MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

DIRECCIÓN GENERAL

RESOLUCIÓN NÚMERO 08310 DE 28 DIC 2016

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

EL DIRECTOR GENERAL DE LA POLICÍA NACIONAL DE COLOMBIA

En uso de las facultades legales, y en especial de las conferidas por el artículo 2º, numeral 8 del Decreto 4222 de 2006, y,

CONSIDERANDO:

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

Que el numeral 8 del artículo 2º de la norma en cita, faculta al Director General de la Policía Nacional de Colombia, expedir resoluciones, manuales, reglamentos y demás actos administrativos necesarios para administrar la Policía Nacional en todo el territorio nacional.

Que el artículo 24 de la norma ibídem, establece que el Director General de la Policía Nacional de Colombia podrá 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 y puede delegar esta función de conformidad con las normas legales vigentes.

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 a través de la Resolución 03049 del 24 de agosto de 2012, se adoptó el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional.

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

Que en atención a los preceptos normativos sobre el Sistema de Gestión de Seguridad de la Información, se hace necesario derogar la Resolución 03049 del 24 de Agosto de 2012 "Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional", y expedir nuevos lineamientos enfocados a la preservación de los activos de información, que permitan a la vez la consulta de los deberes institucionales y orientación a los funcionarios en el uso de las buenas prácticas para alcanzar los estándares de calidad, seguridad y ciclo de vida de la información, con el objeto de lograr mayor eficiencia, eficacia, efectividad y calidad de los activos de información, mediante las prácticas que se deben utilizar dentro de la Institución a través de la elaboración y aplicación de pautas para el desempeño de sus funciones y alcance de los objetivos en la prestación del servicio de Policía.

Que es necesario establecer el Sistema de Gestión de Seguridad de la Información de la Policía Nacional, el cual cuenta con herramientas que incluyen normas, protocolos 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 del negocio, para lo cual.

RESUELVE:

ARTÍCULO 1. EXPEDICIÓN. Expedir el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional.

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

CAPÍTULO I

GENERALIDADES

ARTÍCULO 3. ALCANCE DEL MANUAL. El presente Manual es de cumplimiento para los funcionarios de la Policía Nacional y personal externo que le proporcione algún bien o servicio; quienes están obligados a adoptar los parámetros aquí descritos y los controles adicionales que pueden implementar las diferentes unidades de acuerdo a su misionalidad.

La política de Seguridad de la Información busca cubrir toda la información impresa o escrita en papel, recopilada electrónicamente en cualquier medio de almacenamiento actual o futuro, transmitida a través de medio electrónico actual o futuro; mostrada en videos o hablados, y todo lo considerado información de carácter institucional que se convierte en activos de información.

ARTÍCULO 4. ALCANCE DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN, SGSI. Las Unidades de Policía que se certifiquen e implementen el Sistema de Gestión de Seguridad de la Información, deberán definir los límites del alcance y la declaración de aplicabilidad de acuerdo a la Norma ISO 27001:2013, identificando los siguientes requisitos:

1. **CONTEXTO DE LA ORGANIZACIÓN:** Determinar factores internos y externos que pueden afectar la capacidad funcional de la Institución para lograr los objetivos definidos en cumplimiento de los resultados previstos en el Sistema de Gestión de la Seguridad de la Información.

   A. **FACTORES EXTERNOS**: Se deben identificar los siguientes elementos del contexto externo:

   - Avances tecnológicos accesibles.
   - Cambios de políticas.
   - Cambios normativos.
   - Exigencias de la comunidad de Seguridad de la Información.

   B. **FACTORES INTERNOS:** Para el Sistema de Gestión de Seguridad de la Información es importante tener en cuenta, algunos conceptos contemplados en el marco estratégico institucional, así:

   - Misión
   - Visión
   - Mega
   - Políticas institucionales:
     1. Políticas Institucionales Misionales.
        - Servicio de Policía.
        - Unidad Institucional.
        - Integridad Policial.
        - Gestión humana y calidad de vida óptima.
        - Educación e Innovación Policial.
        - Comunicaciones Efectivas.
        - Buen Uso de los Recursos.
     2. Políticas Institucionales de Sistemas de Gestión
   - Principios y valores éticos institucionales

2. **COMPRENSION DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS:** Son aquellos factores que configuran la razón de ser de las diferentes unidades de la Policía Nacional; es decir, sectores sociales o clientes hacia los que la Institución focaliza sus esfuerzos y pretende atender de forma eficiente, por lo tanto cada unidad de acuerdo a su misionalidad debe identificar los clientes (partes interesadas) que impactan con su

función, y que con las actividades que realizan deben tener en cuenta el cumplimiento de las políticas del Sistema de Gestión de Seguridad de la Información.

GRUPOS SOCIALES OBJETIVO O CLIENTES		
COMUNIDAD	**Población**	General
	Organizada	Gremios, asociaciones y sector productivo
		Medios de comunicación
	Internacional	Policías de otros países
		Organismos multilaterales
ESTADO	**Ramas del poder público**	Ejecutiva
		Judicial
		Legislativa
	Órganos de Control	Órganos de Control
COMUNIDAD POLICIAL	**Usuarios**	Personal Activo
		Personal en uso de buen retiro y pensionados

3. **PARTES INTERESADAS:** están definidas como**:**

A. **COMUNIDAD:** Grupo social, colombianos y extranjeros que se encuentren en el territorio nacional a quienes la Policía Nacional brinda servicios de protección.

La relación que existe entre la Policía Nacional y la comunidad, es la de crear condiciones necesarias para la convivencia y la seguridad, así mismo la de garantizar la integridad policial, la transparencia y la veeduría social.

B. **ESTADO:** La relación de la Policía Nacional y el Estado se fundamenta con el principio constitucional de garantizar la seguridad de todos los habitantes del territorio nacional, por lo tanto el compromiso de la Institución es respetar y promover el Estado Social de Derecho, cumpliendo todos los requisitos legales, contractuales y regulatorios que sean de aplicación para la Seguridad de la Información.

Cumplimiento normativo:

- Ley 80 del 28/10/1993 "Estatuto general de contratación de la administración pública"
- Ley 87 del 29/11/1993 "Control interno en los organismos del estado"
- Ley 527 del 18/08/1999 "Comercio electrónico"
- Ley 594 del 14/07/2000 "Ley General de archivo"
- Ley 599 del 24/07/2000 "Código penal colombiano"
- Ley 603 de 2000 "Control de Legalidad del Software"
- Ley 734 del 05/02/2002 "Código Disciplinario Único"
- Ley 962 de 2005 "Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;"
- Ley 1015 del 07/02/2006 "Régimen Disciplinario para la Policía Nacional"
- Ley 1150 de 2007 "Seguridad de la información electrónica en contratación en línea"
- Ley 1266 del 31/12/2008 "Por lo cual se dictan disposiciones generales del habeas data y se regula el manejo de la información"
- Ley 1273 del 05/01/2009 "Protección de la información y de los datos"
- Ley 1341 de 2009 "Tecnologías de la Información y aplicación de seguridad"
- Ley 1480 de 2011 "Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas".
- Ley 1581 del 17/10/2012 "Por la cual se dictan disposiciones generales para la protección datos personales" y su decreto reglamentario 1377 del 27 de junio de 2013.
- Ley 1621 del 17/04/2013 "Inteligencia y Contrainteligencia"

- Ley 1712 del 06/03/2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- Decreto Ley 019 de 2012 "Racionalización de trámites a través de medios electrónicos. Criterio de seguridad".
- Decreto 103 del 20/01/2015 "por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones"
- Decreto 1070 de 2015 del 26/05/2015 "por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa"
- Manual para la implementación de la estrategia de gobierno en línea en las entidades del orden nacional de la República de Colombia.
- Documento CONPES 3854 11/04/2016 "Política Nacional de Seguridad Digital"
- Norma técnica Colombiana NTC-ISO/IEC 27000.
- Metodología para análisis y evaluación de riesgos de la Policía Nacional.
- Directiva 18 del 19/06/2014 Ministerio de Defensa Nacional "Políticas de Seguridad de la Información para el Sector Defensa"

Así mismo se dará cumplimiento a las nuevas Leyes, Decretos y Normas emitidas por las autoridades competentes que involucren a las entidades públicas relacionadas con Seguridad de la Información y protección de datos.

C. **COMUNIDAD POLICIAL:** Los funcionarios de la Policía Nacional son todos aquellos quienes con su talento, compromiso, responsabilidad y liderazgo garantizan el orden público de la nación. La responsabilidad ante el Sistema de Gestión de Seguridad de la Información es velar por la protección de la información a la cual se tiene acceso en cumplimiento de sus funciones.

4. **INTERFACES Y DEPENDENCIAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:** Cada unidad de Policía debe identificar las dependencias que desarrollan actividades que interactúan con otras organizaciones y unidades de Policía, con el fin de dar aplicabilidad al SGSI en la protección de los activos de información.

ARTÍCULO 5. LIDERAZGO Y COMPROMISO. La Policía Nacional demuestra su apoyo y compromiso con la protección de la información institucional a través de:

1. La aprobación y establecimiento de la Política de Seguridad de la Información, cuyos objetivos están alineados con las directrices estratégicas de la Institución.
2. La disposición de los recursos necesarios para la adecuada operación del Sistema de Gestión de Seguridad de la Información.
3. El aseguramiento del cumplimiento de los objetivos definidos para la Gestión de Seguridad de la Información.
4. La alta gerencia de cada unidad en donde se tiene implementado un Sistema de Seguridad de la Información ha de comunicar la importancia del cumplimiento de los controles establecidos para la protección de los activos de información.
5. Los lineamientos institucionales que apoyan al personal que soporta la gestión de Seguridad de la Información dentro de la Institución.
6. La mejora continua.

CAPÍTULO II

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA POLICÍA NACIONAL

ARTÍCULO 6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. La Policía Nacional de Colombia se compromete a salvaguardar sus activos de información con el fin de protegerlos de las amenazas que se ciernen sobre ellos, a través de la implementación de un Sistema de Gestión de Seguridad de la Información que permita la adecuada gestión del riesgo, la generación de estrategias de seguridad basada en las mejores prácticas y controles, el cumplimiento de los requisitos legales, la oportuna gestión de los incidentes, y el compromiso Institucional de mejora continua.

ARTÍCULO 7. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. Con el fin de minimizar la materialización del riesgo frente a los activos de información de la Policía Nacional se han establecido los siguientes objetivos del SGSI, así:

- Crear una cultura de Seguridad de la Información en cada unidad Policial mediante sensibilizaciones y capacitaciones en cuanto a las mejores prácticas para evitar la materialización de riesgos asociados al SGSI.

- Identificar mediante una adecuada evaluación del riesgo, el valor de la información así como las vulnerabilidades y las amenazas a las que está expuestas.

- Dar un tratamiento efectivo a los incidentes de seguridad, con el fin de identificar sus causas y realizar las acciones correctivas.

- Implementar y mantener el Sistema de Gestión de Seguridad de la Información promoviendo la mejora continua.

ARTÍCULO 8. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. El Comité de Seguridad de la Información será el responsable de realizar las revisiones de la política del SGSI y lo hará al menos una vez al año o cuando ocurran cambios en el entorno organizacional, marco legal o ambiente técnico.

CAPÍTULO III

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 9. ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN. La Policía Nacional, con el fin de realizar un adecuado aseguramiento de la administración del Sistema de Gestión de Seguridad de la Información (SGSI), define los siguientes roles de quienes deben apoyar y cumplir esta política, así:

1. COMITÉ DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA POLICÍA NACIONAL:

El Comité del Sistema de Gestión de Seguridad de la Información de la Policía Nacional planea, orienta, gestiona los recursos, implementa y realiza seguimiento del SGSI, realizando actividades de análisis de riesgos, implementación de controles con el fin de evitar la materialización de acciones que afecten los pilares de seguridad de la información (confidencialidad, integridad, disponibilidad), así mismo la realización de acuerdos de niveles de servicio entre las unidades certificadas y la Oficina de Telemática.

1.1 **INTEGRANTES COMITÉ DEL SGSI:**

- Jefe del Grupo del Equipo de Respuesta a Incidentes de Seguridad Informática "CSIRT - PONAL" o quien haga sus veces.

- Jefe de Centro de Protección de Datos "CPD" o encargados del Sistema de Gestión de Seguridad de la Información (SGSI) de cada Dirección.

- Jefe Grupo Direccionamiento Institucional de la Oficina de Planeación (Encargado de Sistema de Gestión de Calidad (SGC)).

- Invitados

1.2 FUNCIONES COMITÉ DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA POLICÍA NACIONAL:

- Liderar y definir las actividades tendientes al fortalecimiento y mejora continua de la Seguridad de la Información en las unidades certificadas.
- Promover el cumplimiento, por parte del personal de la unidad, de las políticas de Seguridad de la Información Institucional
- Definir, evaluar e implementar en la unidad los controles preventivos alineados a la ISO27001:2013 y el Manual de Seguridad de la Información de la Institución.
- Evaluar y dar trámite a las conductas contrarias que afectan la política de Seguridad de la Información de la Policía.
- Verificar y aprobar el inventario de los activos de información.

- Realizar seguimiento a los acuerdos de nivel de servicios entre la Oficina de Telemática y las unidades certificadas.
- Gestionar los riesgos de Seguridad de la Información de la unidad a través del seguimiento al tratamiento de riesgo institucional que afecte la Seguridad de la Información
- Resolver las controversias y conflictos entre la entidad de certificación (PKI, Infraestructura de llave publica de la Policía Nacional) y sus suscriptores, cuya función será resolver cualquier controversia o diferencia que pudiera surgir entre la PKI-PONAL y sus suscriptores, en relación con la interpretación y/o aplicación de la Declaración de Prácticas de Certificación Digital – DPC, que no pueda ser resuelta, dentro de los treinta (30) días calendario siguientes al momento en que dicha controversia o diferencia haya sido planteada.

1.3 PERIODICIDAD DE CONVOCATORIA:

El Comité del Sistema de Gestión de Seguridad de la Información de la Policía Nacional es presidido y convocado por el Jefe Grupo Seguridad de la Información o quien haga sus veces, deberá reunirse semestralmente o cuando se requiera extraordinariamente.

2. COMITÉ INTERNO DE SEGURIDAD DE LA INFORMACIÓN.

Es el Comité Interno de Seguridad de la Información conformado en las unidades de Policía, en el cual se planea, orienta, gestiona los recursos, implementa y realiza seguimiento del SGSI, realizando actividades de concientización sobre las mejores prácticas, gestión de activos de información, gestión del riesgo y atención de los incidentes de seguridad con el fin de garantizar el fortalecimiento de la política de seguridad de la información.

2.1 INTEGRANTES COMITÉ INTERNO DEL SGSI.

DIRECCIONES, OFICINAS ASESORAS, ESCUELAS:

- Director o Subdirector.
- Jefe Planeación.
- Jefe Administrativo.
- Jefe Comunicaciones Estratégicas (COEST).
- Jefe Grupo Telemática.
- Jefe Centro Protección de Datos, CPD (donde este creado) o su delegado.
- Jefe Seguridad e Instalaciones.
- Jefe Grupo Talento Humano.
- Jefe Gestión Documental.
- Analista de Seguridad de la Información.
- Asesor Jurídico.

DEPARTAMENTOS y METROPOLITANAS:

- Comandante o Subcomandante.
- Jefe Planeación.
- Jefe Administrativo.
- Jefe Comunicaciones Estratégicas (COEST).
- Jefe Grupo Telemática.
- Jefe Seguridad de Instalaciones o Comandante de Guardia.
- Jefe Grupo Talento Humano.
- Jefe Gestión Documental.
- Asesor Jurídico.
- Analista de Seguridad de la Información.
- Jefe Seccional de Investigación Criminal, SIJIN.
- Jefe Seccional de Inteligencia Policial, SIPOL.

En las reuniones del Comité Interno de Seguridad de la Información en caso de no asistir el titular deberá hacerlo su delegado.

2.2 FUNCIONES DEL COMITÉ INTERNO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:

- Liderar y definir las actividades tendientes al fortalecimiento y mejora continua de la Seguridad de la Información en la unidad.
- Promover el cumplimiento, por parte del personal de la unidad, de las políticas de Seguridad de la Información Institucional.

- Desplegar las políticas de Seguridad de la Información definidas por el Comité de Seguridad de la Información de la Policía Nacional.
- Definir, evaluar e implementar en la unidad los controles preventivos alineados a la ISO27001:2013 y el Manual de Seguridad de la Información de la Institución.
- Divulgar y realizar campañas pedagógicas a los funcionarios y contratistas de la unidad sobre las mejores prácticas en la gestión de activos de información.
- Evaluar y dar trámite a las conductas contrarias que afectan la política de Seguridad de la Información de la Policía.
- Verificar y aprobar el inventario de los activos de información realizado por el analista de seguridad de la información de la unidad o quien haga sus veces.
- Resolver las controversias y conflictos entre la entidad de certificación (PKI, Infraestructura de llave publica de la Policía Nacional) y sus suscriptores, cuya función será resolver cualquier controversia o diferencia que pudiera surgir entre la PKI-PONAL y sus suscriptores, en relación con la interpretación y/o aplicación de la Declaración de Prácticas de Certificación Digital – DPC, que no pueda ser resuelta, dentro de los treinta (30) días calendario siguientes al momento en que dicha controversia o diferencia haya sido planteada.

2.3 PERIODICIDAD DE CONVOCATORIA:

El Comité de Seguridad de la Información es presidido y convocado por el señor Director o Subdirector, Comandante o Subcomandante según sea el caso, deberá reunirse trimestralmente o cuando se requiera extraordinariamente.

3. RESPONSABILIDADES INDIVIDUALES:

Los roles y responsabilidades de quienes deben apoyar y cumplir la Política de Seguridad de la Información los cuales son responsables de la implementación del Sistema de Gestión de Seguridad de la Información, verificando la efectividad y eficiencia del Sistema acorde con los objetivos de la Policía Nacional, tomando las acciones correctivas que hubiese lugar, serán los siguientes:

a. **Oficina de Telemática**. Administra las herramientas tecnológicas de la Policía Nacional que son gestionadas desde el Nivel Central, así mismo efectúa las tareas de desarrollo y mantenimiento de Sistemas de Información, siguiendo una metodología de ciclo de vida, la cual debe contemplar medidas de seguridad.

b. **Grupo de Seguridad de la Información:** La Oficina de Telemática lidera el desarrollo, implementación, mantenimiento y actualización del Sistema de Gestión de Seguridad de la Información.

c. **Propietarios de los activos de información:** Son todos aquellos funcionarios que identifican, elaboran, clasifican y gestionan el riesgo de los activos de información de acuerdo al grado de sensibilidad de la misma.

d. **Dirección de Incorporación:** Tiene como función seleccionar el talento humano de planta de tal manera que se certifique que el aspirante posee competencias que cumplan con el perfil del cargo al cual se postula de acuerdo al protocolo de selección del Talento Humano para la Policía Nacional.

e. **Inspección General:** Investiga las conductas contrarias que afectan la Política de Seguridad de la Información.

f. **Área de Control Interno:** Revisa y verifica el cumplimiento de la presente Resolución, a través de las auditorias programadas a las unidades, así mismo a aquellas que cuenten con un Sistema de Seguridad de la Información.

Parágrafo: Para las unidades que no cuentan con un Sistema de Seguridad de Información, el Área de Control Interno revisará y verificará el cumplimiento de los controles transversales, así:

- Seguridad del cableado.
- Mantenimiento de los equipos.
- Seguridad de los equipos fuera de las instalaciones.
- Destrucción o reutilización segura de equipos.
- Normas de escritorios y pantallas limpias.
- Retiro de bienes de las instalaciones.
- Suministro de energía.
- Seguridad de los equipos.

- Controles de las redes.
- Seguridad de los servicios de red.
- Manejo de los medios de almacenamiento.
- Mensajería electrónica.
- Responsabilidad de los usuarios
- Identificación y autenticación de usuarios.
- Sensibilización y concienciación a funcionarios y terceros.
- Atención de incidentes de seguridad de la información.
- Disponibilidad de canales de comunicaciones.
- Antivirus.

g. **Secretaría General:** Asesora en materia legal los aspectos pertinentes a Seguridad de la Información.

h. **Equipo de respuesta a incidentes de seguridad informática "CSIRT PONAL." - Computer Security Incident Response Team:** Atiende e investiga los incidentes de Seguridad de la Información Institucional y propende por el restablecimiento del servicio en caso de verse afectado.

i. **Centro Cibernético Policial, CCP:** Investiga los incidentes que se sospechan constituyen un delito, a través del control y liderazgo de la Dirección de Investigación Criminal e Interpol (DIJIN).

j. **Funcionarios:** Todo el personal que labora o realiza actividades para la Policía Nacional, son responsables por el cumplimiento de la presente Resolución y es deber informar cualquier incidente de Seguridad de la Información que se tenga conocimiento.

ARTÍCULO 10. SEPARACIÓN DE DEBERES. En los cargos donde se realicen labores sensibles o sean identificados como perceptivos a corrupción, se debe realizar la separación de tareas entre distintos funcionarios o contratistas con el fin de reducir el mal uso de los sistemas e informaciones deliberadas o acciones por negligencia.

ARTÍCULO 11. CONTACTO CON LAS AUTORIDADES. Las diferentes unidades de la Policía Nacional, realizan un listado de contacto con las autoridades la cual debe incluir a las empresas de servicios públicos, servicios de emergencia, proveedores de electricidad, salud y seguridad.

ARTÍCULO 12. CONTACTO CON GRUPOS DE INTERÉS ESPECIAL. El Equipo de Respuesta a Incidentes de Seguridad Informática "CSIRT"-PONAL, será el encargado de mantener las membrecías con grupos o foros de interés especial como un medio para:

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

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

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

- Brindar los enlaces adecuados cuando se trata de incidentes que afectan la Seguridad de la Información.

- Emitir los respectivos boletines con el fin de mantener al día al personal de la Policía Nacional sobre los incidentes de Seguridad Informática y de esta manera difundir las recomendaciones para adoptar las mejores prácticas.

ARTÍCULO 13. SEGURIDAD DE LA INFORMACIÓN EN GESTIÓN DE PROYECTOS. Cada vez que la Policía Nacional planee, desarrolle, ejecute e implemente nuevos proyectos de adquisición o mejora de recursos tecnológicos, físicos o de cualquier índole, hace el estudio de conveniencia y oportunidad en el cual deberá considerar los riesgos jurídicos y operativos del proyecto, así como realizar la inclusión de cláusulas de firma de acuerdos de confidencialidad y estudios de confiabilidad.

La adquisición de nuevos recursos y servicios tecnológicos de Información y comunicaciones, así como software y hardware asociado, serán autorizados únicamente por el proceso de Direccionamiento Tecnológico de la Policía Nacional de Colombia.

ARTÍCULO 14. PLANIFICACIÓN. La Policía Nacional se basa en los aspectos determinados en el contexto de la organización y una acertada gestión de los riesgos asociados a la información, lo cual permite determinar el impacto para la Institución y sus procesos en caso que se produzca una situación de pérdida de confidencialidad, integridad o disponibilidad en la información.

La adecuada identificación de riesgos sobre la información permitirá a la Institución tomar decisiones y priorizar las acciones sobre los mismos, enfocándose en requerimientos de seguridad de la información (inversión, priorización de necesidades, etc.). La metodología de riesgos definida por la Policía Nacional para el Sistema de Gestión de Seguridad de la Información incluye:

1. Criterios de aceptación y evaluación de riesgos.
2. Identificar los riesgos de Seguridad de la Información (incluyendo las fases de identificación y evaluación del riesgo relacionados con la pérdida de confidencialidad, integridad y disponibilidad de la información).
3. Definición de los responsables de la información como dueños del riesgo.
4. Categorización del impacto, probabilidad de ocurrencia y las consecuencias potenciales sobre la Institución si se materializaran.
5. Definición de tratamiento de riesgos de seguridad de la información y la aprobación de los mismos por parte del dueño del riesgo.

Una vez concluido el análisis de riesgos y generados los planes de tratamiento tal como lo describe la metodología de riesgos de la Policía Nacional, se debe generar o actualizar (según sea el caso) la declaración de aplicabilidad de la unidad, en la que se incluyan los controles necesarios y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles conforme al anexo A de la norma técnica de calidad ISO 27001:2013.

Esta declaración de aplicabilidad debe contener como mínimo la siguiente información:

- Numeral y Control de la norma.
- Nombre del control.
- Responsable.
- Descripción
- Razón para la selección y/o justificación para exclusión.
- Tipo de control: automático o manual.
- Aplica: SI o No.
- Formato o procedimiento asociado.
- Cómo se aplica.

Antes de definir la Declaración de Aplicabilidad, es importante que cada unidad realice las siguientes actividades, con el fin de determinar los activos de información a proteger.

1. Levantamiento e inventario de activos de información (de acuerdo a la guía 1DT-GU-0011 identificación y valoración de activos de información).
2. Realización análisis de riesgos.
3. Realización de planes de tratamiento de riesgo.
4. Implementación controles.

ARTÍCULO 15. RECURSOS. La Policía Nacional, consciente de la importancia de la seguridad de la información, prevé los recursos de acuerdo a la disponibilidad presupuestal para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información a través de la inclusión en el Plan Anual de Necesidades, dentro del cual se consideran los requerimientos necesarios para la implementación de controles técnicos-administrativos.

ARTÍCULO 16. CONOCIMIENTO. El Sistema de Gestión de la Seguridad de la Información de la Policía Nacional, define y mantiene programas de formación, planes de sensibilización y toma de conciencia a través de los Grupos de Telemática.

El plan de sensibilización se revisará, definirá y ejecutará de acuerdo con las necesidades y en coordinación con los demás sistemas de gestión de la Institución. Estas actividades de definición estarán coordinadas entre el Grupo de Seguridad de la Información de la Oficina de Telemática y las áreas encargadas de la generación de competencias en el talento humano y en el manejo de la cultura y la gestión del cambio organizacional.

Dentro de la sensibilización se deberán incluir como mínimo los siguientes temas:

a. Normatividad, incluyendo la Política de Seguridad de la Información de la Institución.
b. La importancia y los beneficios del Sistema de Gestión de Seguridad de la Información.
c. El aporte de cada uno de los funcionarios al sistema desde su cargo o rol.
e. Las implicaciones de la no conformidad con los requisitos descritos en la norma ISO 27001:2013 para el Sistema de Gestión de Seguridad de la Información.

ARTÍCULO 17. COMUNICACIÓN. La Policía Nacional cuenta con la Oficina Asesora de Comunicaciones Estratégicas (COEST), a través de la cual se socializan y difunden los diferentes componentes del Sistema, entre ellos el Manual del Sistema de Gestión de Seguridad de la Información, las políticas, los protocolos, guías que lo soportan y los elementos necesarios para la sensibilización de los funcionarios de la Policía Nacional.

Por lo tanto se debe realizar las coordinaciones necesarias con los responsables de COEST para la comunicación de los temas relacionados con el Sistema de Gestión de Seguridad de la Información.

ARTÍCULO 18. INFORMACIÓN DOCUMENTADA. Todas las decisiones y acciones en cuanto al Sistema de Gestión de Seguridad de la Información estarán documentadas. Para ello se llevará registro de las decisiones tomadas por la Dirección de cada unidad y de los demás documentos que representen un registro para el SGSI (reportes de incidentes, valoraciones de eficacia de los controles, actas, entre otros). En cuanto a los documentos relacionados con el SGSI, también deben estar protegidos y disponibles en sus últimas versiones. Para dar cumplimiento a lo anterior, se debe considerar lo siguiente:

1. **Creación y actualización de documentos:** Se realiza de acuerdo con las tablas de retención documental (TRD) definidas para cada una de las Direcciones y Oficinas Asesoras (dando cumplimiento a la Ley 594 de 2000 Ley general de archivo), liderado por el área de Archivo de la Secretaría General.

   Dentro de las TRD se describe el código, nombre y tiempo de retención de la información definida por los productores de la información.

2. **Control de la información documentada:** El control de la información recibida y enviada por la Institución es administrado por la aplicación de Gestión de Contenidos Policiales (GECOP), a través de la cual se tiene una clasificación inicial de la información que incluye un nivel básico de confidencialidad.

ARTÍCULO 19. EVALUACIÓN DEL DESEMPEÑO. La Policía Nacional ha definido dentro del alcance la medición de indicadores, la evaluación del desempeño de la Seguridad de la Información y la eficacia del Sistema de Gestión de Seguridad de la Información.

La definición de los indicadores del SGSI se describe en el documento 1DS-GU-0013 Guía de Herramientas de Seguimiento y Medición en la Policía Nacional, en donde se establece:

1. Las acciones, procesos y controles de Seguridad de la Información a las que se debe hacer seguimiento.
2. Los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar la mejora continua.
3. Cuándo se deben llevar a cabo el seguimiento y la medición.
4. Quién debe llevar a cabo el seguimiento y la medición.
5. Cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición.
6. Quién debe analizar y evaluar estos resultados.

ARTÍCULO 20. AUDITORÍA INTERNA. Para el monitoreo del Sistema de Gestión de Seguridad de la Información, se incluyó los lineamientos de Seguridad de la Información dentro del alcance del procedimiento de auditorías internas. Este procedimiento se encuentra documentado en el documento 1CI-GU-0002 guía para realizar auditorías internas, en esta se relaciona el desarrollo y la ejecución del programa de auditorías, estableciendo las responsabilidades de las unidades sujeto de auditoría y se establecen los parámetros para que las unidades auditadas elaboren y ejecuten el Plan de Mejoramiento Interno por procesos en la Policía Nacional.

Para las auditorías al Sistema de Gestión de Seguridad de la Información SGSI se debe validar si las actividades de gestión y cumplimiento se encuentran en los siguientes ítems:

1. Son conforme con:
   a. Los propios requisitos de la Institución.
   b. Los requisitos de la Norma ISO 27001:2013.

2. Está implementado y su mantenimiento se realiza eficazmente.

ARTÍCULO 21. REVISIÓN POR LA DIRECCIÓN. La Dirección General de la Policía Nacional deberá revisar el Sistema de Gestión de Seguridad de la Información como mínimo una vez cada año, para ratificar su conveniencia, adecuación y eficacia siguiendo la Guía de Revisión por la Dirección. La revisión de seguridad de la información debe:

1. Identificar cambios en los niveles de riesgo, nuevas amenazas y vulnerabilidades.
2. Identificar cambios en la Institución.
3. Identificar cambios en la Legislación.
4. Revisar el estado del sistema y su implementación.
5. Analizar el cumplimiento de los objetivos de seguridad.
6. Analizar la efectividad de los controles implementados (evolución del estado de la seguridad).
7. Establecer acciones preventivas, correctivas y de mejora.
8. Retroalimentar sobre el desempeño de la Seguridad de la Información (no conformidades, acciones correctivas, seguimiento y resultados de medición, auditorías)
9. Disponer de los registros que evidencien las revisiones.
10. Identificar y solicitar la implementación de oportunidades de mejora continua.

Para conocer el estado de implementación de los controles y su evolución en el tiempo, se aplicará la escala de madurez de acuerdo a los objetivos de control para la información y tecnologías relacionadas de la guía COBIT v4.1.

Como resultado de esta revisión se establecen las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad del cambio del Sistema de Gestión de Seguridad de la Información.

Escala de Madurez

Nivel de Implementación	% de Cumplimiento	Descripción
Gestionado	**100%**	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua.
		Es posible hacer seguimiento y medir el cumplimiento de los protocolos, así como tomar acciones correctivas o preventivas cuando se detectan fallas y hacer seguimiento dichas acciones.
Medible	**80%**	Es posible hacer seguimiento y medir el cumplimiento de los protocolos, aunque no es constante que se tomen acciones correctivas o preventivas.
Definido	**60%**	Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.
Repetible	**40%**	Los procesos se han desarrollado hasta un punto en el cual protocolos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.
Inicial	**20%**	Se ha identificado una situación que debe ser tratada y se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones.
Inexistente	**0%**	Carencia total de procesos relacionados con el SGSI.
		La organización no ha identificado una situación que debe ser tratada.

ARTÍCULO 22. NO CONFORMIDADES Y ACCIONES CORRECTIVAS. De acuerdo con lo establecido en el Manual del Sistema de Gestión Integral de la Policía Nacional se han definido los siguientes procedimientos:

- **Procedimiento acción correctiva y procedimiento acción preventiva**: se encuentra documentado con el código 1MC-PR-0005 "Ejecutar acción correctiva, preventiva y corrección"

en donde se establece la metodología para la identificación y tratamiento de las oportunidades de mejoramiento que surgen en el desarrollo del Sistema.

Así mismo las acciones correctivas deben ser aprobadas por los dueños de proceso de acuerdo a los efectos de las no conformidades encontradas.

Adicionalmente los registros generados por esta gestión deben ser almacenados por el Grupo de Seguridad de la Información quienes son los encargados de realizar el seguimiento y hacer la medición correspondiente de su efectividad.

El Sistema de Gestión de Seguridad de la Información de la Policía Nacional será revisado para su actualización anualmente y/o extraordinariamente cuando sea necesario atendiendo las necesidades de mejora continua.

ARTÍCULO 23. 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.

ARTÍCULO 24. TÉRMINOS Y DEFINICIONES. 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, así:

- 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.

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, 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 protocolo 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. Sobreescritura, desmagnetización 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. 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 que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Controversia. Inconformidad presentada por el usuario de PKI-PONAL durante la generación, renovación o cancelación del certificado digital.

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 (Ethical hacking). 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 disco duro, CD-ROM, y también hace referencia al cableado, circuitos, gabinete, etc. e incluso a elementos externos como impresora, mouse, teclado, monitor y demás periféricos.

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

Incidente de seguridad. Es un evento adverso, confirmado o bajo sospecha, que afecta a un sistema de información, a una red, 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 puede 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 autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les conceden acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios que se encuentran dentro del mismo grupo.

Plan de recuperación ante desastres. Es un conjunto de protocolos 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 busca 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 de las dimensiones están estandarizadas para que 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 cómputo 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 back up 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 que 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 que permite a un sistema o computadora 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 equipos electrónicos que están conectados a él después de un apagado durante un tiempo prudencial, con el fin de realizar un apagado seguro de estos.

Virtualización. Capacidad de 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 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 (Virtual Private Network) Red Privada Virtual. Es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local.

Vulnerabilidades. Son las debilidades, huecos 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 Services es un contenedor que encapsula funciones específicas y hace que estas funciones puedan ser utilizadas en otros servidores.

ARTÍCULO 25. APLICACIÓN EN PROGRAMAS DE FORMACIÓN. La Dirección Nacional de Escuelas en coordinación con la Oficina de Telemática, 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 26. OBLIGATORIEDAD. El presente manual, será de obligatorio cumplimiento para todos los usuarios externos e internos de la Policía Nacional en aras de preservar el Sistema de Gestión de Seguridad de la Información.

ARTÍCULO 27. REVISIÓN Y ACTUALIZACIÓN. El Comité de Seguridad de la Información de la Policía Nacional será el encargado de revisar, actualizar y publicar las modificaciones a los anexos al presente manual donde se describen las buenas prácticas y controles a implementar en la Policía Nacional de acuerdo a la norma técnica ISO 27002:2013.

ARTÍCULO 28. VIGENCIA. La presente Resolución rige a partir de la fecha de su expedición y deroga las disposiciones que le sean contrarias, en especial la Resolución 03049 del 24 de agosto de 2012.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D. C.

Original firmado
General **JORGE HERNANDO NIETO ROJAS**
Director General Policía Nacional de Colombia

Elaboró: PT. PABLO ANDRES GAVIRIA MUÑOZ /OFITE
CT. WILLIAM MUIÑOZ ROJAS/OFITE
Revisó: IJ. GLORIA CECILIA HERNANDEZ TINJACA / OFITE
CT MARLON FAVIAN VALENCIA ORJUELA/OFPLA CENPO
CR MARIO HERNANDO CHAVEZ RODRIGUEZ/OFPLA GUDIR
BG CEIN CASTRO GUTIÉRREZ /OFITE
BG FABIAN LAURENCE CÁRDENAS LEONEL/JEFE OFPLA
Fecha: 12/12/2016

Carrera 59 No 26 21 Piso 5 CAN Bogotá
Teléfonos 3159227 / 9192
ofite.jefat@policia.gov.co
www.policia.gov.co

Anexo No. 1

SEGURIDAD DE LOS RECURSOS HUMANOS

ARTÍCULO 1. SELECCIÓN. El procedimiento para confirmar la veracidad de la información suministrada por el personal que se postula como candidato a ingresar a la Policía Nacional 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 2. TÉRMINOS Y CONDICIONES DEL EMPLEO. Todos los funcionarios de planta, prestación de servicios o cualquier otro tipo de vinculación con la Institución, deben diligenciar los formatos 1DT-FR-0015 Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Servidor Público. El personal externo o contratista diligenciará el formato 1DT-FR-0016 Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Contratistas o Terceros y este hará parte integral del contrato o acuerdo de cooperación que debe reposar junto con las hojas de vida en las oficinas de Talento Humano de cada unidad.

Los funcionarios que sean vinculados a unidades policiales que ejerzan funciones de inteligencia deberán suscribir acta de compromiso de reserva de conformidad con el artículo 33 de la Ley 1621 de 2013

ARTÍCULO 3. TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN. Con el fin de garantizar una correcta gestión, protección, uso y procesamiento de los activos de información de la Institución, a través de los Analistas de Seguridad de cada unidad bajo la supervisión del Comité de Seguridad de la Información, desarrollarán actividades o programas de concienciación relacionados con la Seguridad de la Información dirigido a los funcionarios, terceros o contratistas que desarrollan actividades en la Policía Nacional.

ARTÍCULO 4. TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO. Para la Seguridad de la Información se tendrán en cuenta los siguientes parámetros:

1. La Dirección de Talento Humano a través de los grupos de talento humano de cada unidad, debe actualizar en tiempo real las novedades de cada funcionario en el Sistema de Información para la Administración del Talento Humano "SIATH", para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados.

2. Quien tiene personal externo bajo su supervisión informa de manera inmediata a la Oficina de Telemática y/o grupo de telemática de la unidad o quien haga sus veces la terminación del contrato, con el fin de realizar los trámites de cancelación de derechos de acceso sobre los recursos tecnológicos, sistemas de información y acceso físico a las instalaciones.

3. Los grupos de Talento Humano en coordinación con los encargados de los grupos de Telemática verifican periódicamente las novedades del personal y proceden a bloquear las cuentas de acceso en los recursos tecnológicos, sistemas de información asignados para desempeñar funciones administrativas y/o operativas, y controles de acceso físico a instalaciones de la Institución del personal que presenta algún tipo de novedad.

4. Todos los usuarios están en la obligación de entregar su puesto de trabajo al funcionario designado por el jefe inmediato, junto con la información que produce y administra para el desarrollo del cargo, en el momento que se produzca una novedad administrativa que genere cambios en el desarrollo de las funciones. De igual manera, hacen entrega de todos los recursos tecnológicos y otros activos que les fueron suministrados para el cumplimiento de sus labores.

5. En caso que por fuerza mayor un funcionario no pueda hacer entrega formal del cargo y los activos de información que gestiona, el jefe inmediato deberá solicitar a la Oficina de Telemática el acceso y traspaso de la información institucional al funcionario designado para continuar con dichas funciones.

ARTÍCULO 5. RESPONSABILIDADES DE LOS USUARIOS. Con el fin de disminuir el riesgo de uso inadecuado de la información y los sistemas puestos a disposición para el cumplimiento de las funciones asignadas a los funcionarios, contratistas o personal que tiene algún vínculo con la Institución, se definen las siguientes políticas, así:

a. Las unidades de Policía que cuentan con acceso a servidor de archivos, guardarán la información que se crea importante y sobre ella se garantizará la disponibilidad en caso de presentarse un daño en el equipo asignado, para las unidades que no cuentan con este servicio se dispondrá de la realización de respectivos back up coordinados con el Grupo de

Telemática de la unidad, la custodia de esta información será por el dueño de los activos de información cumpliendo con las Políticas de Seguridad, para la información catalogada como confidencial deberá ser guardada en medios magnéticos debidamente cifrados.

b. La Oficina de Telemática dispondrá en la carpeta de software autorizado ubicada en la intranet institucional (Polired), las copias correspondientes a los softwares utilizados por la Institución para el cumplimiento de las funciones, en caso que una unidad policial requiera la instalación de un producto que no se encuentre en este recurso, deberá contar con la autorización correspondiente del Grupo de Seguridad de la Información, el uso de programas sin su respectiva licencia e instalación sin autorización por parte del Direccionamiento Tecnológico de la Policía Nacional obtenidos por otras fuentes (internet, ejecutables portables, dispositivos USB), puede implicar materialización del riesgo por realizar acciones no autorizadas.

c. Todo software utilizado en la plataforma tecnológica debe contar con licencia y su cumplimiento debe estar acorde a las condiciones de uso establecidas.

d. El uso de dispositivos de almacenamiento masivo externo extraíble (DVD, CD, Dispositivos móviles, pendrives (USB), equipos celulares), puede generar la materialización de riesgos al ser conectados a los equipos de cómputo al llegar a transferir archivos maliciosos o generar la extracción de información Institucional no autorizada, por lo tanto la activación de los puertos USB de los equipos institucionales o conectados a la red LAN deben contar con la autorización del Grupo de Seguridad de la Información mediante previa justificación a través del Sistema de Información para la Gestión de Incidentes en TIC´s SIGMA.

e. Los usuarios son responsables de la información que administran en los equipos asignados, por lo tanto se debe evitar el almacenamiento de información no institucional (música, videos, imágenes, software, ejecutables portables) que pueda presentar violación a derechos de autor y propiedad intelectual, tanto en equipos de cómputo, como en servidor de archivos en los lugares donde este implementado.

f. Los funcionarios solo tendrán acceso a datos y recursos tecnológicos asignados, y serán responsables disciplinaria, administrativa y legalmente de la divulgación de información no autorizada.

g. Cada funcionario tiene como responsabilidad proteger la información contenida en documentos, formatos, y toda la producida como resultado de los procesos que se realizan en la Institución.

h. Cualquier incidente de seguridad informática debe ser reportado al grupo de Telemática de la unidad y su vez al grupo CSIRT-PONAL.

i. El uso del internet está enfocado al cumplimiento de las actividades institucionales, por lo tanto los usuarios harán uso de los equipos y medios asignados, no se permite la conexión de dispositivos como módems externos, o equipos celulares que habilitan el acceso a internet, a no ser que se encuentre autorizado por la Oficina de Telemática para el caso de las unidades en donde el acceso a la red LAN no es viable por diferentes restricciones.

j. Los equipos de cómputo deben contar con los controles necesarios para poder acceder a los servicios de internet, como antivirus, actualizaciones y demás controles establecidos por la Oficina de Telemática.

k. Se debe ejercer un control de acceso a la red, por lo tanto los funcionarios no usarán conexiones distintas a las que provee la Oficina de Telemática, por lo tanto el uso de túneles VPN o conexiones TOR como complemento de los navegadores no están autorizados, y las conexiones que se generen y se evidencien en los sistemas de control adoptados por el Direccionamiento Tecnológico tendrán las sanciones a que haya lugar.

l. Las unidades o dependencias que adquieran redes inalámbricas deben cumplir con la política y condiciones de seguridad de las redes cableadas, estas deben estar separadas de las redes LAN con el respectivo control de contenido y controles necesarios, además de estar debidamente autorizadas por la Oficina de Telemática de la Policía Nacional.

m. El acceso a redes sociales, paginas interactivas como chats se encuentra restringido por lo que solo se hará uso de las herramientas para tal fin que provee la Oficina de Telemática, en caso de ser necesario su uso para el cumplimiento de las funciones asignadas por el cargo o dependencia, debe ser solicitada previa justificación a través del Sistema de Información para la Gestión de Incidentes en TIC´s SIGMA para su respectivo análisis por parte del Grupo de Seguridad de la Información.

n. El uso de canales de streaming debe estar regulados y solo se permite a los usuarios que en cumplimiento de sus funciones lo requieren, ya que se debe dar prioridad al sostenimiento de las aplicaciones y sistemas de información Institucional.

o. La descarga P2P o de archivos de páginas en donde se almacena contenido multimedia se debe controlar con el fin de evitar que sean descargados archivos maliciosos o que atenten contra la propiedad intelectual y derechos de autor.

Anexo No. 2

GESTIÓN DE ACTIVOS

ARTÍCULO 1. INVENTARIO DE ACTIVOS. Para el manejo de los activos de información de la Policía Nacional se tiene en cuenta lo siguiente:

1. Cada unidad de Policía debe nombrar un funcionario, el cual es responsable de realizar el inventario de activos, su clasificación y recomendar ante el Comité de Seguridad de la Información el tratamiento de los mismos de acuerdo a los requerimientos de la Institución, para ello se debe nombrar mediante acto administrativo que el Comandante bajo sus facultades legales disponga.

2. Para efectuar el inventario se deben aplicar la Guía 1DT-GU-0011 identificación y valoración de activos de información, en la cual se describe la metodología que permite identificar, valorar y clasificar los activos de información, servicios, medios de procesamiento que soportan la gestión de los procesos y establecer su nivel de clasificación de acuerdo con las escalas contenidas en la misma.

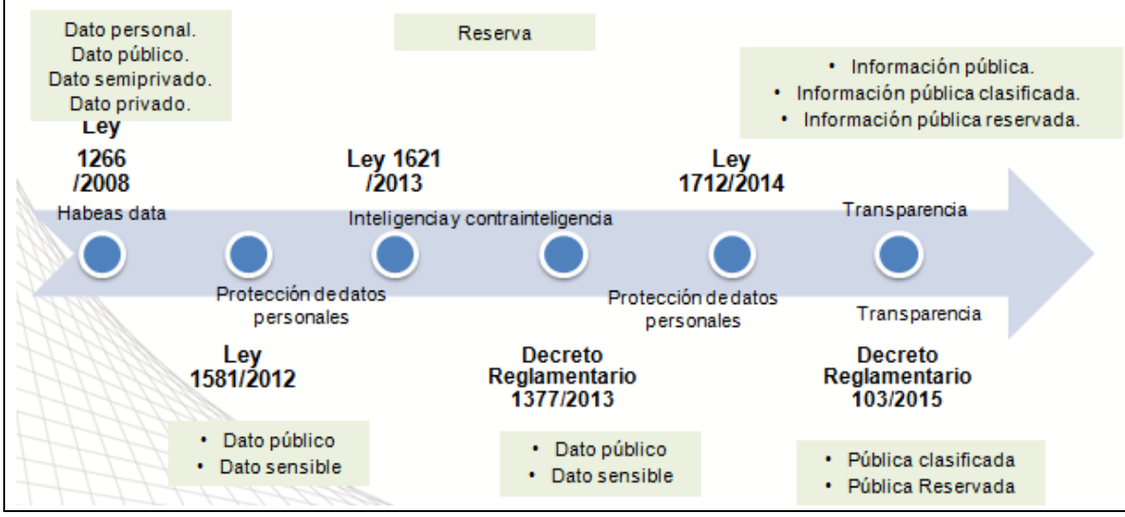
3. El inventario debe actualizarse como mínimo una vez al año y ser avalado por el Comité de Seguridad de la Información interno de cada unidad.

4. Los dueños de procesos o quien haga sus veces deben gestionar con el responsable designado la identificación, valoración y clasificación de sus activos de información dentro del inventario, manteniendo información detallada para cada activo sobre su valoración y clasificación en confidencialidad, integridad, disponibilidad. Igualmente deberá hacer el tratamiento adecuado correspondiente a su clasificación y corrección de inconsistencias detectadas dentro de la matriz de riesgos.

5. Todos los funcionarios, personal que tenga vínculo directo con la Institución, propietario o custodio de activos de información, debe informar al dueño del activo o al grupo de Telemática, falencias en el tratamiento de la información con el fin de adoptar las acciones pertinentes para su protección.

6. Una vez realizado el inventario de activos se debe dar a conocer el responsable, propietario y/o custodio de los mismos, esta actividad de notificación se puede realizar mediante acta, comunicado oficial o una notificación en la cual se le indique cual es el activo, su clasificación, sus responsabilidades y los controles aplicados a ese activo.

ARTÍCULO 2. CLASIFICACIÓN DE LA INFORMACIÓN. La Policía Nacional para clasificar la información Institucional, se basa en las Leyes y Decretos vigentes, como se muestra la siguiente imagen.



Por lo tanto los parámetros descritos a continuación son de obligatorio cumplimiento para los funcionarios de Policía Nacional, los cuales deben garantizar y velar por el cumplimiento de los mismos. La Policía Nacional tiene dos grupos de clasificación, así:

1. **INFORMACIÓN PÚBLICA CLASIFICADA**. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas, necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 del 06/03/2014. En este sentido se consideran las siguientes definiciones:

a. **Pública**. Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. (Ley 1581/2012). Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377/2013).

b. **Dato semiprivado.** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios. (Ley 1266/2008).

c. **Dato privado**. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1266/2008).

d. **Datos sensibles.** Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. Ley 1581/2012- Decreto Reglamentario 1377/2013.

2. **INFORMACIÓN PÚBLICA RESERVADA.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en la Ley 1712 /2014.

Reserva. Por la naturaleza de las funciones que cumplen los organismos de inteligencia y contrainteligencia sus documentos, información y elementos técnicos estarán amparados por la reserva legal por un término máximo de treinta (30) años contados a partir de la recolección de la información y tendrán carácter de información reservada. (Artículo 33 Ley Estatutaria 1621/2013).

ARTÍCULO 3. DOCUMENTOS DE INTELIGENCIA Y CONTRAINTELIGENCIA. Son todos aquellos documentos originados, procesados y/o producidos en los organismos de inteligencia y contrainteligencia con los niveles de clasificación establecidos en la Ley 1621 de 2013. Estos documentos de conformidad con la ley están protegidos por la reserva legal. Los documentos de inteligencia y contrainteligencia pueden estar contenidos en medios físicos, digitales o similares, de acuerdo con los desarrollos científicos o tecnológicos y deben encontrarse bajo la administración, protección, custodia y seguridad de los organismos de inteligencia y contrainteligencia, los receptores autorizados o las entidades del Estado que de acuerdo con la ley deban conocer de ellos. (Decreto 1070/2015)

ARTÍCULO 4. NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN DE INTELIGENCIA Y CONTRAINTELIGENCIA. Los documentos, información y elementos técnicos de los organismos de inteligencia y contrainteligencia estarán amparados por la reserva legal y se les asignará un nivel de clasificación (Decreto 1070/2015), así:

a. **Ultrasecreto**. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al exterior del país los intereses del Estado o las relaciones internacionales.

b. **Secreto**. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior del país los intereses del Estado.

c. **Confidencial**. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar directamente las instituciones democráticas.

d. **Restringido**. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información de las instituciones militares, de la Policía Nacional o de los organismos y dependencias de inteligencia y contrainteligencia, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes.

Parágrafo**.** Los documentos de inteligencia y contrainteligencia que contengan información relacionada con diferentes niveles de clasificación de seguridad, asumirán la del nivel más alto que tenga la información contenida en ellos.

ARTÍCULO 5. SEGURIDAD Y RESTRICCIONES EN LA DIFUSIÓN DE PRODUCTOS E INFORMACIÓN DE INTELIGENCIA Y CONTRAINTELIGENCIA. Los organismos y dependencias de inteligencia y contrainteligencia deberán a los receptores autorizados por la ley, indicar la reserva legal a la que está sometida la información y expresar, al receptor autorizado de la misma, si se trata de un producto de inteligencia o contrainteligencia "de solo conocimiento" o "de uso exclusivo" teniendo como referencia las siguientes restricciones para cada caso, (Decreto 1070/2015) así:

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

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

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

ARTÍCULO 6. ETIQUETADO DE LA INFORMACIÓN Y MANEJO DE ACTIVOS. Todos los documentos físicos de la Policía Nacional estarán etiquetados de acuerdo con las tablas de retención documental que aplique para cada unidad de Policía y se define su tiempo de permanencia en cada etapa del ciclo de vida de los documentos de acuerdo a estas mismas y los lineamientos del proceso de Gestión Documental.

ARTÍCULO 7. GESTIÓN DE MEDIOS DE SOPORTE REMOVIBLES. No está permitido que los funcionarios de Policía y/o terceros que tengan vínculo contractual o se encuentren desarrollando actividades para la Institución usen medios de almacenamiento masivo de su propiedad para almacenar información institucional sin que se cuente con las técnicas criptográficas para su protección.

ARTÍCULO 8. DISPOSICIÓN DE LOS MEDIOS DE SOPORTE. La eliminación de los medios de almacenamiento (USB, discos duros, etc.) se hace a través de borrado seguro ya sea mediante el desmagnetizador para aquellos dispositivos que así lo permitan o perforación, Es importante mencionar que la destrucción y/o eliminación segura se documenta mediante acta, registro documental y/o fotográfico para garantizar la no restauración o recuperación de información.

Parágrafo: Los receptores de productos de inteligencia y contrainteligencia, atenderán, aplicarán y responderán por el cumplimiento de la Ley 1621 de 2013, así mismo, no podrán generar carpetas personales, físicas y/o virtuales, como antecedentes de los productos e información suministrada por el Servicio de Inteligencia Policial. Igualmente, garantizarán la reserva, recepción y uso de la información, destrucción final del documento o devolución del mismo, así como, el deber objetivo de cuidado, de no acatar dichas disposiciones podrá ser causal de mala conducta y se accionará

las medidas necesarias para establecer la responsabilidad en materia administrativa, disciplinaria y penal correspondiente.

- La información ultrasecreta deberá ser destruida o devuelta a la unidad de inteligencia que entregó el documento en 1 hora.
- La información secreta deberá ser destruida o devuelta a la unidad de inteligencia que entregó el documento en 3 horas.
- La información confidencial deberá ser destruida o devuelta a la unidad de inteligencia que entregó el documento en 6 horas.
- La información restringida deberá ser destruida o devuelta a la unidad de inteligencia que entregó el documento en 12 horas.

Por lo anterior, se deberá indicar al personal de la Policía Nacional y de otros organismos designados como "receptores del Servicio de Inteligencia Policial", que les corresponderá adoptar las medidas establecidas para impedir que se copie, porte, reproduzca, almacene, manipule o difunda cualquier tipo de información de inteligencia y contrainteligencia con fines distintos al cumplimiento de su misión.

El control y la observancia frente a la correcta aplicación de lo dispuesto anteriormente es responsabilidad de todo el personal uniformado, bajo liderazgo de los directores, jefes y comandantes en sus diferentes niveles de gestión, con el fin de optimizar, preservar y fortalecer los preceptos establecidos para la disposición final de la información de inteligencia y contrainteligencia.

ARTÍCULO 9. TRANSFERENCIA DE MEDIOS DE SOPORTE FÍSICO. Para el transporte de información en medios físicos (digital o impresa) se establecen mecanismos para su transporte los cuales contemplan:

1. Uso de servicios de mensajería por correo certificado, a través de contratos formales para la protección de la información, durante el transporte se debe considerar las siguientes medidas, así:
   a. Uso de recipientes cerrados.
   b. Entrega certificada.
   c. Embalaje con sellos de seguridad o a prueba de apertura no autorizada.
   d. Uso de rutas diferentes, para las entregas.

2. La entrega física de información reservada se realiza por funcionarios de la Institución, cumplen con las mismas características, estipulados en el ítem anterior.

Anexo No. 3

CONTROL DE ACCESO

ARTÍCULO 1. CONTROL DE ACCESO. La Policía Nacional establece como control a los recursos tecnológicos, el modelo de Administración de identidades y Control de acceso (IAM), implementado mediante el Sistema de Identificación Policial Digital, que de manera integrada al Sistema para la Administración del Talento Humano (SIATH), 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. Por tanto, todos los desarrollos de Sistemas de Información para uso de la Institución deben estar integrados al IPD (Sistema de Identificación Policial Digital).

La Identificación Policial Digital o usuario empresarial es entregado al funcionario de Policía una vez es dado de alta como alumno en el SIATH (Sistema de Información y Administración del Talento Humano), e ingresa por primera vez al PSI (Portal de Servicios Internos) y acepta términos de uso que allí encuentra.

El usuario empresarial es único e intransferible, por lo cual el uso no adecuado, su préstamo o uso de otra cuenta de la cual no sea titular acarreará las acciones de tipo penal, disciplinario, administrativo y fiscal a que haya lugar, toda vez que se está exponiendo la información a modificaciones, alteraciones o divulgaciones no autorizadas. Por tanto la fuga, pérdida, alteración y/o modificación de la información que sea manipulada a través del usuario empresarial, sea esta en forma intencional, negligente o con violación al deber objetivo de cuidado, será únicamente responsabilidad del funcionario a quien se le asignó el mismo, e implicaran las acciones correspondientes, así mismo se deberá tener en cuenta las recomendaciones dadas al momento de la asignación de usuario y términos de uso.

ARTÍCULO 2. ACCESO A REDES Y A SERVICIOS EN RED. Las conexiones no seguras a los servicios de red pueden afectar a toda la Institución, por lo tanto, se realiza el control 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.

Por lo tanto se desarrollan actividades con el fin de activar y desactivar derechos de acceso a las redes las cuales comprenden:

a. La identificación de los equipos en la red se realiza de acuerdo a lo estipulado en la guía estándar nomenclatura de usuario.

b. Los equipos que se encuentren conectado a la red LAN de la Policía Nacional deben estar promovidos al dominio policia.gov.co.

c. 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.

d. Los ámbitos de red del servicio DHCP deben tener direcciones IP excluidas de la distribución para evitar accesos no autorizados a la red de datos.

ARTÍCULO 3. CONTROL DE CAMINO FORZADO. Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de la Policía Nacional, o para el uso no autorizado de servicios de información, por esto, el camino de las comunicaciones debe ser controlado; se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales se encuentra autorizado acceder, mediante la implementación de controles en diferentes puntos de la misma, en atención a lo anterior se debe tener en cuenta:

- La navegación ilimitada en internet por la plataforma tecnológica es controlada.
- Las comunicaciones con origen y destino autorizados se debe controlar a través de firewalls de red.

ARTÍCULO 4. REGISTRO, SUMINISTRO DE ACCESO Y CANCELACIÓN DE USUARIO. Para realizar solicitud de acceso a un recurso tecnológico de la Institución, se debe registrar el caso en el Sistema de Información para la Gestión de Incidentes en TIC´S SIGMA, verificando que el usuario haya diligenciado el formato 1DT-FR-0015 Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Servidor Público, el personal externo diligenciará el formato 1DT-FR-0016 Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Contratistas o Terceros, y el formato de asignación de usuario y términos de uso.

A través de IPD cada vez que el funcionario este en una novedad administrativa se cancelará el acceso a los recursos, no obstante es deber del funcionario informar mediante caso SIGMA o al grupo de Telemática, cuando el cargo o función cambie y no requiera acceso a los recursos tecnológicos que tiene asignados, para lo cual el jefe directo y los grupos de Telemática a nivel nacional deben supervisar mediante revistas aleatorias los accesos asignados a los funcionarios de su unidad y seguir el protocolo para realizar remoción de derechos de acceso.

Los funcionarios que tienen a cargo usuarios con privilegios y/o administradores, deben diligenciar el formato 1DT-FR-0005 entrega de usuario con altos privilegios e informar cuando se les presente novedad administrativa de vacaciones, retiro, cambio de cargo, licencia y demás novedades.

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, así como las políticas de protección de usuario desatendido, escritorio despejado y pantalla limpia.

ARTÍCULO 5. GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO. La Policía Nacional ha restringido y controla la asignación y uso de acceso privilegiado de acuerdo a las siguientes directrices, así:

1. 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.

2. 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 computadores 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.

El acceso remoto se debe realizar mediante herramientas autorizadas por la Oficina de Telemática.

3. 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 están restringidas, para su implementación en las unidades deben tener un concepto de viabilidad por parte de la Oficina de Telemática, y seguir las recomendaciones del Grupo de Seguridad de la Información para su adecuada gestión y protección.

ARTÍCULO 6. GESTIÓN DE AUTENTICACIÓN USUARIOS Y CONTRASEÑAS. La identificación y autenticación de usuarios se encuentra definido en la guía estándar nomenclatura de usuarios, si es usuario empresarial se realiza a través del Sistema de Información IPD (Sistema de Identificación Policial Digital)

El sistema de gestión de contraseñas en la Policía Nacional, es administrado a través de la herramienta IPD, en donde se cumple con los siguientes controles, así:

1. Permite que los usuarios seleccionen y cambien sus propias contraseñas.
2. Exige que se escojan contraseñas de calidad.
3. Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez.
4. Lleva un registro de las contraseñas usadas previamente, e impide su reúso.
5. No visualizar contraseñas en la pantalla cuando se está ingresando.
6. Almacena y transmite las contraseñas en forma protegida.

Para los recursos tecnológicos que no están asociados a IPD, se registra la solicitud en el Sistema de Información para la Gestión de Incidentes en TIC´S SIGMA, para ser escalado al administrador del sistema.

ARTÍCULO 7. REVISIÓN, CANCELACIÓN O ELIMINACIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS. La Oficina de Telemática verifica periódicamente las novedades del personal y procede a bloquear las cuentas de acceso en los recursos tecnológicos, Sistemas de Información y acceso a instalaciones de la Institución del personal que presenta algún tipo de novedad administrativa.

ARTÍCULO 8. RESTRICCIÓN DE ACCESO A INFORMACIÓN. La restricción de acceso a la información a través de una aplicación, se realiza mediante 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.

Estas condiciones deben ser definidas en la planeación, desarrollo e implementación de recursos tecnológicos, para lo cual debe quedar por escrito la política de accesos y roles.

ARTÍCULO 9. CONEXIÓN SEGURA. El acceso a los equipos que utiliza el personal de la Policía Nacional 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.
7. De igual forma, de acuerdo a la criticidad del área o sistemas de información se solicitara métodos de autenticación fuerte como lectores biométricos, tarjetas inteligentes y/o tokens.
8. 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.

9. 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.
10. Por la misionalidad de la Policía Nacional, no se limita el tiempo de conexión, ni se establecen restricciones en la jornada laboral.
11. El control a la conexión se realiza a los usuarios, a través del protocolo de administración de identidades, el cual bloquea los usuarios, ante una ausencia laboral.

ARTÍCULO 10. USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS. La Policía Nacional cuenta con un control de dominio, que no permite la instalación de software y cambios de configuración del sistema, por lo tanto, los usuarios finales no deben tener privilegios de usuario administrador excepto los técnicos de Telemática a nivel país, quienes hacen uso de usuario administrador para configurar los equipos de cómputo de su unidad; por tanto, es deber de los usuarios finales informar oportunamente cuando su usuario permita instalar programas o hacer cambios de configuración.

ARTÍCULO 11. CONTROL DE ACCESO A CÓDIGOS FUENTE DE PROGRAMAS. El acceso al código fuente y demás documentación de los sistemas de información están protegidos de acceso o modificaciones no autorizadas, para lo cual el proceso de Direccionamiento Tecnológico, implementó los siguientes controles:

1. Suministrar al grupo de desarrollo o funcionarios que desempeñe estas funciones el código fuente para su modificación, garantizando la correlación entre fuente y ejecutable.
2. Registrar todos los programas fuente en uso, indicando nombre del programa, programador, responsable que autorizó el cambio, versión, fecha de última modificación, fecha del último ejecutable, estado (modificación, desarrollo).
3. Llevar versiones del código fuente y los sistemas de información.
4. Garantizar que un mismo código fuente, no sea modificado por más de una persona a la vez.
5. Propender porque un programa ejecutable en producción este asociado a un único programa fuente.
6. Generar el programa ejecutable solo desde el ambiente de producción.
7. Ejercer la protección de códigos fuente por parte del personal del grupo de administración de recursos tecnológicos o los grupos de Telemática donde se realice desarrollo o ajuste de aplicaciones.
8. Evitar que programas fuentes históricas reposen en los ambientes de producción.
9. Realizar copias de respaldo de los programas fuentes.

ARTÍCULO 12. POLÍTICA DISPOSITIVOS MÓVILES Y TELETRABAJO. La Policía Nacional de Colombia aprueba el uso de los dispositivos móviles autorizados por la Institución por parte de los funcionarios de la entidad siempre y cuando no pongan en riesgo la Seguridad de la Información, de igual manera se tendrá en cuenta lo siguiente:

1. No será permitido almacenar en dispositivos móviles personales información de la Policía Nacional que no esté clasificada como pública.
2. Es responsabilidad del funcionario garantizar el adecuado uso del medio móvil asignado, conectándolo siempre a redes confiables, que no sean de acceso público para evitar que se contagien de cualquier amenaza pertinente a estos dispositivos (virus, troyanos, malware).
3. Estos dispositivos deberán mantenerse cifrados o monitoreados por medio de las herramientas que la Policía Nacional designe para tal fin.
4. El trabajo remoto solo es autorizado por el responsable de la unidad de la cual dependa el funcionario que solicite el permiso. Dicha autorización solo se otorgará por la Oficina de Telemática una vez se verifique las condiciones de seguridad del ambiente de trabajo.
5. Los funcionarios autorizados podrán acceder a la red de la Policía Nacional únicamente por medio de túneles SSL o VPN y utilizando los equipos de cómputo institucionales asignados para realizar sus funciones o equipos externos previamente autorizados con su debida justificación.

ARTÍCULO 13. CONTROL DE CONEXIONES DE LAS REDES INALAMBRICAS. En las unidades que se cuentan con accesos inalámbricos previa validación y autorización por parte del Direccionamiento Tecnológico de la Policía Nacional, estas deben contemplar los siguientes controles de seguridad, así:

1. Las redes inalámbricas deben estar separadas de las redes LAN, en donde se garantiza que no se tenga acceso a los recursos de red Institucional.

2. Debe contar con el respectivo control de acceso y filtrado web.
3. Se deben asignar contraseñas a las redes inalámbricas cambiando la contraseña por defecto de los dispositivos WI-FI asignando sistema de cifrado WAP2 o superior.
4. Las contraseñas por defecto de administración de los dispositivos WI-FI deben ser cambiadas por contraseñas seguras.

ARTÍCULO 14. USO ADECUADO DE LA PLATAFORMA TECNOLÓGICA. La Policía Nacional cuenta con un canal de datos apto para la realización de las actividades y conexiones que permiten que los múltiples accesos al centro de datos de la Institución responda de una manera eficaz, por lo tanto se han implementado controles que a su vez contribuyen a mitigar la materialización del riesgo de fuga de información, la propagación de software de código malicioso de forma interna y externa los cuales pueden comprometer directamente la Seguridad de la Información y afectar los pilares fundamentales de confidencialidad disponibilidad e integridad; en atención a lo anterior se restringen los siguientes usos así;

a. Navegación en sitios de contenidos sexuales, o que tengan relación con información de carácter explícita en el cual se pueda materializar un delito informático.

b. Publicación o envío e información categorizada como confidencial fuera de las unidades y dependencias de la Policía Nacional sin previa autorización y sin contar con los previos controles que permitan salvaguardar la información.
c. Uso de servicios disponibles en internet que permitan establecer una conexión o intercambios no autorizados.

d. Publicación de anuncios comerciales o publicidad mediante la plataforma tecnológica, salvo aquellas dependencias que lo requieran dentro de sus funciones, para lo cual deberá contar con una justificación previa del jefe la oficina.

e. Promover o mantener asuntos o negocios personales a través de la red o infraestructura tecnológica de la Policía Nacional.

f. Descarga, instalación y utilización de programas, aplicaciones, software no licenciado, software portable no relacionados con la actividad laboral y que afecte el rendimiento o procesamiento de las estaciones de trabajo y pueda poner en peligro la red institucional.

g. Uso de cuentas de correos no institucionales o de terceros, para el manejo de la información o recepción de actividades realizadas por la Policía Nacional.

h. Empleo de herramientas de mensajería instantánea no autorizada por la Oficina de Telemática de la Policía Nacional para el manejo de información Institucional o coordinación de servicio de Policía.

i. No se permite la publicación de avisos clasificados en los portales internos, difusión mediante las plataformas de correo electrónico sobre compra o adquisición de material de guerra, y contenido sexual explícito.

j. Teniendo en cuenta que la Policía Nacional cuenta con una Oficina de Comunicaciones Estratégicas encargada de realizar la promoción de sus servicios, no se permite la creación de páginas web, blogs, o sitios diferentes a los oficiales manejados por esa oficina.

Anexo No.4

CONTROLES CRIPTOGRÁFICOS

ARTÍCULO 1. POLÍTICA SOBRE EL USO DE 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.

El uso de controles criptográficos, contempla los siguientes aspectos, así:

1. Se utilizan controles criptográficos en los siguientes casos:

   a. Protección de contraseñas de acceso a sistemas y demás servicios que requieran autenticación.

b. Transmisión de información sensible al interior de la Policía Nacional y fuera de ella.
c. Transmisión de información de voz a través de los radios de comunicación.
d. Servicios institucionales que recopilen información de terceros.
e. Uso de correo electrónico institucional, vía web.
f. Mensajería instantánea institucional.
g. 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 protocolos 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. La información que se encuentra bajo la protección de la Ley 1621 de 17 de abril de 2013, usará los controles criptográficos definidos por la Dirección de Inteligencia Policial.

5. 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 las unidades.

ARTÍCULO 2. GESTIÓN DE CLAVES. Las claves criptográficas son protegidas contra modificación, destrucción, copia o divulgación no autorizada, así mismo, las claves criptográficas raíz de la infraestructura de llave pública Institucional, estarán protegidas en caja fuerte.

Anexo No. 5

SEGURIDAD FÍSICA Y DEL ENTORNO

ARTÍCULO 1. PERÍMETRO DE SEGURIDAD FÍSICA. La Policía Nacional realiza el mayor esfuerzo en implementar y garantizar la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro en todas las unidades policiales, así como en entornos abiertos. Del mismo modo, controla las amenazas físicas externas e internas y las condiciones medioambientales de sus instalaciones.

Para la seguridad de instalaciones, se deben contemplar los siguientes aspectos:

1. Antecedentes.
2. Ubicación y límites.
3. Características topográficas.
4. Características de la población.
5. Problemática social.
6. Análisis del índice delincuencial.
7. Vías de acceso.
8. Unidades de apoyo.
9. Estructura arquitectónica.
10. Distribución interna.
11. Barreras perimetrales.
12. Sistemas de vigilancia y control.
13. Controles de acceso.
14. Plan de emergencia.
15. Seguridad en áreas de procesamiento y/o almacenamiento de información sensible.
16. Seguridad industrial.
17. Salud ocupacional y las demás que sean necesarias para garantizar el fortalecimiento de la seguridad física de las instalaciones.

ARTÍCULO 2. CONTROLES FÍSICOS DE ENTRADA. En las unidades de Policía se deberá seguir las siguientes directrices para la aplicación de los controles de entrada, así:

1. Al ingreso de las instalaciones se debe llevar un registro de la fecha, hora de entrada y salida de los visitantes; todos los visitantes deben ser supervisados.

2. En las unidades que se cuente con controles de entrada a las oficinas y/o áreas específicas asistidas por dispositivos biométricos y/o RFID, se debe verificar mensualmente el personal autorizado en cada uno de estos.
3. Todos los funcionarios, contratistas y partes externas deben portar algún tipo de identificación visible, y se debe notificar de inmediato al personal de seguridad de instalaciones si se encuentran visitantes no acompañados, y sin la identificación visible.

ARTÍCULO 3. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES. Las unidades de Policía cuentan con los grupos de emergencia, brigadistas, planes de evacuación los cuales deben ser socializados como mínimo una vez en el semestre. Así mismo, los servicios de seguridad de instalaciones velan por la protección en cuanto a prevención de ataques con explosivos realizando las coordinaciones para las respectivas revistas con el fin de evitar la materialización de riesgos asociados a posibles atentados.

ARTÍCULO 4. TRABAJO EN ÁREAS SEGURAS. Las áreas seguras de las unidades de Policía son identificadas por el Comité de Seguridad de la Información tomando como referencia la protección de activos de información vitales como unidades de procesamiento (servidores, almacenamiento) equipos de activos y donde se maneje información sensible, para ello se debe considerar las siguientes directrices:

1. Las áreas seguras deben estar cerradas con llave o con sistemas de control de acceso y se revisarán periódicamente.
2. El acceso a las instalaciones debe llevar un registro de la fecha, hora de entrada y salida del personal que ingresa a las áreas seguras y acompañar al visitante en su recorrido.
3. No se debe permitir equipo fotográfico, de video, audio u otro equipo de grabación tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.

ARTÍCULO 5. ÁREAS DE DESPACHO Y CARGA. En las áreas que se cumplan estas actividades se deberá cumplir con lo siguiente:

1. El acceso a las zonas de despacho y carga desde el exterior de las instalaciones debe estar restringida solo al personal identificado y autorizado.
2. Las áreas de despacho y carga deben estar limitadas de manera que los suministros se puedan cargar o descargar sin que el personal de despacho tenga acceso a otras áreas de las instalaciones.
3. Los elementos que ingresan se deben inspeccionar y examinar para determinar la presencia de explosivos, químicos u otras sustancias o materiales peligrosos, antes que se retire el personal que está realizando la entrega.
4. Todos los elementos que ingresan se deben registrar de acuerdo a los protocolos de gestión de inventarios.

ARTÍCULO 6. UBICACIÓN Y PROTECCIÓN 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, así:

1. Los centros de procesamiento y almacenamiento institucionales propenden por el cumplimiento de la norma internacional EIA/TIA 942.
2. Los equipos de cómputo tipo servidor de cada unidad están agrupados en un solo lugar. Estos lugares deben contar con controles de accesos físicos.
3. 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.
4. El acceso a los centros de procesamiento y almacenamiento está restringido y su ingreso debe estar documentado dejando la trazabilidad correspondiente. .
5. En los centros de datos se deben implementar controles ambientales con el fin de minimizar la materialización de riesgos asociados a la pérdida de información.

ARTÍCULO 7. SERVICIOS PÚBLICOS DE SOPORTE. 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:

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

2. Se disponen de múltiples toma corrientes o líneas de suministro.
3. 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.
4. 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.
5. 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.
6. Las instalaciones eléctricas están protegidas por sistemas de tierras de protección, que cumplen con los estándares vigentes para sistemas de comunicaciones.
7. Toda instalación eléctrica está protegida contra fluctuaciones de voltaje por dispositivos adecuados tales como breakers y supresores de picos.
8. 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.
9. 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.
10. Se cuenta con iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.
11. Se cuenta con protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

ARTÍCULO 8. SEGURIDAD DEL CABLEADO. Para el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información con el fin de protegerlos contra intercepción o daño, se debe cumplir con:

1. El reglamento técnico de instalaciones eléctricas – RETIE, expedido por el Ministerio de Minas y Energía.
2. Los estándares ISO/IEC/11801, ANSI/EIA/TIA 568A o 568B o con la reglamentación vigente expedida al respecto.
3. Las instalaciones de cableado estructurado están protegidas contra la influencia o daño causado por agentes externos.
4. Los elementos metálicos que forman parte de los cableados estructurados están conectados al sistema de tierras del edificio.
5. Los equipos se albergan en sitios acondicionados a temperaturas entre 16 y 22 grados centígrados.
6. 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.
7. Las instalaciones de cableado se deben realizar siguiendo la arquitectura de los edificios, debidamente protegidos con canaleta en caso de realizarlas al interior, o con tubo metálico en caso de instalación tipo intemperie

ARTÍCULO 9. MANTENIMIENTO DE EQUIPOS. El mantenimiento a la plataforma tecnológica posibilita su disponibilidad e integridad, teniendo en cuenta los siguientes controles:

1. Mantenimiento preventivo a los equipos de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.
2. Uso de un sistema de información que permite llevar el control del detalle de la frecuencia de mantenimiento de los equipos.
3. Sólo el personal de mantenimiento autorizado puede llevar a cabo reparaciones en los equipos.
4. El responsable técnico de los equipos registra todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
5. El responsable técnico de los equipos registra el retiro de los equipos de las instalaciones de la Policía Nacional para su mantenimiento, en caso de extraer unidades de almacenamiento de las instalaciones policiales, estas deben ser borradas de manera segura.
6. En las especificaciones técnicas para contratos de mantenimiento o garantía se contempla el suministro de nuevos discos sin realizar la entrega del disco dañado.
7. Eliminación de manera segura de la información confidencial que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de respaldo.
8. El responsable funcional del equipo acompañará el mantenimiento de los equipos que contengan información sensible.

ARTÍCULO 10. RETIRO DE ACTIVOS. Los equipos, información o software no se pueden retirar de su sitio sin previa autorización, para lo cual se debe realizar un documento controlado (Acta, comunicado oficial), donde se especifique el estado del activo al momento de salir de las instalaciones, el tiempo que se va a encontrar fuera de las mismas y el motivo por el cual el activo debe ser retirado de su lugar habitual, de igual manera se deben realizar verificaciones periódicas para detectar retiros no autorizado.

ARTÍCULO 11. SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DEL PREDIO. El uso de equipos institucionales, para uso fuera de las instalaciones policiales, está restringido a equipos portátiles y móviles. La seguridad para estos equipos es equivalente a la suministrada a los recursos tecnológicos ubicados dentro de las unidades de Policía y controles adicionales para mitigar los riesgos que por sí mismo conlleva el uso estos, así:

1. Los equipos institucionales no pueden conectarse a redes inalámbricas públicas o no conocidas.
2. El software instalado en los equipos institucionales de uso externo debe estar totalmente licenciado y avalado por la Oficina de Telemática.
3. Los usuarios por defecto o de fábrica de los equipos de cómputo deben ser deshabitados y el acceso a estos se debe realizar mediante el uso de usuario y contraseña.
4. Los usuarios usados en estos equipos no deben tener privilegios de administración.
5. Los equipos de cómputo portátiles deben tener controles criptográficos (discos e información cifrada) con el fin de proteger la información que allí se almacena.

ARTÍCULO 12. DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS. Cuando el equipo se encuentra en óptimas condiciones y puede ser asignado a otro funcionario, se realiza borrado seguro de la información, en el momento en que los dispositivos cumplen el ciclo vida y se va a realizar disposición final se efectúa destrucción física del dispositivo de almacenamiento, estas acciones se encuentra descritas en el procedimiento 1DT-PR-0020 Borrado Seguro de la Información.

ARTÍCULO 13. EQUIPOS SIN SUPERVISIÓN DE LOS USUARIOS. Los usuarios deberán cerrar la sesión cuando hayan terminado de realizar los respectivos trabajos en la plataforma institucional, de igual forma los equipos de cómputo deben contar con un mecanismo de bloqueo automático como el de protector de pantalla después de cinco (5) minutos de inactividad.

ARTÍCULO 14. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA. Estas políticas tienen como fin reducir los riesgos de acceso no autorizado, pérdida y daño de la información. Para lo cual se establecen las siguientes pautas:

1. 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.
2. 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.

3. Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
4. Retirar inmediatamente la información sensible, una vez impresa.
5. El escritorio de los equipos de cómputo no deben tener accesos directos a archivos.

Anexo No. 6

SEGURIDAD DE LAS OPERACIONES

ARTÍCULO 1. PROTOCOLO DE OPERACIÓN DOCUMENTADO. Los protocolos 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, los cuales están debidamente actualizados en la Suite Vision Empresarial, dentro de los que se encuentran:

1. Control de cambios sobre la plataforma tecnológica.
2. Aprobación, implementación de nuevos productos y servicios tecnológicos.
3. Instalación de nuevas versiones/actualizaciones.
4. Manejo de incidentes y vulnerabilidades.
5. Uso correcto del correo electrónico, usuario empresarial, certificado digital.
6. Administración de identidades.
7. Entrega de información bajo deber de reserva.
8. Protección contra software malicioso.
9. Protección de usuarios con altos privilegios.
10. Elaboración y recuperación de copias de respaldo.
11. Borrado seguro de información.
12. Eliminación de dispositivos de almacenamiento.
13. Instalación y mantenimiento de equipos de procesamiento y comunicaciones.

ARTÍCULO 2. GESTIÓN DE CAMBIOS. Toda modificación a la plataforma tecnológica es evaluada previamente en los aspectos técnicos y de seguridad, acorde con los protocolos establecidos en el procedimiento 1DT-PR-0014 gestión de cambios, para ello se tienen en cuenta las diferencias entre funcionalidad y seguridad las cuales se ajustan a decisiones arquitecturales que satisfacen los requisitos mínimos de seguridad, estos 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. Protocolos para cancelación del cambio en caso de fallo.
9. Verificación del cambio realizado.

ARTÍCULO 3. GESTIÓN DE 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 4. SEPARACIÓN DE LOS 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:

1. Ejecutar el software de desarrollo y producción en diferentes ambientes.
2. Las actividades de desarrollo y pruebas deberán realizarse en ambientes separados.
3. Los datos de producción no deberán usarse en ambientes de desarrollo o pruebas.

4. No usar compiladores, editores y otros utilitarios que no sean necesarios para el funcionamiento de los ambientes de producción.

ARTÍCULO 5. CONTROLES CONTRA CÓDIGOS MALICIOSOS. Con el fin de prevenir y detectar código malicioso, se definen mediante aspectos que se basan en software, concienciación de usuarios y gestión del cambio, por lo tanto los controles implementados contemplan las siguientes directrices:

1. No se permite el uso de software no autorizado por la Oficina de Telemática.
2. No se permite el intercambio de información a través de archivos planos.
3. 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.
4. Mantiene los sistemas con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.
5. 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.
6. 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.
7. Concientiza al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.
8. La herramienta de antivirus que se implemente en la Institución tendrá carácter de corporativo y por lo tanto será obligatoria su instalación y uso en toda la plataforma tecnológica sean estos servidores, estaciones de trabajo, notebook y otros dispositivos tanto móviles como fijos. Cualquier equipo que no cuente con los controles establecidos, no podrá ser conectado a la red de datos de la Institución.
9. No se permite la conexión de equipos de contratistas o terceros a la plataforma tecnológica, o equipos que no cuenten con los controles establecidos para su funcionamiento dentro de la red institucional.

ARTÍCULO 6. COPIAS DE RESPALDO DE LA INFORMACIÓN. La realización incluye actividades de prueba de recuperación de la información. Las instalaciones alternas garantizan las condiciones de seguridad y ambientales necesarias para la conservación de los respaldos de información; el protocolo de back up contempla las siguientes directrices:

1. Un esquema de rótulo de las copias de respaldo, para permitir su fácil identificación.
2. Destrucción de las copias de respaldo, cuando se venza la vida útil de los medios de almacenamiento, de acuerdo al procedimiento 1DT-PR-0020 Borrado Seguro de la Información
3. 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 protocolos de restauración.
4. Pruebas periódicas de la restauración de los medios de respaldo, según lo estipulado en el Plan de Continuidad del Negocio (establece los parámetros para la permitir el normal funcionamiento de los sistemas de archivos y aplicaciones dentro de la Institución).

Parágrafo: En las unidades que no se cuente con un servidor de archivos, y los respaldos de información se realizan localmente, la información categorizada como reservada o sensible debe estar almacenada en dispositivos que cuenten con los controles criptográficos establecidos (cifrados).

ARTÍCULO 7. REGISTRO DE EVENTOS. Los sistemas de información, así como los servidores, dispositivos de red y demás servicios tecnológicos, guardan registros de auditoría y logs, los cuales contemplan, siempre y cuando sea posible, lo siguiente:

1. Id del usuario.
2. Fecha y hora de la transacción.
3. Dirección IP y nombre del dispositivo desde el cual se realizó la transacción.
4. Tipo de transacción.
5. Id de la transacción.
6. Datos consultados, modificados o borrados.

7. Intentos fallidos de conexión.
8. Cambios en la configuración del sistema.
9. Cambio o revocación de privilegios.
10. Archivos a los que ha tenido acceso.
11. Alarmas originadas por los sistemas de control.
12. Desactivación de los mecanismos de protección.

ARTÍCULO 8. PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO. Los registros de auditoría están protegidos de acceso o modificaciones, con el fin de evitar cualquier tipo de alteración en el nivel de integridad, por tal circunstancia como mecanismo de seguridad todos los registros poseen copias de respaldo.

ARTÍCULO 9. REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR. Teniendo en cuenta las múltiples fuentes de datos de registros (logs) y auditoría, estos se almacenan en un servidor de syslog y se implementa un correlacionador de eventos, que permita realizar inteligencia de negocios, estos registros son de los servicios administrados por la Oficina de Telemática. Los registros de auditoría de los Sistemas de Información están consolidados en ambientes separados a los transaccionales, para las unidades que poseen servicios no administrados por la Oficina de Telemática, implementan su correlacionador de eventos y propenden por los registros (logs) del sistema.

ARTÍCULO 10. SINCRONIZACIÓN DE RELOJES. Para garantizar la exactitud de los registros de auditoría, la Policía Nacional, dispone de un servicio de tiempo de red NTP que está sincronizado a su vez con la hora legal Colombiana.

ARTÍCULO 11. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS. Cada sistema de información, tiene un responsable de su soporte y mantenimiento, sin embargo, para cualquier cambio sobre el software de producción deberá estar avalado por el Direccionamiento Tecnológico.

ARTÍCULO 12. ADMINISTRACIÓN DE RECURSOS TECNOLÓGICOS. El Direccionamiento Tecnológico y las unidades de policía donde se administran recursos tecnológicos dispondrá un grupo o funcionario para que realice las siguientes funciones:

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

ARTÍCULO 13. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS. El Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), es el encargado 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 protocolo formal, que contempla:

1. Realizar análisis de vulnerabilidades semestralmente.
2. Mantener información actualizada de nuevas vulnerabilidades.
3. Definir la línea de tiempo para aplicar actualizaciones de remediación para las vulnerabilidades conocidas.
4. Probar las actualizaciones de remediación de vulnerabilidades antes de su despliegue en los ambientes de producción.
5. Detección de ataques reales.

ARTÍCULO 14. RESTRICCIONES SOBRE LA INSTALACIÓN DE SOFTWARE. El uso de utilitarios licenciados del sistema está restringido a usuarios administradores. Se estableció una política a nivel del controlador de dominio, que no permite la instalación de software y cambios de

configuración del sistema, por lo tanto ningún usuario final, tiene privilegios de usuario administrador.

ARTÍCULO 15. CONTROLES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN. Las tablas de auditoría y archivos de logs usados para auditar los Sistemas de Información, están separados de los ambientes transaccionales, estos pueden ser verificados por el analista de continuidad de la información cuando se requiera por la autoridad competente o dentro de proceso administrativo, disciplinario o penal, así mismo pueden ser accedidos por personal del Área de Control Interno quienes realizan verificaciones sobre estos.

Anexo No. 7

SEGURIDAD DE LAS COMUNICACIONES

ARTÍCULO 1. CONTROLES DE 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 la norma ISO/IEC 18028 Tecnología de la información - Técnicas de seguridad - la seguridad de TI de la Red, estos controles contemplan salvaguardas especiales para:

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

ARTÍCULO 2. SEGURIDAD DE LOS SERVICIOS DE RED. Los niveles de servicio contemplan, características de seguridad, requisitos de gestión de los servicios de red y valores agregados en dispositivos de seguridad, así mismo es importante realizar un control a través de:

1. Chequeo del tráfico de la red.
2. Monitoreo de los puertos en la red.
3. Auditoría, trazabilidad y respaldo de archivos de logs.

ARTÍCULO 3. POLÍTICAS Y PROTOCOLOS DE TRANSFERENCIA DE INFORMACIÓN. Para el intercambio de información se utiliza el formato acuerdo para la revelación de información confidencial bajo deber de reserva, así mismo se documentan los controles adicionales que contemplen:

1. Sistemas informáticos, redes, computación y comunicaciones móviles, correo electrónico, comunicaciones de voz, servicio de correo tradicional, fax e impresoras.
2. Uso de modelos de control de acceso.
3. Implementación de webservices con autenticación

ARTÍCULO 4. ACUERDOS SOBRE TRANSFERENCIA DE INFORMACIÓN. El intercambio de información al interior de la Policía Nacional se realiza aplicando el formato 1DT-FR-0010 acuerdo para la revelación de información confidencial bajo deber de reserva y otras entidades bajo acuerdos de cooperación u órdenes judiciales, si esta información es de inteligencia y/o contrainteligencia se desarrollará según lo establecido en el artículo 42 de la Ley 1621 de 2013

ARTÍCULO 5. MENSAJES ELECTRÓNICOS. 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 se encuentra regulada por los términos de uso adecuado. Por tanto, no está permitido intercambiar información institucional a través de otras plataformas de mensajería instantánea, no obstante en caso de requerirse otro medio debe solicitarse concepto al Grupo de Seguridad de la información de la Policía Nacional.

ARTÍCULO 6. COMPROMISO CON LA CONFIDENCIALIDAD O NO DIVULGACIÓN. 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.

La Institución estableció un compromiso de confidencialidad mediante el formato 1DT-FR-0015 declaración de confidencialidad y compromiso con la seguridad de la información servidor público, el cual debe ser suscrito por todos los funcionarios o personal que tienen un vínculo laboral o contractual con la Policía Nacional, el cual es parte de su hoja de vida, junto con el acta de posesión y/o contrato. Mediante este, los funcionarios se comprometen 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, es de aclarar que todas las actividades en la plataforma tecnológica de la Policía Nacional, pueden ser monitoreadas y auditadas.

Todos los servidores públicos de la Policía Nacional deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento en ejercicio de sus funciones legales, cualquier persona que acceda a las instalaciones de la Policía Nacional, podrá ser monitoreada y grabada por medio de circuito cerrado de televisión.

ARTÍCULO 7. COMPROMISO DE RESERVA. Los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia en la Policía Nacional, los funcionarios que adelantan actividades de control, supervisión y revisión de documentos o bases de datos de inteligencia y contrainteligencia y los receptores de productos de inteligencia de que trata el artículo 36 de la Ley 1621 de 2013, están obligados a suscribir acta de compromiso de reserva en relación a la información que tenga conocimiento. Así mismo, los asesores externos y contratistas solo podrán conocer, acceder y/o recibir información de inteligencia y contrainteligencia de conformidad con el artículo 37 de la Ley 1621 de 2013 y deberán suscribir acta de compromiso de reserva, previo estudio de credibilidad y confiabilidad. El deber de reserva de los servidores públicos de los organismos que desarrollan actividades de inteligencia y contrainteligencia, y los receptores antes mencionados, permanecen aún después del cese de sus funciones o retiro de la Institución hasta el término máximo que establezca la ley para este tipo de información .

Anexo No. 8

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

ARTÍCULO 1. ANÁLISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN. El procedimiento 1DT-PR-0017 Desarrollar Sistemas de Información, para la adquisición de productos contempla 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 2. SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS. La información pública producida por la Policía Nacional, está resguardada de posibles modificaciones que afecten la imagen Institucional. Se estableció un protocolo formal para autorizar la publicación de información, antes que 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. El contenido publicado en los servicios Institucionales, requiere de la revisión y aprobación de la Oficina de Comunicaciones Estratégicas.

ARTÍCULO 3. PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES. Las siguientes consideraciones se deben tener en cuenta para las unidades que realizan transacciones en línea:

1. El uso de firmas electrónicas por cada una de las partes involucradas en la transacción.
2. La trayectoria de las comunicaciones entre todas las partes involucradas debe estar cifrada.

ARTÍCULO 4. POLÍTICA DE DESARROLLO SEGURO. Los Sistemas de Información como soporte importante de los procesos misionales de la Policía Nacional, busca brindar seguridad a los aplicativos institucionales desde el momento mismo del levantamiento de requerimientos, por lo tanto las necesidades de seguridad, hacen parte integral de las decisiones de arquitectura del software a construir y/o adquirir. El procedimiento 1DT-PR-0017 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.

Las unidades en las cuales se desarrolle software, deberá en lo posible segregar las funciones de desarrollo, pruebas y producción, con el fin de impedir 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:

1. Todos los sistemas cuentan con un módulo de auditoría, que permite almacenar los registros de transacciones realizados desde la interfaz de usuario final o desde cualquier otra herramienta.
2. Todos los equipos de procesamiento y comunicaciones tiene activos los archivos de logs y se envían a un syslog.
3. Se asegura la independencia entre el inicio de una actividad y su autorización, para evitar la posibilidad de conspiración para un fraude.
4. Se documenta de manera formal la razón por la cual no es posible segregar funciones.

ARTÍCULO 5. CONTROL DE CAMBIOS EN SISTEMAS. Busca minimizar la alteración a los sistemas de información, mediante el control de cambios, el cual contempla:

1. 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.
2. Registrar los niveles de autorización acordados.
3. Solicitar autorización al propietario del activo de información, cuando se trate de cambios que modifiquen los sistemas de información que procese dicho activo.
4. Identificar software, hardware, bases de datos, que deben ser modificados.
5. Realizar los cambios en el ambiente de pruebas.
6. Actualizar la documentación, con el cambio realizado.
7. Efectuar pruebas de calidad y seguridad, sobre los cambios efectuados
8. Llevar el control de versión de los sistemas de información.
9. Implementar los cambios, en ventanas de mantenimiento, para no afectar la disponibilidad del servicio.

ARTÍCULO 6. REVISIÓN TÉCNICA DE APLICACIONES DESPUÉS DE CAMBIOS EN LA PLATAFORMA DE OPERACIONES. 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 protocolo para la revisión contempla:

1. Copias de respaldo de la versión anterior del Sistema de Información.
2. Revisión de las antiguas funcionalidades del sistema.
3. Actualizar el plan de recuperación de desastres con los cambios realizados, de ser necesario.

ARTÍCULO 7. RESTRICCIONES SOBRE CAMBIOS EN LOS PAQUETES DE SOFTWARE. Las modificaciones de paquetes de software suministrados por un proveedor, deben validar:

1. Análisis de los términos y condiciones de la licencia, para determinar si los cambios a realizar están permitidos.
2. Analizar la conveniencia de realizar las modificaciones por personal de la Institución o contratarlas con el proveedor o un tercero.
3. Evaluar el impacto de asumir el cambio por personal de la Institución.
4. Guardar una copia del software a modificar, documentar los cambios realizados.

ARTÍCULO 8. DESARROLLO CONTRATADO EXTERNAMENTE. Para la tercerización del desarrollo de software, se tiene en cuenta el procedimiento 1DT-PR-0017 Desarrollar Sistemas de Información, además de las siguientes recomendaciones:

1. Cumplir con la Ley 23 de 1982.
2. Atender las recomendaciones de la Circular Conjunta 01/2006 sobre los delitos de propiedad intelectual e industrial.
3. Las especificaciones técnicas contemplarán los acuerdos de licencias de propiedad del código y demás derechos de propiedad.

4. Las especificaciones técnicas establecen los requerimientos con respecto a la calidad del código y la existencia de garantías así como los acuerdos de custodia de los códigos fuentes del software y cualquier otra documentación necesaria, en caso de requerir modificación en el software.
5. Someter el software desarrollado a pruebas que permitan establecer el cumplimiento de requerimientos funcionales y de seguridad, detección de código malicioso, entre otros.

ARTÍCULO 9. PRUEBA DE ACEPTACIÓN DE SISTEMAS. 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:

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

ARTÍCULO 10. PROTECCIÓN DE DATOS DE PRUEBA. Las pruebas de los Sistemas de Información, se realizan en ambientes separados al de producción, siguiendo las siguientes pautas:

1. Los datos de prueba, están alojados en bases de datos independientes a la de producción.
2. Los ambientes de pruebas tienen la misma estructura del ambiente de producción.
3. Los datos no corresponden a datos reales de producción y en caso de ser tomados de este ambiente, deben ser transformados.

Anexo No. 9

RELACIONES CON TERCEROS

ARTÍCULO 1. RELACIONES CON PROVEEDORES. La Policía Nacional establece los mecanismos de control en sus relaciones con personal externo que le provean bienes o servicios. Los funcionarios responsables de la realización 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:

1. Todos los contratos deben tener claramente definidos los acuerdos de niveles de servicios y ser contemplados como un numeral de las especificaciones técnicas.
2. Diligenciar y firmar el formato 1DT-FR-0016 declaración de confidencialidad y compromiso con la seguridad de la información contratistas o terceros y 1DT-FR-0010 acuerdo para la revelación de información confidencial bajo deber de reserva.
3. 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.
4. Antes de permitir el acceso o la entrega de información a un tercero, se debe realizar una evaluación del riesgo, por parte del propietario del activo de información, con el fin de establecer la viabilidad de permitir el acceso a la información, para salvaguardar la confidencialidad, integridad y disponibilidad de la información.
5. El acceso a la información deberá ajustarse a los parámetros establecidos en el procedimiento 1DT-PR-0006 entrega de Información bajo deber de reserva, proceso de gestión documental y sus procedimientos asociados.
6. En los grupos de Talento Humano se debe definir una persona responsable de supervisar el personal externo, contratista o terceros que realicen labores en las instalaciones de la unidad policial, verificando que se encuentren debidamente diligenciados los documentos como compromiso con la seguridad de la información y exista la documentación requerida en los pliegos de condiciones del contrato (hoja de vida, estudios de seguridad, certificaciones solicitadas en las especificaciones técnicas, etc), este funcionario será el encargo de coordinar con el supervisor del contrato, la firma por parte de los terceros del acta correspondiente a las medidas, controles o políticas de seguridad que se tienen en la organización.

Anexo No. 10

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 1. GESTIÓN DE INCIDENTES. Un incidente de seguridad de la información se manifiesta por un solo evento o una serie de eventos inesperados o no deseados, que tienen una probabilidad significativa de poner en peligro las operaciones del negocio y amenazar la seguridad de los activos de 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 Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) 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 los activos de información. En atención a lo anterior se debe tener en cuenta que los incidentes deben ser documentados de acuerdo al procedimiento 1DT-PR-0004 Atención a Incidentes

Las unidades de Policía a nivel nacional deben reportar los incidentes generados y efectuar el respectivo análisis, estos eventos deben ser registrados por el analista de seguridad de cada unidad en el Sistema de Información para la Gestión de incidentes en TIC´S SIGMA.

Anexo No. 11

CONTINUIDAD DE LA INFORMACIÓN

ARTÍCULO 1. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA 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 plan integral que identifica el impacto de posibles incidentes que amenazan de manera grave el desarrollo de las actividades institucionales y genera un plan de respuesta efectivo para garantizar su recuperación, para ello el Direccionamiento Tecnológico y las unidades de Policía donde se cuente con procesamiento de información crítica para la Institución, deben documentar un Plan de Continuidad del Negocio alineado con las normas ISO 22301, elaborar un Análisis de Impacto del Negocio (BIA) en el que se determinan los procesos esenciales para la continuidad de las operaciones y un Plan de Recuperación ante Desastres (DRP) en materia tecnológica.

Teniendo en cuenta lo anterior el Comité de Seguridad de la Información, debe:

1. Identificar las amenazas que pueden ocasionar interrupciones de los procesos o actividades que afecten el servicio de Policía.
2. Evaluar y aprobar los riesgos para determinar el impacto de dichas interrupciones.
3. Determinar los controles preventivos.
4. Desarrollar un plan para establecer el enfoque integral con el que se abordará la continuidad de las actividades de la Institución.
5. Elaborar los planes de actividades necesarios para garantizar la continuidad de los procesos de la Policía Nacional, mientras se restablecen los servicios en el sitio principal.

Anexo No. 12

CUMPLIMIENTO

ARTÍCULO 1. DERECHOS DE PROPIEDAD INTELECTUAL. La Policía Nacional implementó pautas para el cumplimiento de restricciones legales al uso del material protegido por normas de propiedad intelectual, para ello se consideran las siguientes medidas:

1. Todos los miembros de la Policía Nacional deberán velar por el cumplimiento de normas de derechos de autor y derechos conexos.

2. 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.

3. 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.

4. La Oficina de Telemática de la Policía Nacional y/o los grupos de Telemática de las unidades desconcentradas, tienen las siguientes responsabilidades:
   a. Elaborar y mantener actualizado un inventario del software utilizado en la Institución.
   b. Velar por el buen uso de licencias adquiridas por la Institución, para la utilización de los usuarios finales.
   c. Verificar que el software que a instalar en un dispositivo cuente con su respectiva licencia y esté autorizado.
   d. Utilizar herramientas de auditoría adecuadas.

ARTÍCULO 2. PROTECCIÓN DE LOS REGISTROS. 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 almacenamiento se realizará de acuerdo a estas; con el fin de cumplir requisitos legales, normativos y/o respaldar actividades esenciales de la Institución, además se siguen las siguientes consideraciones:

1. 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.
2. 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.
3. 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.
4. El sistema de almacenamiento y manipulación garantizará una clara clasificación de los registros y de su periodo de retención legal o normativa. Así mismo, se 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 expiden los siguientes controles:

1. Elaborar y divulgar las instrucciones para la retención, almacenamiento, manipulación y eliminación de registros e información.
2. Mantener un inventario de programas fuentes de información institucionales.

ARTÍCULO 3. REGLAMENTOS 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 4. 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 5. CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD. 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, cada unidad velará por el cumplimiento de la Política de Seguridad, mediante las buenas practicas, que servirán para el fortalecimiento de los procesos en cada uno de los grupos que conformen la unidad, de igual manera, para la verificación del seguimiento el Área de Control Interno realizará auditorías periódicas al Sistema de Gestión de Seguridad de la Información y ayudará a elaborar los respectivos planes para la mejora continua.

Dentro de las políticas los funcionarios incurrirán en infracciones del Sistema de Seguridad de la Información en el momento que se materialicen las siguientes acciones:

- 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, plataformas de mensajería instantánea y diferente 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.
- Promocionar o mantener actividades personales, o utilizar los recursos tecnológicos de la Policía Nacional para beneficio personal.
- Usar 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.

ARTÍCULO 6. REVISIÓN DEL CUMPLIMIENTO TÉCNICO. El Grupo de Seguridad de la Información y/o los responsables del SGSI en las unidades, verificarán los sistemas, equipos de procesamiento, bases de datos y demás recursos tecnológicos, para que cumplan con los requisitos de seguridad esperados, teniendo en cuenta las solicitudes internas, para esta validación se pueden realizar pruebas de vulnerabilidades y pruebas de penetración, las cuales son una forma para mejorar los controles, pero nunca reemplazarán el análisis de riesgo sobre los activos de información.