MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN GENERAL

RESOLUCIÓN NÚMERO 04408 **DEL** 26 DIC 2024

"Por la cual se expide el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional"

EL DIRECTOR GENERAL DE LA POLICÍA NACIONAL DE COLOMBIA

En uso de las facultades legales que le confiere el artículo 2º, numeral 3 del Decreto 113 de 2022, y,

CONSIDERANDO:

Que el artículo 218 de la Constitución Política de Colombia, establece que la "Policía Nacional es un cuerpo armado permanente de naturaleza civil, a cargo de la Nación, cuyo fin primordial es el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz".

Que la Ley 23 del 28 de enero de 1982 "Sobre derechos de autor", modificada por la Ley 1915 del 12 de julio 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.", establece disposiciones en materia de derecho de autor y derechos conexos.

Que la Ley 594 de 14 de julio de 2000, "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones" en su artículo 3, define el patrimonio documental como el conjunto de documentos conservados por su valor histórico o cultural.

Que mediante la Ley 872 del 30 de diciembre de 2003 "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios", se creó el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios, como una herramienta de gestión sistemática y transparente que permite dirigir y evaluar el desempeño institucional, en términos de calidad y satisfacción social en la prestación de los servicios a cargo de las entidades y agentes obligados, la cual está enmarcada en los planes estratégicos y de desarrollo de las entidades.

Que la Ley 962 del 8 de julio de 2005, "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos", establece en el artículo 6, los medios tecnológicos para atender los trámites y procedimientos de competencia de las entidades de la administración pública.

Que la Ley 1266 del 31 de diciembre 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.", busca respetar y hacer respetar la información contenida en las bases de datos personales.

Que la Ley 1273 del 5 de enero de 2009, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y

se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones", adiciona el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos".

Que la Ley 1341 del 30 de julio de 2009, "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones", determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la sociedad de la información.

Que la Ley 1437 del 18 de enero de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo".

Que la Ley Estatuaria 1581 del 17 de octubre de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales", tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Que mediante la Ley Estatutaria 1621 del 17 de abril de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", en su artículo 28 crea los "centros de protección de datos de inteligencia y contrainteligencia, donde cada uno de los organismos que desarrolla actividades de inteligencia y contrainteligencia tendrá un centro de protección de datos y archivos de inteligencia y contrainteligencia, tendrá un responsable que garantizará que los procesos de recolección, almacenamiento, producción y difusión de la información de inteligencia y contrainteligencia estén enmarcados en la Constitución y la Ley.

Que mediante la Ley Estatutaria 1712 del 6 de marzo 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", con el fin de regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y se establecen los índices de clasificación o excepciones de acceso a la información.

Que mediante la Ley 1952 del 28 de enero de 2019, "Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario", establece en su artículo 23 la "garantía de la función pública, con el fin de salvaguardar la moralidad pública, transparencia, objetividad, legalidad, honradez, lealtad, igualdad, imparcialidad, celeridad, publicidad, economía, neutralidad, eficacia y eficiencia que debe observar en el desempeño de su empleo, cargo o función, el sujeto disciplinable ejercerá los derechos, cumplirá los deberes, respetará las prohibiciones y acatará el régimen de inhabilidades, incompatibles, impedimentos y conflictos de intereses, establecidos en la Constitución Política y en las Leyes".

Que mediante la Ley 1955 del 25 de mayo de 2019 "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad", se establece en su artículo 147 "... Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios, la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la cuarta revolución industrial, entre otros".

Que mediante la Ley 2196 del 18 de enero de 2022 "Por medio de la cual se expide el estatuto disciplinario policial", que regula el comportamiento del personal uniformado de la Policía Nacional.

Que el Decreto 019 del 10 de enero de 2012, "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios, existentes en la administración pública", en el artículo 1, estipula que la finalidad es, proteger y garantizar la efectividad de los derechos de las personas naturales y jurídicas ante las autoridades y facilitar las relaciones de los particulares.

Que mediante el Decreto 857 del 2 de mayo de 2014 "Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones", se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, y establece los niveles de clasificación de la información para los organismos que realizan funciones de inteligencia y contrainteligencia.

Que el Decreto 2573 del 12 de diciembre de 2014, "Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones"; instituye lineamientos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones.

Que el Decreto 1070 del 26 de mayo de 2015 "Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa", establece en su capítulo 6 la reserva legal, niveles de clasificación, sistema para la designación de los niveles de acceso a la información y desclasificación de documentos.

Que el Decreto 1083 del 26 de mayo de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública",establece las políticas de Gestión y Desempeño Institucional entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Que el Decreto 113 del 25 de enero de 2022, modificó la estructura del Ministerio de Defensa Nacional, norma que en su numeral 3 del artículo 2, faculta al director general de la Policía Nacional de Colombia, expedir resoluciones, manuales, reglamentos y demás actos administrativos necesarios para administrar la Policía Nacional en todo el territorio nacional.

Que el Decreto 338 del 8 de marzo de 2022, "Por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital".

Que el Decreto 767 del 16 de mayo de 2022 "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 Tecnologías de la Información y las Comunicaciones", establece los lineamientos generales de la Política de Gobierno Digital.

Que mediante Resolución 001519 del 24 de agosto de 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos", se definen los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 del 2014, estableciendo los criterios para la estandarización de contenidos e información, accesibilidad web, seguridad digital, datos abiertos y formulario electrónico para Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD).

Que mediante Resolución 02229 del 25 de septiembre de 2020 "Por la cual se adopta la Política de Tratamiento de Datos Personales de la Policía Nacional", la institución adopta la Política de tratamiento de Datos personales definida a través de la Ley Estatutaria 1581 del 17 de octubre de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".

Que mediante Resolución 00500 del 10 de marzo de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digita", se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital, que busca mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital en las organizaciones del Estado, mediante la incorporación de estándares internacionales que establezca las mejores prácticas en la materia.

Que mediante Resolución 0463 del 9 de febrero de 2022 "Por la cual se define el uso de las tecnologías en la nube para el sector defensa y se dictan otras disposiciones", el Ministerio de Defensa Nacional define el uso de las tecnologías en la nube para el sector defensa con el fin de establecer los lineamientos mínimos necesarios para habilitar el uso de los servicios de tecnologías en la nube en las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al sector defensa.

Que mediante Resolución 7870 del 26 de diciembre de 2022 "Por la cual se emite y adopta la política general de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de los servicios tecnológicos en las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al sector defensa, y se dictan otras disposiciones", el Ministerio de Defensa Nacional emite y adopta la política general de seguridad y privacidad de la información, seguridad digital, ciberseguridad, y continuidad de los servicios tecnológicos en las unidades ejecutoras o dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al sector defensa.

Que mediante Resolución 1528 de 15 de mayo de 2024 "Por la cual se expide el Reglamento de Doctrina de la Policía Nacional", con el fin de establecer normas y parámetros que cada integrante de la Policía Nacional debe seguir para la generación, actualización, transferencia, apropiación, aplicación y evaluación de la doctrina de la Policía Nacional, como parte fundamental para la movilización del conocimiento entorno al servicio de Policía.

Que mediante Directiva Presidencial 02 del 24 de febrero de 2022, "Reiteración de la política pública en materia de Seguridad Digital", se imparten directrices para asegurar la información en las entidades públicas de la rama ejecutiva del orden nacional.

Que la Norma Técnica Colombiana NTC-ISO/IEC 27001:2022, se refiere a los requisitos para adoptar Sistemas de Gestión de la Seguridad de la Información (SGSI).

Que la Policía Nacional mediante la implementación del Sistema de Gestión de Seguridad de la Información, busca proteger los activos de la información como insumo fundamental para el cumplimiento de la misión y asegurar la continuidad de la institución, protegiéndola a través de la aplicación efectiva de las mejores prácticas para alcanzar los estándares de calidad, seguridad y ciclo de vida de la información, contribuyendo así a la gobernabilidad del país, a través de la implementación de principios, políticas, procedimientos, manuales, formatos y lineamientos para la gestión de la seguridad de la información.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1. EXPEDIR. El Manual del Sistema de Gestión de Seguridad de la Información (SGSI) para la Policía Nacional.

TÍTULO I

DE LAS GENERALIDADES

CAPÍTULO I

OBJETO Y ALCANCE

ARTÍCULO 2. OBJETO. Establecer lineamientos para implementar, gestionar y mantener Sistema de Gestión de Seguridad de la Información necesario para minimizar riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de la Policía Nacional, bajo estándares normativos y requisitos legales relacionados con la Seguridad de la Información.

ARTÍCULO 3. ALCANCE. Aplica a todas las personas que integran o prestan un servicio a la institución de manera permanente o temporal, según corresponda y que en el desempeño de sus

funciones constitucionales, legales y reglamentarias, apliquen los presentes lineamientos desde su generación hasta la eliminación del dato, sin importar el medio, formato, presentación, ubicación, entre otras en la que se encuentre.

CAPÍTULO II

FUNDAMENTOS Y PRINCIPIOS

ARTÍCULO 4. FUNDAMENTOS. Este Sistema de Gestión de Seguridad de la Información se fundamenta en el marco legal, normativo y demás estándares internacionales para la seguridad de la información; incorporando los controles necesarios para contribuir al aseguramiento de la disponibilidad, integridad y confidencialidad de la información institucional.

ARTÍCULO 5. PRINCIPIOS. Este SGSI se fundamenta en los principios institucionales[1] y aquellos inmersos en la operacionalización del Sistema de Gestión de Seguridad de la Información, los cuales se fundamentan entorno al Marco de Gerencia Policial y el Sistema de Gestión Institucional, así:

- **VERACIDAD.** "La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error". (Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, 17 de octubre de 2012, D.O[2]. No. 48587).

- **CONFIDENCIALIDAD:** propiedad de la información para asegurar que solo las personas autorizadas puedan acceder a ella. (ISO[3],2018).

- **INTEGRIDAD:** propiedad de la información para asegurar que los datos no sean alterados de manera no autorizada y que permanezcan coherentes y correctos a lo largo de su ciclo de vida. (ISO,2018).

- **DISPONIBILIDAD:** propiedad que asegura que la información es accesible y utilizable, cuando se requiera por personas autorizadas.(ISO,2018).

- **PRIVACIDAD:** "protege los datos personales y garantiza que se cumplan los derechos de privacidad de los individuos en el manejo de su información". (Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, 17 de octubre de 2012, D.O. No. 48587).

- **ACCESO:** "Los individuos tienen el derecho de acceder a la información que poseen las entidades públicas y privadas, siempre y cuando no existan restricciones legales o de privacidad". (Ley 1712 de 2014, la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, 6 de marzo de 2014, D.O. No. 49084).

- **RESPONSABILIDAD EN EL USO DE LA INFORMACIÓN:** "en virtud de este, cualquier persona que haga uso de la información que proporcionen los sujetos obligados, lo hará atendiendo a la misma". (Ley 1712 de 2014, la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, 6 de marzo de 2014, D.O. No. 49084).

[1] Ley 62 del 12 de agosto de 1993, artículo 2 "principios"
[2] D.O. Diario Oficial: publicación del Gobierno de Colombia que contiene las leyes, los decretos, los actos y la mayoría de los documentos pertinentes y los avisos públicos del presidente, el Congreso y las agencias gubernamentales de Colombia. (Decreto de 28 de abril de 1864 [Presidencia de la República de Colombia], mediante el cual se informa la creación del Diario del Tesoro, el cual tendrá una frecuencia semanal y reemplazará a la publicación Registro Oficial, 28 de abril de 1864).
[3] ISO – International Organization for Standardization: Organización Internacional de Normalization

CAPÍTULO III

DEFINICIÓN Y ESTRUCTURA

ARTÍCULO 6. DEFINICIÓN. El Sistema de Gestión de Seguridad de la Información (SGSI) establece los lineamientos basados en estándares internacionales para proteger la información contra cualquier tipo de amenaza deliberada o accidental; contribuyendo así a garantizar la confidencialidad, integridad y disponibilidad de la información que permite brindar confianza a las partes interesadas.

ARTÍCULO 7. ESTRUCTURA. El Sistema de Gestión de Seguridad de la Información se estructura bajo el enfoque del ciclo de mejoramiento continuo, partiendo de la (I) Planeación del SGSI; (II) Implementación y operación del SGSI; (III) Seguimiento y revisión del SGSI; (IV) Mantenimiento y mejora del SGSI.

Fuente. Adaptado del estándar internacional ISO 27001 - Policía Nacional

TÍTULO II

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO I

PLANEACIÓN

ARTÍCULO 8. PLANEACIÓN. Diseño de las bases para garantizar la protección frente a amenazas, riesgos y vulnerabilidades a la que pueden estar expuestos de los activos de información de la institución, conformado por los siguientes elementos:

- **CONTEXTO**: análisis del entorno interno y externo en el que opera la institución y que afecta o influye en la forma en que se gestiona y protege la información, de acuerdo a lo indicado en la misión, visión, mega, políticas y otros elementos del direccionamiento o formulación estratégica vigente.

- **LIDERAZGO**: compromiso de la alta dirección para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, asegurando que esta sea aplicada de forma transversal en la operacionalización de la gestión institucional, definiendo una política y lineamientos específicos que contribuyan a asegurar la disponibilidad, integridad y confidencialidad de la información institucional.

- **PLANIFICACIÓN:** establece los objetivos de seguridad de la información los cuales deberán ser específicos, medibles, alcanzables, relevantes y temporales; de igual forma se debe realizar la identificación de los riesgos acorde a los parámetros definidos por la política integral de gestión del riesgo institucional, selección de los controles y define las acciones necesarias para garantizar la protección de sus activos de información, alienadas con los requisitos institucionales, normativos y de las partes interesadas.

- **APOYO**: recursos, competencias, capacidades y acciones necesarias para garantizar que el Sistema de Gestión de Seguridad de la Información sea implementado, sostenido y mejorado de manera eficaz, incluyendo personal idóneo, infraestructura tecnológica adecuada, asignación de presupuesto, documentación relevante y la promoción de una cultura organizacional que priorice la seguridad de la información.

ARTÍCULO 9. POLÍTICA. La Policía Nacional de Colombia se compromete a proteger los activos de información institucionales, contribuyendo al aseguramiento de la disponibilidad, integridad y confidencialidad; con el objetivo de salvaguardarlos de amenazas y vulnerabilidades; promoviendo una cultura de protección de la información, gestionando adecuadamente los riesgos, respondiendo de manera oportuna ante los incidentes de seguridad de la información, fortaleciendo la continuidad tecnológica e institucional, mediante acciones basadas en estándares internacionales que definan las mejores prácticas y controles necesarios para asegurar la información institucional.

ARTÍCULO 10. OBJETIVOS. El Sistema de Gestión de Seguridad de la Información tendrá los siguientes objetivos, los cuales aportan al cumplimiento de la Política de Seguridad de la Información:

1. Crear una cultura de seguridad de la información en la institución para fortalecer el conocimiento, la apropiación de prácticas seguras y la conciencia sobre la importancia de proteger los activos de información, mediante campañas de sensibilización, capacitaciones y la implementación de lineamientos basados en las buenas prácticas, incrementando el nivel de protección y reducir los riesgos asociados a la gestión de la información institucional.

2. Identificar, analizar, valorar y gestionar de forma proactiva los riesgos de seguridad de la información de acuerdo a los lineamientos institucionales para la gestión de riesgo, con el fin de minimizar el impacto de posibles vulnerabilidades en los activos de información institucionales, mediante la ejecución de un proceso de evaluación continua de riesgos, el establecimiento de controles preventivos y correctivos, y la actualización periódica de estrategias de mitigación, reduciendo la probabilidad de ocurrencia de incidentes de seguridad de la información por la misma causa.

3. Implementar mejores prácticas y capacidades para identificar, proteger, detectar, responder y recuperarse ante incidentes de seguridad de la información, para reducir la probabilidad y el impacto de dichos incidentes en los activos de información institucional, mediante el fortalecimiento de protocolos, la capacitación continua del personal y la integración de herramientas de monitoreo y respuesta, con el fin de disminuir el tiempo de afectación a la plataforma tecnológica en producción.

4. Adoptar mejores prácticas para garantizar la disponibilidad, integridad y confidencialidad de los datos ante posibles eventos adversos o amenazas que puedan afectar la continuidad tecnológica de la institución, para minimizar el impacto de dichos eventos en las operaciones críticas, mediante la implementación de protocolos de respaldo, planes de recuperación y controles de acceso, con el fin de asegurar que los sistemas catalogados como críticos puedan ser restaurados en un plazo máximo de 24 horas tras un incidente.

CAPÍTULO II

IMPLEMENTACIÓN Y OPERACIÓN

ARTÍCULO 11. IMPLEMENTACIÓN Y OPERACIÓN. Se desarrolla a través de los procedimientos asociado al proceso de direccionamiento tecnológico de código 1DT-CP-0001, el cual despliega las actividades de implementación, ejecución y seguimiento, que permiten proteger la información de la institución, a través de acciones planificadas para gestionar los riesgos, manteniendo la seguridad de los activos de información que contribuyan a garantizar el cumplimiento de los objetivos del SGSI, mediante:

a. Lineamientos específicos.
b. Controles.

ARTÍCULO 12. LINEAMIENTOS ESPECÍFICOS. Directrices detalladas para abordar aspectos concretos de la seguridad de la información para contribuir al aseguramiento de la disponibilidad, integridad y confidencialidad de los activos de información, entre los cuales se encuentran:

1. Control de acceso.
2. Seguridad física.
3. Uso aceptable de la información y otros activos asociados.
4. Transferencia de información.
5. Configuración y gestión segura de dispositivos finales de usuario.
6. Seguridad de redes.
7. Gestión de incidentes de seguridad de la información.
8. Copia de seguridad de la información.
9. Clasificación y tratamiento de la información.
10. Gestión de vulnerabilidades técnicas.
11. Ciclo de vida de desarrollo seguro.
12. Uso de la criptografía.
13. Acuerdos con los proveedores.
14. Uso de servicios en la nube.
15. Continuidad de negocio.
16. Cumplimiento de requisitos legales.
17. Proceso disciplinario.
18. Confidencialidad o de no divulgación.
19. Trabajo remoto.
20. Escritorio y pantalla limpia.
21. Gestión de medios de almacenamiento.
22. Eliminación de información.
23. Seguridad del capital humano.
24. Operaciones de protección de los activos de información.
25. Seguridad en las comunicaciones.
26. Interoperabilidad.

ARTÍCULO 13. CONTROL DE ACCESO. Todos los funcionarios de la Policía Nacional que tengan acceso a la información institucional en aplicaciones o sistemas de información, deben disponer de un usuario único denominado usuario empresarial, que estará asociado a la identidad humana, el cual será único e intransferible[4], por lo cual, el uso no adecuado, préstamo o uso de otra cuenta de la cual no sea titular, acarreará las sanciones a que haya lugar. Por tanto, la fuga, pérdida, alteración o modificación de la información que sea manipulada a través este usuario, sea esta en forma intencional, negligente[5] o con violación al deber objetivo de cuidado, será únicamente responsabilidad del funcionario a quien se le asignó el mismo, por lo que se deberá tener en cuenta las recomendaciones dadas al momento de la asignación de usuario y términos de uso, por lo tanto, todos los sistemas de información de la Policía Nacional y aquellos que sean entregados o

[4] Intransferible: se refiere a algo que no puede ser transferido, cedido o traspasado a otra persona o entidad. (Microsoft,2024)
[5] Negligente: persona que no cumple con sus responsabilidades o deberes con el cuidado o la atención adecuados. (Microsoft,2024)

desarrollados por terceros para uso exclusivo de la institución, deben ser integrados con el Sistema de Identificación Policial Digital (IPD).

La asignación de identidades no humanas para la gestión de dispositivos, aplicaciones, servicios, o cualquier entidad no humana que interactúa con sistemas de información, debe cumplir con el procedimiento liderado por la Oficina de Tecnologías de la Información y las Comunicaciones, dejando los registros de asignación.

Se deben establecer medidas de control de acceso a los activos de información institucional teniendo en cuenta los niveles de criticidad obtenidos en la ejecución del procedimiento de identificación y valoración de activos de información.

La Oficina de Tecnologías de la Información y las Comunicaciones emitirá el lineamiento complementario que permita operacionalizar el uso de la red institucional a través de la navegación y uso adecuado de la plataforma tecnológica de la Policía Nacional, para los usuarios de los servicios ofrecidos por el proceso de Direccionamiento Tecnológico, en los que se incluya el control de dispositivos y cifrado de equipos.

PARÁGRAFO. Para el acceso a los equipos de cómputo que se encuentran fuera de la red institucional se debe implementar controles de acceso en los que se exija un usuario y contraseña con el principio de mínimos privilegios[6].

ARTÍCULO 14. SEGURIDAD FÍSICA. Todas las unidades de la Policía Nacional, adoptarán medidas para la protección del perímetro de seguridad de sus instalaciones físicas, alineándose al manual de seguridad física de instalaciones policiales, con el fin de controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas destinadas al procesamiento o almacenamiento de información clasificada, reservada, o con niveles de clasificación de la información de inteligencia y contrainteligencia (Ley Estatutaria 1621 de 2013, la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones, 17 de abril de 2013, D.O 48764); así como, la información gestionada en los equipos y demás infraestructura que soporte la gestión institucional en los sistemas de información y las comunicaciones, que permita mitigar los riesgos, amenazas externas y ambientales, que contribuyan a evitar la afectación de la confidencialidad, disponibilidad e integridad de la información institucional.

ARTÍCULO 15. USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS. Los funcionarios de la Policía Nacional, uniformados, no uniformados, contratistas y quienes generan o hacen uso de la información institucional, deberán atender las directrices emitidas para el uso correcto de la información de acuerdo a los niveles de clasificación adoptados por la institución; a través de la Oficina de Tecnologías de la Información y las Comunicaciones, se debe emitir lineamientos que permitan operacionalizar el uso aceptable del uso de los activos asociados a los servicios de internet, correo electrónico, redes inalámbricas, segregación de redes, computación en la nube, sistemas de información de acceso público y los recursos tecnológicos dispuestos para el soporte del servicio de policía.

ARTÍCULO 16. TRANSFERENCIA DE INFORMACIÓN. Los funcionarios de la Policía Nacional, uniformados, no uniformados, contratistas y quienes generan o hacen uso de la información institucional, dueño y custodios de los datos deberán asegurar en todo momento los controles que permitan proteger la información en todos los tipos de transferencia en sus diferentes niveles de clasificación.

ARTÍCULO 17. CONFIGURACIÓN Y GESTIÓN SEGURA DE DISPOSITIVOS FINALES DE USUARIO. La Policía Nacional adopta el principio de mínimos privilegios en las configuraciones de los dispositivos finales de usuario, por ende, únicamente pueden hacer gestiones de configuración en los dispositivos de la institución el personal autorizado de los Grupos o Responsables de Tecnologías de la Información y las Comunicaciones previa asignación de privilegios de acuerdo a roles y funciones.

[6] Principio de mínimos privilegios: este principio establece que a los usuarios, aplicaciones y procesos se les debe otorgar únicamente los permisos necesarios para realizar sus funciones. (Microsoft,2024)

ARTÍCULO 18. SEGURIDAD DE REDES. El proceso de Direccionamiento Tecnológico define los controles de seguridad de la red de datos institucional, usando como referencia la Norma Técnica ISO/IEC 27033-1:2018 Tecnología de la información - Técnicas de seguridad – seguridad de redes, o el que haga sus veces, en la que se contemplen mejores prácticas para asegurar la infraestructura tecnológica.

ARTÍCULO 19. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. La Policía Nacional promueve entre los funcionarios y contratistas el reporte y seguimiento de eventos o incidentes relacionados con la seguridad de la información y los activos asociados, con el fin de responder oportunamente ante la materialización de riesgos asociados a la afectación de la disponibilidad, integridad y confidencialidad de la información institucional.

ARTÍCULO 20. COPIA DE SEGURIDAD DE LA INFORMACIÓN. La Oficina de Tecnologías de la Información y las Comunicaciones, cuenta con el procedimiento o lineamiento emitido para la administración de copias de respaldo o backup y restauración de información o el que haga sus veces, a través del cual, establece la forma de realizar el respaldo de la información contenida en las bases de datos, administrada por el centro de datos principales, donde al principio de cada vigencia realizará la proyección de la planeación de los respaldos y pruebas de restauración a ejecutar durante el año y debe ser documentado.

PARÁGRAFO 1. Para las unidades en la cual no se cuenta con un servidor de archivos, el propietario, dueño o custodio de la información son los responsables de asegurar que se realicen las copias de seguridad correspondientes de la información de gestión, los cuales deben contar con controles de seguridad como cifrado de los medios en los cuales se almacena el respaldo de información clasificada, reservada o con niveles de inteligencia y contrainteligencia.

PARÁGRAFO 2. Las unidades que administren bases de datos de sistemas de información, y servidores de archivos con datos no estructurados, realizarán la planeación de los respaldos y pruebas de restauración, de acuerdo con el procedimiento o lineamiento emitido por el Direccionamiento Tecnológico, para la administración de backup y restauración de información.

PARÁGRAFO 3. No se contemplarán los respaldos de información personal, software no autorizado o no licenciado, archivos que atentan contra los derechos de propiedad intelectual, como música, videos, juegos y demás que no sean producto de la ejecución de los procesos institucionales.

ARTÍCULO 21. CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN. Todos los funcionarios deben realizar clasificación de la información de acuerdo a los lineamientos emitidos por la Policía Nacional en el índice de información clasificada y reservada o con niveles de inteligencia y contrainteligencia; por lo tanto, los dueños y custodios de los activos de información, son los responsables de asegurarse que cumplan los niveles de acceso a la información de acuerdo a los niveles de clasificación establecidos.

ARTÍCULO 22. GESTIÓN DE VULNERABILIDADES TÉCNICAS. A través de la Oficina de Tecnologías de la Información y las Comunicaciones se debe realizar el análisis de la explotación de vulnerabilidades técnicas[7], que podrían poner en riesgo la plataforma tecnológica institucional en producción y su información, y deben ser gestionadas y remediadas por los administradores del componente tecnológico y los sistemas de información, manteniendo la información actualizada de nuevas vulnerabilidades, mediante la suscripción a las bases de datos de conocimiento de seguridad informática, por lo tanto, ningún funcionario de la Policía Nacional diferente a los designados por el Direccionamiento Tecnológico está autorizado para realizar análisis de vulnerabilidades o pruebas de penetración[8] (pentesting) a los sistemas de información o a los componentes que conforman la plataforma tecnológica en producción.

ARTÍCULO 23. CICLO DE VIDA DE DESARROLLO SEGURO. La Oficina de Tecnologías de la Información y las Comunicaciones, debe velar porque el desarrollo de sistemas de información o aplicaciones, realizado de forma interna (in-house) o adquirido para soportar la gestión institucional,

[7] Vulnerabilidades técnicas: debilidades o fallos en los sistemas de información que pueden ser explotados por atacantes para comprometer la seguridad de la información. (Microsoft,2024)
[8] Pruebas de penetración: evaluaciones de seguridad que simulan ataques reales contra sistemas informáticos, redes o aplicaciones para identificar y explotar vulnerabilidades. (Microsoft,2024)

cumplan con los requerimientos de seguridad adecuados para la protección de la información de la Policía Nacional, para lo cual, desplegará una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas y puesta en producción de los sistemas de información, en cumplimiento del procedimiento establecido para tal fin.

La Oficina de Tecnologías de la Información y las Comunicaciones, es la encargada de avalar los proyectos de desarrollo presentados mediante la evaluación de tecnologías de la información y las comunicaciones - TIC; así como la adquisición y recepción de software de cualquier tipo, en el marco de convenios y contratos con terceros, conforme a los requerimientos establecidos; con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la Policía Nacional. En consecuencia, cualquier herramienta tecnológica gestionada y administrada por otra unidad, diferente a la Oficina de Tecnologías de la Información y las Comunicaciones, deben mediante comunicado oficial informar a esta oficina asesora, para ser incluido en el sistema de inventarios de la institución, cumpliendo con los lineamientos técnicos, presupuestales y de seguridad, con el fin de salvaguardar la información almacenada en las bases de datos, brindar el soporte, y demás procesos técnicos que permitan su recuperación en caso de algún incidente de seguridad de la información o siniestro.

Todos los desarrollos autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones, a partir de la fecha deberán contar con el módulo de auditoría, que permita almacenar los registros de transacciones realizadas desde la interfaz de usuario final o desde cualquier otra herramienta; igualmente, para que dicho sistema de información pueda ser visualizado desde el entorno de producción, deberá ser aprobado por el Comité Asesor de Gestión del Cambio de la Oficina de Tecnologías de la Información y las Comunicaciones, y este a su vez, tiene la función de validar que se haya cumplido con el procedimiento de desarrollo de software (1DT-PR-0017) en su totalidad y en especial, que se visualicen las guías técnicas y funcionales del sistema de información.

PARÁGRAFO. El propietario del sistema de información en coordinación con el líder funcional, deben realizar la guía de usuario final de cada formulario que este en producción, así como, la guía para la asignación de derechos de acceso; además, deben socializar con todos los usuarios finales la ejecución de dichas guías, con el fin de ajustar cualquier inquietud o novedad que se pueda presentar en la fase de implementación del sistema.

ARTÍCULO 24. USO DE LA CRIPTOGRAFÍA. Se deben utilizar sistemas y técnicas criptográficas[9] para la protección de la información, con el fin de procurar una adecuada protección de la disponibilidad, integridad, confidencialidad y autenticidad de los activos de información, que permita asegurar la transferencia y gestión de la información.

PARÁGRAFO 1. La información que se encuentra bajo la protección de la Ley Estatutaria 1621 del 17 de abril de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", usará los controles criptográficos definidos por la Dirección de Inteligencia Policial - DIPOL.

PARÁGRAFO 2. El Grupo Seguridad de la Información y Respuesta a Incidentes Informáticos - CSIRT, de la Oficina de Tecnologías de la Información y las Comunicaciones, es el encargado de establecer los lineamientos necesarios para el control y el uso criptográfico de los servicios acreditaos para la Entidad de Certificación Digital de la Policía Nacional.

ARTÍCULO 25. ACUERDOS CON LOS PROVEEDORES. Se deben establecer mecanismos de control en la relación con los proveedores[10], teniendo en cuenta que, se fundamental asegurar la información que genere, custodie, procese o se tengan acceso, supervisando el cumplimiento de lo

[9] Técnicas criptográficas: métodos basados en algoritmos matemáticos que transforman los datos en una forma que solo puede ser leída por personas autorizadas con el fin de proteger la información, asegurando su confidencialidad, integridad y autenticidad. (Microsoft,2024)

[10] Proveedores: empresas o entidades que suministran productos, servicios o soluciones adquiridas para fortalecer el apoyo al servicio de policía. (Microsoft,2024)

establecido en el marco de la seguridad de la información. El supervisor de cada contrato o convenio, será responsable de divulgar la política y lineamientos de seguridad de la información.

La persona jurídica proveedora de servicios, deberá diligenciar y entregar el formato Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Contratistas o Terceros o el que haga sus veces, suscrito por el representante legal de la empresa, el cual hará parte de la carpeta que reposa el respectivo contrato.

PARÁGRAFO 1. El personal contratista y quienes hagan parte del contrato (ayudantes, obreros, implementadores, desarrolladores, personal de servicios, entre otros), deberá diligenciar y entregar el formato Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Contratistas o Terceros o el que haga sus veces, en cada proceso contractual vigente con la Policía Nacional, el cual será conservado en original y archivados en forma segura en la carpeta de supervisión del proceso contractual.

PARÁGRAFO 2. Los contratistas o personal de soporte que labora y realizan actividades por prestación de servicios, obra o labor para la Dirección de Inteligencia Policial, deberán suscribir el compromiso de reserva o el que haga sus veces y aprobar el estudio de credibilidad y confiabilidad en cumplimiento a la Ley Estatutaria 1621 del 17 de abril de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", este último, en los casos que sea necesario; el cual será conservado en original y archivados en forma segura en la carpeta de supervisión del proceso contractual o en el que disponga la unidad.

ARTÍCULO 26. USO DE SERVICIOS EN LA NUBE. Los servicios adquiridos en la nube o Cloud Computing[11] que contemplen ya sea hardware o software, deben aplicar las medidas y controles de seguridad necesarios para garantizar la integridad, disponibilidad y confidencialidad de la información de la plataforma tecnológica de la Policía Nacional, cumpliendo con todos los requisitos y normatividad vigente, durante la adquisición, uso, gestión y finalización de dichos servicios en la nube, documentando de forma expresa y clara:

- La evaluación de los riesgos, asociando la identificación del activo, la evaluación de vulnerabilidades y el análisis de impacto; con el fin de determinar qué datos, servicios o aplicaciones pasarían a la gestión en nube, evaluando las vulnerabilidades en los servicios en la nube y posibles incidentes de seguridad.
- Acuerdos y niveles de servicio para gestionar la seguridad de la información, especialmente en términos de seguridad y disponibilidad.
- La topología de la red que se utiliza en la solución.
- Tipo de nube a utilizar (nube privada, nube pública o servicio híbrido)
- Modelo de servicio utilizado en la nube, IaaS[12] (Infraestructura como Servicio), PaaS[13] (Plataforma como Servicio), SaaS[14] (Software como Servicio).
- Modelo de responsabilidad compartida entre el proveedor de servicio y la institución.
- Seguridad proporcionada en los datos almacenados en la nube.
- Política de actualizaciones y parches de seguridad.

[11] Cloud Computing - Computación en la nube: modelo de entrega de servicios de tecnología de la información (TI) en el que los recursos, como servidores, almacenamiento, bases de datos, redes, software y análisis, se ofrecen a través de Internet. (Microsoft,2024)
[12] IaaS - Infraestructura como Servicio: modelo de computación en la nube que proporciona recursos de infraestructura virtualizados a los usuarios a través de Internet. (Microsoft,2024)
[13] PaaS – Plataforma como Servicio: modelo de computación en la nube que proporciona una plataforma gestionada y lista para el desarrollo, prueba, implementación y gestión de aplicaciones o sistemas de información. (Microsoft,2024)
[14] SaaS – Software como Servicio: modelo de distribución de software en el que las aplicaciones se alojan en la nube y son accesibles a través de Internet. (Microsoft,2024)

- Productos de seguridad de detección antimalware[15] o detección de intrusos en los equipos en los cuales se aloja la información.

- Cifrado utilizado en el tráfico de la información desde y hacia la nube.

- Política de respuesta a incidentes de seguridad informática establecida por el proveedor del servicio en la nube.

- Lugares o países en los cuales se encuentran los servidores que prestan el servicio de gestión, almacenamiento y replicación.

- Política de retención o borrado seguro de los datos una vez no se haga uso del servicio en la nube.

- Cumplimiento normativo de entrega de información en caso de ser requerido por una entidad judicial

- Por ningún motivo se podrá almacenar información clasificada, reservada o con niveles de inteligencia y contrainteligencia en servicios en la nube públicos o híbridos.

PARÁGRAFO. El lineamiento se adoptará de acuerdo con la Resolución Ministerial 0463 del 9 de febrero de 2022 "por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones".

ARTÍCULO 27. CONTINUIDAD DE NEGOCIO. La Policía Nacional dispondrá de planes necesarios para la continuidad de la operación de los servicios tecnológicos, los cuales serán operados por los líderes de los procesos. La Oficina de Tecnologías de la Información y las Comunicaciones y las unidades de policía donde se cuente con procesamiento de información crítica para la institución, deben documentar un plan de continuidad del negocio alineado con estándares internacionales basado en la Norma Técnica ISO 22301:2019; así mismo, elaborar el Análisis de Impacto del Negocio (BIA)[16] determinando los procedimientos esenciales para la continuidad de las operaciones y un Plan de Recuperación ante Desastres (DRP)[17] en materia tecnológica, a fin de garantizar la continuidad de la operación de los servicios tecnológicos críticos de la Policía Nacional.

ARTÍCULO 28. CUMPLIMIENTO DE REQUISITOS LEGALES. La Policía Nacional velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad de la información, de acuerdo con lo establecido por el Gobierno Nacional, entre ellos, los referentes a derechos de autor y propiedad intelectual, protección de datos personales, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y Política de Seguridad Digital.

ARTÍCULO 29. PROCESO DISCIPLINARIO. La Policía Nacional cuenta con el proceso de integridad policial, donde a través del estatuto disciplinario policial, en el cual se establecen las medidas disciplinarias a tomar, en caso de presentarse afectaciones a la disponibilidad, integridad y confidencialidad de la información institucional.

PARÁGRAFO. La Oficina de Tecnologías de la Información y las Comunicaciones, realizará la identificación de las conductas que pueden afectar la política de seguridad de la información y que su ocurrencia inicial no conlleva a una falta disciplinaria, y definirá las acciones a seguir para evitar su recurrencia[18].

ARTÍCULO 30. CONFIDENCIALIDAD O DE NO DIVULGACIÓN. La institución ha establecido los formatos declaración de confidencialidad y compromiso con la seguridad de la información servidor público, declaración de confidencialidad y compromiso con la seguridad de la información contratistas o terceros, así como el formato compromiso de reserva o el que haga sus veces, en el

[15] Antimalware: antimalware es un tipo de software diseñado para detectar, prevenir y eliminar software malicioso, como virus, gusanos, ransomware, spyware, y troyanos, de los dispositivos. (Microsoft,2024)
[16] Análisis de Impacto del Negocio (BIA): proceso sistemático que ayuda a identificar y evaluar los posibles efectos de interrupciones en las operaciones esenciales para la unidad. (Microsoft,2024)
[17] Plan de Recuperación ante Desastres (DRP): documento formal que describe cómo la unidad se prepara, responde y se recupera de eventos catastróficos que afectan las operaciones esenciales de la unidad. (Microsoft,2024)
[18] Recurrencia: acción repetitiva de una falta que afecta la política de seguridad de la información. (Microsoft,2024)

cual, se instauran los lineamientos de la confidencialidad y el tiempo de reserva de esta, una vez terminado el vínculo laboral.

PARÁGRAFO 1. Todas las actividades en la plataforma tecnológica de la Policía Nacional pueden ser monitoreadas y auditadas, donde todos los servidores públicos de la Policía Nacional deben conocer las restricciones, al tratamiento de los datos y de la información, respecto a la cual tengan conocimiento en ejercicio de sus funciones legales. Cualquier persona que acceda a las instalaciones de la Policía Nacional, podrá ser monitoreada y grabada por medio de circuito cerrado de televisión.

PARÁGRAFO 2. Los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia en la Policía Nacional, los funcionarios que adelantan actividades de control, supervisión y revisión de documentos o bases de datos de inteligencia y contrainteligencia y los receptores de productos de inteligencia de que trata el artículo 36 de la Ley Estatutaria 1621 del 17 de abril de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", están obligados a, suscribir acta de compromiso de reserva con relación a la información de la que tenga conocimiento. Así mismo, los asesores externos y contratistas solo podrán conocer, acceder o recibir información de inteligencia y contrainteligencia de conformidad con el artículo 37 de la norma ibidem, y deberán suscribir acta de compromiso de reserva, previo estudio de credibilidad y confiabilidad. El deber de reserva de los servidores públicos de los organismos que desarrollan actividades de inteligencia y contrainteligencia y los receptores antes mencionados, permanecen aún después del cese de sus funciones o retiro de la institución hasta el término máximo que establezca la ley para este tipo de información.

ARTÍCULO 31. TRABAJO REMOTO. La Policía Nacional autoriza el uso de dispositivos personales para acceder a la red interna mediante el rol asignado de VPN (Virtual Private Network). Este acceso debe cumplir con el procedimiento y lineamientos establecidos para la gestión de identidades (1DT-PR-0003). El objetivo es facilitar que los funcionarios continúen desarrollando sus funciones asignadas mientras realizan actividades fuera de la unidad policial, siempre que se haya realizado una verificación de seguridad de los equipos de cómputo, utilizando la herramienta adecuada para tal fin.

De igual manera, con el fin de realizar trabajo móvil, la Policía Nacional adquiere dispositivos móviles con líneas corporativas, habilitando a través de estos la conexión a los sistemas de información, que apoyan técnicamente la prestación del servicio policial, mediante el servicio de APN (Access Point Name) de la Policía Nacional, siendo asignados a través del sistema de información dispuesto para tal fin.

PARÁGRAFO. La autorización para que el funcionario pueda acceder a la red interna de la institución, así como, utilizar equipos de cómputo de la Policía Nacional fuera de los complejos institucionales a través de la VPN, solo podrá ser otorgada previo requerimiento, cumpliendo lo definido en el artículo de excepciones del presente manual.

ARTÍCULO 32. ESCRITORIO Y PANTALLA LIMPIA. Se deben establecer directrices que permitan reducir los riesgos de acceso no autorizado, pérdida o daño de la información. Estableciendo controles para asegurar la confidencialidad, integridad y disponibilidad de la información física y bloqueo de acceso a los sistemas de información y equipos que registren inactividad después de cinco (5) minutos.

ARTÍCULO 33. GESTIÓN DE MEDIOS DE ALMACENAMIENTO. La Policía Nacional con el fin de contribuir a la protección de la información gestionada en los equipos de cómputo institucional, realiza control de los medios de almacenamiento, a través de reglas que permiten controlar la extracción de información no autorizada. Por lo tanto, los equipos de cómputo de la institución por defecto cuentan con la asignación de bloqueo de los puertos USB[19], razón por la cual, las excepciones serán tramitadas de acuerdo a las definidas en el presente manual.

[19] Puertos USB (Universal Serial Bus): interfaces estándar que permiten conectar dispositivos periféricos a una computadora. (Microsoft,2024)

Los usuarios son responsables de la información que administran en los equipos asignados, por lo tanto, está prohibido el almacenamiento de información personal como música, videos, imágenes, software, ejecutables portables, que pueda presentar violación a derechos de autor y propiedad intelectual, tanto en equipos de cómputo, como en el servidor de archivos en los lugares donde esté implementado.

PARÁGRAFO. La autorización de activación de los puertos USB de los equipos institucionales o conectados a la red LAN[20], que hagan parte del Servicio de Inteligencia Policial, será dada por el director de Inteligencia Policial - DIPOL, toda vez que esta unidad cuenta con la administración de políticas de prevención de perdida de información - DLP (Data Loss Prevention)[21].

ARTÍCULO 34. ELIMINACIÓN DE INFORMACIÓN. Para la eliminación de información de los dispositivos de almacenamiento, que son dispuestos para el servicio, como reasignación o disposición final, la Policía Nacional adopta procedimientos o lineamiento para el borrado seguro de la información (1DT-PR-0020), el cual, se realiza de forma mecánica o con el software adquirido por la Oficina de Tecnologías de la Información y las Comunicaciones.

Para la eliminación de información contenida en los sistemas de información, debe surtir el trámite de conceptos, mediante el comité de baja de software, liderado por el Direccionamiento Tecnológico.

ARTÍCULO 35. SEGURIDAD DEL CAPITAL HUMANO. Los grupos de talento humano o soporte y apoyo según corresponda, desplegarán esfuerzos de articulación en coordinación con la Oficina de Tecnologías de la Información y las Comunicaciones y sus grupos de nivel desconcentrado, para que todos los funcionarios entiendan sus responsabilidades frente a la seguridad de la información, mediante la programación de actividades de sensibilización a todo nivel, que permita contribuir a fortalecer la disponibilidad, integridad y confidencialidad de la información.

ARTÍCULO 36. OPERACIONES DE PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN. La Oficina de Tecnologías de la Información y las Comunicaciones y sus grupos desconcentrados, serán los encargados de la operación y administración de los recursos tecnológicos que soportan la plataforma tecnológica en producción en la Policía Nacional; quienes velarán por la eficiencia de los controles asociados a los recursos tecnológicos, protegiendo la disponibilidad, integridad y confidencialidad de la información, para que los cambios efectuados sobre los recursos tecnológicos de los sistemas de información, en ambientes de prueba y producción sean controlados y autorizados.

De igual manera, proveerá la capacidad de procesamiento requerida por los recursos tecnológicos y sistemas de información, efectuando proyecciones de incremento y provisiones en la plataforma tecnológica, de acuerdo al crecimiento de la Policía Nacional, e implementará mecanismos de contingencia[22], recuperación ante desastres y continuidad de las operaciones tecnológicas, con el fin de propender por la disponibilidad de los servicios de tecnologías de la información y las comunicaciones en el marco de la operación.

Por consiguiente, la Oficina de Tecnologías de la Información y las Comunicaciones realizará y mantendrá copias de seguridad de la información en medio digital, con el objetivo de recuperarla en caso de ser necesario. De la misma forma, efectuará la copia requerida de acuerdo con el esquema definido previamente, en un procedimiento que enmarque la gestión, copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos; por ende, el diseño de estas actividades se hará en conjunto con los responsables de los sistemas de información o aplicaciones, con el fin de determinar la información a respaldar y la periodicidad del respaldo, los tiempos de recuperación y restauración, y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información. Así mismo, realizará el diagnóstico de seguridad de la información, el cual deberá tener el estado actual, nivel de madurez de la gestión de seguridad y privacidad de la información y las debilidades encontradas en las pruebas de vulnerabilidad.

[20] Red LAN (Local Area Network): red de comunicación de datos que conecta computadoras y dispositivos dentro de un área geográfica limitada, como una oficina, un edificio o un campus. (Microsoft,2024)
[21] Prevención de perdida de información - DLP (Data Loss Prevention): prevención de perdida de información - DLP (Data Loss Prevention). (Microsoft,2024)
[22] Mecanismos de contingencia: estrategias y procedimientos diseñados para anticipar y responder a situaciones imprevistas que puedan afectar las operaciones normales de la institución. (Microsoft,2024)

PARÁGRAFO. Los cambios en la plataforma tecnológica institucional, deberán realizarse de acuerdo al procedimiento de gestión del cambio[23] (1DT-PR-0014) o el que haga sus veces, liderado por la Oficina de Tecnologías de la Información y las Comunicaciones.

ARTÍCULO 37. SEGURIDAD EN LAS COMUNICACIONES. La Oficina de Tecnologías de la Información y las Comunicaciones, establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas, gestionando el intercambio de información interna y externa, de ser necesario, mediante el desarrollo de servicios web (webservices[24]) o cualquier medio de transmisión tecnológico con los controles criptográficos necesarios. De igual forma, dispondrá y monitoreará los mecanismos de seguridad para proteger la disponibilidad, integridad y la confidencialidad de la información.

Todos los servidores públicos independientemente de su nivel jerárquico, firmarán el formato declaración de confidencialidad y compromiso con la seguridad de la información servidor público, en primera instancia al ingreso y durante la relación laboral; finalmente, cada vez que sea objeto de modificación este tipo de vínculo con la institución, el cual será diligenciado de forma física, o digital a través del Portal de Servicios Internos – PSI o el que haga sus veces.

ARTÍCULO 38. INTEROPERABILIDAD[25]. Se deberá establecer una comunicación eficaz entre las entidades del Estado Colombiano y la Policía Nacional, para lograr el intercambio de servicios, datos o documentos entre los sistemas de tecnología de información y comunicación (TIC), de acuerdo con la disponibilidad de tecnologías implementadas por la Policía Nacional, estableciendo la taxonomía de la información[26] de acuerdo a los niveles de clasificación definidos por la institución, que permita identificar claramente la información que por parte de la institución se podrá compartir a través de este marco.

ARTÍCULO 39. CONTROLES. Medidas diseñadas para garantizar la confidencialidad, integridad y disponibilidad de la información, cumpliendo con los requisitos legales, regulatorios y organizacionales, implementados para reducir los riesgos de seguridad de la información y proteger los activos contra amenazas, divididos en la siguiente categoría:

a. Controles organizacionales.
b. Controles de personas.
c. Controles físicos.
d. Controles tecnológicos.

ARTÍCULO 40. CONTROLES ORGANIZACIONALES. Permiten establecer una estructura sólida y eficiente de lineamientos, roles y responsabilidades que permita a la institución proteger de manera efectiva la confidencialidad, integridad y disponibilidad de la información, garantizar el cumplimiento normativo y minimizar los riesgos asociados a amenazas internas y externas, definiendo los siguientes:

1. Roles y responsabilidades
2. Segregación de deberes.
3. Responsabilidades de la dirección.
4. Contacto con las autoridades.
5. Contacto con grupos de interés especial.
6. Inteligencia de amenazas
7. Seguridad de la información en la gestión de proyectos

---

[23] Gestión del cambio: enfoque estructurado para guiar la transición desde un estado actual a un estado futuro deseado. (Microsoft,2024)

[24] Webservices: sistemas de intercambio de información basados en XML que utilizan Internet para la comunicación directa entre aplicaciones(Microsoft,2024)

[25] Interoperabilidad: capacidad de diferentes sistemas, aplicaciones y dispositivos para comunicarse, intercambiar datos y utilizar la información de manera efectiva. (Microsoft,2024)

[26] Taxonomía de la información: disciplina que se enfoca en la organización y clasificación de datos e información en categorías y subcategorías lógicas. Su objetivo principal es hacer que la información sea fácilmente accesible y comprensible, lo que facilita su uso, búsqueda y gestión. (Microsoft,2024)

8. Inventario de información y otros activos asociados.
9. Devolución de los activos.
10. Etiquetado de la información.
11. Seguridad y restricciones en la difusión de productos e información de inteligencia y contrainteligencia.
12. Gestión de identidades
13. Información de autenticación.
14. Derechos de acceso.
15. Seguridad de la información en la relación con proveedores.
16. Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y telecomunicaciones (tic).
17. Seguimiento, revisión y gestión del cambio de los servicios de los proveedores.
18. Evaluación y decisión sobre eventos de seguridad de la información.
19. Respuesta a incidentes de seguridad de la información
20. Aprendizaje de los incidentes de seguridad de la información.
21. Recopilación de evidencias.
22. Seguridad de la información ante una interrupción.
23. Requisitos legales, reglamentarios y contractuales.
24. Derechos de propiedad intelectual.
25. Protección de registros.
26. Privacidad y protección de la información de identificación personal.
27. Revisión independiente de la seguridad de la información.
28. Cumplimiento de políticas, reglas y estándares de seguridad de la información
29. Procedimientos operativos documentados.

ARTÍCULO 41. ROLES Y RESPONSABILIDADES. Con el fin de realizar un adecuado aseguramiento de la administración del Sistema de Gestión de Seguridad de la Información - SGSI, define los siguientes roles que permiten contribuir al aseguramiento, apoyo y cumplimiento de la política de seguridad de la información, los lineamientos específicos y los controles establecidos para proteger los datos institucionales, así:

a. Comité técnico de seguridad de la información
b. Comité interno de seguridad de la información
c. Otras responsabilidades

ARTÍCULO 42. COMITÉ TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN. El comité técnico de seguridad de la información de la Policía Nacional será el encardado de planear, orientar, implementar controles y realizar seguimiento del SGSI a nivel institucional, estructurado de la siguiente manera:

a. Integrantes comité técnico de seguridad de la información.
b. Funciones comité técnico del sistema de gestión de seguridad de la información de la Policía Nacional.
c. Secretaría del Comité técnico de Seguridad de la Información.
d. Sesiones del Comité técnico de Seguridad de la Información

ARTÍCULO 43. INTEGRANTES COMITÉ TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN: estará conformado de la siguiente manera:

- **OFICINA DE PLANEACIÓN.** Asesora la alineación del Sistema de Gestión de Seguridad de la Información, con el Sistema de Gestión Institucional adoptado por la Policía Nacional.

- **OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.** A través del Grupo Seguridad de la Información y Respuesta a Incidentes Informáticos - CSIRT cumplirá las siguientes funciones:

  - Asume la secretaría del ComitéTécnico de Seguridad de la Información.
  - Consolida e informa sobre los incidentes de afectación a la disponibilidad, integridad y confidencialidad de la plataforma tecnológica en producción, presentando informe sobre

aquellos que fueron dados a conocer, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia COLCERT y CSIRT Gobierno.
- Informa sobre los resultados de la evaluación de la Política de Seguridad Digital.
- Consolida la información relacionada con el Sistema de Gestión de Seguridad de la Información, para ser presentado ante el Comité Institucional de Gestión y Desempeño.

- **SECRETARÍA GENERAL.** Realiza la asesoría jurídica, frente a la expedición de lineamientos y mejores prácticas a implementar en la Policía Nacional relacionada con Seguridad de la Información.

- **INSPECCIÓN GENERAL Y RESPONSABILIDAD PROFESIONAL.** Socializa ante el Comité Técnico de Seguridad de la Información, la estadística relacionada con procesos disciplinarios, relacionados con la vulneración de la disponibilidad, integridad y confidencialidad de la información institucional por parte de los funcionarios de la Policía Nacional.

- **DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL.** Socializa ante el Comité Técnico de Seguridad de la Información, las estadísticas relacionadas con delitos informáticos, y acciones relacionadas con ciberseguridad.

- **OFICINA DE COMUNICACIONES ESTRATÉGICAS.** Asesora al comité sobre el despliegue de actividades que permitan el fortalecimiento de la toma de conciencia, en el personal de la Policía Nacional en temas relacionados con seguridad de la información.

- **OFICINA DE CONTROL INTERNO.** Socializa ante el comité los hallazgos o no conformidades relacionadas con el Sistema de Gestión de Seguridad de la Información en los ejercicios de auditoría a nivel país.

- **DIRECCIÓN DE EDUCACIÓN POLICIAL.** Asesora al comité con acciones que permitan la articulación de la seguridad de la información, en los procesos de formación con los que cuenta la institución en los diferentes niveles y categorías.

- **DIRECCIÓN DE PROTECCIÓN Y SERVICIOS ESPECIALES**. Asesora al comité frente la alineación de los controles de seguridad de la información con el manual de seguridad física de instalaciones policiales.

Las acciones adelantadas, y los temas de impacto institucional que se traten en el Comité Técnico de Seguridad de la Información, serán socializadas ante el Comité Institucional de Gestión y Desempeño de la Policía Nacional.

PARÁGRAFO. En caso de ser necesario la intervención de otras dependencias de la Policía Nacional, serán convocadas como invitados para atender temas relacionados con el fortalecimiento del SGSI de la institución.

ARTÍCULO 44. FUNCIONES COMITÉ TÉCNICO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA POLICÍA NACIONAL. El Comité Técnico de Seguridad de la Información tendrá definida las siguientes funciones:

- Revisión de las políticas de seguridad de la información con el fin de mantenerlas actualizadas, vigentes y operativas para asegurar su permanencia y nivel de eficacia.

- Aprobar iniciativas que permitan fortalecer la seguridad de la información en la institución.

- Realizar revisiones periódicas al contexto organizacional o cuando ocurran cambios significativos que afecten el SGSI.

- Promover la difusión y sensibilización de la seguridad de la información en la institución.

- Monitorear los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

- Evaluar y coordinar la implementación de controles específicos que permitan el fortalecimiento de la protección de los activos de información de la institución.

- Atender, recepcionar, revisar y responder ante eventos, incidentes y problemas presentados en materia de seguridad de la información que afecten la institución.

- Acordar y aprobar normas, metodologías y procesos que aporten a la seguridad de la información institucional.

- Liderar y definir las actividades tendientes al fortalecimiento y mejora continua de la seguridad de la Información en la institución.

- Promover el cumplimiento de las políticas de seguridad de la información, por parte del personal de la institución.

- Analizar las conductas contrarias que afectan la política de seguridad de la información de la Policía Nacional, materializadas por parte del personal de la institución.

- Definir herramientas de medición de la eficacia del Sistema de Gestión de Seguridad de la Información,

- Resolver las diferencias o conflictos que pudieran surgir entre la Entidad de Certificación Digital de la Policía Nacional ECD-PONAL y sus suscriptores, en relación con la interpretación o aplicación de la Declaración de Prácticas de Certificación – DPC y las Políticas de Certificados – PC para los Servicios de Certificación Digital en la Policía Nacional, que no pueda ser resuelta, dentro de los treinta (30) días calendario siguientes al momento en que dicha diferencia o conflicto haya sido planteada.

ARTÍCULO 45. SECRETARÍA DEL COMITÉ TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN. Estará a cargo del jefe del Grupo Seguridad de la Información y Respuesta a Incidentes Informáticos - CSIRT o quien haga sus veces, y desarrollará las siguientes funciones:

- Resguardar la información producida por el Comité Técnico de Seguridad de la Información de la Policía Nacional.

- Administrar la gestión documental del comité, mediante el manejo del archivo impreso, digital o electrónico.

- Consolidar la información y los temas a tratar en cada sesión del comité.

- Elaborar el registro documental de cada sesión realizada por el comité.

- Convocar las sesiones ordinarias y extraordinarias del Comité Técnico de Seguridad de la Información.

ARTÍCULO 46. SESIONES DEL COMITÉ TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN. El Comité Técnico de Seguridad de la Información de la Policía Nacional, sesionará de manera ordinaria por solicitud de la secretaría al menos dos (02) veces al año, y de manera extraordinaria, cuando sea necesaria la revisión de temas relacionados con la seguridad de la información de la institución.

Los integrantes del Comité Técnico de Seguridad de la Información, deberán informar con anterioridad a la secretaría técnica la inasistencia a las sesiones, nombrando un delegado que lo represente.

Se podrá sesionar con la totalidad de los miembros principales o sus delegados, quienes tendrán voz y voto.

ARTÍCULO 47. COMITÉ INTERNO DE SEGURIDAD DE LA INFORMACIÓN. En cada unidad de la Policía Nacional, se implementará el comité interno de seguridad de la información; en el cual, se planea, orienta, gestionan los recursos, implementa y realiza seguimiento del SGSI, ejecutando actividades de sensibilización sobre las mejores prácticas, gestión de activos de información, gestión del riesgo y atención de los incidentes de seguridad de la información ocurridos a nivel interno, con el fin de aportar al fortalecimiento de la política de seguridad de la información.

a. Integrantes comité interno de seguridad de la información
b. Funciones del comité interno de seguridad de la información.
c. Secretaría del comité interno de seguridad de la información.
d. Sesiones del comité interno de seguridad de la información

ARTÍCULO 48. INTEGRANTES COMITÉ INTERNO DE SEGURIDAD DE LA INFORMACIÓN. El comité interno de seguridad de la información estará conformado así:

- **OFICINAS ASESORAS Y JEFATURAS:**

  - Jefe oficina o su delegado.
  - Asesor jurídico.
  - Jefe o responsable grupo Tecnologías de la Información y las Comunicaciones o quien haga sus veces.
  - Jefe o responsable de comunicaciones estratégicas o quien haga sus veces.
  - Jefe o responsable de gestión documental o quien haga sus veces.
  - Jefe o responsable de talento humano o quien haga sus veces.
  - Jefe o responsable de planeación o quien haga sus veces.
  - Jefe o responsable de atención al ciudadano o quien haga sus veces.
  - Jefe o responsable de seguridad física de instalaciones policiales o quien haga sus veces.
  - analista o administrador de seguridad de la información o quien haga sus veces.
  - Invitados.

PARÁGRAFO. Para la Oficina de Tecnologías de la Información y las Comunicaciones, también hará parte del comité, el jefe Grupo de Seguridad de la Información, especialista de seguridad de la Información y el especialista de atención de incidentes Informáticos.

- **DIRECCIONES Y ESCUELAS**

  - Director o subdirector.
  - Asesor jurídico.
  - Jefe grupo Tecnologías de la Información y las Comunicaciones o quien haga sus veces.
  - Jefe centro de protección de datos (donde se encuentre implementado).
  - Jefe grupo de comunicaciones estratégicas o quien haga sus veces.
  - Jefe grupo de gestión documental o quien haga sus veces.
  - Jefe grupo de talento humano o quien haga sus veces.
  - Jefe grupo de planeación o quien haga sus veces.
  - Jefe grupo de atención al ciudadano o quien haga sus veces.
  - Jefe grupo de seguridad física de instalaciones policiales o quien haga sus veces.
  - analista o administrador de seguridad de la información o quien haga sus veces.
  - Invitados.

- **DEPARTAMENTOS Y METROPOLITANAS**

  - Comandante o subcomandante.
  - Asesor jurídico
  - Responsable de atención al ciudadano o quien haga sus veces.
  - Responsable de comunicaciones estratégicas o quien haga sus veces.
  - Jefe grupo tecnologías de la información y las comunicaciones o quien haga sus veces.
  - Jefe grupo de talento humano o quien haga sus veces.
  - Jefe grupo de planeación o quien haga sus veces.
  - Jefe grupo de gestión documental o quien haga sus veces.
  - Jefe grupo de seguridad física de instalaciones policiales o quien haga sus veces.
  - Jefe seccional de inteligencia policial.
  - Jefe seccional de investigación judicial y criminal.
  - analista o administrador de seguridad de la información o quien haga sus veces.
  - Invitados.

ARTÍCULO 49. FUNCIONES DEL COMITÉ INTERNO DE SEGURIDAD DE LA INFORMACIÓN. El comité interno de seguridad de la información tendrá a cargo las siguientes funciones:

- Liderar y definir las actividades tendientes al fortalecimiento y mejora continua de la seguridad de la información en la unidad.
- Promover el cumplimiento de las políticas de seguridad de la información, definidas por la institución, por parte del personal de la unidad.
- Desplegar los lineamientos de seguridad de la información, definidas por el comité técnico de seguridad de la información de la Policía Nacional.
- Evaluar en la unidad los controles preventivos, definidos en el Manual del Sistema de Gestión de Seguridad de la Información de la institución para la Policía Nacional.
- Divulgar y realizar campañas pedagógicas a los funcionarios y contratistas de la unidad, sobre las mejores prácticas en la gestión de activos de información.
- Evaluar y dar trámite a las conductas contrarias que afectan la política de seguridad de la información de la Policía Nacional.
- Verificar y aprobar el inventario de los activos de información, realizado por el analista o administrador de seguridad de la información o quien haga sus veces.
- En las unidades que administren servicios tecnológicos, sistemas de información o centros de almacenamiento con niveles críticos y muy críticos que soportan la actividad del servicio de policía, se debe revisar y aprobar el plan de continuidad de la información.
- El comité deberá nombrar un promotor de seguridad de la información por área, grupo o dependencia, quien será el responsable de apoyar al administrador o analista de seguridad de la información o quien haga sus veces, para el cumplimiento de la Política de Seguridad de la Información en la unidad con el fin de lograr los objetivos establecidos en el presente manual.

ARTÍCULO 50. SECRETARÍA DEL COMITÉ INTERNO DE SEGURIDAD DE LA INFORMACIÓN: La secretaría del comité interno de seguridad de la información, estará a cargo del Grupo de Tecnologías de la Información y las Comunicaciones y desarrollarás las siguientes funciones:

- Resguardar la información producida por el Comité interno de seguridad de la información.
-
- Administrar la gestión documental del comité, mediante el manejo del archivo impreso, digital o electrónico.
- Consolidar la información y los temas a tratar en cada sesión del comité.
- Elaborar el registro documental de cada sesión realizada por el comité.
- Convocar las sesiones ordinarias y extraordinarias del Comité interno de seguridad de la información.

ARTÍCULO 51. SESIONES DEL COMITÉ INTERNO DE SEGURIDAD DE LA INFORMACIÓN. El comité interno de seguridad de la información sesionará de manera ordinaria cuatro (04) veces al año de forma trimestral, y de manera extraordinaria, cuando sea necesario la revisión de temas relacionados con la seguridad de la información de la unidad.

Los integrantes del comité interno de seguridad de la información, deberán informar con anterioridad la inasistencia a las sesiones, a la secretaría para consolidar la información, nombrando un delegado que lo represente.

Se podrá sesionar con la totalidad de los miembros principales o sus delegados, quienes tendrán voz y voto.

ARTÍCULO 52. OTRAS RESPONSABILIDADES. Los roles y responsabilidades de quienes deben apoyar el cumplimiento de la Política de Seguridad de la Información en la institución, los cuales son responsables de la implementación del Sistema de Gestión de Seguridad de la Información, verificando la efectividad y eficiencia del sistema, acorde con los objetivos de la Policía Nacional, tomando las acciones correctivas que hubiese lugar, serán los siguientes:

- **JEFATURAS, DIRECCIONES, OFICINAS ASESORAS, REGIONALES DE POLICÍA, ESCUELAS DE FORMACIÓN.** Cada unidad debe velar que se cuente con un funcionario nombrado en el cargo de administrador, analista de Seguridad de la Información, o asignadas sus funciones donde sea necesario, quien realizará revisión de forma aleatoria de los controles de seguridad de la información, con el propósito de verificar el cumplimiento a lo dispuesto en el presente manual. Los resultados encontrados deben ser presentados al comité interno de seguridad de la información.

- **OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.** Lidera el Sistema de Gestión de Seguridad de la Información, mediante el desarrollo del proceso de Direccionamiento Tecnológico, emitiendo lineamientos y realizando las coordinaciones necesarias que permitan la implementación de controles, que aseguren la disponibilidad, integridad y confidencialidad de la información de la Policía Nacional.

- **INSPECCIÓN GENERAL Y RESPONSABILIDAD PROFESIONAL.** Investiga las conductas contrarias que afectan el cumplimiento de la Política de Seguridad de la Información.

- **SECRETARÍA GENERAL.** Asesora en materia legal los aspectos pertinentes a seguridad de la información.

- **OFICINA DE CONTROL INTERNO**. Revisa y verifica el cumplimiento de la presente resolución, a través de las auditorías programadas a las unidades.

  PARÁGRAFO. Para las unidades que no estén certificadas en el Sistema de Gestión de Seguridad de Información, la Oficina de Control Interno o el dueño del proceso, revisará y verificará de forma aleatoria el cumplimiento de controles transversales, como:

  - Operaciones seguras.
  - Gestión de incidentes
  - Identificación de activos de información.
  - Identificación y autenticación de usuarios.
  - Clasificación de la información.
  - Retención y destrucción final de información.
  - Seguridad de la información en el desarrollo de software.
  - Seguridad de la información en la relación con terceros o proveedores.
  - Mantenimiento de los equipos.
  - Mensajería electrónica.
  - Sensibilización y concienciación a funcionarios y terceros
  - Controles contra códigos maliciosos.
  - Sincronización de relojes con la hora legal colombiana.

- **OFICINA DE COMUNICACIONES ESTRATÉGICAS.** Contribuye con la elaboración y difusión de piezas gráficas, que permitan fortalecer la toma de conciencia en la protección de los activos y seguridad de la información.

- **DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL.** Investiga los incidentes de seguridad de la información, que se sospechan constituyen un delito.

- **DUEÑO DEL ACTIVO DE INFORMACIÓN**. Parte designada en la institución, un cargo, proceso, área o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso estén identificados y valorados, que permitan definir periódicamente restricciones de acuerdo a su nivel de clasificación.

- **CUSTODIO DEL ACTIVO DE INFORMACIÓN.** Es una parte designada de Policía Nacional la cual puede ser un cargo, un proceso o un grupo de trabajo, quien se encuentra encargado de administrar y hacer efectivos los controles de seguridad que el propietario del activo haya

definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

- **FUNCIONARIOS.** Todo el personal que labora o realiza actividades para la Policía Nacional, son responsables por el cumplimiento de la presente resolución, preservar la confidencialidad, integridad y disponibilidad de los activos de información institucional, y es deber informar cualquier incidente de seguridad de la información que se tenga conocimiento.

ARTÍCULO 53. SEGREGACIÓN DE DEBERES. Se debe realizar una separación de responsabilidades, en aquellas áreas y grupos que pueden ser sensibles en el manejo de la información o que se hayan identificado como susceptibles a posibles casos de corrupción, realizando la separación de tareas entre distintos funcionarios, con el fin de reducir riesgos asociados a posibles fraudes, abusos de privilegios de acceso a la información, modificaciones no autorizadas, de forma no intencional o realizar un uso indebido de los activos de información.

ARTÍCULO 54. RESPONSABILIDADES DE LA DIRECCIÓN. La alta dirección debe demostrar el apoyo a la política de seguridad de la información institucional y los lineamientos específicos definidos para el aseguramiento de la disponibilidad, integridad y confidencialidad de los datos institucionales, cumpliendo y difundiendo los lineamientos y controles establecidos por la Policía Nacional.

ARTÍCULO 55. CONTACTO CON LAS AUTORIDADES. Las diferentes unidades de la Policía Nacional, deben realizar un inventario de las autoridades que permitan gestionar la seguridad de la información y la continuidad del negocio, o quienes puedan contribuir a la atención oportuna de incidentes de seguridad de la información que se identifiquen en la institución, el cual, deberá estar publicado y actualizado por el responsable de comunicaciones estratégicas, en el micrositio de cada unidad o el dispuesto para tal fin para conocimiento del personal.

ARTÍCULO 56. CONTACTO CON GRUPOS DE INTERÉS ESPECIAL. El Grupo Seguridad de la Información y Respuesta a Incidentes Informáticos - CSIRT, será el encargado de mantener las membrecías con grupos o foros de interés especial como un medio para:

- Obtener el conocimiento sobre las mejores prácticas y permanecer actualizado con la información sobre seguridad informática pertinente.

- Recibir advertencias tempranas de las alertas, avisos y actualizaciones, acerca de ataques y vulnerabilidades.

- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.

- Brindar los enlaces adecuados cuando se trata de incidentes, que afectan la seguridad de la información.

- Emitir los boletines informativos, con el fin de mantener al día a las partes interesadas sobre los incidentes de seguridad informática y, de esta manera, difundir las recomendaciones para adoptar las mejores prácticas y prevenir la recurrencia.

ARTÍCULO 57. INTELIGENCIA DE AMENAZAS. Se debe recopilar, analizar y utilizar la información relacionada con amenazas cibernéticas con el propósito de tomar decisiones informadas y proactivas que contribuyan al establecimiento de acciones que contribuyan a prevenir y responder ante ataques cibernéticos que puedan desencadenar afectaciones a la disponibilidad, integridad y confidencialidad de la información institucional.

ARTÍCULO 58. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS. La Policía Nacional busca proteger la información clasificada, reservada o con niveles de inteligencia garantizando que los proyectos se ejecuten de manera segura, cumpliendo la política general de seguridad de la información, los lineamientos específicos y los controles establecidos para asegurar la disponibilidad, integridad y confidencialidad de la información en las diferentes fases de los proyectos.

ARTÍCULO 59. INVENTARIO DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS. Para el manejo de los activos de información de la Policía Nacional, se debe realizar el inventario, clasificación y valoración de los mismos, conforme a los lineamientos establecidos por el Direccionamiento Tecnológico, los cuales se deben socializar ante el Comité interno de seguridad de la información el consolidado de los niveles de criticidad, como resultado de la valoración de los activos y se determinará las acciones que permitan disminuir el riesgo a los cuales se encuentran expuestos.

ARTÍCULO 60. DEVOLUCIÓN DE LOS ACTIVOS. Todos los funcionarios activos, personal no uniformado, contratistas o quienes hayan recibido activos de información institucionales para el cumplimiento de sus funciones, son responsables de la devolución de los mismos en el momento de registrar novedad administrativa temporal o definitiva en la institución; por lo tanto, deberán realizar la entrega mediante paz y salvo electrónico o la medida adoptada en la unidad para la entrega de los activos.

ARTÍCULO 61. ETIQUETADO DE LA INFORMACIÓN. Todos los documentos físicos y electrónicos de la Policía Nacional estarán etiquetados de acuerdo con la clasificación de la información siguiendo los lineamientos del proceso de Gestión Documental.

ARTÍCULO 62. SEGURIDAD Y RESTRICCIONES EN LA DIFUSIÓN DE PRODUCTOS E INFORMACIÓN DE INTELIGENCIA Y CONTRAINTELIGENCIA. Los organismos y dependencias de inteligencia y contrainteligencia, deberán indicar a los receptores autorizados por la ley, la reserva legal a la que está sometida la información y expresar al receptor autorizado de la misma, si se trata de un producto de inteligencia o contrainteligencia "de solo conocimiento" o "de uso exclusivo" teniendo como referencia las siguientes restricciones para cada caso, (Decreto 1070 de 2015 "Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa") así:

- **De solo conocimiento:** es aquel producto de inteligencia y contrainteligencia que tiene un receptor autorizado por ley, solo para conocimiento directo y, únicamente, como referencia o criterio orientador para tomar decisiones dentro de su órbita funcional. El receptor autorizado recibe el producto bajo las más estrictas medidas de seguridad, reserva legal y protocolos adecuados. El receptor autorizado no podrá difundir la información contenida en el producto de inteligencia y contrainteligencia.

- **De uso exclusivo:** es aquel producto de inteligencia y contrainteligencia que tiene un receptor autorizado por ley, solo para su conocimiento directo y uso exclusivo. Este producto solo podrá ser empleado como referencia para tomar decisiones dentro de su órbita funcional. El receptor autorizado recibe el producto bajo las más estrictas medidas de seguridad, reserva legal y protocolos adecuados. El receptor autorizado podrá difundir esta clase de información bajo su responsabilidad, únicamente, para establecer cursos de acción que permitan la toma de decisiones para el cumplimiento de los fines establecidos en la Constitución y la ley.

En ninguno de los anteriores casos, se podrá revelar fuentes, métodos, procedimientos, identidad de quienes desarrollan o desarrollaron actividades de inteligencia y contrainteligencia, o poner en peligro la seguridad y defensa nacional. Las autoridades competentes y los receptores de productos de inteligencia o contrainteligencia deberán garantizar, en todo momento, la reserva legal de la misma.

ARTÍCULO 63. GESTIÓN DE IDENTIDADES. A través de la Oficina de Tecnologías de la Información y las Comunicaciones, la Policía Nacional establecerá el lineamiento o procedimiento para la gestión de identidades (1DT-PR-0003) que permita el correcto funcionamiento de la plataforma tecnológica en producción y a los funcionarios asegurar el acceso adecuado a los recursos y sistemas de información.

ARTÍCULO 64. INFORMACIÓN DE AUTENTICACIÓN. Se debe establecer mecanismos y procedimientos para realizar la verificación de la identidad de los usuarios que utilizan los recursos tecnológicos dispuestos para la gestión institucional, con el propósito de asegurar que solo personas autorizadas puedan acceder a la gestión de los activos de información, por lo tanto, la Oficina de Tecnologías de la Información y las Comunicaciones establece el Sistema de Identificación Policial Digital - IPD, en donde se cumple con los siguientes controles:

- Permitir que los usuarios seleccionen y cambien sus propias contraseñas.
- Exigir que se escojan contraseñas de calidad.
- Forzar a los usuarios, a cambiar sus contraseñas cuando ingresan por primera vez.
- Llevar un registro de las contraseñas usadas previamente, e impedir su reutilización.
- No permitir visualizar contraseñas en la pantalla cuando se está ingresando.
- Almacenar y transmitir las contraseñas en forma segura.

La información de autenticación asociada a las identidades no humanas, debe estar asignado a un funcionario responsable, el cual debe informar los cambios en caso de presentarse para la reasignación de las responsabilidades asociadas en el uso adecuado acorde a la información a la cual tenga acceso y gestión.

ARTÍCULO 65. DERECHOS DE ACCESO. La gestión adecuada de los derechos de acceso permite proteger la información institucional, garantizando el cumplimiento de lineamientos establecidos para mitigar riesgos asociados a afectación de integridad y confidencialidad de los datos; por lo tanto, la asignación y revocación de derechos de acceso a los usuarios, se realiza de acuerdo con el procedimiento o lineamiento dispuesto para la gestión de identidades (1DT-PR-0003) y el lineamiento específico de control de acceso.

Todos los servidores públicos o terceros, que tienen un usuario en la plataforma tecnológica de la Policía Nacional, deben conocer y cumplir los términos de uso del mismo, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado; así como, las políticas de protección para usuario desatendido, escritorio y pantalla limpia.

PARÁGRAFO 1. Para la creación de usuarios de bases de datos, estos deberán ser sometidos a la aprobación del comité asesor de gestión del cambio de la Oficina de Tecnologías de la Información y las Comunicaciones, estableciendo el alcance de permisos, derechos de acceso o privilegios de sistema o de objeto. Una vez aprobado, el funcionario deberá solicitar la creación y asignación de usuario mediante el Sistema de Gestión de Requerimientos en TIC o el dispuesto para tal fin, con visto bueno del jefe inmediato.

Cada usuario tendrá una vigencia de 180 días a partir de su creación, habilitación o renovación, o cuando se presente novedad administrativa del responsable por vacaciones, retiro, traslado, licencia y demás novedades. El trámite de asignación de usuario de base de datos, lo debe realizar el funcionario que asume la responsabilidad del mismo, solicitando la asignación del usuario mediante diligenciamiento del formato asignación de usuario y términos de uso, el cual se encuentra inmerso digitalmente en el Sistema de Gestión de Requerimientos en TIC o el sistema de información dispuesto para tal fin.

PARÁGRAFO 2. La cancelación de registro de usuarios, se realiza una vez es registrada novedad administrativa en el Sistema de Información para la Administración del talento humano o el que haga sus veces, por lo que, el usuario solo tendrá acceso a los sistemas de información para la administración de beneficios de los funcionarios de la Policía Nacional como Portal de Servicios Internos (modo consulta) – PSI, plataforma tecnológica institucional educativa, sistemas de información de bienestar social, Portal de Servicios de Salud y demás la alta dirección defina.

PARÁGRAFO 3. Los derechos de acceso a sistemas biométricos o sistemas que no consumen las novedades administrativas registradas en el Sistema de Sistema de Información para la administración del talento Humano, deben revisarse de forma mensual por parte del Grupo de Tecnologías de la Información y Comunicaciones de la unidad o quien haga sus veces, el responsable de personal en los grupos de talento humano y responsable de seguridad física, con el fin de adelantar las acciones administrativas que permitan la desactivación de los accesos autorizados durante la vigencia de la novedad administrativa.

ARTÍCULO 66. SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON PROVEEDORES. La Policía Nacional establece los mecanismos de control en sus relaciones con personal externo que le provean bienes o servicios. Los funcionarios responsables de la realización o quienes

realizan la firma de contratos, acuerdos o convenios con personal externo deben garantizar el cumplimiento del Manual de Seguridad de la Información por parte de estos.

Para lo cual se definen las siguientes directrices:

- Todos los contratos deben tener claramente definidos los acuerdos de niveles de servicios y ser contemplados como un numeral de las especificaciones técnicas.

- Diligenciar y firmar el formato declaración de confidencialidad y compromiso con la seguridad de la información contratistas o terceros y acuerdo para la revelación de información clasificada o reservada o los que hagan sus veces, cuando se requiere la entrega de información con niveles de clasificación.

- De acuerdo al objeto del contrato y al acceso a la información por parte del personal externo, estos deben someterse a un estudio de confiabilidad y de ser necesario estudio de credibilidad y confianza.

- Antes de permitir el acceso o la entrega de información a un tercero, se debe realizar una evaluación del riesgo, por parte del propietario del activo de información, con el fin de establecer la viabilidad de permitir el acceso a la información, para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

ARTÍCULO 67. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA CADENA DE SUMINISTRO DE LA TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES (TIC). Los proveedores, socios y subcontratistas que participan en la provisión, desarrollo, mantenimiento y soporte de los sistemas y servicios de Tecnologías de la Información y las Comunicaciones que soportan la plataforma tecnológica institucional, deben cumplir los lineamientos específicos de seguridad de la información y controles definidos para asegurar los estándares de seguridad necesarios para proteger la información y los sistemas críticos de la Policía Nacional.

Cada vez que la Policía Nacional planee, desarrolle, ejecute e implemente nuevos proyectos de adquisición o mejora de recursos tecnológicos, físicos o de cualquier índole, hace el estudio de conveniencia y oportunidad, en el cual deberá considerar la inclusión de cláusulas de firma de acuerdos de confidencialidad y estudios de confiabilidad, incluyendo:

- Requisitos de seguridad de la información para aplicar a la adquisición de productos o servicios de tecnologías de la información y de comunicaciones.

- Exigir que los proveedores no divulguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro.

- Implementar un proceso de seguimiento y métodos aceptables, para validar que los productos y servicios de tecnología de información y comunicación cumplan los requisitos establecidos.

- Obtener la seguridad que los componentes críticos y su origen se pueden rastrear a todo lo largo de la cadena de suministro.

Se debe tener en cuenta que, para la adquisición de cualquier elemento, bien o servicio orientado a fortalecer los componentes tecnológicos, se debe acordar que la utilización de infraestructura, información suministrada o facilitada por la Policía Nacional, será mantenida en estricta confidencialidad, y solo podrá ser revelada a quienes estén autorizados, en forma previa por la entidad, aplicando principios de confidencialidad, integridad y duración.

En caso de adquirir software comercial, se deben aplicar los siguientes aspectos:

- La licencia de funcionamiento será de cubrimiento nacional, ya que generalmente se accederá al sistema de información en todas las unidades de policía.

- Dada la diversidad de las soluciones que se implementarán, si en alguna de ellas se requiere la incorporación de software, base adicional para la construcción o mantenimiento de las aplicaciones, estas deberán ser entregadas a la Policía Nacional, de propiedad a perpetuidad (en caso de que aplique).

- El licenciamiento será a perpetuidad y el mantenimiento por espacio de al menos un (1) año contado a partir de la entrega a satisfacción de la solución.

- El licenciamiento de uso correspondiente será propiedad de la Policía Nacional.

Los paquetes propietarios deben ser entregados a la institución en código fuentes, con el fin de validar que no contengan scripts maliciosos[27] o no acorde a las necesidades de la Policía Nacional.

La adquisición de nuevos recursos y servicios tecnológicos de información y comunicaciones, así como software y hardware asociado, serán autorizados únicamente por la Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional.

ARTÍCULO 68. SEGUIMIENTO, REVISIÓN Y GESTIÓN DEL CAMBIO DE LOS SERVICIOS DE LOS PROVEEDORES. Los supervisores de contratos o convenios con la Policía Nacional, deben realizar revisión y seguimiento a los servicios de los proveedores dejando documentado de forma periódica el cumplimiento de los requisitos establecidos en los procesos contractuales, con el propósito de minimizar los riesgos y permitir el aseguramiento de la continuidad operativa y la seguridad de la información.

ARTÍCULO 69. EVALUACIÓN Y DECISIÓN SOBRE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN. La Policía Nacional cuenta con el procedimiento de gestión de incidentes de seguridad de la información (1DT-PR-0004), en el cual se establecen los pasos a seguir frente a la atención de eventos de seguridad de la información, los cuales deben ser consolidados por el Grupo de Seguridad de la Información y Respuesta a Incidentes Informáticos - CSIRT, con el propósito de realizar la identificación de las lecciones aprendidas para la mejora continua y la gestión de riesgos del Sistema de Gestión de Seguridad de la Información de la Policía Nacional.

ARTÍCULO 70. RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. Se debe contar con un procedimiento de gestión de incidentes de seguridad de la información (1DT-PR-0004),, en el cual se establecen los niveles de criticidad y se dejen documentadas las lecciones aprendidas frente a los mismos, con el fin de ser tenidos en cuenta en la toma de decisiones y mejora continua del Sistema de Gestión de Seguridad de la Información

ARTÍCULO 71. APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. Con el propósito de realizar mejora continua al Sistema de Gestión de Seguridad de la Información, las lecciones aprendidas de los incidentes de seguridad de la información, deben ser tenidos en cuenta en la gestión de riesgos de seguridad de la información en cada vigencia, con el fin de fortalecer los controles establecidos por la institución y disminuir la probabilidad de ocurrencia de las mismas causas en la plataforma tecnológica institucional en producción.

ARTÍCULO 72. RECOPILACIÓN DE EVIDENCIAS. En el momento que sea identificado un incidente de seguridad de la información, se debe asegurar que la información relevante se recoja de manera precisa, íntegra y legalmente admisible para que pueda ser utilizada en investigaciones internas, auditorías, o procedimientos legales; en caso de que el incidente requiera de la intervención de organismos judiciales, se debe realizar las coordinaciones correspondientes para que se recopilen las evidencias relevantes y proteja la cadena de custodia que se requiera ante una actividad catalogada como delito.

ARTÍCULO 73. SEGURIDAD DE LA INFORMACIÓN ANTE UNA INTERRUPCIÓN. La Oficina de Tecnologías de la Información y las Comunicaciones, y las unidades que gestionan Sistemas de información y componentes esenciales para la gestión institucional, deberán realizar la identificación de los requisitos de seguridad de la información, los cuales deben ser incorporados en la actualización del plan de continuidad tecnológica, con el propósito de ser tenido en cuenta durante un evento disruptivo ante una posible afectación de los activos de información.

ARTÍCULO 74. REQUISITOS LEGALES, REGLAMENTARIOS Y CONTRACTUALES. Las unidades de policía deberán realizar la identificación de los requisitos legales, reglamentario y

[27] Scripts maliciosos: fragmentos de código diseñados para ejecutar acciones dañinas en un sistema informático. (Microsoft,2024)

contractuales relacionados con el Sistema de Gestión de Seguridad de la Información de acuerdo a su contexto organizacional, realizando la documentación, manteniendo un registro actualizado que permita mitigar posibles riesgos legales y regulatorios.

La Oficina de Control Interno dentro del plan anual de auditorías, deberá realizar la revisión del cumplimiento de la Política de Seguridad de la Información definida en el presente manual, buscando el mejoramiento continuo del sistema; cada unidad velará por el cumplimiento de la Política de Seguridad de la Información, mediante la aplicación de las buenas prácticas, que servirán para el fortalecimiento de los procesos en cada una de las áreas o grupos que conformen la unidad.

ARTÍCULO 75. DERECHOS DE PROPIEDAD INTELECTUAL. La violación de los derechos de autor, puede conducir a la institución a acciones administrativas, que pueden involucrar multas y procesos legales y contractuales, razón por la cual, todo software utilizado en la Policía Nacional debe contar con su licenciamiento de carácter corporativo; el uso de software libre[28], debe tener el concepto de seguridad y autorización por parte de la Oficina de Tecnologías de la Información y las Comunicaciones.

No está permitido el almacenamiento, distribución de material gráfico o video, diferente al producido por la institución, o que no se puede demostrar los derechos sobre estos medios, razón por la cual, está prohibido el almacenamiento de contenido de video y música en los equipos de cómputo, servidor de archivos o servicios en la nube adquiridos por la Oficina de Tecnologías de la Información y las Comunicaciones, para apoyar la gestión institucional.

El personal técnico adscrito a los grupos o responsables de Tecnologías de la Información y las Comunicaciones a nivel país, realizarán listas de chequeo con el fin de efectuar los ajustes pertinentes para el cumplimiento de la política o para la instalación de software adquirido por la Policía Nacional en la plataforma tecnológica institucional en producción.

ARTÍCULO 76. PROTECCIÓN DE REGISTROS. Los registros de la Policía Nacional se deben proteger contra pérdida o destrucción, estos se deben clasificar según las tablas de retención documental y su tiempo de almacenamiento se realizará de acuerdo a las condiciones específicas y disponibilidad técnica de conservación de cada sistema, que permita cumplir requisitos legales, normativos o respaldar actividades esenciales de la institución, además se debe tener en cuenta las siguientes consideraciones:

- Las claves criptográficas asociadas con archivos cifrados, se mantienen en forma segura y están disponibles para su uso por parte de personas autorizadas cuando resulte necesario.

- Al seleccionar medios de almacenamiento electrónico, se incluyen en los procedimientos para garantizar la capacidad de acceso a los datos durante el periodo de retención, con el fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

- Los sistemas de almacenamiento de datos son seleccionados de modo tal, que los datos requeridos puedan recuperarse, resultando aceptable en formato y plazo para cualquier entidad que los requiera.

- El sistema de almacenamiento y manipulación garantizará una clara clasificación de los registros y de su periodo de retención legal o normativa. Así mismo, se permite una adecuada destrucción de los registros una vez transcurrido dicho periodo, si ya no resultan necesarios para la Policía Nacional.

ARTÍCULO 77. PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN DE IDENTIFICACIÓN PERSONAL. El tratamiento de los datos personales en la Policía Nacional, se adelantarán en el marco de las leyes estatutarias dispuestas sobre la materia, y en cumplimiento de la política, legislación y reglamentación pertinente con una estructura y control de gestión dando aplicabilidad a la Política de Tratamiento de Datos Personales de la Policía Nacional.

[28] *Software* libre: tipo de software que otorga a los usuarios la libertad de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Es una filosofía que promueve la colaboración y el acceso abierto al código fuente. (Microsoft,2024)

PARÁGRAFO. La Secretaría General asesorará y apoyará a las unidades que dentro de su proceso administren y den manejo de información personal en los sistemas de información, quienes deberán implementar en los mismos la Política de Tratamiento de Datos Personales que debe ser aceptada por el ciudadano o funcionario policial.

ARTÍCULO 78. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN. Con el propósito de evaluar y asegurar que las políticas, lineamientos, y controles de seguridad adoptados por la Policía Nacional, sean eficaces y estén alineados con las mejores prácticas y normativas aplicables, de forma anual se realizarán las coordinaciones para la realización de revisiones, auditorías o asesorías al Sistema de Gestión de Seguridad de la Información, por parte de la Oficina de Control Interno - OCINT o entidad de tercera parte que la institución determine.

ARTÍCULO 79. CUMPLIMIENTO DE POLÍTICAS, REGLAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN. La Policía Nacional asegura que los controles y procesos establecidos para proteger los activos de información sean efectivos y con el fin que la institución opere dentro de los marcos normativos y regulatorios aplicables, se realiza de forma anual la revisión de la política, lineamientos específicos y documentos asociados al Sistema de Gestión de Seguridad de la Información.

ARTÍCULO 80. PROCEDIMIENTOS OPERATIVOS DOCUMENTADOS. Las actividades, procedimientos, responsabilidades, revisión y actualizaciones asociadas al Sistema de Gestión de Seguridad de la Información de la Policía Nacional se deben documentar, clasificar y etiquetar de acuerdo a las tablas de retención documental establecidas, las cuales harán parte del archivo de gestión de la unidad para futuras revisiones de cumplimiento.

ARTÍCULO 81. CONTROLES DE PERSONAS. Corresponde a aquellos controles que contribuyen a asegurar que las personas que interactúan con los activos de información, comprendan, respeten y apliquen los principios, lineamientos establecidos por la institución, minimizando los riesgos asociados al factor humano, en los cuales se establecen los siguientes:

1. Selección.
2. Términos y condiciones del empleo.
3. Conciencia de seguridad de la información, educación y formación.
4. Responsabilidades después de la terminación o cambio de empleo.
5. Informes de eventos de seguridad de la información.

ARTÍCULO 82. SELECCIÓN. El procedimiento para confirmar la veracidad de la información suministrada, por el personal que se postula como candidato a ingresar a la Policía Nacional, se realiza acorde con lo establecido por el proceso de Direccionamiento del Talento Humano a través de la Dirección de Incorporación.

ARTÍCULO 83. TÉRMINOS Y CONDICIONES DEL EMPLEO. Todos los funcionarios activos y quienes le presten un servicio a la Policía Nacional, deben diligenciar el formato declaración de confidencialidad y compromiso con la seguridad de la información servidor público, de forma digital mediante el Portal de Servicios Internos – PSI, el cual, se deberá renovar cada vez que se presente un ascenso, traslado y cuando se generen cambios o actualizaciones.

El personal externo o contratista, diligenciará el formato declaración de confidencialidad y compromiso con la seguridad de la información contratistas o terceros, en forma física y este hará parte integral del contrato o acuerdo de cooperación que debe reposar junto con las hojas de vida en las carpetas de seguimiento del proceso contractual.

PARÁGRAFO. Los funcionarios que sean vinculados a unidades policiales que ejerzan funciones de inteligencia y contrainteligencia deberán suscribir acta de compromiso de reserva de conformidad con el artículo 33 de la Ley Estatutaria 1621 del 17 de abril de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

ARTÍCULO 84. CONCIENCIA DE SEGURIDAD DE LA INFORMACIÓN, EDUCACIÓN Y FORMACIÓN. La Policía Nacional genera las necesidades asociadas al fortalecimiento de la toma de conciencia en temas relacionados con el Sistema de Gestión de la Seguridad de la Información, y a través de la Dirección de Educación Policial, se desarrollan programas complementarios para fortalecer las competencias de seguridad de la información de los funcionarios, y en coordinación de la Oficina de Comunicaciones Estratégicas y los Grupos de Tecnologías de la Información y las Comunicaciones, se desplegarán planes de sensibilización.

El plan de sensibilización se revisará, definirá y ejecutará de acuerdo con las necesidades y en coordinación con los demás sistemas de gestión de la institución. Estas actividades de definición, estarán coordinadas entre el Grupo Seguridad de la Información y Respuesta a Incidentes Informáticos - CSIRT, de la Oficina de Tecnologías de la Información y las Comunicaciones, en conjunto con las áreas encargadas de la generación de competencias en el talento humano, manejo de la cultura y la gestión del cambio organizacional.

Dentro de las actividades de sensibilización se deberán tener en cuenta temas relacionados con:

- Normatividad, incluyendo la Política de Seguridad de la Información de la institución.
- Socialización de los objetivos de la Política de Seguridad de la información.
- La importancia y los beneficios del Sistema de Gestión de Seguridad de la Información.
- El aporte de cada uno de los funcionarios al sistema desde su cargo, rol o función.
- Las implicaciones de la no conformidad con los controles establecidos para la protección de los activos de información de la Policía Nacional.

ARTÍCULO 85. RESPONSABILIDADES DESPUÉS DE LA TERMINACIÓN O CAMBIO DE EMPLEO. Se deben implementar acciones que permitan realizar el bloqueo de los accesos en los recursos tecnológicos y sistemas de información asignados para desempeñar funciones administrativas u operativas, y controles de acceso físico a las instalaciones institucionales una vez se haya terminado la relación laboral con la institución.

PARÁGRAFO. En caso de que por fuerza mayor un funcionario no pueda hacer entrega formal del cargo y los activos de información que gestiona, el jefe inmediato deberá solicitar al Grupo de Tecnologías de la Información y Comunicaciones o dueño del activo de información, mediante el Sistema de Gestión de Requerimientos en TIC o el dispuesto para tal fin, el acceso y traspaso al funcionario designado para continuar con dichas funciones.

ARTÍCULO 86. INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Es responsabilidad de todos los usuarios de los servicios de tecnologías de la información y comunicaciones de la Policía Nacional, informar a través de los Grupos de Tecnologías de la Información y Comunicaciones de las unidades o los canales habilitados como el Sistema de Información para la Gestión de Incidentes en TIC o el que haga sus veces, correo electrónico ponal.csirt@policia.gov.co, cuando se evidencie una debilidad en los controles u ocurra una afectación de la disponibilidad, integridad y confidencialidad de la información o a través del o los dispuestos para la atención de peticiones quejas reclamos, reconocimiento y sugerencias en caso de que se desee realizar de forma anónima.

ARTÍCULO 87. CONTROLES FÍSICOS. Con el propósito de proteger los activos de información, en donde se encuentren equipos, infraestructura y documentos, contra amenazas físicas como accesos no autorizados, daños, robos o desastres, que contribuyan a garantizar la disponibilidad, integridad y confidencialidad de la información, en los cuales se han definido los siguientes:

1. Perímetro de seguridad física.
2. Entrada física
3. Asegurar oficinas e instalaciones.
4. Monitoreo de la seguridad física

5. Protección contra amenazas físicas y ambientales.
6. Trabajar en áreas seguras.
7. Emplazamiento y protección de equipos.
8. Seguridad de los activos fuera de las instalaciones.
9. Servicios públicos de apoyo
10. Seguridad en el cableado.
11. Mantenimiento de equipos.
12. Disposición segura o reutilización de equipos.

ARTÍCULO 88. PERÍMETRO DE SEGURIDAD FÍSICA. La Policía Nacional realiza el mayor esfuerzo en implementar y garantizar la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro en todas las unidades policiales, así como en entornos abiertos, controlando las amenazas físicas externas e internas y las condiciones medioambientales de sus instalaciones mediante una adecuada gestión de riesgos, teniendo en cuenta los lineamientos definidos en el manual de seguridad física de instalaciones Policiales y demás lineamientos establecidos por el responsable de las actividades relacionadas con la seguridad física a instalaciones, dentro del cual por parte de los Grupos de Tecnologías de la Información y las Comunicaciones, deben realizar la identificación de las zonas de procesamiento de información clasificada, reservada o con niveles de inteligencia y contrainteligencia con el propósito de evaluar junto con el Comité interno de seguridad de la información los controles implementados o si es necesario reforzarlos para asegurar la disponibilidad, integridad y confidencialidad de la información institucional.

ARTÍCULO 89. ENTRADA FÍSICA. Las zonas de procesamiento de información clasificada, reservada o con niveles de inteligencia y contrainteligencia, deben estar protegidas por controles de acceso de entrada, y a través del Comité interno de seguridad de la información se evaluará la implementación de controles adicionales que permitan asegurar la disponibilidad, integridad y confidencialidad de la información allí gestionada.

ARTÍCULO 90. ASEGURAR OFICINAS E INSTALACIONES. En las unidades de policía se realiza la identificación de las zonas de procesamiento de información clasificada o reservada, en donde de acuerdo a las capacidades se deben establecer controles de acceso que permitan asegurar la confidencialidad, integridad y disponibilidad en las oficinas, habitaciones o instalaciones policiales.

ARTÍCULO 91. MONITOREO DE LA SEGURIDAD FÍSICA. La Policía Nacional cuenta con el manual de seguridad física de instalaciones policiales, por lo tanto, las unidades deben realizar la optimización de medidas de protección con unos mínimos de protección que permita asegurar la institución, y de acuerdo a esto se contribuye a la protección de los activos de información.

ARTÍCULO 92. PROTECCIÓN CONTRA AMENAZAS FÍSICAS Y AMBIENTALES. Se deben implementar controles que permitan fortalecer las amenazas físicas y ambientales, las cuales para las unidades que cuentan con un Sistema de Gestión de Seguridad de la Información certificable, deben tener en cuenta para el establecimiento del plan de continuidad tecnológica de los servicios puestos en producción en la plataforma tecnológica.

ARTÍCULO 93. TRABAJAR EN ÁREAS SEGURAS. Las áreas seguras de las unidades de policía deber ser identificadas y socializadas ante el Comité de Seguridad de la Información, tomando como referencia la protección de activos de información críticos, como pueden ser las unidades de procesamiento donde se alojen servidores, almacenamiento, equipos activos de red y donde se maneje información clasificada o reservada para la institución; por lo tanto, se deben establecer controles que permitan mitigar posibles riesgos de afectación a la disponibilidad, integridad y confidencialidad de estos activos de información de la unidad.

ARTÍCULO 94. EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS. Los equipos de cómputo deben ser ubicados y protegidos para reducir la exposición a riesgos ocasionados por amenazas ambientales y oportunidades de acceso no autorizado, adoptando las siguientes directrices, así:

- Los centros de procesamiento y almacenamiento institucionales propenden por el cumplimiento de la norma internacional ANSI/TIA 942.

- Los equipos de cómputo tipo servidor de cada unidad deben estar agrupados en un solo lugar. Estos lugares deben contar con controles estrictos de accesos físicos.

- Los equipos de cómputo, se ubican de tal manera que se reduzca el riesgo de visualización de la información procesada, por parte de personas no autorizadas.

- El acceso a los centros de procesamiento y almacenamiento está restringido y su ingreso debe estar documentado dejando la trazabilidad correspondiente.

- En los centros de datos se deben implementar controles ambientales con el fin de minimizar la materialización de riesgos asociados a la pérdida de información.

ARTÍCULO 95. SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES. El uso de equipos institucionales para uso fuera de las instalaciones policiales, está restringido a equipos portátiles y aquellos que apoyan el trabajo móvil[29]. Por lo tanto, la seguridad para estos equipos es equivalente a la suministrada a los recursos tecnológicos, ubicados dentro de las unidades de policía, aplicando controles adicionales que contribuyan a mitigar los riesgos que, por sí mismo conlleva el uso de estos equipos fuera las instalaciones, así:

- Los equipos institucionales fuera de las instalaciones policiales deben contar con un ingreso seguro[30] (usuario y contraseña).

- Los usuarios administradores, están restringidos únicamente a los encargados de realizar mantenimiento de estos, en los Grupos de Tecnologías de la Información y Comunicaciones.

- El usuario final, no debe tener privilegios de administración[31] que permita la instalación de software no autorizado.

- El software instalado en los equipos institucionales de uso externo, debe estar licenciado y avalado por la Oficina de Tecnologías de la Información y las Comunicaciones.

- Los equipos de cómputo portátiles deben tener controles criptográficos (discos e información cifrada) con el fin de proteger la información que allí se almacena.

- La información institucional gestionada en dispositivos móviles, debe ser eliminada una vez haya cumplido su finalidad o ciclo de vida.

- La información física clasificada o reservada, debe ser transportada en sobre sellado, que permita tener trazabilidad del documento.

- No está permitido el retiro de los equipos de cómputo tipo escritorio de las instalaciones policiales.

ARTÍCULO 96. SERVICIOS PÚBLICOS DE APOYO. Las unidades que soportan sistemas de información, aplicaciones y componentes críticos de la plataforma tecnológica institucional en producción, deben asegurar que se cuente con protección ante interrupciones causadas por fallos en los servicios públicos de apoyo.

[29] Trabajo móvil: modalidad laboral que permite a los funcionarios realizar sus tareas desde cualquier lugar utilizando dispositivos móviles y tecnología de comunicación. (Microsoft,2024)
[30] Ingreso seguro: prácticas y tecnologías que aseguran que solo usuarios autorizados puedan acceder a sistemas y datos sensibles. (Microsoft,2024)
[31] Privilegios de administración: permisos y derechos que se otorgan a los usuarios para realizar tareas específicas en un sistema informático o red. (Microsoft,2024)

ARTÍCULO 97. SEGURIDAD EN EL CABLEADO. Para el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a las instalaciones de procesamiento de información, con el fin de protegerlos contra intercepción o daño, se debe cumplir con:

- El reglamento técnico de instalaciones eléctricas – RETIE, expedido por el Ministerio de Minas y Energía.
- Los estándares ISO/IEC/11801, ANSI/EIA/TIA 568A o 568B o con la reglamentación vigente expedida al respecto.
- Las instalaciones de cableado estructurado están protegidas contra la influencia o daño causado por agentes externos.
- Los elementos metálicos que forman parte de los cableados estructurados están conectados al sistema de tierras del edificio.
- Los equipos se deben almacenar en sitios acondicionados a temperaturas entre 16 y 22 grados centígrados.
- Los centros de cableado cuentan con rack[32] para alojar los equipos y terminaciones de los cableados cumpliendo las normas técnicas y asegurados con chapas o cerraduras de seguridad, cuyas llaves sean administradas por personal técnico capacitado.
- Las instalaciones de cableado se deben realizar siguiendo la arquitectura de los edificios, debidamente protegidos con canaleta en caso de realizarlas al interior, o con tubo metálico en caso de instalación tipo intemperie.

ARTÍCULO 98. MANTENIMIENTO DE EQUIPOS. El mantenimiento a la plataforma tecnológica posibilita su disponibilidad, integridad y confidencialidad, teniendo en cuenta controles que permitan asegurar el mantenimiento preventivo de acuerdo con los intervalos de servicio y especificaciones recomendadas por el fabricante, en donde solo el personal de mantenimiento autorizado puede llevar a cabo reparaciones en los equipos.

ARTÍCULO 99. DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS. Cuando un equipo de cómputo se encuentra en óptimas condiciones y pueda ser asignado a otro funcionario, se debe realizar borrado seguro de la información. En el momento en que los dispositivos cumplen el ciclo vida y se va a realizar la disposición final, se efectúa la destrucción física del dispositivo de almacenamiento, cumpliendo las acciones descritas en el procedimiento o lineamiento emitido para el borrado seguro de la información (1DT-PR-0020).

ARTÍCULO 100. CONTROLES TECNOLÓGICOS. Permiten implementar herramientas y soluciones tecnológicas que protejan los sistemas de información, redes, aplicaciones y datos frente a amenazas cibernéticas, accesos no autorizados, alteraciones y pérdidas, contribuyendo a garantizar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, se definen los siguientes relacionados con:

1. Dispositivos de punto final de usuario.
2. Derecho de acceso privilegiado
3. Restricción de acceso a información.
4. Acceso al código fuente.
5. Autenticación segura.
6. Gestión de la capacidad.
7. Protección contra malware.
8. Gestión de la configuración.
9. Enmascaramiento de datos.
10. Prevención de fuga de datos.

[32] Rack: estructura diseñada para montar equipos electrónicos, como servidores, unidades de almacenamiento, conmutadores de red (switches) y otros dispositivos de hardware. (Microsoft,2024)

11. Redundancia de las instalaciones de procesamiento de información
12. Registro de eventos.
13. Actividades de seguimiento.
14. Sincronización de relojes.
15. Uso de programas de utilidad privilegiados.
16. Instalación de software en sistemas operativos.
17. Segregación de redes.
18. Seguridad de los servicios de red.
19. Filtrado web.
20. Requisitos de seguridad en las aplicaciones.
21. Arquitectura de sistemas seguros y principios de ingeniería.
22. Codificación segura.
23. Pruebas de seguridad en el desarrollo y aceptación.
24. Desarrollo externalizado.
25. Separación de entornos de desarrollo, evidencias y producción
26. Gestión del cambio.
27. Información de pruebas.
28. Protección de los sistemas de información durante las pruebas de auditoría.
29. Mensajes electrónicos.

ARTÍCULO 101. DISPOSITIVOS DE PUNTO FINAL DE USUARIO. La Policía Nacional cuenta con herramientas de seguridad perimetral y seguridad de puntos finales, cuyo objetivo es el de proteger cualquier dispositivo que se conecta a la red desde fuera o dentro del firewall[33], como lo son computadores portátiles, computadores de escritorio, tabletas, impresoras y otros dispositivos, con el fin que no sean explotados por ataques maliciosos de piratas informáticos y otras amenazas cibernéticas, por lo tanto, los equipos de cómputo deben contar con los controles necesarios para poder acceder a los servicios de internet, como productos de seguridad adquiridos por la institución, para asegurar los servicios de la plataforma tecnológica institucional.

ARTÍCULO 102. DERECHO DE ACCESO PRIVILEGIADO. Los usuarios con acceso privilegiado[34], corresponden a aquellos que poseen permisos extendidos para acceder, administrar o modificar sistemas, aplicaciones y datos clasificados, reservados o recursos protegidos por la institución.

Una vez asignados estos usuarios, deben cumplir con el procedimiento o lineamiento emitido para la protección de contraseña de usuarios con altos privilegios (1DT-PR-0002), con el fin de usarlas en caso de gestión funcional del componente tecnológico requerida con el usuario de altos privilegios conservando los adecuados niveles de autorización, entregar a un funcionario del mismo grupo donde ocurrió la novedad, la clave de acceso al sistema de información y esquema de base de datos, para subsanar el requerimiento, mientras se realiza la asignación formal del usuario.

ARTÍCULO 103. RESTRICCIÓN DE ACCESO A INFORMACIÓN. El acceso a la información gestionada mediante la plataforma tecnológica de la Policía Nacional, está dado de acuerdo a los niveles de clasificación de la información y los roles de acceso asignados para el cumplimiento de las funciones asignadas al cargo.

Así mismo, se asignan perfiles de navegación y accesos a controles de dispositivos de acuerdo a los lineamentos emitidos por la Oficina de Tecnologías de la Información y las Comunicaciones, para asegurar el acceso a la información.

ARTÍCULO 104. ACCESO AL CÓDIGO FUENTE. Se debe controlar el acceso al código fuente[35] de las aplicaciones, lo que permite disminuir el riesgo de modificaciones no autorizadas o malas

[33] Firewall: Herramienta tecnológica diseñada para monitorear y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas, el cual actúa como una barrera protectora entre una red interna segura y las amenazas externas potencialmente dañinas, como internet. (Microsoft,2024)

[34] Usuarios con acceso privilegiado: identidades que tienen permisos y derechos especiales para realizar tareas críticas en un sistema informático los cuales desempeñan funciones de administración y mantenimiento de la infraestructura de tecnologías de la información y las comunicaciones. (Microsoft,2024)

[35] Código fuente: conjunto de instrucciones y declaraciones escritas en un lenguaje de programación que definen el comportamiento y las funcionalidades de un software o aplicación. (Microsoft,2024)

prácticas en el desarrollo del software, protegiendo la información que se gestiona mediante los diferentes sistemas de información y aplicaciones producidas, adquiridas y autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones, por lo tanto a través del Comité Asesor de Gestión del Cambio, se debe analizar las modificaciones y adiciones de los sistemas de información, de ser necesario también las publicaciones de estos, una vez ha cumplido con los requisitos necesarios para asegurar su disponibilidad, integridad y confidencialidad.

ARTÍCULO 105. AUTENTICACIÓN SEGURA. Es responsabilidad del usuario final, hacer correcto uso de la autenticación secreta para acceder a los recursos tecnológicos. En atención a esto, no se deben escribir en documentos que estén a la vista de los demás; al momento de realizar la asignación de usuario el funcionario diligencia el formato asignación de usuario y términos de uso, en donde se encuentran establecidos los términos que debe tener con el usuario y se le indica que estas credenciales de accesos son únicas e intransferibles.

Adicionalmente, la Oficina, grupos o responsables de Tecnologías de la Información y las Comunicaciones, deben realizar sensibilizaciones a los funcionarios de la institución, para dar a conocer el lineamiento de contraseñas seguras.

ARTÍCULO 106. GESTIÓN DE LA CAPACIDAD. La Oficina, grupos o responsables de Tecnologías de la Información y las Comunicaciones de la Policía Nacional, que gestionan componente tecnológico en producción, que soporta las actividades administrativas y operativas, deben realizar un monitoreo a los recursos tecnológicos, con el propósito de generar líneas base que les permita, proyectar necesidades de crecimiento en procesamiento, almacenamiento y transmisión de la información, con el fin de, evitar inconvenientes que se conviertan en una amenaza a la seguridad o a la continuidad de los servicios prestados por la plataforma tecnológica institucional.

ARTÍCULO 107. PROTECCIÓN CONTRA MALWARE. Se deben implementar controles contra el software malicioso en el que se incluyen virus, spyware, ransomware, y otros tipos de software malicioso que representa una de las mayores amenazas para los datos institucionales, estos controles deben incluir la respuesta a incidentes informáticos, protecciones de dispositivo final, actualizaciones permanentes en los sistemas operativos y campañas de toma de conciencia, con el fin de prevenir afectaciones a la seguridad, disponibilidad e integridad de la información.

ARTÍCULO 108. GESTIÓN DE LA CONFIGURACIÓN. Se debe llevar un registro del versionamiento de los sistemas de información y aplicaciones, así como de las configuraciones en cada uno de los mismos desarrollos implementados, sin embargo, las adiciones, modificaciones o eliminaciones que pueden afectar de forma directa o indirecta los servicios de las operaciones tecnológicas de la institución pasan por un comité asesor de gestión del cambio, en el cual se analizan los riesgos y las condiciones técnicas antes ser puestos en producción en la plataforma tecnológica.

ARTÍCULO 109. ENMASCARAMIENTO DE DATOS. Se debe realizar la protección de la información que se encuentra en producción en los sistemas de información y las bases de datos, por lo tanto, las pruebas a nuevos desarrollos no se deben realizar con la información real, por lo que se debe enmascarar[36] para la realización de pruebas; en el caso de que reportes generados por los diferentes sistemas de información, contengan información clasificada o reservada esta debe ser aplicada técnicas de enmascaramiento y clasificación de la información para la entrega de la misma.

ARTÍCULO 110. PREVENCIÓN DE FUGA DE DATOS. Se debe realizar las gestiones que permita la adquisición de herramientas que permiten detectar la fuga de información mediante la prevención de perdida de datos (DLP – Data Loss Prevention) y equipos que detecten comportamientos anómalos y potenciales de incidentes de seguridad, con sistemas de administración de eventos e información de seguridad - SIEM (Security Information and Event Management), mitigando así eventos asociados a fuga de datos e información.

[36] Enmascarar: : Proceso de ocultar datos sensibles o personales en bases de datos, informes y otros lugares donde no debería ser visible. (Microsoft,2024)

ARTÍCULO 111. REDUNDANCIA DE LAS INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN. Con el propósito de asegurar la disponibilidad de los servicios identificados como críticos de la plataforma tecnológica institucional en producción, las unidades de policía que gestionan Sistemas de información y componentes esenciales para la gestión institucional, deben implementar redundancia[37] que permita asegurar la disponibilidad de la información institucional, los cuales deben estar documentados en la ejecución del procedimiento de continuidad del negocio (1DT-PR-0024).

ARTÍCULO 112. REGISTRO DE EVENTOS. Los diferentes registros que se generen en la plataforma tecnológica institucional en producción, relacionados con actividades, excepciones, fallas y otros que se presenten, deben ser documentados bajo la ejecución de los diferentes procedimientos, herramientas tecnológicas dispuestas para ello.

ARTÍCULO 113. ACTIVIDADES DE SEGUIMIENTO. Los administradores del componente tecnológico institucional en producción, deben realizar un monitoreo permanente a los recursos, servicios y capacidades con los que se cuentan, en los cuales se debe adoptar medidas en caso de que se presenten fallas o afectaciones a la disponibilidad, integridad y confidencialidad de la información, realizando el registro de los eventos o incidentes que se lleguen a materializar.

ARTÍCULO 114. SINCRONIZACIÓN DE RELOJES. Para garantizar la exactitud de los relojes en los diferentes componentes tecnológicos, la Policía Nacional, cuenta con el servicio de tiempo de red NTP (Network Time Protocol), sincronizado con la hora legal colombiana, por lo tanto, todos los equipos de cómputo, servidores y equipos que se encuentren conectados a la red LAN institucional, deben estar configurados a este servicio; para aquellos equipos que no cuentan con conexión a la red, se debe realizar por parte de los dueños o custodios de los activos, la verificación permanente con el fin de realizar la sincronización de relojes de forma manual a la hora legal colombiana.

ARTÍCULO 115. USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS. Se debe controlar el software que se utiliza en la plataforma tecnológica, mitigando que no se presenten afectaciones a la disponibilidad, integridad y confidencialidad de la información. Por lo tanto, la Policía Nacional cuenta con un controlador de dominio, que no permite la instalación de software no autorizado o cambios de configuración en el sistema operativo, de los computadores en el usuario final, solo el personal que cuenta con el rol de Técnico en Tecnologías de la Información y las Comunicaciones, tiene asignado usuario de administración, con el fin de, realizar configuraciones en los equipos de cómputo de la unidad, previa solicitud realizada por el usuario final mediante el Sistema de Gestión de Requerimientos en TIC o el dispuesto para tal fin.

El personal de técnicos de los Grupos de Tecnologías de la Información y Comunicaciones, deben realizar revistas aleatorias a los computadores institucionales, utilizando la lista de chequeo equipos de cómputo, la cual debe ser diligenciada digitalmente mediante el Sistema de Gestión de Requerimientos en TIC o el dispuesto para tal fin, con el propósito de controlar el uso de software no autorizado, en los equipos de cómputo de propiedad de la institución; con el fin de, garantizar que el equipo tenga actualizado el sistema operativo, antivirus y controladores del sistema, así como la desinstalación de programas mal intencionados o que no sean autorizados por la Policía Nacional.

Sin embargo, en caso que el personal de los Grupos de Tecnologías de la Información y Comunicaciones, requiera el uso de software utilitario para la gestión de actividades técnicas en los equipos de cómputo y servidores institucionales, deben contar con la viabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones, estos programas no deben ser instalados de forma permanente en los equipos por lo que deben ser desinstalados una vez hayan cumplido su función de gestión y debe contar con la respetiva licencia de uso, no está autorizado el uso de software utilitario que realice anulación de controles de seguridad de la información.

ARTÍCULO 116. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS. El software utilizado en la Policía Nacional debe ser únicamente el adquirido o aquellos que tienen el aval de la Oficina de Tecnologías de la Información y las Comunicaciones para su uso. Es responsabilidad de los usuarios de los equipos de cómputo de la Policía no realizar cambios en los equipos, ya que el

[37] Redundancia: Uso de almacenamiento adicional, servidores y redes para asegurar la disponibilidad y la recuperación de datos en caso de fallos. (Microsoft,2024)

usuario final no cuenta con privilegios de administración, razón por la cual, el escalamiento de usuarios administradores se encuentra bajo la responsabilidad de los técnicos o responsables de tecnologías de la información y las comunicaciones de la unidad.

Los equipos de cómputo que no se encuentran conectados a la red de la Policía Nacional, y que cuentan con una justificación para las excepciones de los controles, su usuario por defecto con privilegios de administración debe ser deshabilitado y así crear los usuarios de forma local con las mismas características de seguridad de los equipos de cómputo conectados a la red institucional.

ARTÍCULO 117. SEGREGACIÓN DE REDES. La Policía Nacional utiliza dispositivos de seguridad de red tipo firewalls y switch Core[38], para controlar el tráfico de datos.

Los servicios ofrecidos por la Oficina de Tecnologías de la Información y las Comunicaciones, tienen controles que garantizan el cifrado de la información desde su origen o en tránsito, para lo cual cuenta con herramientas de seguridad perimetral que permiten proteger y controlar todos los accesos desde o hacia la red LAN, estableciendo la segmentación del bloque de direcciones a través de zonas lógicas de seguridad que delimiten el acceso entre host, servidores, aplicaciones y bases de datos.

ARTÍCULO 118. SEGURIDAD DE LOS SERVICIOS DE RED. Los niveles de servicio deben contemplar características de seguridad, requisitos de gestión de los servicios de red y valores agregados en dispositivos de seguridad, realizando un control a través de chequeo del tráfico de la red, monitoreo de los puertos en la red, auditoría, trazabilidad y respaldo de archivos de registro (logs).

Los requerimientos contractuales que solicitan cifrado de punta a punta en los canales de datos, los segmentos de red permanecen cerrados y solo se permiten equipos diferentes a los institucionales mediante la solicitud de un ticket a través del Sistema de Información para la Gestión de Incidentes en TIC y con acceso restringido a los servicios de la red LAN.

Los equipos de cómputo que no hacen parte del inventario de la institución o personal visitante podrán hacer uso de los servicios de internet que provee la institución siempre y cuando, estén conectados a redes de visitantes de acuerdo a la disponibilidad técnica de la unidad, o los servicios de internet inalámbrico de los cuales no se podrá acceder a los recursos de gestión de administración de la infraestructura tecnológica institucional en producción.

ARTÍCULO 119. FILTRADO WEB. Se debe establecer lineamientos que permitan reducir el riesgo de acceso a contenidos maliciosos y que aseguren la disponibilidad de los servicios que soporta la gestión institucional, por lo tanto, se establecen perfiles de navegación de acuerdo al cumplimiento de las funciones que contribuyen a la filtración de contenido web, en caso que se requiera el acceso o modificación de los mismos, se debe realizar de acuerdo a las excepciones establecidas en el presente manual.

ARTÍCULO 120. REQUISITOS DE SEGURIDAD EN LAS APLICACIONES. El desarrollo de aplicaciones cumple los requisitos establecidos en el procedimiento o lineamientos sobre desarrollar sistemas de información (1DT-PR-0017), realizando la implementación y aseguramiento de la disponibilidad, confidencialidad e integridad de la información, a través de:

- La documentación y registros de los requerimientos.
- Gestión de contraseñas de forma segura.
- Control de acceso a la información.
- Revisión y registro de los accesos privilegiados.
- Cifrado de información a través de certificados.

[38] Switch Core: dispositivo de red de alta capacidad que se utiliza en el núcleo de una red para conectar diferentes segmentos de la red y gestionar el tráfico de datos de manera eficiente. (Microsoft,2024)

- Separación de instancias entre aplicación y bases de datos.
- Copias de respaldo.
- Informe de incidentes de seguridad de la información.
- Copias de versiones.

ARTÍCULO 121. ARQUITECTURA DE SISTEMAS SEGUROS Y PRINCIPIOS DE INGENIERÍA. Los sistemas de información como soporte importante de los procesos misionales de la Policía Nacional, buscan brindar seguridad a los aplicativos institucionales desde el momento mismo del levantamiento de requerimientos. Por lo tanto, las necesidades de seguridad hacen parte integral de las decisiones de arquitectura del software a construir o adquirir.

La Policía Nacional cuenta con una herramienta licenciada donde se encuentran los usuarios empresariales, para el proceso de gestión de identidades (personalizar roles y perfiles); el contratista o desarrollador deberá integrarse con dicha plataforma para el control de autenticación y autorización de usuarios, para lo cual, se aplica el procedimiento o lineamiento emitido para la gestión de identidades (1DT-PR-0003).

De igual forma, se contemplan los siguientes requerimientos en la construcción o adquisición de sistemas de información:

- Inicios de sesión una sola vez.
- Control de cierre de aplicación a los 5 minutos de inactividad.
- Verificación campos que no admitan códigos SQL para inyección[39].

ARTÍCULO 122. CODIFICACIÓN SEGURA. El desarrollo de sistemas de información y aplicaciones para la Policía Nacional se debe aplicar los principios de codificación segura, que contribuya a la reducción de riesgos de afectación a la disponibilidad, integridad y seguridad de la información gestionada, para lo cual se debe tener en cuenta:

- Configuración segura en las plataformas de alojamiento y sistemas de gestión de bases de datos que permitan proteger los datos contra inyección SQL.
- Autenticación segura entre aplicaciones y gestores de bases de datos.
- Comunicación cifrada de la información.
- Gestión de sesiones en las aplicaciones y sistemas de información deben ser controladas.
- Vencimiento de las sesiones una vez se detecte inactividad por parte del usuario final.
- Clasificar la información gestionada y establecer roles que permitan proteger el acceso no autorizado.

ARTÍCULO 123. PRUEBAS DE SEGURIDAD EN EL DESARROLLO Y ACEPTACIÓN. El Grupo de Seguridad de la Información y Respuesta a Incidentes Informáticos - CSIRT, es el encargado del análisis de la explotación de vulnerabilidades que podrían poner en riesgo la plataforma tecnológica institucional y su información, por lo tanto, estas vulnerabilidades deben ser gestionadas y remediadas por los desarrolladores, para lo cual se implementó un protocolo formal, que contempla:

- Realizar análisis de vulnerabilidades de forma semestral.

[39] Códigos SQL para inyección: técnica de ataque que explota vulnerabilidades en una aplicación para ejecutar comandos SQL maliciosos. (Microsoft,2024)

- Mantener información actualizada de nuevas vulnerabilidades.

- Detección de ataques reales.

Se debe aplicar el procedimiento o lineamiento emitido para desarrollar sistemas de información (1DT-PR-0017), que contempla la realización de pruebas de seguridad, así como efectuar las pruebas funcionales que permitan determinar el correcto funcionamiento del software de acuerdo a los requerimientos solicitados, en los que se incluyan requisitos de seguridad basados en el ingreso de usuarios finales, permisos y roles.

ARTÍCULO 124. DESARROLLO EXTERNALIZADO. Los desarrollos de sistemas de información o aplicaciones que sean adquiridos, donados o desarrollados de forma externa a la institución deben cumplir con los lineamentos definidos por el proceso del Direccionamiento Tecnológico, ante el procedimiento evaluaciones de tecnologías de la información y las comunicaciones – TIC (1DT-PR-0019), y el desarrollar sistemas de información (1DT-PR-0017), con el propósito de cumplir con los diferentes requisitos establecidos para asegurar la disponibilidad integridad y confidencialidad de la información.

Para la tercerización del desarrollo de software se debe tener en cuenta el procedimiento o lineamiento para desarrollar sistemas de información (1DT-PR-0017), atendiendo las siguientes recomendaciones:

- Cumplir con la Ley 23 de 1982 sobre derechos de autor.

- Atender las recomendaciones de la Circular Conjunta 01/2006 sobre los delitos de propiedad intelectual e industrial.

- Las especificaciones técnicas contemplarán los acuerdos de licencias de propiedad del código y demás derechos de propiedad.

- Las especificaciones técnicas establecen los requerimientos con respecto a la calidad del código y la existencia de garantías, así como los acuerdos de custodia de los códigos fuentes del software y cualquier otra documentación necesaria, en caso de requerir modificación en el mismo.

- Someter el software desarrollado a pruebas que permitan establecer el cumplimiento de requerimientos funcionales y de seguridad, análisis dinámico y estático de código, entre otros.

PARÁGRAFO. Es necesario que, durante el ciclo de vida del software o sistema de información, se mantenga la separación de los entornos de desarrollo de pruebas y producción, así como la protección de los registros asociados a estas.

ARTÍCULO 125. SEPARACIÓN DE ENTORNOS DE DESARROLLO, EVIDENCIAS Y PRODUCCIÓN. La Oficina de Tecnologías de la Información y las Comunicaciones y las unidades autorizadas para realizar desarrollo de aplicaciones y sistemas de información, deben dar aplicabilidad al procedimiento desarrollar sistemas de información (1DT-PR-0017), en donde se cuente con un ambiente de desarrollo seguro de software, en el cual se lleve el registro de las versiones y su documentación, implementando roles de acceso únicamente al personal autorizado.

ARTÍCULO 126. GESTIÓN DEL CAMBIO. Toda adición, modificación o eliminaciones que pueden afectar de forma directa o indirecta los servicios de la plataforma tecnológica en producción de la institución, con el fin de mitigar riesgos de afectación a la disponibilidad, integridad y confidencialidad de los activos de información de la Policía Nacional, por lo tanto, debe ser evaluada previamente, para analizar los riesgos en los aspectos técnicos y de seguridad, acorde con los protocolos establecidos en el procedimiento para la gestión del cambio (1DT-PR-0014). Para ello, se tienen en cuenta las diferencias entre funcionalidad y seguridad, las cuales se ajustan a decisiones de arquitectura que los cuales deben satisfacer los requisitos mínimos de seguridad.

ARTÍCULO 127. INFORMACIÓN DE PRUEBAS. Las pruebas de los sistemas de información se deben realizar en ambientes separados al de producción, siguiendo las siguientes pautas:

- Los datos de prueba están alojados en bases de datos independientes a la de producción.

- Los ambientes de pruebas tienen la misma estructura del ambiente de producción.

- Los datos sensibles no corresponden a datos reales de producción.

Las diferentes pruebas que se realicen a los sistemas de información o aplicaciones deben estar documentadas, clasificadas y protegidas.

ARTÍCULO 128. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DURANTE LAS PRUEBAS DE AUDITORÍA. Teniendo en cuenta que las auditorías, tanto internas como externas, son esenciales para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) de la institución y asegurar el cumplimiento con los requisitos del estándar, durante estos ejercicios, es importante proteger los sistemas y la información clasificada y reservada de posibles vulnerabilidades y accesos no autorizados, por lo tanto, en caso de requerirse evidencias o accesos durante la ejecución de las auditorías a los sistemas de información con información clasificada o reservada, se debe realizar la planificación entre el auditor y la dirección dueña de la información para que este dentro del alcance, se debe realizar la documentación correspondiente y se deben cumplir con los controles que permitan asegurar la divulgación, enmascaramiento de datos o clasificación de la información en caso de ser necesarios.

ARTÍCULO 129. MENSAJES ELECTRÓNICOS. La mensajería electrónica en la Policía Nacional, debe estar asociada a los servicios de correo electrónico de los dominios @policia.gov.co, @correo.policia.gov.co, @dipol.gov.co, @policia.edu.co, y aquellos autorizados por la institución, así como los servicios de mensajería instantánea electrónica adquiridos por la institución para la gestión de información, por lo tanto, es un medio valido para notificaciones, citaciones, comunicados y cualquier requerimiento de carácter institucional y deben estar regulados y licenciados de acuerdo a los términos de uso adecuado, e incorporados a la plataforma tecnológica; por lo tanto, no está permitido intercambiar información institucional a través de otras herramientas no corporativas institucionales, o herramientas de mensajería instantánea de uso comercial.

La Policía Nacional se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos los funcionarios y contratistas que cuenten con una licencia asignada, además podrá realizar copias en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información propios previa solicitud expresa por entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial. (Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, 17 de octubre de 2012, D.O[40]. No. 48587).

Las cuentas de correo electrónico asignadas a los funcionarios, contratistas o terceros son administradas por la Policía Nacional, y la información que se almacene en los mismos que no esté relacionada con información de carácter personal, es propiedad de la institución, por lo que la Oficina de Tecnologías de la Información y las Comunicaciones podrá verificar y realizar auditorías cuando así lo soliciten las diferentes unidades policiales o se requiera para investigaciones administrativas, disciplinarias o judiciales, previo cumplimiento de los requisitos legales.

PARÁGRAFO 1. Las cuentas de correos electrónico asociados al dominio @policia.gov.co y @correo.policia.gov.co será administradas por la Oficina de Tecnologías de la Información y las Comunicaciones, y será el encargado de definir los lineamientos de uso aceptable del servicio.

PARÁGRAFO 2. La cuenta con dominio @policia.edu.co, será administrada por la Dirección de Educación Policial - DIEPO, siendo única y exclusiva para el uso de entornos educativos; no obstante, la difusión de información institucional y personal estará restringida o no será aceptada como información veraz. De hecho, esta cuenta será asignada a los funcionarios que tengan el cargo de estudiantes o docentes, quienes una vez culminen su proceso de formación, se le retirará el acceso a la cuenta por término de la actividad.

[40] D.O. Diario Oficial: publicación del Gobierno de Colombia que contiene las leyes, los decretos, los actos y la mayoría de los documentos pertinentes y los avisos públicos del presidente, el Congreso y las agencias gubernamentales de Colombia. (Decreto de 28 de abril de 1864 [Presidencia de la República de Colombia], mediante el cual se informa la creación del Diario del Tesoro, el cual tendrá una frecuencia semanal y reemplazará a la publicación Registro Oficial, 28 de abril de 1864).

PARÁGRAFO 2. La gestión y administración de las cuentas asociadas al dominio @dipol.gov.co y las herramientas de mensajería instantánea que sean adquiridas para la gestión de información de inteligencia y contrainteligencia serán administradas y supervisadas por la Dirección de Inteligencia Policial cumpliendo lo establecido en la Ley Estatutaria 1621 de 17 de abril de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

CAPÍTULO III

SEGUIMIENTO Y REVISIÓN

ARTÍCULO 130. SEGUIMIENTO Y REVISIÓN. Medición, análisis y verificación de la eficacia y eficiencia de las actividades, controles y procedimientos implementados dentro del SGSI. Esta evaluación busca asegurar que el sistema cumple con los objetivos establecidos y que la seguridad de la información está protegida adecuadamente, efectuando una revisión que permita determinar que los riesgos se gestionan de manera efectiva, contribuyendo al mantenimiento del Sistema de Gestión frente a nuevas amenazas, cambios tecnológicos, y evolución de las normativas, por lo tanto, se hará mediante los procedimientos asociados a control interno de código 1CI-CP-0001 y revisión por la dirección.

PARÁGRAFO: con el propósito de evaluar periódicamente la eficacia, adecuación y alineación del Sistema de Gestión de Seguridad de la Información (SGSI) con los objetivos estratégicos, los requisitos de la organización y las normativas aplicables, identificando áreas de mejora y asegurando el compromiso continuo de la alta dirección en la gestión de la seguridad de la información, se debe realizar la revisión por la dirección, teniendo en cuenta las entradas del mismo, así:

a) Estado de las acciones provenientes de previas revisiones por la dirección
b) Los cambios en las cuestiones externas e internas que sean pertinentes para el Sistema de Gestión de Seguridad de la Información.
c) Los cambios en las necesidades y expectativas de las partes interesadas que sean pertinentes para el Sistema de Gestión de Seguridad de la Información.
d) La retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en:
    1) Las no conformidades y las acciones correctivas.
    2) Los resultados del seguimiento y la medición.
    3) Resultados de las auditorías
    4) El cumplimiento de los objetivos de seguridad de la información.
e) La retroalimentación de las partes interesadas
f) Los resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos
g) Las oportunidades de mejora continua.

Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el Sistema de Gestión de Seguridad de la Información.

CAPÍTULO IV

MANTENIMIENTO Y MEJORA

ARTICULO 131. MANTENIMIENTO Y MEJORA. Corresponde al proceso continuo de perfeccionamiento de los lineamientos y controles implementados para garantizar la seguridad de la información dentro de la institución, aplicando lo definido dentro del proceso de mejora continua e innovación de código 1MC-CP-0001, con el propósito de aumentar la efectividad del SGSI, reducir los riesgos asociados con la seguridad de la información y adaptarse de manera proactiva a los cambios en el entorno, tales como nuevas amenazas, avances tecnológicos, o modificaciones regulatorias.

TÍTULO III

DISPOSICIONES VARIAS

CAPITULO ÚNICO

CERTIFICACIÓN O ACREDITACIÓN, EXCEPCIONES, DECÁLOGO DE SEGURIDAD DE LA INFORMACIÓN Y GLOSARIO

ARTÍCULO 132. CERTIFICACIÓN O ACREDITACIÓN. La Policía Nacional busca la evaluación y certificación por una tercera parte independiente de sus sistemas de gestión como medio para asegurar que la institución ha implementado un conjunto de prácticas, políticas, lineamientos, procedimientos y controles adecuados para proteger la información contra accesos no autorizados, pérdidas, alteraciones, destrucción o diversas amenazas, contribuyendo a asegurar la confidencialidad, integridad y disponibilidad de los activos de información, por lo tanto, las unidades que en el marco del Sistema de Gestión adoptado por la Policía Nacional, deseen acceder a la certificación deben informar al líder del Sistema de Gestión de Seguridad de la Información y definir el alcance que será certificado por parte de entidades auditoras independientes de tercera parte; esto no implica que los procesos que queden fuera del alcance de la certificación estén exentos de implementar los lineamientos y controles establecidos por la Policía Nacional, esenciales para garantizar la disponibilidad, integridad y confidencialidad de los activos de información institucionales.

ARTÍCULO 133. EXCEPCIONES. Las excepciones son exclusiones permanentes o transitorias a los controles descritos en este documento que obligan a la valoración y toma de decisiones sobre los riesgos inherentes a dicha exclusión, por lo que se debe guardar un registro que contenga la fecha de solicitud, solicitante, nombre del control excluido, persona que autoriza, tiempo de la exclusión, a quien aplica la exclusión, dependencia, justificación y previa revisión del cumplimiento de los controles de seguridad dispuestos por la Oficina de Tecnologías de la Información y las Comunicaciones.

ARTÍCULO 134. DECÁLOGO DE SEGURIDAD DE LA INFORMACIÓN: Para el fortalecimiento de la cultura en seguridad de la información, la institución crea el "Decálogo de Seguridad de la Información" para observancia y aplicación estricta de todos los funcionarios de la Policía Nacional.

1. Conocer y cumplir el Manual del Sistema de Gestión de Seguridad de la Información.
2. No divulgar información institucional sin autorización.
3. Nunca compartir el usuario y la contraseña institucional.
4. Proteger la seguridad física de las instalaciones policiales.
5. Utilizar adecuadamente la red de datos institucional (Intranet e internet).
6. Nunca acceder a enlaces o archivos de dudosa procedencia.
7. No abandonar el lugar de trabajo sin antes asegurar la información a cargo.
8. No utilizar los medios tecnológicos institucionales para beneficio personal.
9. No confiar ni replicar información de la que no se tenga veracidad.
10. Reportar el incumplimiento del presente decálogo al administrador o analista de Seguridad de la Información de la unidad.

ARTÍCULO 135. GLOSARIO. A continuación se encuentra los términos o conceptos clave junto con las respectivas definiciones, que se utiliza para facilitar la comprensión del Sistema de Gestión de Seguridad de la Información, así:

- **Activos de información.** De acuerdo con la norma ISO 27001, un activo de información es "cualquier cosa que tenga valor para la organización y en consecuencia deba ser protegido". No obstante, este concepto es bastante amplio y debe ser limitado por una serie de consideraciones: el impacto que para la institución supone la pérdida de confidencialidad, integridad o disponibilidad de cada activo, el tipo de información que maneja en términos de su sensibilidad y criticidad y sus productores y consumidores. Los activos de información se traducen en dispositivos tecnológicos, archivos, bases de datos, documentación física, personas, sistemas de información, entre otros. (ISO, 2013).

- **Acuerdos de confidencialidad.** Documentos en los que los funcionarios de la Policía Nacional o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la institución, comprometiéndose a no divulgar, usar o explotar la información clasificada o reservada a la que tengan acceso en virtud de la labor que desarrollan dentro de sus funciones.

- **Acuerdos de intercambio de información.** Documentos constituidos entre la Policía Nacional y entidades externas de origen nacional o extranjero en donde se concretan las condiciones del intercambio de información, los compromisos de los terceros de mantener la confidencialidad y la integridad de la información a la que tengan acceso, las vigencias y las limitaciones a dichos acuerdos.

- **Análisis de riesgos de seguridad de la información.** Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

- **APN**: Access Point Name, es el nombre de un punto de acceso para servicio general de paquetes vía radio que permite la conexión a internet desde un dispositivo móvil celular.

- **Autenticación:** es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

- **Back up**: copia de seguridad o backup de información, realizada con el fin de utilizarse para restaurar la original después de una eventual pérdida de datos.

- **Borrado seguro de información**: procedimiento que permite garantizar que la información existente en un medio de almacenamiento no se pueda recuperar mediante una técnica especializada, y que consisten en realizar sobreescritura, desmagnetización y destrucción física de medios de almacenamiento.

- **Ciberseguridad.** Conjunto de prácticas, tecnologías, procesos y medidas diseñados para proteger los sistemas informáticos, las redes, los datos y los dispositivos de ataques cibernéticos y amenazas digitales. Su objetivo principal es garantizar la confidencialidad, la integridad y la disponibilidad de la información en un entorno digital cada vez más interconectado y propenso a riesgos.(Amazon Web Services, 2024).

- **Centros de procesamiento:** zonas específicas para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. Los centros de cómputo deben cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

- **Cifrado:** transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso a los repositorios de información de la institución.

- **Controversia**: inconformidad presentada por el usuario de la infraestructura de llave pública PKI-PONAL durante la generación, renovación o cancelación del certificado digital.

- **Criptografía:** disciplina que agrupa a los principios, medios y métodos para la transformación de datos, con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, o prevenir su uso no autorizado.

- **CSIRT - Computer Security Incident Response Team**: Equipo de Respuesta a Incidentes de Seguridad Informática, es un grupo especializado que se encarga de gestionar y responder a incidentes de seguridad informática.

- **Derechos de autor**: conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya realizado.

- **DHCP**: Dynamic Host Configuration Protocol, protocolo de configuración dinámica de host que permite a los clientes de una red de datos, obtener sus parámetros de configuración automáticamente.

- **DLP**: Data Loss Prevention, prevención de perdida de datos, herramienta de seguridad que identifica y contribuye a evitar el uso compartido, la transferencia o el uso indebidos o no seguros de datos con niveles de clasificación.

- **Desarrollo de software seguro.** Metodología en la cual se considera la seguridad de las aplicaciones durante todo el ciclo de vida, considerando las posibles vulnerabilidades que puede tener el desarrollo sin esperar iteraciones[41] posteriores.

- **Dispositivos de almacenamiento**: materiales físicos donde se almacenan datos electrónicos o digitales.

- **Dueño de activos de Información.** Funcionario a cargo de la unidad organizacional que tiene responsabilidad aprobada del alto mando para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.

- **Evento de seguridad de la información.** Ocurrencia identificada en un sistema de información, servicio o estado de la red que indica un posible fallo en los controles de seguridad de la información, en la política de seguridad de la información o una situación previamente desconocida que puede ser relevante para la institución y que genera una alerta de posible afectación a la disponibilidad, integridad y confidencialidad de los activos de información.

- **Hardware**: componente físico tecnológico, que trabaja o interactúa de algún modo con el computador. Incluye elementos internos como el disco duro, CD-ROM, y también hace referencia al cableado, circuitos, gabinete, etc., e incluso a elementos externos como la impresora, el mouse, el teclado, el monitor y demás elementos periféricos.

- **Incidente de seguridad de la información.** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información, aplicación o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 de 2022 [Ministerio de Tecnologías de la Información y las Comunicaciones], el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones, 8 de marzo de 2022).

- **Interoperabilidad**: capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios digitales a ciudadanos, empresas y a otras entidades, mediante el intercambio de datos entre sus sistemas TIC.(Ministerio de Tecnologías de la Información y las Comunicaciones,2019).

- **Llaves criptográficas:** cadena de caracteres que se utiliza en un algoritmo de cifrado para alterar los datos de forma que parezcan aleatorios con el fin de proteger la integridad de la información.

- **Logs**: registro o datos de quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo o sistema en particular.

[41] Iteraciones: Proceso de repetir un conjunto de operaciones, pasos o tareas con el objetivo de aproximarse a una solución o mejorar continuamente un proceso.(Microsoft,2024)

- **Plan de recuperación ante desastres.** Conjunto de procedimientos de recuperación de la plataforma tecnológica de la institución que cubre aspectos como los datos, el hardware[42] y el software[43] crítico para que la Policía Nacional pueda restablecer sus operaciones en caso de un desastre natural o causado por un error humano, en forma rápida, eficiente y con el menor costo y pérdidas posibles. El plan también debe incluir las consideraciones necesarias para enfrentarse a la pérdida inesperada o repentina de personal crítico.

- **Propiedad intelectual:** reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

- **Seguridad de la información.** Preservación de la autenticidad[44], confidencialidad, integridad y disponibilidad de la información, en cualquier medio de almacenamiento: impreso o digital y la aplicación de procesos de resiliencia[45] operativa. (Decreto 338 de 2022 [Ministerio de Tecnologías de la Información y las Comunicaciones], el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza[46] de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones, 8 de marzo de 2022).

- **Seguridad digital.** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas y mediante la gestión de riesgos de seguridad digital; la implementación efectiva de ciberseguridad y el uso efectivo de las capacidades que demanda la voluntad social y política de las múltiples partes interesadas. (Decreto 338 de 2022 [Ministerio de Tecnologías de la Información y las Comunicaciones], el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones, 8 de marzo de 2022).

- **Seguridad informática.** Protección de los sistemas de información, los datos y la infraestructura tecnológica contra amenazas, ataques y riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad. Se centra en la protección de los sistemas informáticos y la infraestructura tecnológica. Esto incluye la protección de las redes, los servidores, los dispositivos y el software contra amenazas cibernéticas como programas maliciosos, ataques de hackers[47], denegación de servicio[48], entre otros. (ISO,2018).

- **Recursos tecnológicos**: componentes de hardware y software tales como: servidores de aplicaciones y de servicios de red, estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, equipos de radio, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la institución.

- **Red LAN**: Local Area Network. Red de área local, es una red que conecta los equipos de cómputo en un área relativamente pequeña y predeterminada.

---

[42] Hardware: componentes físicos que conforman una computadora y otros dispositivos electrónicos. (Microsoft,2024)

[43] Software: conjunto de instrucciones y datos que permiten dirigir y coordinar el funcionamiento del hardware. (Microsoft,2024)

[44] Autenticidad: propiedad de la información que garantiza que la identidad de un usuario, dispositivo o sistema es realmente quien dice ser. (Microsoft,2024)

[45] Resiliencia: capacidad de un sistema, organización o individuo para adaptarse, recuperarse y continuar funcionando frente a cambios, desafíos o adversidades. (Microsoft,2024)

[46] Gobernanza: procesos y estructuras que aseguran que la organización maneje adecuadamente sus recursos de información, cumpla con las regulaciones, y logre sus objetivos estratégicos. (Microsoft,2024)

[47] Hackers: individuos que utilizan sus conocimientos técnicos para explorar, manipular y, en algunos casos, explotar sistemas informáticos y redes. (Microsoft,2024)

[48] Denegación de servicio: intento malicioso de interrumpir el funcionamiento normal de un servidor, servicio o red, haciéndolo inaccesible para los usuarios legítimos. (Microsoft,2024)

- **Registros de auditoría**: archivos donde son registrados los eventos que se han identificado en los sistemas de información y redes de datos de la institución. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

- **SIEM**: Security Information and Event Management, herramienta de seguridad que contribuye a proporcionar una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre los sistemas informáticos.

- **Sistema de información:** conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir, desarrollado por la Policía Nacional o de origen externo, adquirido por la institución como un producto estándar de mercado o desarrollado para las necesidades de ésta.

- **Software**: conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación. (IEEE, 1983)

- **Software malicioso**: variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

- **Spyware**: tipo de software malicioso diseñado para infiltrarse en un dispositivo y recopilar información sobre el usuario sin su conocimiento o consentimiento.

- **SSL**: Secure Socket Layer, es un protocolo que cifra los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico.

- **Switches**: dispositivo de hardware utilizado en redes de computadoras para conectar múltiples dispositivos y gestionar la transferencia de datos entre ellos.

- **TIC**: tecnologías de la información y las comunicaciones.

- **Troyanos**: tipo de software malicioso que se disfraza de software legítimo para engañar a los usuarios y lograr que lo instalen en sus dispositivos.

- **UPS**: Uninterruptable Power Supply, sistema de alimentación ininterrumpida (SAI / UPS) es un dispositivo que permite suministrar energía a los dispositivos que están conectados a él, después de un apagado, durante un tiempo prudencial, para realizar un apagado seguro de dichos dispositivos.

- **VPN:** Virtual Private Network. Red Privada Virtual, es una tecnología que permite la extensión de una red pública como internet a un espacio de red local.

- **Vulnerabilidades**: Debilidades, brechas de seguridad [49]o flaquezas[50] inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la institución (amenazas), las cuales se constituyen en fuentes de riesgo.

[49] Brecha de seguridad: debilidad en los controles de seguridad de la información que pueden conllevar al acceso no autorizado a la información. (Microsoft,2024)
[50] Flaquezas: debilidades o vulnerabilidades dentro de un sistema que pueden ser explotadas por atacantes para comprometer la seguridad de la información. (Microsoft,2024)

TÍTULO IV

DISPOSICIONES FINALES

CAPÍTULO ÚNICO

REVISIÓN Y ACTUALIZACIÓN, VIGENCIA

ARTÍCULO 136. REVISIÓN Y ACTUALIZACIÓN. Las Oficina de Tecnologías de la Información y las Comunicaciones como responsable del Sistema de Gestión de Seguridad de la Información, será la encargada de revisar, implementar los controles que contribuyan a la aplicación de las mejores prácticas de seguridad de la información y proponer las actualizaciones al presente manual.

ARTÍCULO 137. VIGENCIA. La presente resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias, en especial la Resolución No. 00036 del 08 de enero de 2010 "Por la cual se crea el comité de seguridad de la información de la Policía Nacional", la resolución 00934 del 12 de abril del 2010 ""Por medio de la cual se modifica parcialmente y se adiciona la Resolución No. 00036 del 08 de Enero de 2010 "Por la cual se crea el comité de seguridad de la información de la Policía Nacional"." y la Resolución 08310 del 28 de diciembre de 2016 "Por la cual se expide el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional".

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C, a los 26 DIC 2024

General **WILLIAM RENÉ SALAMANCA RAMÍREZ**
Director General Policía Nacional de Colombia

Elaboró: SI. Wilmer Alexander Baracaldo Cifuentes
OFTIC – CSIRT

Elaboró: IT. Pablo Andrés Gaviria Muñoz
OFTIC-CSIRT

Revisó: IT. Sandra Milena Anaya Rodríguez
OFTIC-GUSAP

Revisó: CT. Edwin Javier Ramírez Gil
OFTIC-GUSAP

Revisó: CT. Edwin Alexander Espitia Duarte
OFTIC – CSIRT

Revisó: CT. Stephen Alejandro Mendez Mendoza
OFTIC – CSIRT

Revisó: TC. Wilson Ferney González Medina
OFTIC – SUTIC

Revisó: TC. Cristhian Mauricio Barrero Sánchez
OFPLA-CENPO

Revisó: TC. Jaime Hernán Rojas Parra
Jefe Oficina Tecnologías de la Información y las Comunicaciones

Revisó: CR. Diana Constanza Torres Castellanos
Jefe Oficina de Planeación

Revisó: BG. Hernán Alonso Meneses Gelves
Secretario General

Revisó: BG. Nicolás Alejandro Zapata Restrepo
Subdirector General

Fecha de elaboración: 22/11/2024
Ubicación: \\srvfilespersonal1\OFTIC\CSIRT\2024\30_PLANES\30.14_PLANES DE SEGURIDAD_DE_LA_INFORMACIÓN\MANUAL SGSI

Carrera 59 26-21 CAN, Bogotá
Teléfono: 5159269 - 5159140
oftic.jefat@policia.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA