios de la operación tecnológica de la Dirección Nacional de Bomberos de Colombia, teniendo en cuenta las siguientes recomendaciones para establecerla de manera segura:

- Poseer un nivel de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, cónyuge o mascotas, placas de automóvil, fechas de aniversarios, cumpleaños, nombre de usuario, el nombre real o las siglas DNBC, etc.
- Tener como mínimo ocho (8) caracteres alfanuméricos sin repetición. Estar compuestas por: letras en mayúsculas "A, B, C…", letras en minúsculas "a, b, c…", números "0, 1, 2, 3…", símbolos especiales "@, #, $, %, &, (), ¡, !, ¿, ?, <>…" en cualquier combinación.
- No registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado por el proceso de Gestión de Tecnología e informática.
- Debe cambiarse si se han detectado anomalías en la cuenta de usuario.
- En las plataformas que cuenten con la tecnología de doble factor de autenticación, se debe implementar este protocolo de seguridad en todos los usuarios.

5.4.3 RESPONSABILIDADES DE LOS USUARIOS

Propósito: Establecer e implementar directrices y lineamientos para que los usuarios salvaguarden sus credenciales de acceso a los servicios de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta, su jefe inmediato o supervisor del contrato.

b. Los usuarios deben usar contraseñas seguras, es decir:

- Poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, cónyuge o, mascotas, placas de automóvil, fechas de aniversarios, cumpleaños, nombre de usuario, el nombre real o las siglas DNBC, etc.
- No usar las mismas contraseñas de autenticación laboral para uso personal.
- Los usuarios deben cambiar contraseñas si detectan anomalías en su cuenta de usuario.
- No registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado por el Proceso de Gestión de Tecnología Informática.

c. La contraseña debe cumplir con las siguientes recomendaciones como mínimo:

- Deberá tener como mínimo ocho (8) caracteres alfanuméricos sin repetición.
- Deben ser diferentes de otras contraseñas anteriores proporcionadas, es decir las últimas diez (10) suministradas al dominio no se deberán repetir.

- Deben estar compuestas por: letras en mayúsculas "A, B, C…", letras en minúsculas "a, b, c…", números "0, 1, 2, 3…", símbolos especiales "@, #, $, %, &, (), ¡, !¡, ¿,?, <>…" en cualquier combinación.
- Debe cambiarse obligatoriamente cada 90 días.
- Después de 3 (tres) intentos no exitosos de ingreso de la contraseña el usuario deberá ser bloqueado de manera inmediata y deberá esperar un tiempo determinado de 2 minutos para volver a intentar, o solicitar el desbloqueo a través de la Mesa de Servicios.
- Debe no ser visible en la pantalla, al momento de ser ingresada.

5.4.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Propósito: Establecer e implementar directrices y lineamientos para prevenir el acceso no autorizado a los sistemas y aplicaciones y servicios de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe implementar controles para que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestran los mensajes de identificación apropiados para reducir los riesgos de error.

b. El proceso de Gestión de Tecnología e informática debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

c. El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.

d. Las sesiones inactivas deben cerrarse después de un período de inactividad definido de 5 minutos y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.

e. El Proceso de Gestión de Tecnología Informática debe integrar la autenticación de las aplicaciones con el Directorio Activo.

f. El proceso de Gestión de Tecnología Informática debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo programas utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos sin ser debidamente autorizados.

g. El proceso de Gestión de Tecnología e informática debe monitorear a los administradores de los recursos tecnológicos y servicios de red, para que no hagan uso de programas utilitarios que permitan acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.

h. El proceso de Gestión de Tecnología e informática debe generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información autorizados.

i. El proceso de Gestión de Tecnología e informática debe retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información y bloquear su conexión a través de los servicios perimetrales e internos de seguridad informática.

j. El acceso al código fuente del programa es limitado, solamente será para los ingenieros desarrolladores y de soporte autorizados del proceso de Gestión de Tecnología Informática.

k. Las librerías de los sistemas de información no deberán estar contenidas en el ambiente de producción.

5.5 LINEAMIENTOS DE SEGURIDAD PARA EL USO DE RECURSOS CRIPTOGRÁFICOS

5.5.1 CONTROLES CRIPTOGRÁFICOS

Propósito: Establecer e implementar directrices y lineamientos para el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe establecer los controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas.
- Para la información digital reservada y clasificada.
- Para el envió de correo electrónico con información reservada y clasificada.
- En los canales digitales oficiales de recepción de solicitudes, peticiones y de información, dispuestos en la sede electrónica de la Dirección Nacional de Bomberos de Colombia.

b. El proceso de Gestión de Tecnología e Informática debe verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.

c. El proceso de Gestión de Tecnología e informática debe desarrollar, establecer e implementar estándares para la aplicación de controles criptográficos en los datos y servicios que lo requieran por su criticidad.

d. El proceso de Gestión de Tecnología e informática debe utilizar controles criptográficos para la transmisión de información clasificada o reservada, fuera del ámbito de la Dirección Nacional de Bomberos de Colombia.

e. El proceso de Gestión de Tecnología e Informática en cabeza de los proveedores de desarrollo de software deben asegurar que los controles criptográficos de los sistemas de información construidos cumplen con los estándares establecidos en el contrato por la Dirección Nacional de Bomberos de Colombia.

f. El proceso de Gestión de Tecnología de la Información debe disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.

g. El proceso de Gestión de Tecnología Informática debe establecer mecanismos para documentar la gestión de llaves criptográficas donde se evidencie el ciclo desde su creación hasta el retiro y destrucción.

5.6 LINEAMIENTOS DE SEGURIDAD FÍSICA Y DEL ENTORNO

5.6.1 ÁREAS SEGURAS

Propósito: Establecer e implementar directrices y lineamientos para prevenir el acceso físico no autorizado, el daño e interferencia de la información e instalaciones de procesamiento de información de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. La Subdirección Administrativa y Financiera debe señalizar las áreas seguras de acuerdo con el inventario de áreas seguras. Este trabajo debe realizarse en compañía de la Oficina encargada de la Seguridad Física del Edificio Elemento, el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y El proceso de Gestión de Tecnología e informática de la Dirección Nacional de Bomberos de Colombia.

b. Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.

c. Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o instalación.

d. El perímetro de seguridad de las áreas seguras debe contar con vigilancia mediante CCTV y debe ser monitoreado por el personal de vigilancia.

e. La Subdirección Administrativa y Financiera debe establecer un sistema de control de acceso a las instalaciones de la Dirección Nacional de Bomberos de Colombia en compañía del proceso de Gestión Tecnología de la Información de la Seguridad Física del Edificio Elemento, así como a las áreas seguras, se debe documentar mediante un procedimiento, manual o documento, de acuerdo con la estructura documental de la Dirección Nacional de Bomberos de Colombia y la oficina encargada de este proceso en el Edificio Elemento.

f. El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc., que ingresen los colaboradores o visitantes al momento de ingresar al piso 15 de la Torre Aqua del Edificio Elemento donde se encuentra la Dirección Nacional de Bomberos de Colombia.

g. El personal de vigilancia de la Dirección Nacional de Bomberos de Colombia, debe registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo de cómputo (pc o portátil, mouse, teclado, cargador, etc.), servidor, equipos activos de red o cualquier equipo electrónico diferentes a celular; en caso de que estos equipos sean de propiedad de la Dirección Nacional de Bomberos de Colombia, deberán contar con autorización expresa de la Subdirección Administrativa de acuerdo con los procedimientos establecidos para tal fin.

h. El proceso de Gestión de Tecnología e informática debe controlar el ingreso a los Centros de Datos y Centros de Cableado de la Dirección Nacional de Bomberos de Colombia.

i. El proceso de Gestión de Tecnología e informática será la encargada de autorizar el ingreso a personal ajeno a la Dirección Nacional de Bomberos de Colombia a los Centros de Datos y Centros de Cableado, este deberá estar acompañado por quien sea autorizado, éste se hará responsable de la estadía del personal ajeno a la Dirección Nacional de Bomberos de Colombia durante el tiempo que permanezca en las instalaciones.

j. Todo el personal que ingrese al Centro de Datos y Centros de Cableado deberá portar identificación visible y presentarla en la puerta de acceso antes de su ingreso.

k. La Subdirección Administrativa y Financiera, y el proceso de Gestión de Tecnología Informática mancomunadamente son las responsables de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión (Patch Panel) de los Centros de Cableado.

l. La Subdirección Administrativa y Financiera y el proceso de Gestión de Tecnología e Informática, mancomunadamente son las responsables mantener en buen estado la infraestructura física de los Centros de Cableado y Centros de Datos de la Dirección Nacional de Bomberos de Colombia, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, sensores, entre otros.

m. El proceso de Evaluación y Seguimiento de acuerdo al Programa Anual de Auditoría Interna, aprobado por el Comité Institucional de Coordinación de Control Interno y una vez establecido que la revisión del estado de los centros de cableado es de alto riesgo, debe contemplar como un objetivo la revisión del estado de estos espacios e informar cualquier anomalía presentada de la siguiente manera: daños en el rack y equipos activos de red al proceso de Gestión de Tecnología Informática, y daños en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros) a la Subdirección Administrativa y Financiera de la Dirección Nacional de Bomberos de Colombia.

n. La Subdirección Administrativa y Financiera, es la responsable del cumplimiento del protocolo de aseo en los Centros de Cableado y Centro de Datos, este último contará con el acompañamiento del proceso de Gestión de Tecnología Informática.

o. El proceso de Gestión de Tecnología e informática es responsable de mantener organizado e identificado el cableado en los racks de los Centros Cableado y Centro de Datos.

p. Se debe establecer un plan de mantenimiento locativo para los Centros de Cableado por parte de la Subdirección Administrativa y Financiera, y un plan de mantenimiento de los recursos tecnológicos por parte del proceso de Gestión de Tecnología Informática de tal manera que se corrijan fallas y/o establecer mejoras en los mismos.

q. La Subdirección Administrativa y Financiera en compañía del proceso de Gestión de Tecnología Informática son los responsables de respaldar los videos generados por las cámaras de vigilancia e información generada de los accesos a los Centros Cableado y Centro de Datos y demás instalaciones de la Dirección Nacional de Bomberos de Colombia que cuenten con trol de acceso, se debe tener en cuenta las políticas de respaldo de la información de la entidad.

r. La Subdirección Administrativa y Financiera, y el proceso de Gestión de Tecnología e informática debe mantener libre de objetos o elementos que no sean propios en la operación en el Centro de Datos y Centros de Cableado de la Dirección Nacional de Bomberos de Colombia.

s. La Subdirección Administrativa y Financiera debe establecer mecanismos de seguridad para el ingreso a las áreas de procesamiento de pagos y debe ser monitoreado mediante circuito cerrado de televisión (CCTV), que cubra el acceso al área y al funcionario que utilice los equipos financieros, en ningún caso deberá grabarse o monitorear directamente la pantalla o el teclado de los equipos financieros.

t. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces el proceso de Gestión de Tecnología e Informática y la Subdirección Administrativa y Financiera deben desarrollar la documentación de Seguridad para el manejo y control de los recursos tecnológicos utilizados para la administración y gestión financiera de la Dirección Nacional de Bomberos de Colombia.

u. La Subdirección Administrativa y Financiera con el apoyo del proceso de Gestión de Tecnología Informática establecerán los lineamientos para los controles contra amenazas externas y ambientales y quedarán enmarcadas en los planes de contingencia, de emergencia y de continuidad del negocio.

v. En las áreas seguras se debe restringir el uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello por parte del área encargada, esta prohibición debe estar señalizada.

w. El trabajo en áreas seguras debe estar monitoreado por CCTV, se debe tener en cuenta que las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas.

x. Se prohíbe el consumo de alimentos y bebidas en las áreas seguras de la Dirección Nacional de Bomberos de Colombia esta prohibición debe ser señalizada.

y. La Subdirección Administrativa y Financiera debe señalizar las áreas de cargue y descargue de la Dirección Nacional de Bomberos de Colombia.

z. El personal de vigilancia con el acompañamiento de la Subdirección Administrativa y Financiera debe inspeccionar y examinar el material que ingresa por las áreas de cargue para determinar la presencia de materiales peligrosos.

aa. La Subdirección Administrativa y Financiera debe señalizar las áreas de la Dirección Nacional de Bomberos de Colombia, donde se esté grabando y monitoreadas mediante CCTV.

5.6.2 EQUIPOS

Propósito: Establecer lineamientos para prevenir pérdidas, daños, robos o compromisos de activos y la interrupción de la operación de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. La Subdirección Administrativa y Financiera con el apoyo del proceso de Gestión de Tecnología e informática propenderán que los equipos de cómputo e impresoras estén situados y protegidos en áreas para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.

b. El proceso de Tecnología de la Información debe propender que los equipos de cómputo portátiles suministrados por la Dirección Nacional de Bomberos de Colombia se protejan mediante mecanismos que no permitan su pérdida.

c. La Subdirección Administrativa y Financiera con el apoyo del proceso de Gestión de Tecnología Informática deben establecer los lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deben conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deben conectarse a la red eléctrica no regulada.

d. La Subdirección Administrativa y Financiera con el apoyo del proceso de Gestión de Tecnología e Informática deben implementar mecanismos para regular el flujo de energía e interrupciones causadas por fallas en el soporte de los servicios públicos que puedan afectar los equipos de cómputo y procesamiento de información.

e. Para propender por la continuidad de los servicios y la operación de la Dirección Nacional de Bomberos de Colombia en caso de fallas en el fluido eléctrico externo, la Subdirección Administrativa y Financiera en compañía del proceso de Gestión de Tecnología e informática deben suministrar las UPS de acuerdo con el proceso crítico, cabe resaltar que se debe garantizar el manteamiento preventivo y correctivo de estos Sistema de Alimentación Ininterrumpida.

f. La Subdirección Administrativa y Financiera con el apoyo del proceso de Gestión de Tecnología Informática deben proteger el cableado que transporta voz, datos y suministro de energía eléctrica contra la interceptación, interferencia o daños de cualquier tipo dentro del perímetro de la Dirección Nacional de Bomberos de Colombia.

g. Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para evitar interferencia y ruido. Al momento de instalar o actualizar el cableado estructurado se debe tener en cuenta las consideraciones técnicas de las normas vigentes y el Reglamento Técnico de Instalaciones Eléctricas (RETIE).

h. Solo el personal autorizado por el proceso de Gestión de Tecnología e Informática puede llevar a cabo el mantenimiento o las reparaciones a los equipos de cómputo, servidores activos de red.

i. Los cuartos de cableado solo podrán tener los elementos activos para su funcionamiento y no utilizarse como almacén para guardar cajas, mesas u otros equipos que no estén en uso.

j. El proceso de Gestión de Tecnología e informática debe definir mecanismos de soporte y mantenimiento a los equipos de cómputo, servidores y equipos activos de red y debe llevar registro de estos.

k. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser

programadas por el proceso de Gestión de Tecnología e informática y surtir el proceso de gestión de cambios definido por la Dirección Nacional de Bomberos de Colombia.

l. En los casos en que los equipos requieran salir de las instalaciones de la Dirección Nacional de Bomberos de Colombia por alguno de los siguientes eventos: reparación, mantenimiento o cambio, el proceso de Gestión de Tecnología e informática debe realizar respaldo de la información y un borrado seguro.

m. Cuando un equipo o medio extraíble sea reasignado o retirado de servicio el proceso de Gestión de Tecnología e informática debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad de ésta; en caso de dar de baja para disposición final y no para subastar, se debe tener en cuenta lo establecido en el control de Manejo de Medios literal f.

n. Para el retiro de activos de las instalaciones de la Dirección Nacional de Bomberos de Colombia se debe tener en cuenta lo establecido en el control áreas seguras literal g. del presente documento.

o. Para el retiro de activos del almacén, la Subdirección Administrativa y Financiera deberá llevar un control en el aplicativo de inventarios con el fin de mantener registro de asignación y devolución.

p. Para mantener la seguridad de la información en los equipos y activos fuera de las instalaciones de la Dirección Nacional de Bomberos de Colombia y que contengan información clasificada o reservada, estos deben contar con lo establecido en los Controles Criptográfico literal f.

q. Los Colaboradores de la Dirección Nacional de Bomberos de Colombia durante su ausencia no deberán conservar sobre el escritorio información propia de la Dirección Nacional de Bomberos de Colombia como: documentos físicos o medios de almacenamiento que contengan información clasificada o reservada, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.

r. Los Colaboradores de la Dirección Nacional de Bomberos de Colombia deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el equipo de cómputo.

s. Los Colaboradores de la Dirección Nacional de Bomberos de Colombia que impriman documentos con clasificación (Clasificada – Reservada), estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

t. No se debe reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deben ser destruidos.

u. Los puestos de trabajo de los Colaboradores de la Dirección Nacional de Bomberos de Colombia y terceras partes que prestan sus servicios y cuyas funciones no obliguen a la atención directa de ciudadanos deberán localizarse preferiblemente en ubicaciones físicas que no estén expuestas al público para minimizar los riesgos asociados al acceso no autorizado de la información o a los equipos informáticos.

v. El proceso de Gestión de Tecnología e informática debe configurar como política general que todos los equipos de cómputo que se encuentren en los dominios de la Dirección Nacional de Bomberos de Colombia bloqueen automáticamente la sesión después de Cinco (5) minutos de inactividad. Esto con el fin de garantizar la confidencialidad e integridad de la información que esta almacenada en los equipos de cómputo, y no sea aprovechada la situación por personas inescrupulosas.

w. El proceso de Gestión de Tecnología e informática debe configurar como política general que todos los equipos de cómputo que se encuentren en los dominios de la Dirección Nacional de Bomberos de Colombia oculten de manera automáticas los iconos, accesos directos o documentos que se encuentren en el escritorio.

5.7 LINEAMIENTOS DE SEGURIDAD DE LAS OPERACIONES

5.7.1 PROCEDIMIENTOS OPERACIONALES

Propósito: Establecer e implementar directrices y lineamientos para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.

b. El proceso de Gestión de Tecnología e informática debe poner a disposición de todos los colaboradores los procedimientos de operación mediante los medios que la Dirección Nacional de Bomberos de Colombia disponga.

c. El proceso de Gestión de Tecnología e informática debe establecer mecanismos documentados que permitan asegurar la gestión de cambios normales y de emergencia a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar las actividades y responsables en la gestión de cambios.

d. El proceso de Gestión de Tecnología e informática debe establecer el comité de cambios normales y el de emergencia, quien se encargará de evaluar, aprobar o negar la implementación de los cambios y este a su vez será presidido por el Gestor de Cambios.

e. El proceso de Gestión de Tecnología e informática debe establecer una guía o manual de operación de gestión de cambios normales y de emergencia que contenga el detalle operativo del proceso de cambios.

f. El proceso de Gestión de Tecnología e informática debe documentar la gestión de capacidad de la plataforma tecnológica, definir su responsable y mantenerla actualizada, la cual permita:

- Evaluar las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

- Monitorear el rendimiento de la infraestructura tecnológica para determinar el uso de la capacidad existente.
- Documentar los datos de rendimiento y capacidad de la plataforma tecnológica de la Dirección Nacional de Bomberos de Colombia.
- Documentar los acuerdos de niveles de servicio.
- Asignar los recursos adecuados de hardware y software, para todos los servicios y aplicaciones de tecnología.
- El proceso de Gestión de Tecnología e informática debe documentar las recomendaciones de mejora de la infraestructura de tecnología.
- El proceso de Gestión de Tecnología e informática debe definir los indicadores de monitoreo correspondientes a la gestión de capacidad de la plataforma tecnológica.
- El proceso de Gestión de Tecnología e informática debe propender por la separación de los ambientes de desarrollo, pruebas y producción, los cuales deben estar separados de manera física y lógica.

g. El proceso de Gestión de Tecnología de la Información debe definir, documentar y aplicar lineamientos seguros para la transferencia entre ambientes.

h. El proceso de Gestión de Tecnología e informática debe utilizar en los ambientes de prueba datos que no sean sensibles para la Dirección Nacional de Bomberos de Colombia o utilizar herramientas o técnicas para ofuscar o anonimizar los datos.

i. El proceso de Gestión de Tecnología e informática debe permitir que los ambientes de prueba, desarrollo y producción sean similares para prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores.

j. El proceso de Gestión de Tecnología de la información debe utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusión y diferenciar de manera clara cada ambiente.

k. Proceso de Gestión de Tecnología Información debe garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

5.7.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Propósito: Establecer e implementar directrices y lineamientos para asegurar que la información y las instalaciones de procesamiento de información de la Entidad estén protegidas contra códigos maliciosos.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos.

b. El proceso de Gestión de Tecnología e informática con el apoyo del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces deben realizar campañas de concienciación de usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.

c. El proceso de Gestión de Tecnología e informática debe mantener actualizada la base de datos, base de firmas y parches correspondiente del software antivirus y debe asegurar que esta herramienta no pueda ser deshabilitada de los equipos de la Dirección Nacional de Bomberos de Colombia.

d. El proceso de Gestión de Tecnología Informática debe dictar los lineamientos para la instalación del software antivirus con el fin de brindar protección contra códigos maliciosos en todos los recursos informáticos de la Dirección Nacional de Bomberos de Colombia.

e. El proceso de Gestión de Tecnología e informática debe aplicar las actualizaciones y parches de seguridad de los sistemas operativos de los equipos y servidores de la Dirección Nacional de Bomberos de Colombia para protegerlos contra códigos maliciosos.

f. Todo mensaje sospechoso de procedencia desconocida debe ser inmediatamente reportado al proceso de Gestión de Tecnología Informática a través de la Mesa de Servicios, tomando las medidas de control necesarias.

g. El proceso de Gestión de Tecnología Informática debe establecer mecanismos para evidenciar la gestión de las alertas desplegadas en la consola de antivirus validando las acciones tomadas para su solución.

5.7.3 COPIAS DE RESPALDO

Propósito: Establecer e implementar directrices y lineamientos para proteger la información de la Entidad contra la pérdida de datos.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe definir y documentar un plan o procedimiento de copias de respaldo y restauración de la información de la Dirección Nacional de Bomberos de Colombia, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo, nivel de criticidad y los criterios utilizados para tomar la muestra de la restauración mensual.

b. El proceso de Gestión de Tecnología e informática debe definir y documentar lineamientos para la realización de copias de respaldo de:

- Bases de datos de producción.
- Software de aplicaciones.
- Sistemas operativos.
- Configuraciones de servidores.
- Software base de la Dirección Nacional de Bomberos de Colombia.
- El proceso de Gestión de Tecnología Informática debe realizar y mantener las copias de respaldo de la información digital solicitadas.

c. El proceso de Gestión de Tecnología e informática debe disponer de herramientas tecnológicas para gestionar la información digital de la Dirección Nacional de Bomberos de Colombia y asegurar que estas dispongan de copias de respaldo.

d. El proceso de Gestión de Tecnología e informática debe definir mecanismos para la custodia y almacenamiento de las copias de respaldo.

e. El proceso de Gestión de Tecnología e informática debe tener un inventario y bitácora de las copias de respaldo que se realizan y de las copias de respaldo que se restauran.

f. El proceso de Gestión de Tecnología e informática debe generar mecanismos que mantengan la integridad y confidencialidad de las copias de respaldo.

g. Los colaboradores deben utilizar las herramientas tecnológicas dispuesta por el proceso de Gestión de Tecnología e informática para gestionar y hacer backup de la información de la Dirección Nacional de Bomberos de Colombia.

h. Los colaboradores son responsables de la información que resida en el equipo asignado y serán los encargados de mantener las copias de respaldo de sus archivos, y la información debe ser entregada al supervisor del contrato o jefe inmediato al finalizar su vinculación con la Dirección Nacional de Bomberos de Colombia. En caso de que los colaboradores requieran la ejecución de una copia de respaldo de su información, lo pueden solicitar al proceso de Gestión de Tecnología Informática a través de la Mesa de Servicios.

5.7.4 REGISTRO Y SEGUIMIENTO

Propósito: Establecer lineamientos para registrar los eventos de seguridad de la información de la Entidad y generar las evidencias.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.

b. El proceso de Gestión de Tecnología e informática debe salvaguardar los registros de auditoría que se generen de cada sistema.

c. El proceso de Gestión de Tecnología e informática debe monitorear las excepciones o los eventos de seguridad de la información.

d. El proceso de Gestión de Tecnología e informática debe monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y de la Misión de la Dirección Nacional de Bomberos de Colombia y atender cualquier alerta que se genere.

e. El proceso de Gestión de Tecnología e informática debe sincronizar los relojes de los servidores con una única fuente de referencia de tiempo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría.

f. El proceso de Gestión de Tecnología e informática debe monitorear, identificar e informar sobre las transferencias de grandes volúmenes de información por fuera del dominio, con el fin de prevenir fugas de información. Los responsables técnicos de los sistemas de información, base de datos, equipos de infraestructura tecnológica, deben propender

porque los mismos tengan activados o implementados sus logs de auditoría a fin de evidenciar fallas o cambios no autorizados.

5.7.5 CONTROL DE SOFTWARE OPERACIONAL

Propósito: Establecer e implementar directrices y lineamientos para asegurar la integridad de los sistemas operacionales de la Dirección Nacional de Bomberos de Colombia.
Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios de la Dirección Nacional de Bomberos de Colombia.

b. El proceso de Gestión de Tecnología e informática debe conservar las versiones anteriores del software de aplicación como una medida de contingencia.

c. El proceso de Gestión de Tecnología e informática debe usar controles para proteger todo el software implementado y la documentación del sistema.

5.8 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

Propósito: Establecer lineamientos para prevenir la explotación de las vulnerabilidades técnicas de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe realizar mínimo una vez al año una revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de Ethical Hacking y/o pruebas de penetración.

b. El proceso de Gestión de Tecnología e informática debe establecer mecanismos para documentar, informar, gestionar y corregir las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.

c. El proceso de Gestión de Tecnología e informática debe definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, las pruebas de gestión, la aplicación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.

d. El proceso de Gestión de Tecnología Informática debe probar y evaluar la aplicación de actualizaciones antes de su instalación y valorar los riesgos asociados, para asegurar que son eficaces y no producen efectos secundarios.

e. El proceso de Gestión de Tecnología Informática debe restringir a los usuarios finales la instalación de software en los equipos de la Dirección Nacional de Bomberos de Colombia.

f. El proceso de Gestión de Tecnología Informática debe establecer y monitorear que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas, y atender cualquier alerta que se genere.

g. El proceso de Gestión de Tecnología e informática debe controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole los derechos de autor.

h. El proceso de Gestión de Tecnología e informática debe realizar de manera periódica una inspección del software instalado en los equipos de la Dirección Nacional de Bomberos de Colombia y debe desinstalar el software no autorizado.

i. El proceso de Gestión de Tecnología Informática a través de la mesa de servicios es la responsable de instalar, configurar y dar soporte a los equipos de la Dirección Nacional de Bomberos de Colombia.

j. Sólo está permitido el uso de software licenciado por la Dirección Nacional de Bomberos de Colombia y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por el Proceso de Gestión de Tecnología Informática.

k. Las aplicaciones generadas por la Dirección Nacional de Bomberos de Colombia en desarrollo de su misión institucional deben ser reportadas al proceso de Gestión de Tecnología Informática para su administración.

l. El proceso de Gestión de Tecnología Informática es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales y comerciales.

5.8.1 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

Propósito: Establecer e implementar directrices y lineamientos para minimizar el impacto de las actividades de auditoría sobre los sistemas operativos de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Evaluación y Seguimiento de acuerdo con el Programa Anual de Auditoría Interna, aprobado por el Comité Institucional de Coordinación de Control Interno ejecutará auditorías a los sistemas de información críticos en producción cuando se encuentren contemplados en la planeación y para ello tendrá acceso limitado a los datos en modo de solo consulta.

b. El proceso de Evaluación y Seguimiento debe mantener los documentos, dispositivos y medios utilizados para las auditorías de los Sistemas de Información custodiados de accesos no autorizados.

c. El proceso de Evaluación y Seguimiento debe documentar los resultados de las auditorías de los sistemas de Información de la Dirección Nacional de Bomberos de Colombia.

5.9 LINEAMIENTOS DE SEGURIDAD DE LAS COMUNICACIONES

5.9.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES

Propósito: Establecer e implementar directrices y lineamientos para asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe proporcionar una plataforma tecnológica que soporte los sistemas de información, esta debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.

b. El proceso de Gestión de Tecnología e informática debe realizar segmentación de redes para colaboradores y visitantes de la Dirección Nacional de Bomberos de Colombia.

c. El proceso de Gestión de Tecnología e informática debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

d. El proceso de Gestión de Tecnología e informática es el responsable de garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

e. El proceso de Gestión de Tecnología e informática debe establecer la documentación necesaria para la utilización de los servicios de red y aplicaciones.

f. El proceso de Gestión de Tecnología e informática debe realizar revisiones y monitoreo regularmente a la gestión de los servicios para validar que se encuentran en los acuerdos de servicios de red establecidos con los proveedores.

g. El proceso de Gestión de Tecnología e informática debe definir controles para la transferencia de información a través de redes públicas para las aplicaciones de la Dirección Nacional de Bomberos de Colombia.

h. El proceso de Gestión de Tecnología e informática debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones de la Dirección Nacional de Bomberos de Colombia, teniendo en cuenta los siguientes criterios:

- Contar con información de autenticación secreta de usuario.
- Cifrar las comunicaciones entre DMZ y los servidores de la red interna.
- Los protocolos de comunicación entre la red interna y la DMZ están asegurados con el fin de prevenir fugas de información.
- La información almacenada de las transacciones no se encuentra pública.

i. El proceso de Gestión de Tecnología e informática debe disponer de una zona desmilitarizada o DMZ, entre la red interna de la Dirección Nacional de Bomberos de Colombia y la red externa (internet) con el objetivo de delimitar conexiones desde la red interna hacia Internet y limitar las conexiones desde internet hacia la red interna de la Dirección Nacional de Bomberos de Colombia con los siguientes criterios:

  - El tráfico de la red externa a la DMZ está limitado

- El tráfico de la red externa a la red interna está prohibido
- El tráfico de la red interna a la DMZ está limitado
- El tráfico de la red interna a la red externa está autorizado
- El tráfico de la DMZ a la red interna está prohibido
- El tráfico de la DMZ a la red externa está denegado

j. La DMZ se debe implementar para ofrecer servicios que necesitan acceso desde internet. Estos servicios deberán ser monitoreados con el fin de prevenir ataques.

k. La arquitectura de la DMZ debe estar aislada de la red interna de la Dirección Nacional de Bomberos de Colombia de forma que no permita el acceso no autorizado a la red interna, por lo que se deben diseñar redes perimetrales con los siguientes objetivos:

- No se pueden hacer consultas directas a la red interna de la Dirección Nacional de Bomberos de Colombia desde redes externas e internet.
- Se deberá realizar la segmentación de redes y listas de acceso a los servicios de la Dirección Nacional de Bomberos de Colombia tales como servidores, administración, invitados, etc.

l. El acceso a la red de datos de la Dirección Nacional de Bomberos de Colombia y a los sistemas de información soportados por la misma, es de carácter restringido. Se deben conceder permisos con base a "la necesidad de conocer" y el "acceso mínimo requerido" conforme a los criterios de seguridad de la información contemplados en la presente política.

5.9.2 TRANSFERENCIA DE INFORMACIÓN

Propósito: Establecer lineamientos para mantener la seguridad de la información transferida dentro de la Dirección Nacional de Bomberos de Colombia y con cualquier entidad externa.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe contar con los lineamientos para proteger la información transferida con respecto a la interceptación, copiado, modificación, enrutado y destrucción de esta.

b. El proceso de Gestión de Tecnología e informática debe establecer procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.

c. El proceso de Gestión de Tecnología e informática debe establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico de la Dirección Nacional de Bomberos de Colombia.

d. La Subdirección Administrativa y Financiera debe dictar directrices sobre retención, disposición y transferencia de la información física de la Dirección Nacional de Bomberos de Colombia, de acuerdo con la legislación y reglamentaciones local y nacional aplicable.

e. El proceso de Gestión de Tecnología e informática debe establecer un acuerdo para la transferencia de información entre la Dirección Nacional de Bomberos de Colombia.

f. El proceso de Gestión de Tecnología e informática debe establecer mecanismos para el direccionamiento y transporte correctos del mensaje, así como la confiabilidad y disponibilidad del servicio.

g. El proceso de Gestión de Tecnología e informática debe proporcionar herramientas de mensajería electrónica corporativas, como mensajería instantánea, redes sociales etc.

h. Para los acuerdos o compromisos de confidencialidad y de no divulgación se debe tener en cuenta lo establecido en el control antes de asumir el empleo literal de este documento.

i. Para el personal externo que ejecute tareas propias de la Dirección Nacional de Bomberos de Colombia y haya sido contratado en el marco de un contrato o convenio con la Dirección Nacional de Bomberos de Colombia, debe firmar un compromiso de confidencialidad y no divulgación de la información con el Representante Legal, y este debe reposar en la carpeta de ejecución del contrato.

5.10 LINEAMIENTOS DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

5.10.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Propósito: Establecer e implementar directrices y lineamientos para promover que la seguridad de la información haga parte integral de los sistemas de información durante todo su ciclo de vida.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe disponer de requerimientos para las solicitudes de nuevos Sistemas de Información o modificaciones a los existentes en la Dirección Nacional de Bomberos de Colombia que cuenten con el análisis e implementación de criterios de seguridad del software.

b. El proceso de Gestión de Tecnología e informática debe contar con mecanismos para justificar, acordar y documentar en la fase de requisitos y en la fase de modificación de los sistemas de la Dirección Nacional de Bomberos de Colombia, los criterios de Seguridad de la Información.

c. El proceso de Gestión de Tecnología e informática debe contar en los requisitos de Seguridad de la Información con los siguientes criterios:

- El suministro de acceso y de autorización para usuarios de la Dirección Nacional de Bomberos de Colombia, al igual que para usuarios privilegiados o técnicos.
- Informar a los usuarios y operadores sobre sus deberes y responsabilidades.
- Requisitos derivados de los procesos como registro de transacciones, seguimiento y no repudio.

d. El proceso de Gestión de Tecnología e informática debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones de la Dirección Nacional de Bomberos de Colombia, teniendo en cuenta los siguientes criterios:

- Contar con información de autenticación secreta de usuario.
- Mantener la privacidad en las partes involucradas.

- Cifrar las comunicaciones cuando sea necesario.
- Asegurar los protocolos de comunicación.
- La información almacenada de las transacciones no se encuentra pública.

5.10.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE

Propósito: Establecer e implementar directrices y lineamientos para que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe establecer los mecanismos necesarios para la creación de software, teniendo en cuenta los siguientes aspectos:

- Orientar sobre buenas prácticas de seguridad en el desarrollo del software.
- Requisitos de seguridad en el control de versiones.
- Capacidad de los desarrolladores para evitar, encontrar y resolver vulnerabilidades.
- El proceso de Gestión de Tecnología e informática debe tener en cuenta el punto anterior para la reutilización de códigos.

b. El proceso de Gestión de Tecnología e informática debe proteger los códigos ejecutables y código de desarrollo o compiladores del software operacional y aplicaciones propios de la Dirección Nacional de Bomberos de Colombia.

c. El proceso de Gestión de Tecnología e informática debe definir controles para que los cambios en los Sistemas de Información de la Dirección Nacional de Bomberos de Colombia sean documentados, teniendo en cuenta la integridad de los sistemas desde las primeras etapas de diseño y a través de los mantenimientos posteriores.

d. El proceso de Gestión de Tecnología e informática debe definir un proceso formal para inclusión y cambios importantes en los Sistemas de Información involucrando pruebas, control de calidad e implementación.

e. El proceso de Gestión de Tecnología e informática debe definir para los cambios en los Sistemas de la Dirección Nacional de Bomberos de Colombia los siguientes aspectos:

- Niveles de autorización acordados.
- Presentar los cambios a los usuarios autorizados.
- Revisar la integridad para asegurar que no se vean comprometidos los cambios.
- Identificar y validar el código crítico de seguridad.
- Antes de cualquier cambio, se debe asegurar que los usuarios autorizados aceptan los cambios.
- Mantener un control de versiones para las actualizaciones de los sistemas.
- Mantener un rastro de auditoría de los cambios.
- Se debe asegurar que los cambios se hagan en momentos adecuados y que no afecten los procesos de la Dirección Nacional de Bomberos de Colombia. El proceso de Gestión de Tecnología e informática debe guardar en un repositorio, las versiones anteriores de cada sistema de información que es actualizado.

f. El proceso de Gestión de Tecnología e informática debe definir la manera de revisar después de un cambio importante que el Sistema de Información alterado no se haya comprometido.

g. El proceso de Gestión de Tecnología e informática debe definir la manera para notificar a tiempo los cambios de los sistemas, permitiendo realizar pruebas y revisiones apropiadas antes de su implementación.

h. El proceso de Gestión de Tecnología e informática debe evitar las modificaciones a los paquetes de software, en la medida de lo posible se deberán usar directamente los suministrados por el proveedor; limitándose únicamente a cambios necesarios, cuando se hagan, se deberán tener en cuenta los siguientes aspectos:

- El riesgo en que se puede ver involucrado el Sistema de Información.
- Verificar si se requiere consentimiento del proveedor.
- Verificar la posibilidad que el proveedor realice dichos cambios.
- El impacto en dado caso que el mantenimiento futuro recaiga en manos de la Dirección Nacional de Bomberos de Colombia.
- La compatibilidad con otro software en uso.

i. El proceso de Gestión de Tecnología e informática debe conservar el software original cuando se hayan realizado cambios en los paquetes de este.

j. El proceso de Gestión de Tecnología e informática debe documentar el desarrollo de sistemas de información basados en los principios de seguridad.

k. El proceso de Gestión de Tecnología e informática debe realizar verificación periódica a la documentación de los sistemas de información en relación con los estándares de seguridad que hayan surgido y amenazas potenciales.

l. El proceso de Gestión de Tecnología e informática debe definir ambientes de desarrollo seguro, teniendo en cuenta los siguientes aspectos:

- El carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
- Requisitos externos como reglamentaciones o políticas.
- Controles de Seguridad ya establecidos por la Dirección Nacional de Bomberos de Colombia.
- Separación entre diferentes ambientes de desarrollo.
- Control de acceso al ambiente de desarrollo.
- Seguimiento de los cambios en el ambiente de desarrollo y los códigos almacenados allí.
- Control sobre el movimiento de datos desde y hacia el ambiente de desarrollo.

m. El proceso de Gestión de Tecnología e informática debe definir controles para que los sistemas adquiridos externamente cumplan con los siguientes aspectos:

- Acuerdos de licenciamiento, sucesión de derechos patrimoniales, propiedad de códigos y derechos de propiedad intelectual relacionados con el sistema de información contratado externamente.
- Requisitos contractuales para prácticas seguras de desarrollo, diseño, codificación y pruebas.
- Evidencia del uso de umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.

- Evidencia de pruebas para vigilar que no exista contenido malicioso intencional y no intencional en el momento de la entrega.
- Evidencia de pruebas para proteger contra la presencia de vulnerabilidades conocidas.
- Derecho contractual con relación a procesos y controles de desarrollo de auditorías.
- Documentación del ambiente de construcción usado para crear entregables.
- El proceso de Gestión de Tecnología e informática debe contemplar en los cambios y en los nuevos Sistemas de Información, pruebas asociadas a Seguridad de la Información.
- El proceso de Gestión de Tecnología e informática debe contar en sus pruebas de aceptación de sistemas de información requisitos de Seguridad de la Información.

n. El proceso de Gestión de Tecnología e informática debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deberán contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

o. Los desarrolladores deberán asegurar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

p. Los desarrolladores deberán establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cuál fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

q. Los desarrolladores deberán asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deberán deshabilitar la funcionalidad de recordar campos de contraseñas.

r. Los desarrolladores deberán asegurar que se inhabiliten las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

s. Los desarrolladores deberán asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deberán tener un periodo de validez establecido; se deberán forzar el cambio de las contraseñas temporales después de su utilización.

t. Los desarrolladores deberán establecer que periódicamente se valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

u. Adicional a lo anterior y de manera específica, el proceso de Gestión de Tecnologías e informática, y los proveedores en compañía del Oficial de Seguridad y Privacidad de la Información deberán implementar los controles en el desarrollo de sitios web y aplicaciones de acuerdo a lo establecido en el ANEXO 3: condiciones mínimas técnicas y de seguridad digital de Resolución 1519 de 2020.

5.10.3 DATOS DE PRUEBA

Propósito: Establecer e implementar directrices y lineamientos para proteger los datos usados para pruebas.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática debe utilizar herramientas o técnicas para ofuscar o anonimizar los datos o evitar durante la ejecución de pruebas en ambientes de desarrollo el uso de datos que contengan información personal o información sensible de la Dirección Nacional de Bomberos de Colombia que esté contenida en el ambiente de producción de las aplicaciones.

b. El proceso de Gestión de Tecnología e informática debe tener en cuenta controles de acceso a los ambientes de producción y de prueba.

5.11 LINEAMIENTOS DE SEGURIDAD PARA LA RELACIÓN CON LOS PROVEEDORES

5.11.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Propósito: Establecer e implementar directrices y lineamientos para asegurar la protección de los activos de la organización que son accesibles a proveedores de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión Contractual debe establecer lineamientos para el cumplimiento de las obligaciones contractuales del Sistema de Gestión de Seguridad y Privacidad de la Información con terceros o proveedores.

b. El proceso de Gestión Contractual debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información de la Dirección Nacional de Bomberos de Colombia.

c. El proceso de Gestión Contractual deberá establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.

d. El proceso de Gestión de Tecnología e informática debe documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica de la Dirección Nacional de Bomberos de Colombia.

e. El proceso de Gestión de Tecnología e informática debe verificar mensualmente el cumplimiento de acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.

f. Cada dependencia de la Dirección Nacional de Bomberos de Colombia que establezca relación con proveedores y su cadena de suministro, debe solicitar acompañamiento periódico al Sistema de Gestión de Seguridad y Privacidad de la Información con el fin de dar a conocer las políticas que tiene la Dirección Nacional de Bomberos de Colombia.

5.11.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES

Propósito: Mantener el nivel acorde de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

Lineamientos:

a. El proceso de Gestión Contractual debe documentar las obligaciones generales sobre seguridad y privacidad de la información, seguridad digital y continuidad de la operación, alineado con los formatos para su cumplimiento y verificación por parte del supervisor de contrato.

b. El proceso de Gestión de Tecnología e informática debe establecer un mecanismo que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.

5.12 LINEAMIENTOS PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.12.1 Gestión de incidentes de seguridad de la información y mejoras.

Propósito: Establecer e implementar directrices y lineamientos para asegurar una administración de incidentes de seguridad de la información coherente y eficaz con base a un enfoque de comunicación de los eventos y las debilidades de seguridad de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática en compañía del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y la Subdirección Administrativa y Financiera deben definir un mecanismo para la gestión de incidentes de seguridad de la información.

b. El proceso de Gestión de Tecnología Informática debe definir los canales para que los colaboradores de la Dirección Nacional de Bomberos de Colombia puedan reportar los incidentes de Seguridad de la Información.

c. El proceso de Gestión de Tecnología e informática es la encargada en primera instancia de evaluar y atender los eventos, debilidades e incidentes de seguridad de la información y de tomar decisiones sobre los mismos. En caso de requerir apoyo o asesoría externa de autoridades o profesionales especializados en seguridad se debe solicitar a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces.

d. El proceso de Gestión de Tecnología e informática debe definir los mecanismos para la recolección de evidencias de elementos informáticos, con el fin de garantizar la autenticidad de los elementos materiales de prueba recolectados y examinados, asegurando que pertenecen al caso investigado, sin confusión, adulteración o sustracción.

e. El proceso de Gestión de Tecnología e informática es la encargada de la recolección de evidencias de los incidentes de seguridad de la información.

f. El proceso de Gestión de Tecnología e informática debe contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes establecidos en los lineamientos de Gestión de Incidentes.

g. El proceso de Gestión de Tecnología e informática debe proporcionar los medios para la gestión de conocimiento de los incidentes de Seguridad de la Información presentados.

h. El proceso de Gestión de Tecnología e informática en compañía del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y la Subdirección Administrativa y Financiera deben dar a conocer a los colaboradores de la Dirección Nacional de Bomberos de Colombia los lineamientos establecidos para la Gestión de Incidentes de Seguridad de la Información.

5.13 LINEAMIENTOS PARA DEFINIR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE LA OPERACIÓN

5.13.1 Planificación de la Continuidad de la Seguridad de la Información.

Propósito: Establecer e implementar directrices y lineamientos para asegurar y mantener la seguridad de la información integrada en la gestión de continuidad de la operación de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y el proceso de Gestión de Tecnología e informática deben diseñar una metodología para la identificación y evaluación de riesgos de continuidad de la operación de los servicios de la Dirección Nacional de Bomberos de Colombia.

b. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y el proceso de Gestión de Tecnología e informática deben desarrollar un análisis de impacto al negocio (BIA por sus siglas en inglés), por medio del cual se identifiquen los servicios críticos de la Dirección Nacional de Bomberos de Colombia.

c. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, debe realizar acompañamiento al proceso de Gestión de Tecnología e informática en coordinación con los líderes de los procesos deben diseñar las estrategias y tiempos de recuperación de la operación de los servicios críticos de la Dirección Nacional de Bomberos de Colombia.

d. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y el proceso de Gestión de Tecnología e informática deben realizar un plan de pruebas del plan de continuidad de la operación y deberá ser ejecutado mínimo 2 veces al año.

e. El plan de continuidad del negocio debe ser revisado en sesión de Comité Directivo como mínimo una vez al año o cuando ocurra un cambio en el contexto interno o externo de la Dirección Nacional de Bomberos de Colombia.

f. El proceso de Gestión de Tecnología e informática debe disponer de planes de contingencia de los servicios de TIC y un plan de recuperación ante desastres, enfocados a lograr el retorno a la operación normal.

g. El proceso de Gestión Contractual debe incluir en los procesos una obligación general que exija a los contratistas a disponer de planes de contingencia y se deberá analizar su cobertura y alcance.

h. Se debe estructurar el Plan de Continuidad de la Operación acorde al alcance del sistema de gestión de Seguridad de la Información en coordinación con los líderes de los procesos, conforme a la normativa interna vigente.

i. El Plan de Continuidad de la Operación debe ser comunicado al interior de la Dirección Nacional de Bomberos de Colombia.

j. En caso de presentarse un incidente significativo que conlleve a una interrupción se deberá gestionar el manejo de la crisis y los mecanismos de comunicación apropiados tanto internos como externos durante el estado de contingencia.

k. La Subdirección Administrativa y Financiera debe garantizar la integración de los planes de emergencia y contingencia con el plan de continuidad de la operación de los servicios de la Dirección Nacional de Bomberos de Colombia.

l. El comité directivo debe definir un equipo para la planeación de pruebas, los procesos que estarán involucrados, la infraestructura tecnológica y/u operativa requerida, del plan rollback o plan de retirada, y las actividades a realizar. Los participantes de los equipos deberán recibir sensibilización con respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.

m. El equipo de pruebas del plan de continuidad debe documentar las pruebas y generar reportes o informes después de cada prueba y/o ejercicio que incluya recomendaciones, lecciones aprendidas y acciones para mejorar el plan y presentarlas al Comité Directivo.

n. Se deben ejecutar procedimientos de control de cambios según las acciones preventivas y correctivas que se generaron a partir de las pruebas, para asegurar que el Plan de Continuidad se mantenga actualizado y mejorado.

o. El Oficial de Seguridad y Privacidad de la información o quien haga sus veces debe revisar y aprobar todas las estrategias de continuidad.

5.13.2 Disponibilidad de instalaciones de procesamiento de información.

Propósito: Establecer lineamientos para asegurar la disponibilidad de las instalaciones de procesamiento de información de la Dirección Nacional de Bomberos de Colombia.

Lineamientos:

a. El proceso de Gestión de Tecnología e informática y la Subdirección Administrativa y Financiera, deben implementar redundancia suficiente, para lo cual deberá considerar componentes o arquitecturas redundantes.

b. El equipo de pruebas del Plan de Continuidad debe poner a prueba los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla el componente funcione.

5.14 LINEAMIENTOS PARA EL CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

5.14.1 Cumplimiento de los requisitos legales y contractuales.

Propósito: Establecer lineamientos para evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales.

Lineamientos:

a. Establecer un procedimiento y una herramienta que permita la revisión y verificación del cumplimiento de los requisitos legales y reglamentarios en materia de Seguridad y Privacidad de la Información y de derechos de autor.

b. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces en conjunto con la en proceso de gestión contractual deben identificar, documentar y actualizar todos los requerimientos contractuales, estatutarios y reglamentarios que puedan afectar los sistemas de Información de la Dirección Nacional de Bomberos de Colombia, utilizando la herramienta de verificación de requisitos legales.

c. El proceso de Gestión de Tecnología e informática debe definir controles con el objetivo de proteger adecuadamente la propiedad intelectual de la Dirección Nacional de Bomberos de Colombia, tales como derechos de autor de software, licencias y código fuente. El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.

d. El proceso de Gestión de Prensa debe generar campañas de comunicación con el fin de apropiar a los colaboradores de la Dirección Nacional de Bomberos de Colombia sobre el uso de los derechos de propiedad intelectual (no copiar total ni parcialmente libros, artículo u otros documentos diferentes de los permitidos por la ley de derechos de autor.).

e. La Subdirección Administrativa y Financiera debe generar directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital de la Dirección Nacional de Bomberos de Colombia.

f. La Subdirección Administrativa y Financiera debe establecer e implementar controles para proteger los registros contra pérdida, destrucción y falsificación de información física y digital.

g. La Subdirección Administrativa y Financiera debe establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.

h. El proceso de Gestión Documental deberá disponer de un sistema de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información.

i. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y la Dirección Jurídica, deben definir o actualizar cuando sea necesario la política de tratamiento de datos personales, para la protección de los derechos fundamentales de la información de los ciudadanos en relación con su tratamiento.

j. La Dirección Nacional de Bomberos de Colombia a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, deberá disponer los lineamientos para la protección de la información de los empleados públicos, contratistas y grupos de interés externos, en los términos de la Ley 1581 de 2012 y de acuerdo con lo estipulado en la Política de tratamiento de datos personales y el Manual de lineamientos de seguridad para la protección y tratamiento de datos personales.

k. La Oficina de Gestión Contractual debe incluir los mecanismos para que los supervisores de contrato validen el cumplimiento de las obligaciones generales en materia de seguridad y privacidad de la información.

5.15 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Propósito: Establecer lineamientos para garantizar que se implementa y opera la seguridad de la información de acuerdo con las políticas y procedimientos organizacionales.

Lineamientos:

a. El líder del Sistema de gestión de Seguridad y privacidad de la información de manera autónoma debe revisar o auditar el cumplimiento e implementación de los requerimientos y consideraciones en materia de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios. En el caso que se necesite incluir y/o reprogramar un ciclo de auditoría interna al Sistema de Seguridad de la Información en el Programa Anual de Auditoría Interna, al inicio de cada vigencia, el Líder del Sistema deberá hacer la solicitud mediante memorando o correo electrónico al jefe de la Oficina de Control Interno con copia al Líder del Sistema Integrado de Gestión, para que se coordine su programación y sea aprobado en el Comité Institucional de Coordinación de Control Interno. Lo anterior teniendo en cuenta lo establecido en la Guía de auditoría interna basada en riesgos para entidades públicas del DAFP, y el documento institucional de os Lineamientos previos a la realización del ciclo de auditorías internas del sistema integrado de gestión -SIG".

b. Los líderes de los procesos deberán asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión en auditorías.

c. El proceso de Gestión de Tecnología e informática debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad. Se deberán realizar auditorías periódicas con ayuda de herramientas automatizadas y se deberán generar informes técnicos.

5.16 LINEAMIENTOS PARA LA SEGURIDAD DE LA SEDE ELECTRÓNICA

5.16.1 SEGURIDAD DE LA INFORMACIÓN EN LA SEDE ELECTRÓNICA

Propósito: Establecer los lineamientos para asegurar la sede electrónica

Lineamientos:

a. La Subdirección Administrativa y Financiera con el apoyo del proceso de Gestión de Tecnología e informática deben definir los lineamientos de la implementación de la sede electrónica de la Dirección Nacional de Bomberos de Colombia, en donde se deberán integrar todos los portales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes.

b. La Subdirección Administrativa y Financiera debe identificar los canales digitales oficiales de recepción de solicitudes, peticiones y de información, y la Oficina de Tecnología de la Información, debe implementar los mecanismos de cifrado de información para dichos canales.

c. La Subdirección Administrativa y Financiera con compañía del proceso de Gestión de Tecnología e informática deberán implementar un sistema de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información. Adicionalmente, para la emisión, recepción y gestión de comunicaciones oficiales, a través de los diversos canales electrónicos, deberá asegurar un adecuado tratamiento archivístico.

d. La Subdirección Administrativa y Financiera junto con el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, deben establecer las estrategias que permitan el tratamiento adecuado de los documentos electrónicos y garantizar la confidencialidad, integridad, disponibilidad y acceso a largo plazo conforme a los principios y procesos archivísticos definidos por el Archivo General de la Nación en coordinación con la Dirección Nacional de Bomberos de Colombia.

e. Las dependencias responsables de trámites, procesos y procedimientos dirigidos a los ciudadanos deberán implementar los lineamientos de la sede electrónica definidos por la entidad en concordancia con las medidas jurídicas, organizativas y técnicas que garanticen la calidad, seguridad, privacidad, disponibilidad, integridad, confidencialidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios.

5.17 LINEAMIENTOS PARA LA SEGURIDAD DE SIIF NACIÓN

5.17.1 SEGURIDAD DE LA INFORMACIÓN PARA EL SIIF NACIÓN

Propósito: Establecer los lineamientos para salvaguardar la información del SIIF Nación

Lineamientos:

a. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, el proceso de Gestión de Tecnología e informática, el proceso de Gestión de Tecnología e informática y la Subdirección Administrativa y Financiera deben documentar los lineamientos para el manejo y control de los recursos tecnológicos utilizados para la administración y gestión financiera de la Dirección Nacional de Bomberos de Colombia.

b. Toda la información del SIIF Nación debe ser protegida contra acceso no autorizado para mantener su confidencialidad e integridad.

c. Cumplir con los requerimientos mínimos en seguridad de la información e informática en los equipos utilizados para la realización de transacciones financieras.

d. Para acceder al SIIF Nación se deben definir usuarios, roles y perfiles los cuales deben ser tramitados de acuerdo con lo establecido por la Administración del SIIF Nación y la Dirección Nacional de Bomberos de Colombia.

e. Se debe dar cumplimiento a lo establecido en las políticas de seguridad de la Información del SIIF Nación, establecidas por el Ministerio de Hacienda y Crédito Público, que se encuentren vigentes.

6. FUNCIONES Y RESPONSABILIDADES

Rol	Comité/ Perfil	Responsabilidades	Tipo vinculación	Oficina/Proceso	Perfil mínimo	Backup
Comité de Seguridad y privacidad de la Información	Comité MIG	Las contempladas en el artículo Sexto de la Resolución 587 de 2021, que actualiza el Modelo Integrado de Gestión (MIG), se adopta el Sistema Integrado de Gestión (SIG) de la Dirección Nacional de Bomberos de Colombia. Las contempladas en el MANUAL DE LINEAMIENTOS DE SEGURIDAD PARA LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES, 6. ROLES Y RESPONSABILIDADES.	Funcionarios/Contratistas (Res. 587 de 2021)	Preside: Director DNBC	Ser oficial de Bomberos de máximo grado de reconocida trayectoria institucional Bomberil. (Artículo 5 ley 575 de 2012).	Subdirector estratégico y de coordinación bomberil
Oficial de Seguridad y Privacidad de la Información	Director DNBC o a quién asigne rol y funciones	Las contempladas en la Resolución 587 de 2021 Las contempladas en el artículo DÉCIMO SEXTO, numeral 10 de acuerdo con lo establecido en el contrato de prestación de servicios Número 200 de 2022 - Responsabilidades específicas del líder del sistema de seguridad y privacidad de la información.	Contratista	Despacho del Director DNBC	Postgrado en áreas referentes al cargo	A quién designe el Director DNBC

BOMBEROS COLOMBIA — GUARDIANES DE LA VIDA —
@DNBomberosCol
Av. Calle 26 # 69 - 76 **Edificio Elemento** torre 4 piso 15
Bogotá - Colombia
Línea de atención: (1) 555 7926 Ext. 201 - 205
E-mail: atencionciudadano@dnbc.gov.co
Cel: 310 241 4387

Dimensión de Seguridad Informática	Gestor de TI o a quién delegue	* Liderar la gestión de riesgos de seguridad sobre la gestión de TI de la institución. * Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI. * Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. * Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. * Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. Las contempladas en el MANUAL DE LINEAMIENTOS DE SEGURIDAD PARA LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES, 6. ROLES Y RESPONSABILIDADES	Contratista	GESTIÓN TI	Postgrado en áreas referentes al cargo	A quién designe el Director DNBC en vacancia temporal o definitiva del cargo

Articulador del Modelo de Seguridad y Privacidad con los demás Sistemas de Gestión	Gestor del proceso de Gestión de Análisis y Mejora Continua o quién esta delegue.	Las contempladas entre otras en el artículo DÉCIMO CUARTO, de la Resolución 587 de 2021 Responsabilidades del Representante de la alta dirección y líder del sistema integrado de gestión - SIG, que actualiza el Modelo Integrado de Gestión (MIG), se adopta el Sistema Integrado de Gestión (SIG) de la DNBC.	Funcionarios/Contratistas	Proceso de Gestión de Análisis y Mejora Continua. Subdirección Administrativa y Financiera.	De acuerdo con el manual de funciones. Contratista: Estudios previos con obligaciones asociadas al MIG o SPI.	A quién designe el Director DNBC en vacancia temporal o definitiva del cargo
Equipo de Activos	**Mesa de trabajo instalada por el Oficial de Seguridad y Privacidad de la Información (quién da la línea) con los siguientes miembros:** - Preside: El Gestor del proceso de Gestión Documental - Oficial de seguridad y privacidad de la información **Miembros:** -	Apoyar en la identificación y actualización de los activos de información. Definir lineamientos respecto a la gestión de activos de información, conforme a lo establecido en las Normas.	Funcionarios/Contratistas	- Subdirección Administrativa y Financiera. - Proceso de Gestión TI -Proceso de Gestión de Análisis y Mejora Continua. - Proceso de Gestión Documental - Despacho del Director de la DNBC. - Proceso de Gestión Jurídica.	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI.	Definidos por cada Gestor de proceso u oficina

	Funcionarios o Contratistas del proceso de Gestión TI designados. - Funcionarios o Contratistas del Proceso de Gestión de Análisis y Mejora Continua designados. - Funcionarios o Contratistas Proceso de Gestión Documental designados. - Funcionarios o Contratistas de la Subdirección Administrativa y Financiera. - Funcionarios o Contratistas del proceso de Gestión Jurídica					

	designados.					
Equipo de Incidentes	Mesa de trabajo instalada por el Oficial de Seguridad y Privacidad de la Información (quién da la línea) con los siguientes miembros: - Preside: Despacho del Director de la DNBC. Miembros: - Funcionarios o Contratistas del proceso de Gestión de TI designados -	Apoyar la Gestión de Incidentes de Seguridad y Privacidad de la información, en todas sus etapas	Funcionarios/Contratistas	- Subdirección Administrativa y Financiera. - Proceso de Gestión TI -Proceso de Gestión de Análisis y Mejora Continua. - Proceso de Gestión Documental - Despacho	Funcionarios: De acuerdo al manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI.	Definidos por cada Gestor de proceso o oficina o dependencia

	Funcionarios o Contratistas del Proceso de Gestión de Análisis y Mejora Continua designados. - Funcionarios o Contratistas del Proceso de Gestión Documental designados. - Funcionarios o Contratistas de la Subdirección Administrativa y Financiera. - Representante del CSIRT Gobierno			del Director de la DNBC.		
	Mesa de trabajo instalada por el Oficial de Seguridad y Privacidad de la Información (quién da la línea de					

Equipo de Riesgos de Seguridad de la Información.	acuerdo con el comité CICI) con los siguientes miembros: - Preside: el Oficial de Seguridad y Privacidad de la Información. **Miembros:** - Funcionarios o Contratistas del Proceso de Gestión de Análisis y Mejora Continua designados., de acuerdo al rol transversal del sistema integrado de gestión. - Funcionarios o Contratistas del proceso de Gestión de TI designados. - Funcionarios o	Apoyar la Gestión de Riesgos de Seguridad y Privacidad de la información, en todas sus etapas	Funcionarios/Contratistas	- Subdirección Administrativa y Financiera. - Proceso de Gestión TI -Proceso de Gestión de Análisis y Mejora Continua. - Proceso de Gestión Documental - Despacho del Director de la DNBC.	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI.	Definidos por cada Gestor de proceso u oficina o dependencia

	Contratistas de la Subdirección Administrativa y Financiera. - Funcionarios o Contratistas del Despacho del Director de la DNBC.					
Equipo de Apropiación	Gestor del proceso de Gestión de Comunicaciones o a quién esta delegue. - funcionarios o Contratistas del proceso de Gestión de TI designados. - Oficial de Seguridad y Privacidad de la Información o quien haga sus veces.	Apoyar en la creación de piezas gráficas, material de diseño multimedia etc., que se requiera dentro del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital. - Apoyar en la publicación y difusión de las actividades del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital, en los diferentes medios de comunicación con que cuenta la DNBC.	Funcionario/Contratista	Proceso de Gestión de Comunicaciones Despacho del Director-Oficial de Seguridad y Privacidad de la Información. Proceso de Gestión TI.	De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI.	A quién designe el Director DNBC en vacancia temporal o definitiva del cargo
Comité de Cambios de TI	**Mesa de trabajo instalada por el Gestor del**	Las contenidas en el Manual de Gestión de cambios, Responsabilidades	Funcionarios/Contratistas	Proceso de Gestión TI Despacho del Director de la DNBC.	Estudios previos con obligaciones asociadas	Delegados por el Gestor de TI, A quién designe

	Proceso de Gestión TI: - Preside: Gestor de Cambios designado por el Gestor del proceso de Gestión TI. **Miembros Permanentes:** - Gestor del Proceso de Gestión TI - Oficial de Seguridad y Privacidad de la información o a quién este designe. - Todas los procesos y oficinas: Líderes Funcionales (Solicitante del cambio). - Funcionarios o Contratistas de la Subdirección Administrativa y				a su rol dentro del comité	el Director DNBC en vacancia temporal o definitiva del cargo

	Financiera o a quién este designe. - Despacho del Director de la DNBC o a quién este designe.					
Equipo Auditor	**Segunda Línea de Defensa** (Profesional especializado con funciones de planeación o quien hagan sus veces, el subdirector Administrativo y Financiero (como líder de los procesos de gestión de contratación, gestión financiera y Gestión de Tecnología e Informática) y los supervisores e interventores en los	Los Roles y Responsabilidades de los Líderes de los SG y/o Líder del SIG contenidas en la Resolución 587 de 2021. **Guía de auditoría interna basada en riesgos para entidades públicas del DAFP**	Funcionarios/Contratistas	- Subdirección Administrativa y Financiera. - Proceso de Gestión TI -Proceso de Gestión de Análisis y Mejora Continua. - Proceso de Gestión de Contratación.	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI. Ambos certificados en NTC/ISO 27001:2013	Delegados por el proceso de Evaluación y Seguimiento.

	contratos asignados)					
Gestores	conformado por los líderes de cada uno de los niveles de proceso de la DNBC (procesos estratégicos, procesos misionales, procesos de apoyo y el proceso de evaluación y seguimiento), es decir, el Director General, el Subdirector Administrativo y Financiero, el Subdirector Estratégico y de Coordinación Bomberil y el Asesor de Control Interno, así como	Las contempladas en el artículo DÉCIMO QUINTO de la Resolución 587 de 2021 que actualiza el Modelo Integrado de Gestión (MIG), se adopta el Sistema Integrado de Gestión (SIG) de la DNBC.	Funcionarios/Contratistas	Todos los Procesos	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI. Resolución 587 de 2021	Delegados por el Gestor o responsable de cada proceso u oficina, programa o proyecto

	los Gestores de los procesos interno.					
Líderes de los Procesos	Conformado por los líderes de cada uno de los niveles de proceso de la DNBC (procesos estratégicos, procesos misionales, procesos de apoyo y el proceso de evaluación y seguimiento), es decir, el Director General, el Subdirector Administrativo y Financiero, el Subdirector Estratégico y de Coordinación Bomberil y el Asesor de Control Interno, así como los	Las contempladas en el artículo DÉCIMO QUINTO de la Resolución 587 de 2021 que actualiza el Modelo Integrado de Gestión (MIG), se adopta el Sistema Integrado de Gestión (SIG) de la DNBC. Las contempladas en el MANUAL DE LINEAMIENTOS DE SEGURIDAD PARA LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES, 6. ROLES Y RESPONSABILIDADES	Funcionarios/Contratistas	Todos los Procesos	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI. Resolución 587 de 2021	Delegados por el Gestor de TI, A quién designe el Director DNBC en vacancia temporal o definitiva del cargo

	Gestores de los procesos					
Protección de Datos Personales	A quién asigne rol y funciones	Reportar al Registro Nacional de Bases de Datos (RNBD) de la Superintendencia de Industria y Comercio (SIC) o quien haga sus veces, de conformidad con lo dispuesto en la norma, las bases de datos con datos personales que reposan en la DNBC.	Funcionarios/Contratistas	Despacho del Director DNBC, Proceso de Gestión Documental. - Proceso de Gestión Jurídica. - Proceso de Gestión de Contratación. - Proceso de Gestión de Talento Humano.	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI. Resolución 587 de 2021	A quién designe el Director DNBC en vacancia temporal o definitiva del cargo
Alta Dirección	Comité Directivo	Las contempladas en el MANUAL DE LINEAMIENTOS DE SEGURIDAD PARA LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES, 6.2 ROLES Y RESPONSABILIDADES	Funcionarios (Res. 587 de 2021)	Preside: El Director de la DNBC.	Ser oficial de Bomberos de máximo grado de reconocida trayectoria institucional Bomberil. (Artículo 5 ley 575 de 2012).	Subdirector estratégico y de coordinación bomberil
Dependencias	Todas las áreas de la DNBC	Las contempladas en el artículo VIGÉSIMO (Obligatoriedad -A partir de la publicación de la documentación del Sistema de Gestión en la Entidad, será de obligatorio cumplimiento su aplicación, a todos los funcionarios y contratistas de la DNBC) de la Resolución 587 de 2021, que actualiza el Modelo Integrado de Gestión (MIG), se	Funcionarios/Contratistas	Todos los Procesos	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI. Resolución 587 de 2021	N/A

		adopta el Sistema Integrado de Gestión (SIG) de la DNBC. Las contempladas en el MANUAL DE LINEAMIENTOS DE SEGURIDAD PARA LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES, 6. ROLES Y RESPONSABILIDADES				
Administrador de PQRSD	Gestor del Proceso de gestión de atención al usuario y Gestor de Proceso de Gestión Documental	Las contempladas en el MANUAL DE LINEAMIENTOS DE SEGURIDAD PARA LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES, 6. ROLES Y RESPONSABILIDADES	Funcionarios/Contratistas	Proceso de gestión de atención al usuario y el Proceso de Gestión Documental	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI. Resolución 587 de 2021	Definidos por cada Gestor de proceso o oficina o dependencia
Arquitecto de Seguridad	Oficial de Seguridad y Privacidad de la Información	• Asesorar y formular en elementos normativos de protección de la información. • Asesorar y formular la gestión de riesgos de seguridad y privacidad de la información y de seguridad digital, incluyendo los asociados a infraestructura tecnológica, aplicaciones y componentes de información. • Establecer mecanismos para mitigar el impacto	Funcionarios/Contratistas	Despacho del Director de la DNBC	Funcionarios: De acuerdo con el manual de funciones Contratista: Estudios previos con obligaciones asociadas al MIG o SPI. Resolución 587 de 2021	N/A

		de incidentes de seguridad y privacidad de la información y de seguridad de la información. • Definir los mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, y no repudio de la confidencialidad de la entidad. • Determinar los lineamientos necesarios para el manejo de la información tanto física como digital. • Gestionar un cambio organizacional para la apropiación de la seguridad y privacidad de la información, seguridad digital, y protección de la información personal. • Establecer y mantener el plan de continuidad de la operación de los servicios de la Entidad. • Establecer el modelo, artefactos, componentes, lineamientos del marco de referencia de Arquitectura Empresarial enfocado en el dominio se seguridad para la Entidad.				
Observación	**Cabe resaltar que todos los roles y responsabilidades con referencia a la Seguridad y Privacidad de la Información que se encuentran en la resolución 587 del 2021 del SIG y en la Resolución 397 de 2022 y en el Manual de Seguridad y Privacidad de la Información son de obligatorio cumplimiento por parte de todos los funcionarios y contratistas de la DNBC.**					

7. DESARROLLO

La Política General de Seguridad y Privacidad de la Información, establece la necesidad de planear, implementar y mantener un Sistema de Gestión de Seguridad de la Información en la DNBC, contemplando planes de seguridad, planes de tratamiento de riesgos, políticas específicas, manuales, procedimientos operativos, formatos e instructivos, que estén alineados con la normatividad vigente, la Política de Gobierno Digital y las siguientes técnicas de la seguridad:

- **Organización de la seguridad de la información:**
  Establecer un marco referencial a nivel directivo para iniciar y controlar la implementación de la seguridad de la información dentro de la Entidad.
- **Gestión de los activos:**
  Implementar y mantener una adecuada protección de los activos de información institucionales.
- **Gestión de riesgos de seguridad de la información:**
  Asegurar que el personal de planta, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; así como reducir el riesgo de robo, fraude y mal uso de los medios.
- **Concienciación o Sensibilización y Capacitación:**
  Consiste en dar a conocer mediante un plan de capacitación, los riesgos a los que los sistemas de información, los usuarios, las redes y la información en general están expuestos para generar dentro de los funcionarios y contratistas buenas prácticas respecto a la seguridad de la información, estás buenas prácticas actúan de manera preventiva ayudando a la entidad a salvaguardar los activos de su información.
- **Seguridad de los recursos humanos:**
  Asegurar que el personal de planta, contratistas y terceros entiendan sus responsabilidades, y sean idóneos a los roles para los cuales son considerados; así como reducir el riesgo de robo, fraude y mal uso de los medios, causando la perdida de la información o su afectación.

Asimismo, los mecanismos de control en sus relaciones con terceras partes tienen como objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información para la entidad.

- **Seguridad física y del entorno:**
  Prevenir el acceso no autorizado, daño e interferencia a las instalaciones de la entidad y su información.
- **Gestión de comunicaciones y operaciones:**
  Crear procedimientos y responsabilidades operacionales de tal manera que permita asegurar la operación correcta y segura de los medios de procesamiento de la información.
- **Control de acceso:**
  Asegurar que el acceso al usuario es debidamente autorizado y evitar el acceso no autorizado a los diferentes sistemas de información.
- **Adquisición, desarrollo y mantenimiento de sistemas de información:**
  Garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.
- **Gestión de los incidentes de seguridad de la información**
  Asegurar que las debilidades y eventos de seguridad de la información asociados a sistemas de Información son comunicados de tal manera que se permita tomar acciones correctivas a tiempo.
- **Gestión de la continuidad en el manejo de la información para la entidad:**

Considerar los aspectos de la seguridad de la información para la continuidad operativa, haciendo frente a las interrupciones de las actividades propias en la entidad y protegiendo los procesos críticos que puedan generar fallas críticas o desastres en la información de la entidad, a fin de asegurar correcto funcionamiento en todo momento.

- **Cumplimiento:**
  Velar por el cumplimiento de cualquier ley, obligaciones estatutarias, reglamentarias o contractuales y cualquier requisito o política vigente y aplicable de seguridad y privacidad de la información.

7.1. MODELO DE SEGURIDAD DE LA INFORMACIÓN

El modelo de seguridad de la información de la DNBC está establecido de acuerdo con las cinco (5) fases definidas en las dimensiones en la operación del modelo de seguridad y privacidad de la información de la estrategia de gobierno en línea en la entidad. Estos incluyen objetivos, metas y lineamientos, lo cual permite que la seguridad y protección de datos de la información sea un sistema de gestión sostenible.

Figura 1: Dimensiones en la Operación

Diagnóstico: permite identificar el estado en el que se encuentra la DNBC con respecto a los requerimientos del modelo de seguridad y privacidad de la información. En esta dimensión se pretende identificar el estado actual de la entidad, donde una parte primordial del proceso es la estrategia de política de gobierno digital o gobierno en línea. Se tiene como objetivo el cumplimiento de las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la DNBC.
- Realizar un levantamiento de la información en la entidad, cuyo fin es el de contar con pruebas de eficiencia para poder medir los controles existentes.
- Identificar el nivel de madurez de seguridad y privacidad de la información de la DNBC.

Planificación (planear): en esta dimensión es donde se establecen los objetivos con el fin de encontrar las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos. Esta fase busca generar un plan de seguridad y privacidad alineado con el propósito misional de la DNBC, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, esto se llevará a cabo a través de la metodología acorde a la gestión del riesgo.

- Estado de la entidad: conocer la entidad en cuanto a los niveles y estado de seguridad con los que se cuentan a la fecha; desde sus necesidades, las expectativas y con esto poder determinar su alcance.

- Planeación: es donde se planifican las acciones con las cuales se abordan los riesgos y oportunidades, objetivos y planes para llevarlo a cabo con éxito.

- Funciones: inicialmente la cabeza líder del proceso es la dirección general; es quien determinara y delegara el grupo de trabajo que trabajara con las políticas de seguridad y responsabilidades, de acuerdo con los roles que se determinen.

- Soportes: son los recursos con los que se contara para realizar y el proceso y la documentación.

Una vez culminado este proceso se pretende lograr la aplicación correcta de todos los controles que se han implementado en la DNBC.

Implementación (hacer): se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas. En esta fase y luego de realizar la identificación de las necesidades en la DNBC como paso a seguir se debe elaborar un plan de implementación y luego ejecutar el plan de tratamiento de riesgos del modelo de seguridad y privacidad de la información. De acuerdo con esto se tienen contempladas las siguientes metas, esto luego del resultado de la fase de planeación.

- Implementación del plan de tratamiento de riesgos.
- Planificación y control operacional.

Evaluación de desempeño (verificar): una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas. Durante esta fase debemos tener en cuenta el seguimiento y monitoreo del modelo de seguridad y privacidad de la información. Esto se logra con base en los resultados que ofrecen los indicadores de la seguridad de la información propuestos para la actividad y su eficacia en los controles implementados. Para cumplir con esta fase se tienen contempladas las siguientes metas:

- Plan de revisión y seguimiento al modelo de seguridad y privacidad de la información en la entidad.
- Plan de ejecución de auditorías.
- Análisis del cronograma en búsqueda del cumplimiento de las actividades según lo presupuestado.

Mejora continua (actuar): una dimensión para realizar el análisis de los resultados en las acciones implementadas donde se verifica si se cumplen o no los objetivos definidos para luego analizar las causas de las desviaciones. Una vez terminada esta actividad se prosigue a generar el respectivo plan de acción. Durante esta actividad la DNBC podrá consolidar el alcance de los objetivos planteados en la dimensión de evaluación de desempeño, cuyo fin es el de diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, permitiendo estructurar y realizar el plan de implementación de acciones correctivas identificadas para el modelo de seguridad y privacidad de la información.

Con el fin de lograr el objetivo es necesario recalcar en la importancia de la ejecución del plan de mejora continua con base a los resultados de la dimensión de evaluación de desempeño que debe incluir los resultados de la ejecución del plan de seguimiento, evaluación y análisis del modelo de seguridad y privacidad de la información. Así mismo debe incluir los resultados de la auditoría interna del modelo de seguridad y privacidad de la información. Se deben adoptar, programar e implementar diferentes procesos para la correcta ejecución o implantación del plan de seguridad y privacidad de la información como se expone a continuación:

Responsables: la dirección de la DNBC debe brindar un total compromiso durante todo el proceso (establecimiento, implementación, operación, seguimiento, y mejora) para lograr una excelente

política de seguridad y privacidad de la información, esto se logra mediante: El establecimiento de la política de seguridad y privacidad de la información.

- El establecimiento de funciones y responsabilidades de seguridad de la información.
- Dándole a conocer a los funcionarios de la entidad la importancia de cumplir con los objetivos de seguridad de la información, sus responsabilidades en cuanto a la ley y la necesidad de mejora continua en la DNBC.
- Asegurándose de la realización de las auditorías internas de manera periódica.
- Ejecutando verificaciones durante todo el proceso con el fin de ir acorde al cronograma y cumplimiento de las dimensiones.
- Ofreciendo los recursos suficientes para establecer, implementar, hacer seguimiento, sostener y mejorar la política general de seguridad de la información.

Adopción del protocolo de red ipv6: la DNBC de acuerdo con la implementación de nuevas tecnologías y siguiendo las directrices del ministerio de las tics y gobierno en línea, debe iniciar el proceso de transición del modelo de red ipv4 al nuevo protocolo de red ipv6, verificando que la infraestructura actual sea la acorde. Si bien es sabido que se ha generado una implementación, esta no se encuentra certificada a la fecha, por lo cual se debe realizar una certificación con el fin de contar con la correcta adopción para la entidad.

- Se debe garantizar que todos los equipos de telecomunicaciones en la entidad acepten en un 100% el protocolo de red ipv6, además debe ir de la mano con los proveedores de servicios de conectividad ya que estos deben ofrecer una compatibilidad completa con este nuevo protocolo. Así mismo la infraestructura nueva debe estar diseñada para coexistir con el protocolo ipv4.

Gestión de recursos: la DNBC debe determinar y suministrar recursos para:

- El establecimiento, la implementación, operación, el seguimiento, la verificación, el sostenimiento y mejoras del modelo de la política general de seguridad y privacidad de la información.
- Brindar seguridad en los procedimientos de seguridad de la información, que estos brinden apoyo a los requisitos de la entidad y su trabajo seguro.
- Ofrecer una seguridad adecuada o suficiente mediante la aplicación correcta de todos los controles que se han implementado en la DNBC.

7.2. CUMPLIMIENTO

Todos los funcionarios y contratistas deben conocer, aceptar y cumplir la política y el Manual de Seguridad y Privacidad de la información, para esto el responsable principal de la seguridad de la información de la Entidad, tendrá que socializar o dar a conocer su contenido a las partes interesadas. El incumplimiento será considerado una falta grave o un incidente de seguridad, que de acuerdo con el caso podrá dar lugar a un proceso disciplinario para funcionarios y para el caso de contratistas procederá una denuncia penal, la imposición de sanciones e incluso la terminación de su contrato, sin perjuicio de la iniciación de otro tipo de acciones legales a las que haya lugar.

7.3. VIGENCIA Y ACTUALIZACIÓN DE LA POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

El presente Manual rige a partir de su aprobación y la actualización es responsabilidad del funcionario que sea designado como Oficial de Seguridad de la Información o quien realice sus veces.

8. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
23/12/2021	Emisión Inicial Oficial	1
30/06/2022	Se actualiza las políticas de operación y el documento en general.	2

Elaborado por:	**Revisado y Aprobado por:**	**Revisión metodológica:**
Nombre: Julio Alejandro Díaz de Hoyos	**Nombre:** Comité Directivo	**Nombre:** Catalina Carranza John Beltran
Cargo: Contratista TI	**Cargo:**	**Cargo:** Contratistas Gestión de Análisis y Mejora Continua
Fecha: 30/06/2022	**Fecha:** 30/06/2022	**Fecha:** 30/06/2022
Firma:	**Firma:**	**Firma:**