MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

DIRECCIÓN GENERAL

RESOLUCIÓN __03049_ DEL ___24 de agosto de 2012__

"Por la cual se adopta 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 sus facultades legales y

CONSIDERANDO:

Que el Decreto 4222 del 23 de noviembre de 2006, modificó parcialmente la estructura del Ministerio de Defensa Nacional.

Que el artículo 2º numeral 8 del Decreto 4222 del 23 de noviembre de 2006, "Por la cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional", determinó que el Director General de la Policía Nacional de Colombia, expedirá resoluciones, manuales y demás actos administrativos necesarios para administrar la Policía Nacional en todo el territorio nacional.

Que el artículo 24 de la norma ibídem, facultó al Director General de la Policía Nacional de Colombia para crear y organizar, con carácter permanente o transitorio, escuelas, unidades, áreas funcionales y grupos de trabajo, determinando en el acto de creación de éstas, sus tareas, responsabilidades y las demás disposiciones necesarias para su funcionamiento.

Que mediante la Ley 872 del 30 de diciembre de 2003, 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 para dirigir y evaluar el desempeño institucional, en términos de calidad y satisfacción social en la prestación de los servicios a cargo de las entidades y agentes obligados, la cual estará enmarcada en los planes estratégicos y de desarrollo de tales entidades.

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 supervivencia de la Institución, administrándola y protegiéndola a través de la aplicación efectiva de las mejores prácticas y controles, garantizando la gobernabilidad del país,

Que en atención a los preceptos normativos que rigen sobre este tópico, se hace necesario adoptar el Manual del Sistema de Gestión de Seguridad de la Información, con el fin de contar con un lineamiento en el tema de seguridad, que permita a la vez la consulta de los deberes institucionales y orientación a los funcionarios en lo referente a la seguridad de la información, para alcanzar los estándares de calidad, seguridad y ciclo de vida de la información institucional.

Que con fundamento en los anteriores considerandos, se hace necesario crear y adoptar el Manual del Sistema de Gestión de Seguridad de la Información, con el objeto de lograr mayor eficiencia, eficacia, efectividad y calidad de la información, mediante las prácticas que debe utilizar la Institución a través de la elaboración y aplicación de pautas para el desempeño de sus funciones y alcance de sus objetivos en la prestación del servicio de Policía.

Que es necesario formalizar el Sistema de Gestión de Seguridad de la Información de la Policía Nacional, y por tanto se expide el "Manual de Seguridad de la Información de la Policía Nacional", con el propósito de determinar la política de seguridad de la información, herramienta que establece normas, procedimientos y controles a los activos de información, permitiendo hacer una adecuada gestión del riesgo y fortaleciendo la institución ante posibles amenazas que afecten su continuidad para lo cual.

RESUELVE:

ARTÍCULO 1. CREACIÓN Y ADOPCIÓN. Adoptar en todas sus partes el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional, que forma parte contextual de la presente resolución y que se identificará, así: MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 2. ESTRUCTURA DEL MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. La Estructura del Manual del Sistema de Gestión de Seguridad de la Información**;** estará compuesto por los siguientes capítulos, así:

TÍTULO 1

GENERALIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO 1

GENERALIDADES

ARTÍCULO 3. OBJETIVO

El presente Manual tiene por objetivo dar a conocer a todos los servidores publicos de la Institución los conceptos basicos de seguridad de la información para la Policia Nacional y su alcance generando una unidad de criterio en lo referente a:

- Definir la política de seguridad de la información.
- Establecer normas, procedimientos y controles a los activos de información.
- Establecer responsabilidades con la seguridad de la información.

ARTÍCULO 4. ALCANCE

La observancia del presente Manual es de cumplimiento para todos los funcionarios de la Policía Nacional y al personal externo que le proporcione algún bien o servicio; estando obligados a cumplir los parámetros aquí descritos y los controles adicionales que pueden implementar las diferentes unidades de acuerdo a su misionalidad.

ARTÍCULO 5. CONCEPTO DE SEGURIDAD DE LA INFORMACIÓN

Es la preservación de la Confidencialidad, Integridad y Disponibilidad de la información Institucional y propender por la autenticidad, trazabilidad, no repudio y fiabilidad de la misma.

ARTÍCULO 6. CONCEPTO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información es la adecuada gestión del riesgo, es el diseño de políticas, normas, líneas bases, guías, procedimientos y educación a los usuarios y propietarios de los activos de información; cuyo objetivo es planificar, diseñar, implementar y mantener un programa de seguridad de la información en concordancia con los objetivos estratégicos institucionales que permita proteger a la Institución y sus activos.

ARTÍCULO 7. PRINCIPIOS FUNDAMENTALES DE SEGURIDAD DE LA INFORMACIÓN

El objetivo primordial de un sistema de seguridad de la información es proporcionar la disponibilidad, integridad y confidencialidad de la información institucional, principios que son establecidos por la Institución así:

Figura 1. Principíos de Seguridad de la Información.

PRINCIPIO DISPONIBILIDAD

Establece que la información debe estar disponible para su uso en todo momento, para ser usada o vista solo por personal autorizado.

PRINCIPIO INTEGRIDAD

Consiste en salvaguardar la exactitud y estado completo de los activos de información, es decir que la información solo pueda ser modificada por personal autorizado.

PRINCIPIO CONFIDENCIALIDAD

Establece que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

ARTÍCULO 8. DEFINICIÓN POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información es una declaración general dictada por el alto mando, la cual indica el rol de la seguridad de la información al interior de la institución.

ARTÍCULO 9. NORMAS DE SEGURIDAD DE LA INFORMACIÓN

Las normas en materia de seguridad de la información hacen referencia a las actividades, acciones o reglas de obligatorio cumplimiento por parte de los funcionarios o terceros que interactúan con la Policía Nacional; las normas son de tipo tácticos utilizadas para lograr y apoyar la política de seguridad de la información.

ARTÍCULO 10. LÍNEAS BASE DE SEGURIDAD DE LA INFORMACIÓN

Las líneas base consisten en puntos de partida a partir de los cuales se realizan comparaciones futuras de riesgos y/o controles implementados, así mismo se trata de niveles mínimos de protección requeridos.

ARTÍCULO 11. DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

Consisten en recomendaciones o guías para los usuarios, para tratar excepciones o profundizar en temas en los cuales las normas no son lo suficientemente precisas; las directrices también son usadas para apoyar los procedimientos.

ARTÍCULO 12. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los procedimientos detallan el paso a paso las actividades que deben realizarse para lograr un objetivo, son la operacionalizacion de la política y las normas.

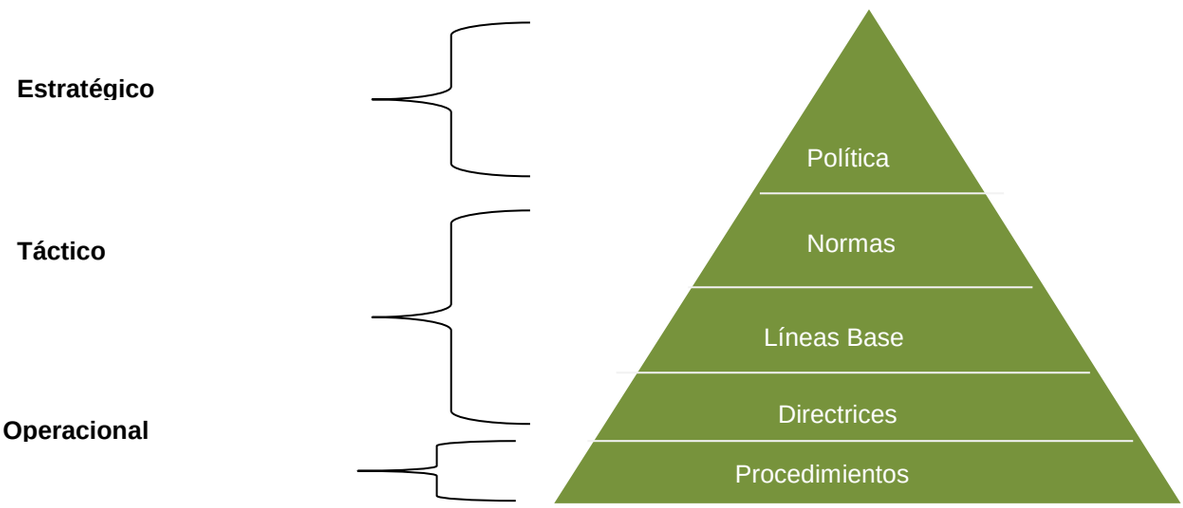

Figura 2 . Piramide Normativo

ARTÍCULO 13. CONTROLES

Los controles son los medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas o físicas.

a) Controles administrativos, están dados por las políticas, normas, directrices, procedimientos, gestión del riesgo, selección de personal, concienciación en seguridad de la información.

b) Controles técnicos o lógicos, se trata de aquellos controles que se soportan en tecnología.

ARTÍCULO 14. DEFINICIONES DE SEGURIDAD

- Vulnerabilidad, consiste en una debilidad que puede proporcionar a un atacante el medio para acceder sin autorización a los activos de información.
- Amenaza, es un peligro potencial que identifique una vulnerabilidad específica y la utiliza para acceder sin autorización a los activos de información.
- Agente de amenaza, es la entidad que se aprovecha de una vulnerabilidad para explotarla.
- Riesgo, es la probabilidad que un agente de amenaza explote una vulnerabilidad y cause un impacto sobre la Institución.
- Contramedida o salvaguarda, son los controles de tipo administrativo, técnico o físico que se implementan para mitigar un riesgo potencial.

CAPÍTULO 2

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Policía Nacional se compromete a salvaguardar sus activos de información, protegiéndolos a través de una adecuada gestión del riesgo, el cumplimiento de los requisitos legales y una estrategia de seguridad basada en las mejores prácticas y controles, con el fin de resguardar los activos de información de las amenazas que se ciernen sobre ellos.

ARTÍCULO 15. OBJETIVOS DE SEGURIDAD

- Establecer los niveles de acceso a la información institucional, brindando confidencialidad, integridad y disponibilidad.
- Cumplir con todos los requisitos estatutarios, reglamentarios y contractuales que estén orientados a seguridad de la información.
- Apoyar al modelo de continuidad de negocio institucional.
- Ser referente ante las entidades del Estado, como líderes en la atención de incidentes en seguridad de la información.
- Informar las conductas que afecten la seguridad de la información.

ARTÍCULO 16. METAS

Identificar por medio de una adecuada evaluación del riesgo el valor de los activos de información, con el fin de comprender sus vulnerabilidades y las amenazas que pueden exponerlos algun riesgo.

Administrar los riesgos a un nivel aceptable a traves del diseño, implementación y mantenimiento de un sistema de gestión de seguridad de la información.

Cumplimiento con la legislación, así:

- Ley 23 de 1982, derechos de autor.
- Ley 527 de 1999, comercio electrónico y firmas digitales.
- Ley 1273 de 2009, título de la protección de la Información y de los datos.
- Circular conjunta 01 de 2006, Orientaciones para el cumplimiento del derecho de autor y derechos conexos.
- Ley 1015 de 2006, Régimen disciplinario Policía Nacional.
- ISO/IEC 27001:2005.

Cumplir con las directivas y reglamentos internos referentes a seguridad de la información.

ARTÍCULO 17. COMPROMISO DE LA DIRECCIÓN

La Dirección General de la Policía Nacional aprueba esta política de seguridad de la información demostrando su apoyo y compromiso en la protección de la información institucional.

ARTÍCULO 18. RESPONSABILIDADES

A continuación se relacionan los roles y responsabilidades de quienes deben apoyar y cumplir la política de seguridad de la información, así:

- **Comité del Sistema de Gestión de Seguridad de la Información**. Implementa el SGSI en cada una de sus fases, divulga y realiza concienciación a los funcionarios de la Policía Nacional sobre el SGSI y gestiona los recursos necesarios para el fortalecimiento y mejora continua del SGSI en cada unidad policial.

- **Grupo de Seguridad de la Información.** La Oficina de Telemática lidera el desarrollo, implementación, mantenimiento, actualización de planes estratégicos de seguridad de la información.

- **Propietarios de los activos de información.** Identifican, elaboran, clasifican y gestionan el riesgo de los activos de información de acuerdo al grado de sensibilidad y criticidad de la misma.

- **Dirección de Incorporación**. Selecciona el talento humano de planta y prestación de servicios de tal manera que se certifique que el aspirante posee competencias que cumplan con el perfil del cargo al cual se postula.

- **Dirección de Talento Humano**, Incluye en el manual de funciones los cargos relaciondos a la seguridad de la información; notifica a todo el personal que se incorpora a la institución de sus obligaciones respecto del cumplimiento del Manual de Seguridad de la Información y de todas las normas, procedimientos y controles que de ella surjan. Así mismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, y la firma del acta de compromiso con la seguridad de la información y los acuerdos de confidencialidad.

- **Dirección de Protección y Servicios Especiales**. Con acompañamiento de la Dirección de Inteligencia, Dirección de Carabineros y Seguridad Rural, la Dirección de Antinarcóticos, Oficina de Telemática, el Grupo de Construcciones de la Dirección Administrativa y Financiera y el jefe de Seguridad del complejo DIPON, elabora el procedimiento de Seguridad de Instalaciones; comunicando, implementando y mejorando, dichos protocolos.

- **Inspección General.** Investiga las conductas contrarias a la política de seguridad de la información.

- **Área de Control Interno**. Revisa y verifica el cumplimiento de la presente política, revisa o audita las transacciones realizadas por los usuarios finales, sobre los sistemas de información; así como las actividades del personal de la oficina de Telemática sobre la plataforma tecnológica.

- **Oficina Asesora de Comunicaciones Estratégicas**. Difunde la presente política a través de la plataforma de medios institucionales.

- **Dirección Nacional de Educación**. Capacita en seguridad de la información, a los funcionarios de la Policía Nacional.

- **Oficina de Planeación**. Actualiza los formatos de todos los documentos institucionales, incluyendo el rotulo de clasificación correspondiente al contenido de cada documento.

- **Oficina de Telemática.** Cumple la función de cubrir los requerimientos de seguridad de la información establecidos para la operación, administración, comunicación de los recursos de tecnología de la Policía Nacional. Así mismo debe efectuar las tareas de desarrollo y mantenimiento de sistemas de información, siguiendo una metodología de ciclo de vida de sistemas apropiada, la cual debe contemplar medidas de seguridad.

- **Secretaría General.** Asesora a la Policía Nacional en lo referente a la seguridad de la información en materia legal y verifica el cumplimiento de la presente política en acuerdos u otra documentación de la institución con terceros.

- **Grupos de Contratación.** Cada unidad incluyen en los contratos con proveedores de servicios de tecnología y cualquier otro bien o servicio cuya actividad afecte directa o indirectamente los activos de información, la obligatoriedad de cumplimiento de la Política de Seguridad de la información y todo lo que con ella esté relacionado.

- **CSIRT PONAL** de la Oficina de Telemática atiende e investiga los incidentes de seguridad de la información institucional y propende por el restablecimiento del servicio.
- **Grupo de Delitos Tecnológicos de la Dirección de Investigación Criminal e Interpol**. Investiga los incidentes que se sospechan constituyen un delito.

- **Funcionarios Y Personal Externo**. Todo el personal que labora o realiza actividades para la Policía Nacional, son responsables por el cumplimiento de la presente política y de informar cualquier incidente de seguridad de la información del que tenga conocimiento.

ARTÍCULO 19. REVISIÓN

La política de seguridad de la información estará vigente desde la fecha de su aprobación y publicación. Será revisada para su actualización anualmente y/o extraordinariamente cuando sea necesario.

CAPÍTULO 3

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 20 ORGANIZACIÓN.

La siguiente política busca establecer funciones y responsabilidades claras que permitan gestionar adecuadamente la seguridad de la información al interior de la Policía Nacional, definiendo los responsables de la aprobación de la política, su implementación, los procesos de autorización de servicios de procesamiento y las relaciones con terceros.

ARTÍCULO 21. ORGANIGRAMA DE LA SEGURIDAD DE LA INFORMACIÓN

El máximo organismo en materia de seguridad de la información, será el Comité del Sistema de Gestión de Seguridad de la Información, cuya conformación, funciones, objetivos, sesiones y obligaciones se establecieron mediante un acto administrativo firmado por el Director General de la Policía Nacional.

ARTÍCULO 22. RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Para una adecuada gestión de la seguridad de la información, a continuación se definen los responsables de la seguridad de la información

- **Comité del Sistema de Gestión de Seguridad de la Información.** El coordinador del comité es el responsable de impulsar la implementación del manual de la seguridad de la información en la Policía Nacional. El comité de seguridad de la información tiene a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la Dirección General, el seguimiento de análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de continuidad, concienciación en materia de seguridad y asignación de funciones.

- **Área Administración de la Información.** Asiste a los funcionarios de la Policía Nacional y terceros en materia de seguridad de la información y coordina la interacción con entidades especializadas. Así mismo, en asocio con los propietarios de los activos de información, analiza el riesgo de los accesos de terceros a la información institucional y verifica la aplicación de las medidas de seguridad necesarias para la protección de la misma.

- **Área de Control Interno**. Realiza revisiones independientes sobre la vigencia y el cumplimiento de las políticas impartidas en este manual.

- **Encargados de Contratación**. Incluyen en los contratos con proveedores de servicios de tecnología y cualquier otro bien o servicio cuya actividad afecte directa o indirectamente los activos de información, la obligatoriedad de cumplimiento de la Política de Seguridad de la información y todo lo que con ella esté relacionado.

- **Secretaría General**.Verifica la inclusión de la presente política en acuerdos u otra documentación de la institución con terceros.

- **Oficina De Telemática**. Autoriza y supervisa la incorporación de nuevos recursos a la plataforma tecnológica de la Policía Nacional.

ARTÍCULO 23. PROCESO DE AUTORIZACIÓN PARA INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN

La adquisición de nuevos recursos y servicios tecnológicos de Tecnologías de la Información y las Comunicaciones son autorizados por el proceso de Direccionamiento Tecnológico y deben estar acordes a recomendaciones de seguridad establecidas por el proceso de Administración de la Información.

Nadie podrá adquirir software y hardware sin la autorización de la Jefatura de la Oficina de Telemática.

Cuando existan diferencias entre la Política de Seguridad y el Direccionamiento Tecnológico, se debe tomar una decisión concertada que satisfaga la Política de Seguridad.

Los recursos de procesamiento de información de terceros, dentro del alcance de un contrato deben ser avalados por el Área de Administración de la Información o quien haga sus veces en cada una de las dependencias.

No se permite el uso de procesamiento de información personal en la infraestructura tecnológica de la Policía Nacional.

ARTÍCULO 24. ASESORAMIENTO ESPECIALIZADO EN MATERIA EN SEGURIDAD DE LA INFORMACIÓN

El Área de Administración de la Información debe coordinar los conocimientos y experiencias que ha adquirido la institución, con el fin de brindar asesoría en la toma de decisiones en materia de seguridad de la información. Así mismo puede asesorarse con otros organismos y establecer convenios de cooperación.

ARTÍCULO 25. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

El Área de Control Interno o un organismo auditor externo, realiza revisiones independientes sobre el cumplimiento de la Política de Seguridad de la Información.

ARTÍCULO 26. RELACIÓN CON TERCEROS

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 y/o 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 los acuerdos de confidencialidad y acuerdos de intercambios de información con personal externo, unidades y dependencias.

- 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, el Asesor Jurídico, el Jefe del Grupo de Telemática y el Jefe del Grupo de Gestión Documental de cada unidad; con el fin de establecer la viabilidad

de permitir el acceso a la información, para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

- El acceso a la información deberá ceñirse a los parámetros establecidos en el procedimiento 2IN-PR-0007 "Entrega de Información Bajo Deber de Reserva", proceso de gestión documental y sus procedimientos asociados.

CAPÍTULO 4

GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

ARTÍCULO 27. ACTIVOS DE INFORMACIÓN.

La información que se produzca, procese, transmita y almacene por cualquier funcionario o tercero vinculado a la institución le pertenece a la Policía Nacional y esta puede ser verificada sin previo consentimiento del funcionario responsable del activo. (Bajo la discrecionalidad del propietario de la información o bajo requerimiento judicial).

ARTÍCULO 28. INVENTARIO DE ACTIVOS

Los dueños de los procesos o quien haga sus veces deben identificar y elaborar un inventario de los activos de información aplicando el procedimiento 2IN-PR-0001 "Identificación y protección de los activos de la información", proceso de gestión documental y sus procedimientos asociados y designar un funcionario, responsable de consolidar y administrar los activos de información.

En este inventario se debe identificar el propietario de cada activo quien es el responsable de:

- Realizar un análisis de riesgos como mínimo una vez al año, de los activos de información de su proceso.
- Tomar decisiones y acciones para eliminar, mitigar, transferir o aceptar los riesgos.
- Verificar anualmente o cada vez que lo amerite, el inventario de los activos de información con el fin de mantener actualizados.
- Clasificar la información de acuerdo a la importancia de esta.
- Revisar anualmente la clasificación de sus activos y re-clasificarlos de ser necesario.
- Almacenar y manejar su información de acuerdo con el nivel de clasificación.

ARTÍCULO 29 CLASIFICACIÓN DE LA INFORMACIÓN

La información de la Policía Nacional se clasifica según su confidencialidad, integridad y disponibilidad de acuerdo con la sensibilidad e importancia de ésta.

- **Según su confidencialidad**

La información se clasificará según su confidencialidad de la siguiente manera:

5. ULTRASECRETO: información pertinente a actividades o planes de la defensa nacional interna o externa y/o a operaciones de inteligencia, cuya divulgación no autorizada podría conducir a un rompimiento diplomático que afecte los intereses de la Nación, a un ataque armado o a destruir la estabilidad interna.

SECRETO: información pertinente a una actividad o planes de defensa nacional interna o externa y a operaciones de inteligencia relativas a la misma, cuya divulgación no autorizada podría afectar las relaciones diplomáticas, lesionar el prestigio del país o poner en peligro la estabilidad interna.

4. RESERVADO: información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la Institución, proporcionar ventajas a la amenaza actual o potencial, o causar bajas o pérdidas propias en acciones de defensa nacional.

3. CONFIDENCIAL: información que por su contenido solo interesa a quienes va dirigida y cuya divulgación no autorizada puede ocasionar perjuicios a una unidad o persona.

2. INTERNO: es aquella información dirigida a los miembros de la Institución, cuya divulgación, uso, alteración o destrucción podría resultar en pérdidas recuperables para la institución, pero implica asuntos de conveniencia, facilidad de la operación, credibilidad o reputación u otros asuntos relacionados con la privacidad.

1. PÚBLICA: información entregada o publicada sin restricciones, sin que esto conlleve un impacto negativo de ninguna índole para la institución.

- **Según su integridad**

La información se clasificará según su integridad de la siguiente manera:

5. No puede repararse y ocasiona pérdidas graves para el país.
4. No puede repararse y ocasiona pérdidas graves para la institución.
3. Difícil reparación y pérdidas significativas.
2. Puede repararse, pérdidas leves.
1. No afecta la operación y puede repararse fácilmente.

- **Según su disponibilidad**

La información se clasificará según su disponibilidad de la siguiente manera:
Es necesario determinar el tiempo máximo tolerable MTD de indisponibilidad que puede soportar la Policía Nacional sin un activo determinado, para lo cual se tendrá en cuenta la siguiente clasificación:

5. **CRÍTICOS**, la interrupción es de minutos y hasta 12 horas.

4. **URGENTE**, la interrupción hasta por 24 horas.

3. **IMPORTANTE**, interrupción hasta por 72 horas.

2. **NORMAL**, interrupción de hasta siete días

1. **NO ESENCIALES**, la interrupción es de hasta 30 días

ARTÍCULO 30. ROTULADO DE LA INFORMACIÓN

Todos los documentos físicos o digitales expedidos por la Policía Nacional, están rotulados de acuerdo al esquema de clasificación definido en el artículo 29, según su confidencialidad.

Se establecerán procedimientos para la reclasificación de la información y su destrucción segura.

CAPÍTULO 5

SEGURIDAD DEL TALENTO HUMANO

El talento humano es el activo más importante de la Policía Nacional y es el responsable de producir, administrar e interactuar con los activos de información, por esto la importancia de contar con personal idóneo para desempeñar las funciones para los cuales han sido vinculados a la institución; así mismo se requiere su compromiso y conocimiento con respecto a la seguridad de la información.

ARTÍCULO 31. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades con respecto a la seguridad de la información se evidencian en el Manual de Funciones de la Policía Nacional en el Formato " Descripción de cargos y perfiles " el generado en el SIATH.

ARTÍCULO 32. SELECCIÓN

Las verificaciones para confirmar la veracidad de la información suministrada por el personal que se postula como candidato a ingresar a la Policía Nacional, antes de su vinculación definitiva se realiza acorde con lo establecido en el proceso 2SP-CP-0001 seleccionar el Talento Humano para la Policía Nacional.

ARTÍCULO 33. TÉRMINOS Y CONDICIONES LABORALES

Todos los funcionarios de planta, prestación de servicios o cualquier otro tipo de vinculación con la institución, firman un acta de aceptación del Manual de Seguridad de la Información de la Policía Nacional, el cual hará parte de su hoja de vida y anexo al acta de posesión. El personal externo firma los acuerdos de confidencialidad para terceros y los documentos de cumplimiento del Manual de Seguridad de la Información de la Policía Nacional y hace parte integral del contrato o acuerdo de cooperación.

ARTÍCULO 34. CONCIENCIACIÓN A LOS USUARIOS

La Policía Nacional en su interés por garantizar que sus funcionarios, así como el personal externo vinculado a la institución, cuenten con el nivel deseado de conocimiento para la correcta gestión de los activos de información, diseño y ejecuta de manera permanente un programa de concienciación en seguridad de la información para promover la protección, uso y procesamiento de la información; a cargo de la Dirección de Talento Humano, la Dirección Nacional de Escuelas y la Oficina de Telemática.

Se promueve constantemente la importancia de la seguridad de la información en los funcionarios de la Policía Nacional, adopción de conciencia y cumplimiento del Manual de Seguridad de la Información, normas, procedimientos y estándares para la seguridad de la información, establecidos por la Institución que protegen y regulen sus activos de información, así como las responsabilidades legales que rigen sobre los mismos; lo cual se realiza a través de la implementación de un módulo evaluable dentro del pensum académico de las escuelas de formación y capacitación, así como foros, diplomados, blogs, seminarios entre otros.

Todos los funcionarios de la Policía Nacional y el personal externo, que por sus funciones hacen uso de recursos tecnológicos, asisten a los entrenamientos y charlas que se programan en temas relacionados con la seguridad de la información y aplican las recomendaciones allí impartidas en sus labores diarias.

Todos los funcionarios son evaluados en seguridad de la información anualmente y aquellos que no aprueban dichas evaluaciones, no pueden desempeñar cargos que conlleven la manipulación de información sensible; esta evaluación está a cargo de la Dirección Nacional de Escuelas.

ARTÍCULO 35. PERSONAL QUE SE ENCUENTRA EN SITUACIONES ADMINISTRATIVAS TALES COMO (LICENCIAS, VACACIONES, EXCUSAS DE SERVICIO, TRASLADO, RETIRO, DESAPARICIÓN, SECUESTRO, ENTRE OTRAS)

La Dirección de Talento Humano a través de los grupos de talento humano de cada unidad, actualiza en tiempo real las novedades de cada funcionario, en el SIATH, para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados.

Quien tiene personal externo bajo su supervisión informa de manera inmediata a la Oficina de Telemática y a las Áreas o Grupos encargados de la seguridad de la información de la terminación del contrato, para la remoción de derechos de acceso sobre los recursos tecnológicos, sistemas de información y acceso físico a las instalaciones.

Se verifica periódicamente las novedades del personal y se procede a bloquear las cuentas de acceso en los recursos tecnológicos, sistemas de información y acceso a instalaciones de la institución.

Todos los usuarios están en la obligación de entregar su puesto de trabajo al funcionario designado por su jefe inmediato, junto con la copia de la información crítica que maneja. De igual manera, hacen entrega de todos los recursos tecnológicos y otros activos que les fueron suministrados en el momento de su vinculación.

ARTÍCULO 36. ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

A continuación se describen algunas acciones identificadas que afectan la seguridad de la información, y que ponen en riesgo la disponibilidad, confidencialidad e integridad de la misma, así:

- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a la Policía Nacional, ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible para la Institución.
- No clasificar y/o etiquetar la información.
- No guardar bajo llave, documentos impresos que contengan información clasificada, al terminar la jornada laboral.
- Hacer uso de la red de datos de la Institución, para obtener, mantener o difundir material publicitario o comercial, así como distribución de cadenas de correos.
- Instalar software en la plataforma tecnológica de la Policía Nacional, cuyo uso no esté autorizado por el comité de cambios de la Oficina de Telemática de la Dirección General, que puedan atentar contra las leyes de derechos de autor o propiedad intelectual.
- Destruir la documentación institucional, sin seguir los parámetros establecidos en el manual de Gestión Documental.
- Descuidar información clasificada de la institución, sin las medidas apropiadas de seguridad que garanticen su protección.
- Enviar información clasificada como no pública de la institución a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información clasificada como no pública por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
- Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la Policía Nacional.
- Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la Policía Nacional.
- Conectar dispositivos de red para acceso inalámbricos a la red de datos institucional.
- Ingresar a la red de datos institucional por cualquier servicio de acceso remoto sin la autorización de la Oficina de Telemática.
- Usar servicios de internet en los equipos de la institución, diferente al provisto por el proceso de Direccionamiento Tecnológico o autorizado por este.
- Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos de la Policía Nacional para beneficio personal.
- Uso de la identidad policial digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario.
- Descuidar dejando al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias de la Policía Nacional.
- Retirar de las instalaciones de la institución, computadores de escritorios, portátiles e información física o digital, clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información clasificada de la Policía Nacional a personas o entidades no autorizadas.
- Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de la Policía Nacional o de terceras partes.
- Ejecutar cualquier acción que difame, afecte la reputación o imagen de la Policía Nacional o alguno de sus funcionarios desde la Plataforma Tecnológica de la Institución.
- Realizar cambios no autorizados en la Plataforma Tecnológica de la Policía Nacional.
- Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.
- Ejecutar acciones para eludir y/o modificar los controles establecidos en el presente manual.
- Comer, beber y fumar cerca a los equipos de cómputo.
- Conectar dispositivos diferentes a equipos de cómputo, a la corriente regulada.
- Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La realización de alguna de estas prácticas u otras que afecten la seguridad de la información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso.

CAPÍTULO 6

SEGURIDAD FÍSICA Y AMBIENTAL

La seguridad física y del entorno busca proteger los activos de información de las amenazas naturales y ambientales como inundaciones, terremotos, tormentas, tornados e incendios; de las amenazas por interrupción de servicios públicos; de las amenazas artificiales como acceso no autorizado (tanto internos como externos), explosiones, daños por empleados, vandalismo, fraude, robo, y finalmente de las amenazas por motivos políticos como huelgas, disturbios, desobediencia civil, ataques terroristas y bombardeos.

ARTÍCULO 37. SEGURIDAD *FÍSICA* Y DEL ENTORNO

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, tanto en Direcciones de Policía, Comandos de Policía, Escuelas de Policía, Estaciones de Policía, Subestaciones de Policía, Centros de Atención Inmediata, áreas restringidas, áreas de carga y descarga, así como entornos abiertos. Del mismo modo, controla las amenazas físicas externas e internas y las condiciones medioambientales de sus instalaciones.

El protocolo de seguridad de instalaciones, tiene en cuenta los siguientes aspectos:

- Antecedentes.
- Ubicación y límites.
- Características topográficas.
- Características de la población.
- Problemática social.
- Análisis del índice delincuencial.
- Vías de acceso.
- Unidades de apoyo.
- Estructura arquitectónica.
- Distribución interna.
- Barreras perimetrales.
- Sistemas de vigilancia y control.
- Controles de acceso.
- Plan de emergencia.
- Seguridad en áreas de procesamiento y/o almacenamiento de información sensible.
- Seguridad industrial.
- Salud ocupacional.

Y los demás aspectos necesarios que garanticen el fortalecimiento de la seguridad física de las instalaciones.

ARTÍCULO 38. ÁREAS SEGURAS

Las áreas seguras y sus controles están definidos de acuerdo a los lineamientos establecidos en el Manual De Seguridad Física y del Entorno.

ARTÍCULO 39. SEGURIDAD DE LOS EQUIPOS

Los equipos de cómputo son ubicados y protegidos para reducir la exposición a riesgos ocasionados por amenazas ambientales y oportunidades de acceso no autorizado.

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

- Los equipos de cómputo tipo servidor de cada unidad, están agrupados en un solo lugar. Estos lugares cuentan con controles de accesos físicos y ambientales.

- Los equipos de cómputo donde se procesa información clasificada en nivel tres (3) o superior, se ubican de tal manera que el monitor no pueda visualizarse a través de ventanas o paredes de vidrio.

- Los equipos de cómputo, se ubican de tal manera que se reduce el riesgo de visualización de la información por personas no autorizadas, durante su uso.

- El acceso a los centros de procesamiento y almacenamiento está restringido y su acceso está documentado a través de un procedimiento.

ARTÍCULO 40. SUMINISTRO DE ENERGÍA

Los centros de procesamiento de datos están protegidos con respecto a posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía está de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía.

Se tiene en cuenta los siguientes controles:

- Los sistemas eléctricos están documentados mediante planos que cumplen con las especificaciones de las normas que apliquen al respecto.

- Se disponen de múltiples toma corrientes o líneas de suministro.

- Se cuenta con un Suministro Redundante De Energía Ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la institución. La determinación de dichas operaciones críticas, son el resultado del análisis de impacto realizado por el Grupo de Seguridad de la información en conjunto con los responsables de los procesos. Los planes de continuidad de negocio y recuperación de desastres contemplan las acciones que han de emprenderse ante una falla de la UPS.

- Los equipos de Suministro Redundante De Energía Ininterrumpible (UPS) son inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida de los cual se deja evidencia documental. Así mismo se verifica que los niveles de carga no superen los establecidos por las normas.

- Se han instalado generadores de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Se realiza un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis es realizado por el Grupo de Seguridad de la información en conjunto con los responsables de los procesos. Se dispone de un adecuado suministro de combustible y mantenimiento para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegura que el tiempo de funcionamiento del Suministro Redundante De Energía Ininterrumpible (UPS) permite el encendido manual de los mismos. Los generadores son inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

- Las instalaciones eléctricas están protegidas por sistemas de tierras de protección, que cumplen con los estándares vigentes para sistemas de comunicaciones.

- Toda instalación eléctrica está protegida contra fluctuaciones de voltaje por dispositivos adecuados tales como breakers y supresores de picos.
- Las instalaciones eléctricas para sistemas de comunicaciones están debidamente aisladas y protegidas contra eventos relacionados con humedad, filtraciones de agua y agentes químicos que lo puedan deteriorar o causar fallas.

- Los interruptores de emergencia están ubicados cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.

- Se cuenta con iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

- Se cuenta con protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

ARTÍCULO 41. SEGURIDAD DEL CABLEADO

Para el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información para protegerlos contra intercepción o daño:

- Se cumple con el reglamento técnico de instalaciones eléctricas – RETIE, expedido por el Ministerio de Minas y Energía.

- Se cumple con 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 albergan en sitios acondicionados a temperaturas entre 16 y 22 grados centígrados.

- Los centros de cableado cuentan con rack 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 se realizan siguiendo la arquitectura de los edificios, debidamente protegidos con canaleta en caso de instalación interior, o con tubo metálico en caso de instalación tipo intemperie.

ARTÍCULO 42. MANTENIMIENTO DE LOS EQUIPOS

El mantenimiento a la plataforma tecnológica posibilita su disponibilidad e integridad, teniendo en cuenta los siguientes controles:

- Mantenimiento preventivo a los equipos de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.

- Uso de un sistema de información que permite llevar el control del detalle de la frecuencia de mantenimiento de los equipos.

- Sólo el personal de mantenimiento autorizado puede llevar a cabo reparaciones en los equipos.

- El responsable técnico de los equipos registra de todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

- El responsable técnico de los equipos registra el retiro los equipos de las instalaciones de la Policía Nacional para su mantenimiento.

- En las especificaciones técnicas para contratos de mantenimiento o garantía se contempla el suministro de nuevos discos sin realizar la entrega del disco dañado.

- Eliminación de manera segura la información confidencial que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de respaldo.

- El responsable funcional del equipo acompañará el mantenimiento de los equipos que contengan información sensible.

ARTÍCULO 43. SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

El uso de equipos institucionales, fuera de las instalaciones policiales, está restringido a equipos portátiles y móviles, y su uso está regulado por el procedimiento de uso de dispositivos móviles.

La seguridad para estos equipos es equivalente a la suministrada dentro de las instalaciones policiales y controles adicionales, para mitigar los riesgos que por sí mismo conlleva el uso estos, así:

- Los equipos móviles institucionales, no pueden conectarse a redes inalámbricas públicas o no conocidas.

- El software instalado en los dispositivos móviles está totalmente licenciado y avalado por la Oficina de Telemática.

- El acceso a los equipos móviles se realiza mediante el uso de usuario y password.

- La información almacenada en los equipos de cómputo portátiles, está cifrada.

ARTÍCULO 44. DESTRUCCIÓN O REUTILIZACIÓN SEGURA DE EQUIPOS

Se realiza borrado seguro de la información o destrucción física del dispositivo de almacenamiento, antes de la reutilización o devolución de cualquier equipo de cómputo.

El borrado seguro y destrucción de dispositivos de almacenamiento, está regulado por el procedimiento de destrucción o reutilización segura de equipos.

ARTÍCULO 45. NORMAS DE ESCRITORIOS Y PANTALLAS LIMPIAS

Estas normas tienen como fin reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

Para lo cual se establecen las siguientes pautas:

- Almacenar bajo llave, los documentos en papel y los dispositivos de almacenamiento removibles, en cajones y/u otro tipo de archivos seguro cuando no están siendo utilizados, especialmente fuera del horario laboral.

- Guardar bajo llave la información clasificada en nivel 3 o superior (preferiblemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso.

- Bloquear la sesión de los computadores personales cuando no se está usando. El protector de pantalla se activa en forma automática después de cinco (5) minutos de inactividad.

- Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.

- Bloquear las fotocopiadoras fuera del horario normal de trabajo.

- Retirar inmediatamente la información sensible, una vez impresa.

- El escritorio de los equipos de cómputo no deben tener accesos directos a archivos.

ARTÍCULO 46. RETIRO DE BIENES DE LAS INSTALACIONES

Para el retiro de los equipos, software e información de las instalaciones policiales, estará documentado para tal fin.

Se realizarán verificaciones periódicas, para detectar el retiro no autorizado de activos.

CAPÍTULO 7

GESTIÓN DE LAS COMUNICACIONES Y LAS OPERACIONES

El proceso de Direccionamiento Tecnológico de la Policía Nacional, es el encargado de la operación y administración de la plataforma tecnológica como soporte a los procesos de la institución, asigna funciones específicas a sus funcionarios quienes deben garantizar la adecuada operación y administración de dicha plataforma. Así mismo, vela por la eficiencia de los controles implantados en los procesos y procedimientos asociados con el objeto de garantizar la confidencialidad, la integridad y la disponibilidad de la información.

Los cambios efectuados sobre la plataforma tecnológica, están adecuadamente controlados y debidamente autorizados por el comité de cambios.

A continuación se establecen responsabilidades con respecto a la gestión y operaciones tecnológicas:

1. La Oficina de Telemática o Grupos de Telemática y los Grupos de Contratos, evalúan los contratos y acuerdos con terceros para garantizar la incorporación de aspectos relativos a la seguridad de la información involucrada en la gestión de productos y servicios prestados a la Policía Nacional.

2. Los Propietarios de Activos de Información en acuerdo con la Oficina de Telemática o Grupos de Telemática, establecen las necesidades de seguridad para cada activo, según la clasificación de estos.

ARTÍCULO 47. DOCUMENTACIÓN DE LOS PROCEDIMIENTOS TECNOLÓGICOS

Los procedimientos tecnológicos identificados en este Manual de Seguridad de la Información y sus cambios son avalados por el dueño del proceso de Direccionamiento Tecnológico y acordes con el control de documentos, así:

- Control de cambios sobre la plataforma tecnológica.
- Aprobación, implementación de nuevos productos y servicios tecnológicos.
- Instalación de nuevas versiones/actualizaciones.
- Manejo de incidentes y vulnerabilidades.
- Uso correcto del correo electrónico, usuario empresarial, certificado digital.
- Administración de identidades.
- Entrega de información bajo deber de reserva.
- Protección contra software malicioso.
- Detección y prevención de intrusos.
- Concienciación de usuarios.
- Protección de usuarios con altos privilegios.
- Uso de dispositivos de almacenamiento extraíbles.
- Elaboración y recuperación de copias de respaldo.
- Borrado seguro de información.
- Eliminación de dispositivos de almacenamiento.
- Gestión de log's.
- Reinicio del sistema y procedimientos de recuperación ante fallas.

- Instalación y mantenimiento de equipos de procesamiento y comunicaciones.
- Instalación y mantenimiento de plataformas de cómputo.
- Monitoreo del procesamiento y comunicaciones.
- Administración de claves de equipos de comunicación y las demás que sean necesarios para el correcto funcionamiento de la plataforma tecnológica institucional.

ARTÍCULO 48. CONTROL DE CAMBIO EN LAS OPERACIONES

Todo cambio es evaluado previamente tanto en los aspectos técnicos como de seguridad acorde con el procedimiento control de cambios sobre la plataforma tecnológica.

Las diferencias entre funcionalidad y seguridad se ajustan a decisiones arquitecturales que satisfacen los requisitos mínimos de seguridad.

Los registros de los cambios son documentados y contemplan los siguientes puntos:

1. Identificación y registro de cambios significativos.
2. Análisis de riesgo del cambio.
3. Aprobación formal del cambio, en junta de comité de cambios.
4. Planificación del proceso de cambio.
5. Prueba del nuevo escenario.
6. Comunicación del cambio a todas las partes interesadas
7. Identificación de los responsables del cambio
8. Procedimiento para cancelación del cambio en caso de fallo.
9. Verificación del cambio realizado.

ARTÍCULO 49. PROCEDIMIENTO MANEJO DE INCIDENTES

El manejo de incidentes se realiza acorde con el procedimiento 2IN-PR-0005 "Atención a Incidentes", el cual garantiza una respuesta rápida, eficaz y sistemática a los incidentes relativos a la seguridad de la información.

Los incidentes que así lo requieran cuentan con la asesoría de Policía Judicial, para el manejo de la evidencia digital y posible judicialización.

ARTÍCULO 50. DISTRIBUCIÓN DE FUNCIONES

Las unidades en donde se construye software, en lo posible se segregan las funciones de desarrollo, pruebas y producción, impidiendo el acceso de los funcionarios de un ambiente a otro. Esto con el fin de minimizar el riesgo de uso no autorizado o fallas por cambios no previstos.

De no ser posible la segregación de funciones, por razones presupuestales, de personal o capacitación, se implementan controles adicionales como:

- Todos los sistemas cuentan con un modulo de auditoría, que permite almacenar los registros de transacciones realizados desde la interfaz de usuario final o desde cualquier otra herramienta.

- Todos los equipos de procesamiento y comunicaciones tiene activos los archivos de log's y se envían a un syslog.

- El área de control interno supervisa y monitorea las transacciones realizadas sobre los sistemas y equipos de procesamiento y comunicaciones.

Se documenta de manera formal la razón por la cual no es posible segregar funciones.

Se asegura la independencia entre el inicio de una actividad y su autorización, para evitar la posibilidad de conspiración para un fraude.

ARTÍCULO 51. SEPARACIÓN DE AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN.

Los ambientes de desarrollo, pruebas y producción, en lo posible estarán separados preferiblemente en forma física o virtualizados la transferencia de software del ambiente de pruebas al ambiente de producción será documentado.

Para lo cual se aplican los siguientes controles:

- Ejecutar el software de desarrollo y producción en diferentes ambientes.
- Las actividades de desarrollo y pruebas deberán realizarse en ambientes separados.
- Los datos de producción no deberán usarse en ambientes de desarrollo o pruebas.
- No usar compiladores, editores y otros utilitarios que no sean necesarios para el funcionamiento de los ambientes de producción.
- El personal de desarrollo no tendrá acceso al ambiente de producción, a menos que sea estrictamente necesario y deberá quedar documentado los accesos que se realicen.

ARTÍCULO 52. GESTIÓN DE LA PRESTACIÓN DE SERVICIOS POR TERCERAS PARTES

La tercerización de la plataforma tecnológica de la Policía Nacional, está supeditada a los controles establecidos en el contrato, contemplando las especificaciones descritas en el artículo 26 relación con terceros.

Así mismo se contemplan las siguientes premisas, antes de tercerizar los servicios de procesamiento:

- Identificación de los riesgos de aquellos servicios y/o infraestructura que se quieran tercerizar.
- Contar con la aprobación de los dueños de los activos de información.
- Identificación de las aplicaciones que manejan información clasificada de la institución con el fin de contemplar medidas de seguridad más fuertes antes de su tercerización.
- Monitoreo permanente con el fin de evaluar el cumplimiento de los acuerdos de niveles de servicio.
- Definición de las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

ARTÍCULO 53. PLANIFICACIÓN DE LA CAPACIDAD

El proceso de Direccionamiento Tecnológico de la Policía Nacional, realiza un análisis estadístico anualmente para generar líneas base que le permitan proyectar necesidades de crecimiento en procesamiento, almacenamiento y transmisión de la información, con el fin de evitar inconvenientes que se convierten en una amenaza a la seguridad o a la continuidad de los servicios prestados.

ARTÍCULO 54. ACEPTACIÓN DEL SISTEMA

El proceso de Direccionamiento Tecnológico de la Policía Nacional, realiza pruebas a los sistemas antes de su salida a producción teniendo en cuenta lo siguiente:

- Analiza cómo afecta el nuevo sistema o sus actualizaciones la capacidad de procesamiento y almacenamiento los sistemas actuales.
- Garantiza la recuperación ante errores.
- Cuenta con mecanismos de restauración del sistema a su estado inicial antes del cambio.
- Valida que el nuevo sistema no afecta a los sistemas actuales de producción.
- Somete a pruebas de calidad antes de salir a producción.
- Capacita a los usuarios de los nuevos sistemas sobre su uso.

ARTÍCULO 55 PROTECCIÓN CONTRA CÓDIGO MALICIOSO

El proceso de Direccionamiento Tecnológico de la Policía Nacional, implementa controles para prevenir y detectar código malicioso, lo cual se basa en software, concienciación de usuarios y gestión del cambio.

Los controles implementados contemplan las siguientes directrices:

- No permite el uso de software no autorizado por la Oficina de Telemática.
- No permite el intercambio de información a través de archivos planos.
- No compartir carpetas en los equipos de cómputo.
- Instala y actualiza software de detección y reparación de virus, IPS de host, anti-spyware examinado computadores y medios informáticos, como medida preventiva y rutinaria.
- Mantiene los sistemas con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.
- Revisa periódicamente el contenido de software y datos de los equipos de procesamiento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verifica antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Concientiza al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

El responsable del ciclo de vida de la información, junto con los propietarios de los activos de información determina los requerimientos de respaldo, según el nivel de criticidad de la información y control de registros.

El procedimiento de resguardo de la información, incluye actividades de prueba de recuperación de la información. Las instalaciones de resguardo garantizan las condiciones de seguridad y ambientales necesarias para la conservación de los respaldos.

El procedimiento de respaldo contempla las siguientes directrices:

- Un esquema de rótulo de las copias de respaldo, para permitir su fácil identificación.
- Destrucción de las copias de respaldo, cuando se venza la vida útil de los medios de almacenamiento, de acuerdo al procedimiento de destrucción o reutilización segura de equipos.

- Almacenamiento de las copias de respaldo en un lugar fuera de las instalaciones del lugar de origen de la información, con un registro exacto y completo de cada una de ellas, así como los procedimientos de restauración.

- Almacenamiento de al menos 5 ciclos de información de copias de respaldo para la información con nivel de clasificación igual o superior a 3 (artículo 29 clasificación de la información). O acorde con lo que ordene la legislación vigente, para las entidades del estado.

- La información respaldada en el sitio alterno considera los niveles de clasificación. (artículo 29 clasificación de la información).

- Almacenamiento de las copias de respaldo en condiciones de seguridad y ambientales adecuadas, consistentes a las aplicadas al sitio principal.

- Pruebas periódicas de la restauración de los medios de respaldo, según lo estipulado en el Plan de Continuidad del Negocio.

ARTÍCULO 56. CONTROLES DE LAS REDES

El proceso de Direccionamiento Tecnológico define los controles de seguridad de la red de datos Institucional, para lo cual usa como referencia el estándar ISO/IEC 18028 Tecnologia de la información-Tecnicas de seguridad – la seguridad de TI de la Red.

Estos controles contemplan salvaguardas especiales para:

- Los equipos activos de las redes LAN, de las unidades de Policía a nivel nacional.
- Mantener la disponibilidad de los servicios de red e infraestructura tecnológica conectada a ella.
- Transmisión de información a través de redes públicas.
- Acceso a la red institucional, desde otras redes.
- Intercambio de información interinstitucional con el sector público y privado.
- Garantizar la trazabilidad de las conexiones a la red institucional.
- Supervisión del cumplimiento de los controles implementados.

ARTÍCULO 57. SEGURIDAD DE LOS SERVICIOS DE RED

Los servicios de red provenientes de un tercero, se ajustan al artículo 26 relación con terceros.

Los acuerdos de niveles de servicio contemplan, características de seguridad, requisitos de gestión de los servicios de red y valores agregados en dispositivos de seguridad.

Así mismo están documentados los procedimientos para:

- Chequeo del tráfico de la red.
- Monitoreo de los puertos en la red.
- Auditoría, trazabilidad y respaldo de archivos de log's.

ARTÍCULO 58. MANEJO DE LOS MEDIOS DE ALMACENAMIENTO

Los medios de almacenamiento, se controlan de forma física, para evitar el mal uso o fuga de la información contenida en dichos dispositivos. Solo está permitido el uso de dispositivos de almacenamiento institucionales que serán gestionados de forma centralizada.

ARTÍCULO 59. GESTIÓN DE LOS MEDIOS DE ALMACENAMIENTO

Para proveer niveles mínimos de seguridad, para la gestión de medios de almacenamiento removibles, se implementaron controles que consideren las siguientes directrices:

- Uso de medios removibles, provistos por la Policía Nacional.
- Cifrado de la información contenida en medios de almacenamiento removibles.
- Eliminación segura de los contenidos, de manera que no sea posible su recuperación.
- Control del retiro de los medios, fuera de las instalaciones policiales.
- Inventario de los medios de almacenamiento.
- Restringir el uso de medios removibles, a los estrictamente necesarios, para cumplir la misionalidad de la institución.
- Almacenar todos los medios en un ambiente controlado y protegido, siguiendo las recomendaciones del fabricante.

ARTÍCULO 60. ELIMINACIÓN DE LOS MEDIOS DE ALMACENAMIENTO

La eliminación de los medios de almacenamiento, se realiza considerando el borrado seguro, para aquellos dispositivos que así lo permitan. La destrucción segura se documenta mediante acta, registro fílmico y fotográfico.

El procedimiento establecido para la eliminación segura de medios de almacenamiento, garantizar la no restauración o recuperación de información.

Ver artículo 44 destrucción o reutilización segura de equipos.

ARTÍCULO 61. PROCEDIMIENTO PARA EL MANEJO DE INFORMACIÓN

Para el intercambio de información, se utiliza el procedimiento 2IN-PR-0007 Entrega Información Bajo Deber Reserva, así mismo se documentan los controles adicionales que contemplen:

- Sistemas informáticos, redes, computación y comunicaciones móviles, correo electrónico, comunicaciones de voz, servicio de correo tradicional, fax e impresoras.
- Uso de modelos de control de acceso.
- Registro de los receptores de información clasificada en nivel 3 o superior.

ARTÍCULO 62. SEGURIDAD EN LA DOCUMENTACIÓN DEL SISTEMA

La documentación de los sistemas se clasifica en nivel 3 y su acceso estará restringido a las personas que lo requieran, para su mantenimiento.

La documentación de los sistemas esta bajo la custodia de la Oficina de Telemática, Grupos de Telemática y Centros de Protección de Datos, quienes aplican los controles necesarios para su protección.

ARTÍCULO 63. INTERCAMBIO DE INFORMACIÓN

El intercambio de información al interior de la Policía Nacional se realiza aplicando el procedimiento 2IN-PR-0007 Entrega Información Bajo Deber de Reserva y otras entidades bajo acuerdos de cooperación u órdenes judiciales.

ARTÍCULO 64. ACUERDOS DE INTERCAMBIO DE INFORMACIÓN Y SOFTWARE

El intercambio de información y software con otras entidades, se realiza previa celebración de convenio interadministrativo en el que se establecen clausulas de responsabilidad, deberes y derechos.

En todo caso, estos acuerdos deben velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo se especifican las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de la misma.

Las partes firman acuerdos de confidencialidad y siguen el procedimiento 2IN-PR-0007 entrega información bajo deber reserva.

Cuando la información sea solicitada por autoridad judicial o administrativa competente, la entrega se realiza siguiendo el procedimiento 2IN-PR-0007 entrega información bajo deber reserva.

El intercambio de información contempla las siguientes directrices:

- Uso de web services, para la publicación y consumo de información electrónica.
- Uso de canales cifrados.
- Respeto por los derechos de autor del software intercambiado, por tratarse de un bien fiscal de la entidad.
- Términos y condiciones de la licencia bajo la cual se suministra el software.
- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendida por el receptor de la información.
- Informar al titular de los datos, el intercambio de estos con otras entidades.
- Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

ARTÍCULO 65. MEDIOS FÍSICOS EN TRÁNSITO

El transporte de información en medios físicos (digital o impresa) contempla mecanismos que no permiten su uso no autorizado, preservando así la confidencialidad, integridad y disponibilidad de la misma.

Los controles establecidos para el transporte de información, contemplan:

1. Uso de servicios de mensajería, a través de contratos formales, donde se establecen los acuerdos de niveles de servicio que contemplen los mecanismos de seguridad que deben ser proporcionado por el contratista.

2. Los acuerdos de niveles de servicio, contemplan como mínimo:

    - Uso de recipientes cerrados.
    - Entrega certificada.
    - Embalaje con sellos de seguridad o a prueba de apertura no autorizada.
    - Uso de rutas diferentes, para las entregas.

3. La entrega física de información realizada por funcionarios de la institución, cumplen con los mismas características, estipulados en el ítem anterior.

ARTÍCULO 66. MENSAJERÍA ELECTRÓNICA

La mensajería electrónica en la Policía Nacional, está asociada a los servicios de correo electrónico de los dominios @policia.gov.co, @correo.policia.gov.co, @dipol.gov.co @correo.dipol.gov.co y a la plataforma de comunicaciones unificada, está regulada por los terminos de uso adecuado.

ARTÍCULO 67. SISTEMAS DE INFORMACIÓN INSTITUCIONALES

Antes de la interconexión de sistemas de información se realiza un análisis de vulnerabilidades que permita establecer los posibles puntos de falla que no satisfagan las condiciones de confidencialidad, integridad y disponibilidad; los cuales son ser corregidos en la medida de lo posible.

ARTÍCULO 68. SISTEMAS DE ACCESO PÚBLICO

La información pública producida por la Policía Nacional, esta resguardada de posibles modificaciones que afecten la imagen institucional. Se estableció un procedimiento formal para autorizar la publicación de información, antes que esta sea puesta a disposición del público.

El portal institucional, contiene la política de privacidad y uso, así como la política de seguridad, del mismo.

La Policía Nacional, garantiza al público que hace uso de los servicios del portal institucional, el derecho de Habeas Data y propende por la seguridad de la información de terceros depositada en custodia de la institución, pero no es responsable de la veracidad de la misma.

La información publicada en el portal institucional o cualquier otro medio, requiere de la revisión y aprobación de la Oficina de Comunicaciones Estratégicas y está debidamente rotulada, según su nivel de clasificación.

ARTÍCULO 69. OTRAS FORMAS DE INTERCAMBIO DE INFORMACIÓN

Se implementaron controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

ARTÍCULO 70. MONITOREO

Con el fin de evitar el mal uso de la plataforma tecnológica institucional, la Policía Nacional, efectúa labores de monitoreo sobre las transacciones realizadas en los sistemas de información, así como el monitoreo sobre los dispositivos de la red, para evidenciar actividades sospechosas o posibles fallas.

Los servidores públicos y terceros que están conectados a la red de datos de la Policía Nacional, conocen y aceptan que están siendo auditados y monitoreados.

ARTÍCULO 71. REQUERIMIENTOS MÍNIMOS PARA EL REGISTRO DE AUDITORÍAS

Los sistemas de información, así como los servidores, dispositivos de red y demás servicios tecnológicos, guardan registros de auditoría y log's, los cuales contemplan, siempre y cuando sea posible:

- Id del usuario.
- Fecha y hora de la transacción.
- Dirección IP y nombre del dispositivo desde el cual se realizó la transacción.
- Tipo de transacción.
- Id de la transacción.
- Datos consultados, modificados o borrados.
- Intentos fallidos de conexión.
- Cambios en la configuración del sistema.
- Cambio o revocación de privilegios.
- Archivos a los que ha tenido acceso.
- Alarmas originadas por los sistemas de control.
- Desactivación de los mecanismos de protección.

ARTÍCULO 72. REGISTRO DE AUDITORÍAS

Teniendo en cuenta las múltiples fuentes de datos de registros de log's y auditoria, estos se almacenan en un servidor de syslog y se implemento un correlacionador de eventos, que permita realizar inteligencia de negocios sobre dichos registros.

Los registros de auditoría de los sistemas de información están consolidados en ambientes separados a los transaccionales.

La gestión de los archivos de Log's y auditoría están definidos en la Guía Gestión de Log's y auditoría.

ARTÍCULO 73. PROTECCIÓN DE LOS REGISTROS DE AUDITORIA

Los registros de auditoría están clasificados en nivel 3, para salvaguardarlos de acceso o modificaciones, que alteren su integridad.

Estos registros poseen copias de respaldo, según el artículo 59 Gestión de los Medios de Almacenamiento.

ARTÍCULO 74. SINCRONIZACIÓN DE RELOJES

Para garantizar la exactitud de los registros de auditoría, la Policía Nacional, dispone de un servicio de protocolo de tiempo de red NTP que esta sincronizado a su vez con la hora legal colombiana.

CAPÍTULO 8

CONTROL DE ACCESO

La Policía Nacional establece como política de control de acceso, el modelo de Administración de identidades y Control de acceso (IAM), implantado mediante el Sistema de Identificación Policial Digital, que de manera integrada al Sistema Para la Administración del Talento Humano (SIATH) le permite administrar el ciclo de vida de los usuarios, desde la creación automática de las cuentas, roles y permisos necesarios hasta su inoperancia; a partir de las novedades reportadas por los grupos de talento humano; lo anterior para que el funcionario tenga acceso adecuado a los sistemas de información y recursos tecnológicos, validando su autenticación, autorización y auditoría.

ARTÍCULO 75. REGLAS PARA EL CONTROL DE ACCESO

Las reglas para el control de acceso, está documentado a través del procedimiento control de acceso a recursos tecnológicos.

ARTÍCULO 76. GESTIÓN DE IDENTIDADES

La Gestión de Identidades en la Policía Nacional, está documentada mediante el procedimiento de "Administración de identidades", el cual contempla el registro de usuarios, gestión de privilegios y gestión de contraseñas.

Los usuarios administradores, cumplen con el procedimiento protección de usuarios con altos privilegios.

ARTÍCULO 77. RESPONSABILIDAD DE LOS USUARIOS

Todos los servidores públicos o terceros que tienen un usuario en la plataforma tecnológica de la Policía Nacional, conocen y cumplen los términos de uso del usuario empresarial, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los usuarios, así como políticas de protección de usuario desatendido, escritorio despejado y pantalla limpia.

ARTÍCULO 78. CONTROL DE ACCESO A LA RED

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controla el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

Las reglas de acceso a la red a través de los puertos, esta basadas en la premisa "Todo está restringido, a menos que este expresamente permitido".

ARTÍCULO 79. POLÍTICA DE UTILIZACIÓN DE LOS SERVICIOS DE RED

Se desarrollo un procedimiento para la activación y desactivación de derechos de acceso a las redes, el cual comprende:

1 Control de acceso a los servicios de red tanto internos como externos.

2 Identificación de las redes y servicios de red a los cuales se permite el acceso.

ARTÍCULO 80. POLÍTICA DE CAMINO FORZADO

Se limitaron las opciones de elección de la ruta entre el usuario final y los servicios de red que tiene autorizados, mediante la implementación de controles que restringen la selección de rutas, por parte del usuario.

ARTÍCULO 81. AUTENTICACIÓN DE USUARIOS PARA CONEXIONES EXTERNAS

La Policía Nacional contempla como servicios de conexiones externas SSL, APN, canales de datos, radio enlaces, VPN Site to Site y primarios para servidores públicos que requieran conexión remota a la red de datos institucional.
El acceso a los servicios SSL está acorde con el artículo 73 Reglas para el control de acceso y 74 Gestión de identidades.

La autenticación a los servicios APN, canales de datos, radio enlaces, VPN Site To Site y primarios, está documentado mediante el procedimiento Autenticación de usuarios para conexiones externas.

ARTÍCULO 82. IDENTIFICACIÓN DE EQUIPOS EN LA RED

La Policía Nacional controla e identifica los equipos conectados a su red, mediante el uso de controladores de dominio y DHCP.

El servicio DHCP para los equipos de cómputo realiza la reserva de las direcciones MAC con respecto a las direcciones IP que asigna el servicio.

El servicio DHCP está cerrado, para evitar accesos no autorizados a la red de datos.

ARTÍCULO 83. PROTECCIÓN DE LOS PUERTOS DE CONFIGURACIÓN Y DIAGNÓSTICO REMOTO

Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, está restringido a los administradores de red o servidores y equipos de soporte.

Los usuarios finales permiten tomar el control remoto de sus equipos para el soporte técnico, teniendo en cuenta, no tener archivos con información sensible a la vista, no desatender el equipo, mientras tenga el control de la máquina un tercero.

ARTÍCULO 84. SEPARACIÓN DE REDES

La Policía Nacional utiliza dispositivos de seguridad "firewalls", para controlar el acceso de una red a otra.

La segmentación se realiza en equipos de enrutamiento mediante la configuración de lista de control de acceso y configuraciones de VLAN´s, en los equipos de conmutación.

Las redes inalámbricas no pueden conectarse a la red alambrada.

ARTÍCULO 85. CONTROL DE CONEXIÓN DE LAS REDES

La asignación del ancho de banda para el servicio de internet es de un 40% del canal de datos de cada unidad.

La capacidad de descarga de cada usuario final es de 10 Mb

La seguridad para las conexiones WiFi es WPA2 o superior.

Dentro de la red de datos institucional se restringe el acceso a:

- Mensajería instantánea comercial.
- La telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer.
- Conexiones a sitios de streaming no autorizado.
- Acceso a sitios de pornografía.
- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

ARTÍCULO 86. CONTROL DE ENRUTAMIENTO DE RED

El acceso a redes desde y hacia afuera de la Policía Nacional cumple con los lineamientos del artículo 75 Control de acceso a la red y adicionalmente se utilizan métodos de autenticación de protocolo de enrutamiento, rutas estáticas, traducción de direcciones y listas de control de acceso.

ARTÍCULO 87. ACCESO A INTERNET

La Policía Nacional, provee a través de un Prestador de Servicios de Internet, el servicio de internet institucional, el cual es administrado por el proceso de direccionamiento tecnológico y es el único servicio de internet autorizado. Este servicio se ajustará al artículo 26 relación con terceros.

El acceso a internet requiere de la autenticación de los usuarios, mediante el uso de usuario y contraseña.

El uso de internet está regulado por los términos de uso adecuado del internet.

ARTÍCULO 88. REGISTRO DE INICIO SEGURO

El acceso a los sistemas operativos está protegido, mediante un inicio seguro de sesión, que contempla las siguientes condiciones:

1. No mostrar información del sistema, hasta tanto el proceso de inicio se haya completado.
2. No suministrar mensajes de ayuda, durante el proceso de autenticación.
3. Validar los datos de acceso, una vez se han diligenciado todos los datos de entrada.
4. Limitar el número de intentos fallidos de conexión a cinco (5) y a continuación bloquear el usuario o la sesión. Auditando los intentos no exitosos.
5. No mostrar las contraseñas digitadas.
6. No transmitir la contraseña en texto claro.

ARTÍCULO 89. IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Está definido un estándar de nomenclatura para usuarios de recursos informáticos de la Policía Nacional.

ARTÍCULO 90. GESTIÓN DE CONTRASEÑAS

Está definido un estándar de nomenclatura para usuarios de recursos informáticos de la Policía Nacional.

ARTÍCULO 91. USO DE UTILITARIOS DEL SISTEMA

El uso de utilitarios licenciados del sistema, está restringido a usuarios administradores. Se estableció una política a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema.

Ningún usuario final, tiene privilegios de usuario administrador.

ARTÍCULO 92. TIEMPO DE INACTIVIDAD DE LA SESIÓN

Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se bloquea la sesión, sin cerrar las sesiones de aplicación o de red.

Los usuarios proceden a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo. Los equipos de cómputo deben quedar apagados al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas.

ARTÍCULO 93. LIMITACIÓN DE TIEMPO DE CONEXIÓN

Por la misionalidad de la Policía Nacional, no se limita el tiempo de conexión, ni se establecen restricciones en la jornada laboral.

El control a la conexión se realiza a los usuarios, a través del procedimiento de administración de identidades, el cual bloquea los usuarios, ante una ausencia laboral.

ARTÍCULO 94. CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN

El procedimiento Administracion de Identidades Funcionarios 2IN-PR-0008.

ARTÍCULO 95. CONTROL DE ACCESO A LA INFORMACIÓN

El control de acceso a la información a través de una aplicación, se realiza a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital, se realiza teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

ARTÍCULO 96. ALISTAMIENTO DE SISTEMAS SENSIBLES

La Policía Nacional, identifica según los niveles de clasificación de información cuales sistemas considera sensibles y que deben gestionarse desde ambientes tecnológicos aislados e independientes.

Al aislar estos sistemas se promueve el intercambio seguro de información, con otras fuentes de datos, ya que no se permite duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

ARTÍCULO 97. COMPUTACIÓN MÓVIL Y TRABAJO REMOTO

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, así mismo el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional, se establecen directrices que permitan regular el uso de la computación móvil y trabajo remoto:

ARTÍCULO 98. COMPUTACIÓN Y COMUNICACIONES MÓVILES

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones policiales.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles, está restringido únicamente a los provistos por la institución y contemplan las siguientes directrices:

1. Uso de usuario y contraseña para acceso al mismo.

2. Cifrado de la información.

3. Uso de software antivirus provisto por la Policía Nacional.

4. Restricción de privilegios administrativos para los usuarios.

5. Uso de software licenciado y provisto por la Policía Nacional.

6. Realización de copias de seguridad periódicas.

7. Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.

8. Adquisición de pólizas que cubran el hardware y la información de los dispositivos, contra perdida o hurto.

9. Capacitación al usuario sobre:

- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención, acerca de portar equipos móviles.
- No identificar el dispositivo con distintivos de la Policía Nacional.
- No colocar datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada
- No conectarse a redes WiFi públicas.
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.
- Informar de inmediato a la Oficina de Telemática sobre la pérdida o hurto del dispositivo, quien procederá

al bloqueo del usuario, de la simcard de telefonía celular e informará a la empresa de seguros.

Para dispositivos de comunicación móvil (telefonía celular) institucionales se aplican los controles antes mencionados y los detallados a continuación:

1. Activar la clave del teléfono, para acceso a la agenda telefónica, mensajes de texto, llamadas entrantes, salientes, pérdidas. archivos de voz, imagen y videos.

2. No hablar de temas confidenciales cerca de personas que no requieran conocer dicha información.

ARTÍCULO 99. TRABAJO REMOTO

El trabajo remoto solo es autorizado por el responsable de la unidad organizativa de la cual dependa el funcionario que solicite el permiso. Dicha autorización solo se otorgará por la Oficina de Telemática, Grupos de Telemática y/o Centro de Protección de Datos, una vez se verifique las condiciones de seguridad del ambiente de trabajo.

CAPÍTULO 9

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Siendo los sistemas de información parte importante del proceso de soporte a los procesos misionales de la Policía Nacional, se busca brindar seguridad a los aplicativos institucionales desde el momento mismo del levantamiento de requerimientos y que las necesidades de seguridad, hagan parte integral de las decisiones arquitecturales del software a construir y/o adquirir.

ARTÍCULO 100. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

El procedimiento 2PI-PR-0001 Desarrollar Sistemas de Información, realiza levantamiento de anti requerimientos y casos de abuso, los cuales son expuestos por el Grupo de Seguridad de la Información.

Para la adquisición de productos se contemplan características de seguridad y realiza un proceso formal de pruebas, que hace parte del proceso de evaluación de las ofertas.

Cuando las características de seguridad no cumplan con los requerimientos definidos por la Policía Nacional y no exista forma de satisfacer la necesidad, se realiza un análisis de riesgo, donde se definen los controles que mitigan dichos riesgos.

ARTÍCULO 101. VALIDACIÓN DE DATOS DE ENTRADA

Los datos de entrada, son validados, para asegurar que son correctos y apropiados y que no facilitan posibles ataques a los sistemas; para lo cual se tienen en cuenta las siguientes directrices:

- Comprobar que los datos estén en un formato especificado.
- Comprobar que los datos ingresados corresponden al tipo de dato solicitado.
- Comprobar que el tamaño de los datos de entrada no superen el tamaño total del campo.
- Usar lista de valores predeterminados, para disminuir ingreso errado de datos.
- Comprobar límites menores e inferiores.
- Comprobar que los datos obligatorios sean diligenciados.
- Usar dígitos de chequeo.
- Los campos de contraseñas no deberán ser legibles.

ARTÍCULO 102. CONTROL DE PROCESAMIENTO INTERNO

El proceso de Direccionamiento Tecnológico implementa en los sistemas de información controles que permitan detectar daños en la integridad de la información, debido a errores de procesamiento o actos deliberados.

Estos controles contemplan:

- Las funciones de agregar, modificar y borrar, hacen parte de roles o perfiles en las aplicaciones y están asignados a usuarios plenamente identificables.
- Evitar que los programas se ejecuten en un orden diferente al establecido.
- Controlar el tamaño de los datos de entrada, para evitar ataques de buffer overflow.
- Usar programas que permitan terminar las transacciones, aun después de fallas.

- Elaborar listas de chequeo que permiten validar la correcta ejecución de los programas.

ARTÍCULO 103. AUTENTICACIÓN DE MENSAJES

Los mensajes enviados desde un sistema de información o a través de flujos de trabajo, cuentan con controles criptográficos, que permiten determinar su origen y autenticidad.

ARTÍCULO 104. VALIDACIÓN DATOS DE SALIDA

Las pruebas de calidad al software valida la calidad y veracidad de los datos de salida de los sistemas de información; que cumplen con las características de esta: contenido apropiado, oportunidad, actualización, exactitud y accesibilidad.

ARTÍCULO 105. CONTROLES CRIPTOGRÁFICOS

Se utilizan sistemas y técnicas criptográficas para la protección de la información, previo análisis de riesgos sobre los activos de información con mayor nivel de clasificación; con el fin de procurar una adecuada protección de su confidencialidad e integridad.

ARTÍCULO 106. NORMAS SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

El uso de controles criptográficos, contempla los siguientes aspectos:

1. Se utilizan controles criptográficos en los siguientes casos:

- Protección de contraseñas de acceso a sistemas y demás servicios que requieran autenticación.
- Transmisión de información sensible al interior de la Policía Nacional y fuera de ella.
- Transmisión de información de voz a través de los radios de comunicación.
- Servicios institucionales que recopilen información de terceros.
- Uso de correo electrónico institucional, vía web.
- Mensajería instantánea institucional.
- Firma digital de documentos y correos electrónicos.

2. Se genera el servicio de certificado digital cerrado, para proveer integridad, autenticidad y no-repudio a la información digital institucional.

3. Los procedimientos que se establezcan respecto a la administración de claves de cifrado, recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves de cifrado.

4. El Grupo de Seguridad de la Información del proceso de Direccionamiento Tecnológico es el encargado de administrar e implementar los controles criptográficos; a excepción de los Centros de Protección de Datos, quienes cumplirán estas funciones, al interior de sus unidades.

ARTÍCULO 107. CIFRADO

El Grupo de Seguridad de la Información o los centros de protección de datos, determinan el nivel requerido de cifrado y la longitud de las claves criptográficas a utilizar.

ARTÍCULO 108. FIRMA DIGITAL

La Policía Nacional, utiliza entidades certificadoras para manejo de la firma digital, así:

1. Intercambio de información al interior de la Policía Nacional, mediante firma digital, expedida por la entidad certificadora institucional.

2. Intercambio de información con entidades ajenas a la Policía Nacional, mediante firma digital, expedida por una entidad certificadora abierta.

El procedimiento de firma digital, cuenta con la asesoría jurídica de la Secretaría General.

ARTÍCULO 109. PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

Las claves criptográficas son protegidas contra modificación, destrucción, copia o divulgación no autorizada.

Las claves criptográficas raíz del la infraestructura de llave pública Institucional, están protegidas en caja fuerte.

ARTÍCULO 110. NORMAS Y PROCEDIMIENTOS CRIPTOGRÁFICOS

Se documentaron las normas y procedimientos para:

- Generar claves para diferentes sistemas criptográficos.
- Generar y obtener certificados de clave pública de manera segura.
- Distribuir claves de forma segura a los usuarios, incluyendo información sobre cómo deben activarse cuando las reciben.
- Almacenar claves, incluyendo la forma de acceso a las mismas por personas autorizadas.
- Cambiar o actualizar claves, incluyendo las reglas sobre periodos de validez.
- Revocar certificados, incluyendo como deben retirarse o desactivarse.
- Recuperar claves perdidas.
- Archivar claves.
- Destruir claves.
- Registrar y auditar las actividades relativas a la administración de claves.

Las claves tienen fecha de inicio y caducidad, de tal manera que esos lapsos no puedan ser alterados. Mediante una guía se estableció el tiempo de caducidad de cada clave o certificado, según la naturaleza de cada uno.

ARTÍCULO 111. SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

El proceso de Direccionamiento Tecnológico, realiza labores tendientes a garantizar el mantenimiento sobre los sistemas de producción.

ARTÍCULO 112. CONTROL DEL SOFTWARE DE PRODUCCIÓN

Los cambios sobre el software de producción están avalados por el Comité de Cambios y cada sistema de información, tiene un responsable de su soporte y mantenimiento.

El responsable del Grupo de Administración de Recursos Tecnológicos debe:

- Coordinar la implementación de modificaciones y nuevas funciones en el ambiente de producción.

- Propender porque los sistemas de información en producción sean los autorizados y aprobados en el comité de cambios.
- Permitir la instalación de las modificaciones, previa validación de pruebas de aceptación unitarias, de testeo, de calidad y de usuario final.
- Rechazar la implementación en caso de encontrar defectos en el software o poca o inexistente documentación.
- Registrar las actualizaciones realizadas.
- Llevar un control de versiones.
- Tener una versión previa a la actualización, en caso de requerir reversar el cambio.
- Otorgar o negar permisos al personal de soporte, para modificar el código fuente.

ARTÍCULO 113. PROTECCIÓN DE LOS DATOS DE PRUEBA

Las pruebas de los sistemas de información, se realizan 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 no corresponden a datos reales de producción y si son tomados de este ambiente, son transformados.

ARTÍCULO 114. CONTROL DE CAMBIOS A DATOS DE PRODUCCIÓN

Las modificaciones, actualización o borrado de datos de producción, son realizados a través de la interfaz de usuario de los sistemas de información que procesan dichos datos, y según los roles de cada usuario.
Las modificaciones realizadas fuera de la interfaz de usuario a los sistemas de información, se consideran una amenaza a la integridad de los mismos.

Para los casos en que no es posible cumplir con los lineamientos anteriormente planteados, se tratará de una excepción, la cual debe contemplar las siguientes directrices:

- La solicitud se realiza por escrito, con visto bueno del dueño del activo.
- La modificación sobre datos deja un registro de auditoría, que es protegido de posibles modificaciones.
- Las modificaciones, solo pueden ser realizadas por el personal de soporte del ambiente de producción.
- Los registros de auditoría, son verificados con regularidad por el personal del grupo de seguridad de la información.

ARTÍCULO 115. CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS

El acceso al código fuente y demás documentación de los sistemas de información están protegidas de acceso o modificaciones no autorizadas, para lo cual el proceso de direccionamiento tecnológico, implemento los siguientes controles:

Se nombró un custodio de los códigos, el cual es responsable por:

- Suministrar al grupo de desarrollo el código fuente para su modificación, garantizando la correlación entre fuente y ejecutable.

- Registrar todos los programas fuentes en uso, indicando nombre del programa, programador, responsable que autorizó el cambio, versión, fecha de última modificación, fecha del último ejecutable, estado (modificación, desarrollo).

- Llevar versionamiento del código fuente y los sistemas de información.

- Garantizar que un mismo código fuente, no sea modificado por más de una persona a la vez.

- Propender porque un programa ejecutable en producción este asociado a un único programa fuente.

- El programa ejecutable solo podrá generarse desde el ambiente de producción.

- La función de custodio de códigos, solo podrá ser ejercida por personal del grupo de administración de recursos tecnológicos.

- Evitar que programas fuentes históricas reposen en los ambientes de producción.

- Realizar copias de respaldo de los programas fuentes.

ARTÍCULO 116. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

La proceso de Direccionamiento Tecnológico velará porque los sistemas de información adquiridos, desarrollados por terceras partes o al interior de la institución, cumplan con el ciclo de vida de desarrollo y con los requerimientos de funcionalidad y seguridad esperados y se acojan a las metodologías para la definición de requerimientos de software y para la realización de pruebas al software desarrollado. Así mismo, asegurará que todo sistema de información adquirido, desarrollado por terceros o al interior de la institución, cuente con el nivel de soporte requerido por la institución.

ARTÍCULO 117. PROCEDIMIENTO DE CONTROL DE CAMBIOS

Buscando minimizar la alteración a los sistemas de información, se documentan un procedimiento de control de cambios, alineado con el artículo 48 control de cambio en las operaciones, el cual contempla:

- Verificar que los cambios autorizados, sean realizados por un usuario autorizado y que se respeten los términos y condiciones de uso de las licencias del software a que haya lugar.

- Registrar los niveles de autorización acordados.

- Solicitar autorización al propietario del activo de información, cuando se trate de cambios que modifiquen los sistemas de información que procese dicho activo.

- Identificar software, hardware, bases de datos, que deben ser modificados.

- Realizar los cambios en el ambiente de pruebas.

- Realizar pruebas de calidad y seguridad, sobre los cambios efectuados.

- Actualizar la documentación, con el cambio realizado.

- Llevar el control de versionamiento de los sistemas de información.

- Implementar los cambios, en ventanas de mantenimiento, para no afectar la disponibilidad del servicio.

- Alinear los cambios de software con el artículo 112 Control del software de producción.

ARTÍCULO 118. REVISIÓN TÉCNICA DE LOS SISTEMAS DE INFORMACIÓN, DESPUÉS DE LOS CAMBIOS EN PRODUCCIÓN

Después de implementados los cambios en los sistemas de información en el ambiente de producción, se realizan revisiones con el fin de evitar fallas que afecten la disponibilidad de los mismos. El procedimiento para la revisión contempla:

✓ Copias de respaldo de la versión anterior del sistema de información.
✓ Revisión de las antiguas funcionalidades del sistema.
✓ Actualizar el plan de recuperación de desastres con los cambios realizados, de ser necesario.

ARTÍCULO 119. RESTRICCIÓN DE CAMBIOS A PAQUETES DE SOFTWARE.

Las modificaciones de paquetes de software suministrados por un proveedor, deben validar:

- Análisis de los términos y condiciones de la licencia, para determinar si los cambios a realizar están permitidos.

- Analizar la conveniencia de realizar las modificaciones por personal de la institución o contratarlas con el proveedor o un tercero.

- Evaluar el impacto de asumir el cambio por personal de la institución.

- Guardar una copia del software a modificar, documentar los cambios realizados.

ARTÍCULO 120. CÓDIGO MALICIOSO

Un código malicioso en los sistemas de información de la Policía Nacional, podría exponer la información de esta a personal no autorizado, por tanto se tomaron las siguientes precauciones:

- Adquirir software con proveedores acreditados o productos ya evaluados.

- Examinar los códigos fuentes siempre que sea posible antes de su implementación.

- Validación en ambientes de pruebas, las nuevas actualizaciones de software existente.

- Controlar el acceso y modificaciones al código fuente.

ARTÍCULO 121. DESARROLLO TERCERIZADO DE SOFTWARE

Para la tercerización del desarrollo de software, se tiene en cuenta el procedimiento 2PI-PR-0001 desarrollar sistemas de información, además de las siguientes recomendaciones:

- Cumplir con la Ley 23 de 1982.

- Cumplir con las recomendaciones de la CIRCULAR CONJUNTA 01/2006 sobre los delitos de propiedad intelectual e industrial.

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

- Las especificaciones técnicas contemplan los requerimientos con respecto a la calidad del código y la existencia de garantías.

- Las especificaciones técnicas contemplan acuerdos de custodia de los códigos fuentes del software y cualquier otra documentación necesaria, en caso de requerir modificación en el software.

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

- Cumplir con las recomendaciones del artículo 26 relación con terceros.

ARTÍCULO 122. GESTIÓN DE VULNERABILIDADES

El Área de Administración de la Información, es la encargada del análisis de la explotación de vulnerabilidades conocidas, que podrían poner en riesgo la plataforma tecnológica institucional y su información, por tanto estas son adecuadamente gestionadas y remediadas, para lo cual se implementó un procedimiento formal, que contempla:

✓ Adicionar a la matriz de inventarios de activos de información los datos correspondientes al proveedor del software, versión, estado actual de despliegue y funcionario responsable del software.

✓ Realizar análisis de vulnerabilidades semestralmente.

✓ Mantener información actualizada de nuevas vulnerabilidades.

✓ Definir la línea de tiempo para aplicar parches de remediación para las vulnerabilidades conocidas.

✓ Probar los parches de remediación de vulnerabilidades antes de su despliegue en los ambientes de producción.

CAPÍTULO 10

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad de la información se manifiesta por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de poner en peligro las operaciones del negocio y amenazar la seguridad de la información**.** Por lo tanto, la Policía Nacional creó el CSIRT-PONAL, por sus siglas en inglés "**Computer Security Incident Response Team**", Equipo de Repuesta a Incidentes de Seguridad Informática de la Policía Nacional.

El CSIRT-PONAL a cargo de la Oficina de Telemática, está compuesto por un equipo de expertos en seguridad de la información, quienes velan por la prevención, atención e investigación de incidentes que afecten la seguridad de la información.

La atención de incidentes está documentada mediante el procedimiento 2IN-PR-0005 "Atención a Incidentes".

CAPÍTULO 11

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Una interrupción imprevista o un evento catastrófico, pueden ser situaciones que afectan la disponibilidad de los servicios que soportan los procesos misionales de la organización y pueden causar pérdidas financieras, de imagen o de confianza en la institución; por eso la Gestión de Continuidad del Negocio, es un proceso integral que identifica el impacto de posibles incidentes que amenazan de manera grave a una organización y desarrollan un plan de respuesta efectivo para garantizar la recuperación de las instituciones.

Por tal razón, la Policía Nacional, cuenta con un Plan de Continuidad del Negocio que le permite recuperarse de incidentes que amenacen la prestación del servicio de policía; para lo cual el comité del Sistema de Seguridad de la Información elaboró el plan de continuidad del negocio y la Oficina de Telemática, elaboró el plan de recuperación de desastres en materia tecnológica.

Los propietarios de los activos de información y el Comité de Seguridad de la Información, tienen como funciones:

- Identificar las amenazas que pueden ocasionar interrupciones de los procesos o actividades que afecten el servicio de policía.
- Evaluar riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque integral con el que se abordará la continuidad de las actividades de la institución.
- Elaborar los planes de actividades necesarios para garantizar la continuidad de las actividades de la Policía Nacional, mientras se restablecen los servicios en el sitio principal.

El plan de continuidad del negocio estará alineado con la BS 25999 continuidad del negocio.

CAPÍTULO 12

CUMPLIMIENTO

La Policía Nacional cumple con las leyes, obligaciones estatutarias, reglamentarias, contractuales y cualquier requisito de legal.

Teniendo como objetivo primordial cumplir con disposiciones legales y contractuales para evitar sanciones administrativas, que puedan incurrir en responsabilidad civil, penal o disciplinaria como resultado de su incumplimiento.

ARTÍCULO 123. IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE

El Comité de Seguridad de la Información en acompañamiento de la SecretarÍa General identificó la normatividad vigente que aplica a la Policía Nacional, con respecto a derechos de autor, uso y manejo de información. Así mismo se documento y se designaron responsables y funciones individuales para cumplir con dichos requisitos.

ARTÍCULO 124. DERECHOS DE PROPIEDAD INTELECTUAL

La Policía Nacional implementó procedimientos adecuados para garantizar el cumplimiento de restricciones legales al uso del material protegido por normas de propiedad intelectual, para ello tomó las siguientes medidas:

- Todos los miembros de la Policía Nacional velan por el cumplimiento de normas de derechos de autor y derechos conexos, en lo pertinente a la contratación estatal de obras protegidas y sus buenas prácticas.

- Todos los servidores públicos y terceros que hacen uso de la plataforma tecnológica institucional, solo pueden utilizar software autorizado por la Oficina de Telemática de la Policía Nacional.

- La Oficina de Telemática solo autoriza el uso de software producido por ella misma, o software autorizado o suministrado al mismo por su titular, conforme a los términos y condiciones acordadas y lo dispuesto por la normatividad vigente.

- Se deben establecer convenios con las entidades autorizadas para la utilización de software institucional de acuerdo a la CIRCULAR CONJUNTA 01 2006 sobre los delitos de propiedad intelectual e industrial.

- La Policía Nacional impartió instrucciones para el cumplimiento del Derecho de Autor y Derechos Conexos, los cuales definen el uso legal de productos de información o de software.

- Divulgo las políticas de adquisición de software y la normatividad aplicable a este tema, de igual manera las sanciones aplicables cuando se presente la infracción a una de estas.

- La Oficina de Telemática de la Policía Nacional y/o los grupos de Telemática de las unidades desconcentradas, tienen las siguientes responsabilidades:

1) Elaborar y mantener actualizado un inventario del software utilizado en la institución.

2) Implementar controles para evitar el exceso del número máximo permitido de licencias adquiridas por la institución, para la utilización de los usuarios finales.

3) Verificar que al software que se vaya a instalar en un dispositivo cuente con su respectiva licencia y este autorizado.

4) Utilizar herramientas de auditoría adecuadas.

ARTÍCULO 125. PROTECCIÓN DE LOS REGISTROS DEL ORGANISMO.

Los registros críticos de la Policía Nacional se protegen contra pérdida, destrucción y falsificación, se deben clasificar según las tablas de retención documental y su tiempo de retención se realizará de acuerdo a estas; con el fin de cumplir requisitos legales o normativos y/o respaldar actividades esenciales de la institución.

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.

Si se seleccionan medios de almacenamiento electrónico, se incluyen en los procedimientos para garantizar la capacidad de acceso a los datos durante el periodo de retención a 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 de una manera que resulte aceptable en formato y plazo para cualquier entidad que los requiera.

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

Con el fin de cumplir con estas obligaciones, se adoptaron los siguientes controles:

1. Elaborar y divulgar los procedimientos para la retención, almacenamiento, manipulación y eliminación de registros e información.

2. Mantener un inventario de programas fuentes de información institucionales.

ARTÍCULO 126. PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL

La Policía Nacional garantiza el derecho al Habeas Data y cumple con la legislación vigente sobre protección de datos personales, con la implementación de procedimientos que permiten a los servidores públicos y ciudadanos en general, conocer la información que la institución tiene sobre ellos, actualizarla y solicitar sean eliminados, en los casos que sea pertinente hacerlo.

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.

La Policía Nacional estableció un compromiso de confidencialidad, el cual fue suscrito por todos los funcionarios o personal que tienen un vínculo laboral o contractual con la institución, el cual es parte de su hoja de vida y acta de posesión y/o contrato.

Mediante este compromiso los funcionarios se comprometieron a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicarla, difundirla o hacerla pública a un tercero, sin la autorización previa del dueño del activo.

Así mismo, se les informo que sus actividades en la plataforma tecnológica de la Policía Nacional, puede ser monitoreada y auditada.

La Policía Nacional informa al personal que acceda a sus instalaciones que está siendo monitoreado y grabado por medio de circuito cerrado de televisión.

ARTÍCULO 127. PREVENCIÓN DEL USO INADECUADO DE LOS SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN

La Policía Nacional debe informar por escrito a sus funcionarios y terceras partes que el uso inadecuado de los recursos de procesamiento de datos no está permitido y lo hará conocer a través de un mensaje en el inicio de sesión de cada funcionario.

ARTÍCULO 128. CUMPLIMIENTO DE LOS CONTROLES CRIPTOGRÁFICOS

La utilización de firmas y certificados digitales para el intercambio de información con entidades ajenas a la Policía Nacional, considera lo dispuesto en la Ley 527 de 1999.

La Policía Nacional puede emplear firmas o certificados digitales expedidos por su propia entidad certificadora, para el intercambio de información al interior de la institución.

ARTÍCULO 129. CUMPLIMIENTO DE LAS POLÍTICAS Y LAS NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

La Policía Nacional, a través de su plan anual de auditorías, garantiza el cumplimiento de la política de seguridad de la información definida en el presente manual, buscando el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

ARTÍCULO 130. CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Cada unidad organizacional al interior de la institución, velará por el cumplimiento de la política de seguridad, para lo cual cuenta con auditores internos certificados, que ayudaran en el cumplimiento de la misma; así mismo el Área de control Interno realiza auditorías periódicas al Sistema de Gestión de Seguridad de la Información y ayuda a elaborar planes para la mejora continua del sistema.

ARTÍCULO 131. VERIFICACIÓN DEL CUMPLIMIENTO TÉCNICO

El grupo de seguridad de la información, verifica periódicamente que los sistemas de información, equipos de procesamiento, bases de datos y demás recursos tecnológicos, cumplan con los requisitos de seguridad esperados.

Para esta validación se pueden realizar pruebas de vulnerabilidades y pruebas de penetración, las cuales son una guía para mejorar los controles pero nunca reemplazarán el análisis de riesgo sobre los activos de información.

ARTÍCULO 132. CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Las auditorías sobre los sistemas de información y recursos de procesamiento de datos, son realizados por el Área de Control Interno, teniendo en cuenta la guía para el desarrollo de auditorías internas y plan de mejoramiento interno por procesos.

ARTÍCULO 133. CONTROLES DE AUDITORÍA SOBRE LOS SISTEMAS DE INFORMACIÓN

Las actividades de auditoría sobre los sistemas de producción, son acordadas previamente con los dueños del activo de información procesado en el sistema de información y de ser necesario con la Oficina de Telemática, se coordinan las actividades previas con el fin de no afectar la disponibilidad del servicio. Se consideran los siguientes lineamientos:

1. Acordar con el área o proceso que corresponda los requerimientos de auditoría.

2. Limitar las verificaciones a acceso de solo lectura a los códigos fuentes y datos de producción.

3. Monitorear y registrar todos los accesos, los cuales deben incluir:

- Fecha y hora.
- Puesto de trabajo.
- Usuario utilizado.
- Tipo de acceso.
- Identificación de los datos verificados.
- Estado previo y posterior de los datos.
- Programas utilizados.
- Documentar los procedimientos, requerimientos y responsables asignados a la auditoria.

ARTÍCULO 134. PROTECCIÓN DE LAS HERRAMIENTAS DE AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Las tablas de auditoría y archivos de log usados para auditar los sistemas de información, están separados de los ambientes transaccionales y solo pueden ser accedidos por personal del Área de Control Interno, quienes realizan verificaciones sobre estos.

CAPÍTULO 13

EXCEPCIONES

Las excepciones son exclusiones permanentes o transitorias a los controles descritos en este documento que obligan a la aceptación de riesgos inherentes a dicha exclusión, por lo que se debe guardar registro que contenga como mínimo fecha de solicitud, solicitante, nombre del control excluido, persona que autoriza, tiempo de la exclusión, a quien aplica la exclusión, dependencia y justificación.

La autorización de una exclusión será responsabilidad del dueño del proceso de primer nivel.

La Dirección de inteligencia Policial, tendrá su propia declaración de aplicabilidad de acuerdo a su misionalidad y administrará sus activos basándose en la reserva que la normatividad vigente le confiere.

Cualquier excepción que se realice, debe quedar soportada en la declaración de aplicabilidad y es avalada por el Comité de Seguridad de la Información.

Para el caso, "control de monitoreo" la Dirección de Inteligencia Policial puede acceder a las evidencias que las herramientas de seguridad generen, por el uso de los elementos asignados a los funcionarios de esta unidad.

ARTÍCULO 135. DEROGACIÓN DE DOCUMENTOS QUE NORMALIZAN SOBRE SEGURIDAD DE LA INFORMACIÓN

El presente resolución deroga cualquier directiva administrativa permanente, e instructivos que en materia de seguridad de la información hayan sido publicados con anterioridad en la Policía Nacional.

CAPÍTULO 14

GLOSARIO Y ANEXOS

ARTÍCULO 136. GLOSARIO.

Para dar claridad a los términos utilizados en el presente manual se enuncian las siguientes definiciones

Activo 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.

Acuerdos de confidencialidad. Son 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 confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Acuerdos de intercambio de información. Son 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.

Acuerdos de niveles de servicio ANS (Service Level Agreement -SLA). Es un protocolo plasmado normalmente en un documento de carácter legal, por lo general un contrato; por el que una organización que presta un servicio a otra se compromete a prestar el mismo bajo unas determinadas condiciones y con unas prestaciones mínimas.

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 GPRS que permite la conexión a internet desde un dispositivo móvil celular.

Arquitectura de software. Es un conjunto de patrones y abstracciones coherentes que proporcionan el marco de referencia necesario para guiar la construcción del software para un sistema de información. Estas guías indican la estructura, funcionamiento e interacción entre las partes del software.

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.

Borrado seguro de información. Sobre escritura, des magnetización y destrucción física de medios de almacenamiento**.**

Capacity Planning. Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la institución para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado. Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los Centros de Cómputo, los Centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centros de procesamiento. Son 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. Es la 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 no autorizado a los repositorios de información de la institución.

Confidencialidad. Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Criptografía. Es la 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, y/o prevenir su uso no autorizado.

Derechos de autor. Es un 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 publicado.

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

Disponibilidad. Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Dispositivos de almacenamiento. Materiales físicos donde se almacenan datos.
Documentos de aceptación de la política de seguridad de la información. Son documentos en los que los funcionarios de la Policía Nacional o provistos por terceras partes aceptan acatar la Política de Seguridad de la Información y se acogen a las sanciones establecidas por el incumplimiento de dicha política.

Guías de clasificación de la información. Directrices para catalogar la información de la institución y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Hacking ético. Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Hardware. Cualquier 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 periféricos.

IP. Es una dirección o etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol).

Incidente de seguridad. Es un evento adverso, confirmado o bajo sospecha, que afecta a un sistema de información, a una red, o la violación, o inminente amenaza de violación de la Política de Seguridad de la Información.

Integridad. Es la protección de la exactitud y estado completo de los activos.

ISO/IEC/11801. Estándar Internacional que especifica sistemas de cableado para telecomunicación de multipropósito cableado estructurado que es utilizable para un amplio rango de aplicaciones (análogas y de telefonía ISDN, varios estándares de comunicación de datos, construcción de sistemas de control, automatización de fabricación). Cubre tanto cableado de cobre balanceado como cableado de fibra óptica. El estándar fue diseñado para uso comercial que pueden consistir en uno o múltiples edificios en un campus.

ISO/IEC/18028. Estándar internacional que especifica una arquitectura de seguridad de red.

Licencia de software. Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Log's. Registro o datos de quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo o sistema en particular.

MAC. Media access control; es un identificador de 48 bits (3 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Es la identificación única de cualquier dispositivo físico que hace parte de la una red de datos.

Perfiles de usuario. Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Plan de recuperación ante desastres. Es un conjunto de procedimientos de recuperación de la plataforma tecnológica de la institución y cubre aspectos como los datos, el hardware y el software crítico, para que la Policía Nacional pueda restablecer sus operaciones en caso de un desastre natural o causado por humanos 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.

Propietario de activos de información. Funcionario, unidad organizacional que tiene responsabilidad aprobada del alto mando por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.

Programa de concienciación en seguridad de la información. Es un conjunto de estrategias que persigue que todos los funcionarios de la Policía Nacional y el personal provisto por terceras partes interioricen y adopten la política, normas, procedimientos y guías existentes al interior de la institución dentro de sus actividades diarias.

Propiedad intelectual. Es el 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.

Rack. Gabinete destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están estandarizadas para sea compatible con equipamiento de cualquier fabricante.

Reasignación de derechos de acceso. Es la modificación de los privilegios con que cuenta un funcionario sobre recursos tecnológicos, la red de datos o los sistemas de información de la institución por cambio de sus funciones.

Recursos tecnológicos. Son aquellos 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 computo en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

Registros de auditoría. Son 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.

Remoción de derechos de acceso. Es el bloqueo o la eliminación de los privilegios o de la cuenta de usuario de la cual dispone un funcionario sobre un recurso informático o la red de datos de la institución.

Requerimientos de nuevas funcionalidades, servicios o modificaciones. Contienen la definición de necesidades y la generación de especificaciones correctas que describan con claridad, en forma consistente y compacta, el comportamiento esperado de las funcionalidades o modificaciones sobre los sistemas de información.

Respaldo. Copia de seguridad o backup de información, realizada con el fin de utilizarse para restaurar la original después de una eventual pérdida de datos.

RETIE. Reglamento técnico de instalaciones eléctricas.

Sistema de información. Es un 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 ya sea adquirido por la institución como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental. Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Sistemas de detección y extinción de incendios. Son sistemas que reaccionan rápidamente para reducir el impacto y la posibilidad de que sI un incendio se propague a otras zonas, contando con algunas de las siguientes características: detección temprana de humo, extinción mediante gas, monitoreo y alarmas contra incendios y sistemas rociadores para zonas comunes.

Software. Es todo programa o aplicación programado para realizar tareas específicas.

Software malicioso. Es una 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.

Partes externas. Personas o entidades que brindan servicios a la Policía Nacional o que interactúan de alguna manera con la información de esta.

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

Tercerización. Proveerse de un servicio o producto de un tercero.

TIC's. Tecnologías de la información y las comunicaciones.

UPS: Suministro redundante de energía ininterrumpible 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.

Virtualización. Capacidad abstracción que se puede hacer de los ambientes físicos, permitiendo en un mismo hardware poner a correr varios ambientes de tal manera que cada uno de estos ambientes pueda operar de manera aislada y puedan ver los mismos dispositivos de almacenamiento, de procesamiento y de red como si se tratara de dispositivos físicos independientes.

VPN. Red Privada Virtual es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local.

Vulnerabilidades. Son las debilidades, hoyos de seguridad o flaquezas 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.

Web services. Permite la comunicación entre aplicaciones o componentes de aplicaciones de forma estándar a través de protocolos comunes (como http) y de manera independiente al lenguaje de programación, plataforma de implantación, formato de presentación o sistema operativo. Un Web service es un contenedor que encapsula funciones específicas y hace que estas funciones puedan ser utilizadas en otros servidores.

ARTICULO 137 . GESTIÓN SOBRE LA CLASIFICACIÓN DE LA INFORMACIÓN.

La gestión sobre la clasificación de la información se basa en la especificación de la normatividad y lineamientos relacionados con el acceso, almacenamiento, transmisión y destrucción de dicha información y establecer los controles necesarios para cumplir con dicha normatividad y lineamientos.

De manera adicional, es importante que un adecuado conjunto de procedimientos sea definido para el acceso, almacenamiento, generación de copias, transmisión, rotulado y destrucción de la información, de acuerdo con el esquema de clasificación adoptado por la Policia Nacional. Estos procedimientos deben cubrir las fuentes de información en formas física y electrónica; a su vez, deben permitir asegurarse de que la introducción de cada nueva fuente de información activa el proceso de la clasificación y/o reclasificación de la información.

Para cada categoría de la clasificación de la información, los procedimientos de manejo deben ser definidos para cubrir los siguientes tipos de actividades de procesamiento de la información siguiendo los lineamientos presentados a continuación:

- Acceso y Divulgación
- Generación de copias de medios físicos e impresión
- Envío de faxes
- Transmisión a través de redes públicas
- Rotulado
- Destrucción
- Divulgación de terceros
- Embalaje correo interno y externo

ARTICULO 138 . ALMACENAMIENTO

El almacenamiento de la información en la Policía Nacional se realizará de acuerdo a la GUÍA DE CONSERVACIÓN PREVENTIVA PARA LOS ARCHIVOS DE LA POLICÍA NACIONAL.

ARTICULO 139 . DESCLASIFICACIÓN Y RECLASIFICACIÓN.

La información clasificada como ultra secreta, secreta, reservada y confidencial podrá desclasificarse o reclasificarse y esta la realizará el propietario de la información, dejando registro del procedimiento y sustentando las causas de su nueva clasificación.

ARTÍCULO 140. **ÁMBITO DE APLICACIÓN**.

La ejecución del Manual del Sistema de Gestión de seguridad de la información para la Policía Nacional, contemplada en el artículo 2°, será realizada por los Servidores Públicos de la Institución.

ARTÍCULO 141. PUBLICIDAD Y DIFUSIÓN.

La Oficina de Planeación o la dependencia en que se delegue esta responsabilidad, pondrán en funcionamiento los mecanismos de difusión necesarios para el conocimiento y aplicación del "Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional", en las unidades policiales. Igualmente, se pondrá a disposición de los usuarios de la Institución en los sistemas de comunicación, consulta y publicidad disponibles para el efecto.

ARTÍCULO 142. APLICACIÓN EN PROGRAMAS DE FORMACIÓN.

Los dueños y responsables de procesos en coordinación con la Dirección Nacional de Escuelas, implementarán actividades pedagógicas para la enseñanza del Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional, a través de los programas de formación, actualización, entrenamiento y capacitación del sistema educativo policial.

ARTÍCULO 143. OBLIGATORIEDAD.

El manual adoptado mediante el presente acto administrativo, será de obligatorio cumplimiento en el desarrollo de las actividades relacionadas con el Sistema de Gestión de Seguridad de la Información.

ARTÍCULO 144. VIGENCIA.

La presente resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D. C.

ORIGINAL FIRMADO
Mayor General **JOSE ROBERTO LEÓN RIAÑO**
Director General Policía Nacional de Colombia

Elaboro: TC. LUIS ERNESTO CASAS FORERO
TE. WILLIAM MUIÑOZ ROJAS
SC ADRIANA CIFUENTES
Reviso: MY FABIO ALEXANDRE CANO JIMENEZ
TC OLGA LUCIA PINEDA ORTIZ
Aprobo TC. JAIME ALBERTO BARRERA HOYOS
Fecha: 15/08/2012

ANEXO 1

Medidas de seguridad según el nivel de clasificación de la información

PROCEDIMIENTO		NIVELES DE CLASIFICACIÓN				
TRATAMIENTO	**MEDIDAS DE SEGURIDAD**	**Ultrasecreta y secreta**	**Reservada**	**Cofidencial**	**Interno**	**Público**
ACCESO Y DIVULGACIÓN	CIFRADO	X	X	X		
	CONTROLES DE ACCESO FÍSICO Y LÓGICO	X	X	X		
	ACUERDO DE CONFIDENCIALIDAD	X	X	X		
GENERACIÓN DE COPIAS DE MEDIOS FÍSICOS E IMPRESIÓN	LA OBTENCIÓN DEL CONSENTIMIENTO DEL PROPIETARIO, SE RECOMIENDA.	X	X	X		
	RESTRICCIÓN EN NÚMERO DE COPIAS POR PARTE DEL PROPIETARIO.	X	X	X		
ENVÍO DE FAXES	PROTEGIDOS CON CONTRASEÑA O DISPOSITIVOS DE RECEPCIÓN PRESENTES DESTINATARIO PARA LA RECEPCIÓN DE LA INFORMACIÓN.	NO SE PUEDE ENVIAR ESTA INFORMACIÓN	NO SE PUEDE ENVIAR ESTA INFORMACIÓN	NO SE PUEDE ENVIAR ESTA INFORMACIÓN	X	X
TRANSMISIÓN A TRAVÉS DE REDES PÚBLICAS	CIFRADO	NO SE PUEDE ENVIAR ESTA INFORMACIÓN	X	X		
ROTULADO	SELLO O STICKER SEGÚN SU CLASIFICACIÓN.	X	X	X	X	
	MARCA DE AGUA O PIE DE PÁGINA QUE INDIQUE SU CLASIFICACIÓN	X	X	X	X	
DESTRUCCIÓN	DESTRUCTORAS DE PAPEL.	X	X	X	X	
	PAPELERA.	X	X	X	X	
	BORRADO SEGURO DE DE LA INFORMACIÓN	X	X	X	X	X
DIVULGACIÓN A TERCEROS	CONSENTIMIENTO DEL PROPIETARIO Y ACUERDO DE CONFIDENCIALIDAD	X	X	X	X	
	DIVULGACIÓN FECHA Y CLASIFICACIÓN	X	X			
	REQUIERE ETIQUETADO	X	X	X	X	X
EMBALAJE CORREO INTERNO Y EXTERNO	DIRIGIDO A UN DESTINATARIO ESPECÍFICO Y SE COLOCA DENTRO DE DOS SOBRES, CON LA ETIQUETA DE CLASIFICACIÓN EN EL SOBRE INTERNO SOLAMENTE.	X	X	X		
	UN SOLO SOBRE SIN NINGÚN TIPO ESPECÍFICO DE ETIQUETADO				X	