
Dadsa
Comprometidos con el Ambiente

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	4/05/2022	Versión inicial del documento

TABLA DE CONTENIDO

PÁG

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, por medio de la Estrategia de Gobierno en línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC.

2. AUDIENCIA

Este documento está elaborado para las entidades públicas de orden nacional, entidades públicas del orden territorial y entidades privadas que deseen una guía para implementar las políticas planteadas en el Modelo de Seguridad de la Información, así como proveedores de servicios de Gobierno en Línea y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la Información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

La política de alto nivel o política general, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

Es así como, teniendo en cuenta la importancia que tiene que la entidad defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Dirección.

De esta forma, una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro de la entidad.

4. PROPÓSITO

El siguiente documento es un formato que puede ser utilizado como plantilla para la elaboración de la política general de seguridad y privacidad de información para las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

5. GLOSARIO

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De manera genérica a continuación se entrega un texto guía para la elaboración de la política general de seguridad de la información, este puede ser base del desarrollo de dicho documento ya que contempla los principios básicos a tener en cuenta en su elaboración dentro de la planeación del sistema de gestión de seguridad de la información en una entidad.

La dirección de DADSA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el DADSA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- *Minimizar el riesgo en las funciones más importantes de la entidad.*
- *Cumplir con los principios de seguridad de la información.*
- *Cumplir con los principios de la función administrativa.*
- *Mantener la confianza de sus clientes, socios y empleados.*
- *Apoyar la innovación tecnológica. ➢ Proteger los activos tecnológicos.*
- *Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.*

- *Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del DADSA*
- *Garantizar la continuidad del negocio frente a incidentes.*
- *DADSA ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.*

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la "Guía de políticas específicas de seguridad y privacidad de la información" y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación se establecen 12 principios de seguridad que soportan el SGSI del DADSA:

- *Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, socios de negocio o terceros**.*

- *El DADSA **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.*

- *EL DADSA **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.*
- *EL DADSA **protegerá su información** de las amenazas originadas por parte **del personal**.*

- *EL DADSA **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.*

- *EL DADSA **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.*

- *EL DADSA **implementará control de acceso** a la información, sistemas y recursos de red.*

- *EL DADSA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.*

- *EL DADSA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.*

- *EL DADSA **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.*

- *EL DADSA garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.***

Formato #2 de Política de Seguridad y Privacidad de la Información

El siguiente documento es un formato de política de Seguridad y Privacidad de la Información

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de EL DADSA con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.
EL DADSA, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- *Minimizar el riesgo de los procesos misionales de la entidad.*
- *Cumplir con los principios de seguridad de la información.*
- *Cumplir con los principios de la función administrativa.*
- *Mantener la confianza de los funcionarios, contratistas y terceros.*
- *Apoyar la innovación tecnológica.*
- *Implementar el sistema de gestión de seguridad de la información.*
- *Proteger los activos de información.*
- *Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.*
- *Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del DADSA Garantizar la continuidad del negocio frente a incidentes.*

Alcance/Aplicabilidad

 Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del DADSA y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de EL DADSA:

- *EL DADSA ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.*
- *Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, contratistas o terceros**.*

- *EL DADSA **protegerá la información** generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.*
- *EL DADSA **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.*
- *EL DADSA **protegerá su información** de las amenazas originadas por parte **del personal**.*
- *EL DADSA **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.*
- *EL DADSA **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.*
- *EL DADSA **implementará control de acceso** a la información, sistemas y recursos de red.*
- *EL DADSA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.*
- *EL DADSA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.*
- *EL DADSA **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.*
- *EL DADSA garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.***

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

7. FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

IMPORTANCIA DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

FASES DE IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN

1. **Desarrollo de las políticas**: En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

- Justificación de la creación de política: Debe identificarse el por qué la Entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.
- Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?
- Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.
- Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de

otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.

- Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de las mismas.

2. **Cumplimiento:** Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

3. **Comunicación:** Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados.

4. **Monitoreo:** Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

5. **Mantenimiento:** Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

6. **Retiro:** Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad.

8. RECOMENDACIONES PARA LA REDACCION DE UNA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

A continuación se presenta una serie de recomendaciones para realizar redacción de políticas de seguridad y privacidad de la información en la Entidad:

- La política debe tener como parte de su texto la declaración en la cual se indica ¿qué es lo que se desea hacer?, ¿qué regula la política?, ¿cuál es la directriz que deben seguir los funcionarios, contratistas y/o terceros?, todo esto alineado con la estrategia de la organización.
- Alinearse con el alcance del Modelo de Seguridad y Privacidad de la Información.
- Debe especificarse a quién (es) va dirigida la política, se debe identificar fácilmente quien (es) deben cumplir la política.
- En los casos que aplique se hace referencia de la regulación mediante la cual se soporta la política.
- En caso que aplique la política debe indicar las excepciones a la misma y a quienes les aplica la excepción.
- Datos de las personas o roles de la entidad que pueden brindar información sobre la política.
- Nombre, rol o responsable de quien autoriza la política.
- Describir los pasos y procedimientos para realizar ajustes a la política.
- Explicación de las consecuencias que se pueden tener en caso de que un funcionario, contratista o tercero incumpla la política. Fecha que inicia la vigencia de la política.

Es importante aclarar que una política NO es un estándar, es decir, no debe indicar como se ejecutará ninguna labor o control de manera específica, NO indica tecnologías específicas de uso. Son declaraciones muy generales y de alto nivel que plasman un objetivo a cumplir por parte de la organización.

EJEMPLO:

Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, EL DADSA, empleará y distribuirá equipos con los controles criptográficos (Contraseñas).

9. POLITICAS ESPECÍFICAS RECOMENDADAS PARA LA IMPLEMENTACIÓN

En este documento presenta algunas recomendaciones de políticas de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para las Entidades del Estado. Este conjunto de recomendaciones no es exhaustivo, se aconseja que cada Entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar. A continuación se agruparan las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

9.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información. Debe tener los siguientes elementos:

- ¿Quiénes conforman el comité directivo de seguridad de la información?
- **Objetivos**: Se deben especificar los objetivos del comité como por ejemplo el mejoramiento continuo de los programas o las distintas actividades que se realizarán en dichos comités, verificación de avance de los distintos proyectos, la revisión del documento de la política de seguridad etc…
- **Cumplimiento:** Debe establecerse que dicho comité verifique el cumplimiento de las políticas.

9.2 GESTION DE ACTIVOS

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

- **Identificación de Activos**: Esta política debe determinar la periodicidad con la cual se va a realizar al interior de la Entidad la identificación y/o actualización del inventario de Activos de Información, la política debe determinar el responsable de realizar la actividad, se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.

- **Clasificación de Activos:** La Entidad debe determinar la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma. En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Entidad, algunos ejemplos: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo a la naturaleza de la entidad.
- **Etiquetado de la Información:** Esta política debe determinar el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.
- **Devolución de los Activos:** Esta política debe determinar el instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad.
- **Gestión de medios removibles:** Esta política debe contemplar los usos y permisos que tienen los usuarios y/o funcionarios de la Entidad frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. Esta política debe describir detenidamente en qué casos se autoriza y en los que no, el uso de medios removibles y los procedimientos en los cuales se determinen las autorizaciones; adicionalmente debe describir el responsable de las autorizaciones y responsabilidades de aquellas personas que tienen autorización para el uso del dicho medio de almacenamiento. El uso de medios removibles en la entidad deben ir alineados a las clasificaciones de activos dispuestas en la política de “Clasificación de Activos”.
- **Disposición de los activos:** Esta política debe determinar la obligatoriedad para la construcción y cumplimiento de un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos. Esta política debe determinar la toma de backup de los activos evitando así el acceso o borrado no autorizado de la información, la política debe indicar quien es el responsable de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.
- **Dispositivos móviles:** Esta política debe determinar los funcionarios, contratistas o terceros que pueden tener acceso a las redes inalámbricas, quiénes pueden realizar instalación de chats corporativos y/o correos electrónicos de la entidad mediante el uso de este tipo de dispositivos, adicionalmente debe describir las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles así como como los controles de

seguridad que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información**.**

9.3 CONTROL DE ACCESO

Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales la Entidad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos; las políticas relacionadas con el control de acceso deben contemplar como mínimo:

- **Control de acceso con usuario y contraseña:** Se debe elaborar una política sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la entidad, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. La política debe enunciar las responsabilidades que los funcionarios, contratistas o terceros tienen al contar con un usuario o contraseña de la entidad, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La entidad debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.
- **Suministro del control de acceso:** Esta política debe determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad.
- **Gestión de Contraseñas:** Esta política debe definir los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad. Esta política debe indicar a los funcionarios, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña, debe determinar que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña

fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.

- **Perímetros de Seguridad**: La política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuales no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.
- **Áreas de Carga:** La política debe definir las condiciones e instalaciones físicas en las cuales se va a realizar despacho y carga de paquetes físicos para bodegas o espacios definidos de carga, esto con el fin de evitar el acceso no autorizado a otras áreas de la entidad. Esta política debe determinar el seguimiento que se debe realizar para garantizar el cumplimiento de dicha política y sus correspondientes responsables.

9.4 NO REPUDIO

La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción.

La política deberá incluir mínimo los siguientes aspectos:

- **Trazabilidad:** La política hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
- **Retención:** La política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad.
- **Auditoría:** La política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
- **Intercambio electrónico de información:** La política incluirá en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

9.5 PRIVACIDAD Y CONFIDENCIALIDAD

Esta política debe contener una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido

en la normatividad vigente. La política de privacidad debe contener como mínimo lo siguiente:

1. Ámbito de aplicación 2. Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales

3. Principios del tratamiento de datos personales:

- Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
- Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
- Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

4. **Derechos de los titulares:** La política debe indicar los derechos de los titulares de los datos, tales como:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
- Ser informado respecto del uso que se le da a sus datos personales.
- Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con el Banco los servicios o productos que dieron origen a dicha autorización.
- Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.

5. **Autorización del titular:** La política debe indicar cómo obtener autorización del titular para el tratamiento de sus datos personales, así como los casos en los cuales no se requiere autorización del titular.
6. **Deberes de los responsables del Tratamiento:** La política debe indicar cuales son los deberes de los responsables y/o encargados del tratamiento de los datos personales.

 Política de controles criptográficos: Esta política deberá especificar como se asegura la confidencialidad y autenticidad de la información que circula o se genera a través de los diferentes sistemas de información.

La política de confidencialidad, debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o tercero vinculado a la Entidad, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Entidad, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

La política deberá indicar desde cuando se firma el acuerdo de confidencialidad, así como la vigencia del mismo.

9.6 INTEGRIDAD

La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Entidad, la cual se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos.

De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

La política de integridad, deberá establecer asimismo la vigencia de la misma acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

9.7 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La Entidad deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

La política de disponibilidad debe incluir como mínimo los siguientes aspectos:

- **Niveles de disponibilidad:** Esta política debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con clientes, proveedores y/o terceros en función de las necesidades de la Entidad, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos.
- **Planes de recuperación:** La política debe incluir los planes de recuperación que incluyan las necesidades de disponibilidad del negocio.
- **Interrupciones:** La política debe velar por la gestión de interrupciones de mantenimiento de los servicios que afecten la disponibilidad del mismo.
- **Acuerdos de Nivel de servicio:** Tener en cuenta los acuerdos de niveles de servicios (ANS) en las interrupciones del servicio.
- **Segregación de ambientes:** Esta política debe establecer la segregación de ambientes para minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción.
- **Gestión de Cambios:** La política debe incluir gestión de cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

9.8 REGISTRO Y AUDITORÍA

Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

Esta política deberá contener:

- **Responsabilidad:** Incluir la responsabilidad de la Oficina de Control Interno y similares, acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.

- **Almacenamiento de registros:** La política debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.
- **Normatividad:** La política de auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.
- **Garantía cumplimiento:** La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar las deficiencias detectadas.
- **Periodicidad:** La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

9.9 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

La entidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

La política debe contemplar para su elaboración los siguientes parámetros:

- Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.
- **Visión General:** ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?
- **Definir Responsables:** Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.
- **Actividades:** Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.
- **Documentación:** Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.
- **Descripción Del Equipo Que Manejará Los Incidentes:** Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.

- **Aspectos Legales:** Deben citarse los aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento.

9.10 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN:

Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y

amenazas relacionadas con el recurso humano.

Dicha política debe contener los siguientes parámetros.

- El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas.
- ¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
- La obligación de los usuarios a asistir a los eventos o cursos de capacitación.
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- Definir los roles y responsabilidades de quienes diseñaran los programa, quienes los comunicarán.
- Documentación sobre planes de estudio y desarrollo de los programas.
- Compromisos y obligaciones por parte del personal capacitado.
- Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios usuarios como las siguientes:
    - *Política De Escritorio Limpio*
    - *Política De Uso Aceptable*
    - *Ética Empresarial.*