SEGURIDAD DE LA INFORMACIÓN, UNA POLÍTICA DE CONTROL

HORLID REINA GUZMÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
NEIVA
2019

SEGURIDAD DE LA INFORMACIÓN, UNA POLÍTICA DE CONTROL

HORLID REINA GUZMÁN

TRABAJO DE GRADO

JAIME RUBIANO LLORENTE
Director de tesis
Docente Asistente

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
NEIVA
2019

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Neiva, 24 mayo 2019

Dedico este trabajo a Dios. *Por haberme permitido llegar hasta este punto en mi vida y haberme dado salud para lograr mis objetivos.* A mis padres Asceneth Guzmán (QEPD) y Jorge Reina (QEPD) por ser el pilar fundamental en todo lo que soy, en toda mi educación y formación para la vida, por su incondicional apoyo.

AGRADECIMIENTOS

Doy gracias.

A mi universidad, por haberme concedido el derecho de formarme profesionalmente en ella.

Al docente Jaime Rubiano Llorente, quien se tomó el arduo trabajo de transmitirme su amplio conocimiento, especialmente en el área de programación y diversos temas inherentes a mi profesión. Pero aparte de eso, ha sido quien me ha orientado y ofrecido sabios conocimientos efectivos para el logro de mis objetivos y metas.

A los tutores que me brindaron su gran apoyo durante la formación académica de mi carrera profesional.

A mi familia quienes me brindaron apoyo permanente y sacrificaron paseos y diversas actividades mientras yo me formaba como profesional.

Les agradezco de corazón, que Dios los bendiga a todos.

CONTENIDO

Pag

1. INTRODUCCIÓN 12

2. OBJETIVOS 13

2.1 OBJETIVO GENERAL 13

2.2 OBJETIVOS ESPECÍFICOS 13

3 PLANTEAMIENTO DEL PROBLEMA 14

3.1 DEFINICIÓN DEL PROBLEMA 14

3.2 JUSTIFICACIÓN 16

4. MARCO TEÓRICO 17

5. MATERIALES Y MÉTODOS 20

5.1 MATERIALES 20

5.2 METODOLOGÍA 21

6 DESARROLLO DEL PROYECTO 22

CONCLUSIONES 31

RECOMENDACIONES 32

BIBLIOGRAFÍA 33

ANEXO 34

LISTA DE FIGURAS

Pág.

Figura 1. Asesoría Personal perteneciente al Proceso de Prevención. 28

Figura 2. Asesoría Personal perteneciente a la Estación Palestina..... 28

Figura 3. Asesoría Personal perteneciente a la Estación San Agustín. 29

Figura 4. Asesoría Personal perteneciente a la Subestación Bruselas 29

Figura 5. Asesoría Personal perteneciente a la Estación Oporapa 30

Figura 6. Asesoría Personal perteneciente a la Estación Colombia. 30

GLOSARIO

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. Sobre escritura, 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.

Dispositivos de almacenamiento. Materiales físicos donde se almacenan datos.

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

SIGMA. Sistema de Información para la Gestión de Incidentes en TIC

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.

RESUMEN

Se realizará asesoría, acompañamiento o sensibilización a las unidades que conforman el departamento del Huila, con el objetivo de verificar el nivel de apropiación y cumplimiento procedimientos, políticas y protocolos inmersos dentro reglamentos institucionales.

Para poder realizar estas actividades se realizarán pruebas de campos en todas las unidades, verificando el cumplimiento de los 38 compromisos que debe estar aplicando cada funcionario policial, así mismo se dan a conocer algunos pautas y recomendaciones sobre acciones para tomar en consideración con respecto a que no se materialicen los riesgos que se han identificado sobre el tema de seguridad de la información.

1. INTRODUCCIÓN

La informática, especialmente, ha permitido que hoy en día los diferentes procesos se realicen con la ayuda de herramientas de hardware y software que pueden realizar validaciones, conexiones y ejecutar instrucciones de forma fácil y rápida, en un periodo de tiempo reducido, comparado con las actividades manuales, e incrementando confiabilidad a los resultados generados.

Esta facilidad de acceso ha promovido una serie de alertas sobre manejo y seguridad de la información.

Los avances tecnológicos con los que se cuenta hoy en día, las nuevas estrategias criminales y la no implementación de políticas de seguridad de la información, se convierten en una fortaleza que utilizan algunas personas con el fin de sacar provecho de información relevante o reservada, que puede afectar una institución y favorecer a criminales o grupos organizados.

El presente trabajo de tesis se desarrolla como opción de grado de Ingeniería de Sistemas de la Universidad Nacional Abierta y A Distancia (UNAD). En este sentido se implementa una estrategia a través de este proyecto, que permite estandarizar una metodología enfocada en la asesoría, acompañamiento o sensibilización a tener en cuenta y ser dirigida a los funcionaros que conforman el departamento de Policía Huila en lo concerniente a la seguridad de la información.

En la policía nacional de Colombia se tiene implementada una política de seguridad de la información, la cual verificare a través de asesoría, acompañamiento o sensibilización a 52 grupos u/o unidades policiales que conforman el departamento de policía Huila; dejando el respectivo soporte documental de lo actuado.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Interiorizar y apropiar lo establecido dentro del sistema de gestión de seguridad de la información en la Policía nacional, a través de una protección de los posibles riesgos que se lleguen a presentar en la unidad.

2.2 OBJETIVOS ESPECÍFICOS

- 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 expuesta.

- 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.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

La Policía Nacional, es un cuerpo armado de naturaleza civil a cargo de la nación, la cual se encuentra conformada por siete direcciones operativas, cinco administrativas y una educativa, contando con un personal idóneo en sus cargos a través del perfil por competencias, es de resaltar que la institución cuenta con un número considerable de funcionarios en la mayor parte del territorio nacional siendo factible que se presenten incidentes de seguridad de la información, los cuales se manifiestan por un evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de poner en peligro las operaciones misionales de la Policía Nacional y amenazar la seguridad de la información, por lo anterior cualquier medio o elementos que tenga valor para la institución y, en consecuencia, deba ser protegido, recibe el nombre de activos de información y se dividen en: (información electrónica, información física, hardware, software, persona, infraestructura y servicio).

Teniendo en cuenta lo anterior se identificó como riesgo institucional “Que se afecte la seguridad de la información”, debido a los riesgos asociados a la fuga de información que afectan la imagen institucional y ponen en riesgo la integridad de los funcionarios. Generando con esto la ya materialización de los siguientes riesgos:

- Suplantación - Uso de información personal para realización de préstamos a nombre de otros funcionarios
- Estafas por internet, mensajes de texto y/o llamadas a los funcionarios de policía por baja cultura en seguridad de la información.
- Entrega de información a grupos al margen de la ley relacionada con (teléfonos, direcciones, nombres núcleo familiar de nuestros policías) por parte de los funcionarios.

Dentro de la institución se encuentra documentado manuales, protocolos y políticas que sirven de insumo en la generación de estrategias que coadyuvan en el planteamiento de acciones que dan como resultado una cultura e impacto sobre la responsabilidad que recae en cada uno de los funcionarios que conforman la Policía Nacional de Departamento del Huila, enfocada a salvaguardar los activos de

información, protegiéndolos a través de una adecuada gestión del riesgo, el cumplimiento de los requisitos legales y una estrategia de seguridad basada en las mejores prácticas y controles

La Policía Nacional de Colombia, a través de su experiencia y trayectoria en el campo de la seguridad de la información y tomando como herramienta de control las auditorías internas, certifica que se estén cumpliendo los parámetros establecidos en las normas, políticas, manuales, entre otros documentos doctrinales enfocados en la Seguridad de la Información, en busca de una mejora continua de las actividades y procesos y al mismo tiempo evitar la materialización de riesgos ya identificados en la institución.

Pregunta de investigación

¿Cómo se puede minimizar los riesgos en la policía nacional, coadyuvando en salvaguardar de manera continua la seguridad de la información?

3.2 JUSTIFICACIÓN

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 amenazas físicas externas e internas y las condiciones medioambientales de sus instalaciones. Para lo cual se hace necesario que una persona realice desplazamientos a todas las unidades que conforman el departamento, con el fin de verificar, interiorizar y apropiar diversos temas que coadyuven al fortalecimiento del sistema de seguridad de la información.

Por lo anteriormente expuesto se realizará un proceso de asesoría, acompañamiento o sensibilización dirigida como mínimo a 330 funcionarios que pertenecen a las 52 unidades que visitara, las cuales se encuentran divididas en estaciones, subestaciones y puestos de policía, como a su vez a funcionarios pertenecientes a modalidades especialidades y procesos que conforman la institución policial.

4. MARCO TEÓRICO

En el marco conceptual y teórico nos centraremos en las actividades prácticas a desarrollar con respecto al conocimiento adquirido; ya que contamos con herramientas básicas y esenciales para poder desarrollar con éxito el logro propuesto en el departamento de policía Huila en lo concerniente a ejecutar una política de control con respecto a la seguridad de la información.

Para el desarrollo y ejecución de las practicas se realizara desplazamiento a todas las unidades que conforman el Departamento de Policía Huila, con el fin de socializar lo establecido en la Norma ISO 27001:2013 y la resolución 08310 del 28 de diciembre de 2016 “manual del sistema de gestión de seguridad de la información para la Policía Nacional”, como a su vez impartir pautas importantes con respecto al manejo de la información a través de confidencialidad, integridad y disponibilidad de la misma; así mismo dentro de las actividades que se realizara en cada unidad se prevé que se ejecuten en seis horas, en las cuales a parte de la socialización se verificara la seguridad de las operaciones enfocada a disminuir el riesgo de uso inadecuado de la información y los sistemas puestos a disposición de los funcionarios, esto a través de una revisión general enfocada en los siguientes objetivos:

Responsabilidades de los usuarios

- Verificación que el software utilizado en la plataforma tecnológica cuente con licencia y su cumplimiento debe estar acorde a las condiciones de uso establecidas.

- Constatar que no se esté utilizando dispositivos de almacenamiento masivo externo extraíble (DVD, CD, Dispositivos móviles, pendrives (USB), equipos celulares), los cuales pueden 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.

- Verificar los equipos de cómputo y recordar a los usuarios la responsabilidad que deben tener con la información que administran, 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.

- Verificar que en los equipos de cómputo no haya acceso a redes sociales, correos comerciales, paginas interactivas como chats que se encuentran 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.

- Verificar que los incidentes de seguridad informática que se hayan presentado se hayan reportado a través del SIGMA.

Gestión de autenticación usuarios y contraseñas

- Orientar a los usuarios sobre el paso a seguir para realizar cambio de contraseñas para poder acceder a los equipos de cómputo con usuario de dominio.
- Verificar que no se esté mostrando en pantalla la contraseña ingresada.
- Verificar que los usuarios y contraseñas no estén apuntados en memo fichas, apuntes o cualquier documento cerca al equipo de cómputo.

Conexión segura

- Verificar que después de cinco (5) minutos de inactividad del sistema se bloquea el equipo de cómputo.
- Constatar que los usuarios cuando no se encuentran en sus sitios de trabajo estén bloqueadas sus sesiones y al finalizar la jornada laboral o cuando la ausencia sea superior a dos horas el equipo de cómputo debe estar apagado.
- Verificar el límite de intentos fallidos con bloqueo de usuario o sección a los 5 intentos.
- Verificar que se encuentre activo el control a la conexión que se realiza a los

usuarios en donde ante la ausencia laboral administrativamente (vacaciones, Excusas Totales, Comisiones), se bloquea la cuenta del usuario.

Uso adecuado de la plataforma tecnológica

- Verificar en el historial que no se observe navegación en sitios de contenidos sexuales, o que tengan relación con información de carácter explícita en el cual se pueda materializar un delito informático.
- Recordar lo concerniente a la 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.
- Recalcar que no se debe promover o mantener asuntos o negocios personales a través de la red o infraestructura tecnológica de la Policía Nacional.
- Recordar verificar que no se puede descargar, instalar y utilizar 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.
- Verificar que no se esté utilizando cuentas de correos no institucionales o de terceros, para el manejo de la información o recepción de actividades realizadas por la Policía Nacional.
- 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.

Mantenimiento de equipos

- Recordar a los usuarios que sólo el personal de mantenimiento autorizado puede llevar a cabo reparaciones en los equipos de cómputo institucional.
- Recalcar que la eliminación de manera segura de la información confidencial que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de respaldo.
- Recordar y recalcar que el responsable funcional del equipo acompañará el mantenimiento de los equipos que contengan información sensible.

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	El señor Horlid Reina Guzmán será el responsable de las actividades dispuesta y contará con el acompañamiento de un funcionario que actuará como conductor	4.160.000
Equipos y Software	Se utilizará computador portátil y video beam	4.000.000
Viajes y Salidas de Campo	Se realizará 52 actividades de asesoría, acompañamiento o sensibilización enfocadas al sistema de seguridad de la información	2.000.000
Materiales y suministros	Será utilizado una resma de papel, combustible vehículos	3.000.000
Bibliografía	Se dará aplicación a lo dispuesto en la Norma ISO 27001:2013 Esta norma contiene sistemas de gestión – seguridad de la información; seguridad de la información – requisitos y Resolución 08310 del 28 de diciembre de 2016 “manual del sistema de gestión de seguridad de la información para la Policía Nacional”	
TOTAL 13.160.000		

Todos los recursos necesarios son suministrados por la empresa, teniendo en cuenta el beneficio que adquiere la institución con el desarrollo de la actividad.

5.2 METODOLOGÍA

Para el desarrollo de la actividad el analista de seguridad de la unidad dará pautas al funcionario que realizara las prácticas de (asesoría, acompañamiento o sensibilización) en todas las unidades del departamento, explicándole la metodología a implementar para que el personal que reciba la socialización se apropie del tema expuesto y logre concienciar a todos sobre la importancia en la implementación del sistema de gestión de seguridad de la información, ya que nuestra institución genera información relevante y confidencial.

Por otra parte, teniendo en cuenta la dinámica institucional y los constantes servicios que se presentan en los municipios del departamento, no se ubica un día en especial para realizar la practica en cada municipio, así mismo por la distancia que hay entre cada uno de ellos se ubica una fecha inicial y una fecha final en un lapso de tiempo para soportar la actividad en cada unidad.

Por consiguiente, se realizará las actividades dispuestas en el ciclo **PHVA**, así:

Realizando una planeación de actividades a través de una (1) **orden de servicio**: Documento de carácter obligatorio para operacionalizar la planeación del servicio, impartir instrucciones internas de cada unidad o desplegar las generales establecidas por las directivas u órdenes relacionadas con el servicio de Policía.

Ejecución de las actividades planteadas soportándose en cincuenta y dos (52) **actas**: Documento interno que constituye la memoria de reuniones, cuyo objetivo es relacionar lo que sucede, se debate, o se acuerda en ella.

Informe de resultados obtenidos y material fotográfico, a través de un (1) **comunicado oficial**: Formato que permite estandarizar las comunicaciones Oficiales en la Policía Nacional.

6 DESARROLLO DEL PROYECTO

Dentro de la policía nacional se ha dispuesto establecer un sistema de gestión de seguridad de la información, definiéndose límites del alcance y la declaración de aplicabilidad de acuerdo con la Norma ISO 27001:2013, a través de la expedición de la resolución 08310 del 28 de diciembre de 2016 “manual del sistema de gestión de seguridad de la información para la Policía Nacional”, en el cual se establece: 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, desarrollando 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.

A continuación, se describen en detalle los pasos necesarios para desarrollar la asesoría, acompañamiento o sensibilización sobre la seguridad de la información.

Paso 1:

Se realiza la **planeación**, en este proceso se analiza el objetivo deseado con el fin de cumplir las necesidades de la institución orientados en estrategias dinamizadas a través de objetivos de calidad, a partir de identificación de responsables, controles, tiempo de ejecución, medios y recursos, entre otras herramientas que coadyuvan en la integración de acciones que conllevan a una efectividad en la toma de decisiones para posteriormente materializar de manera ordenada y sistemática el objetivo propuesta.

Teniendo en cuenta el objetivo de la planeación se Plasmó la orden de servicio No. 065 COMAN PLANE del 05 de febrero del 2018 “Asesoría, acompañamiento y sensibilización dirigida al personal que conforma el departamento del Huila, sobre la importancia en la implementación del sistema de gestión de seguridad de la información”; en la cual se desplego ordenes e instrucciones internas para ejecutarse en un periodo de tiempo determinado.

CRONOGRAMA DE ASESORÍA, ACOMPAÑAMIENTO Y SOCIALIZACIÓN SOBRE EL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

DISTRITO V PITALITO	Fecha Inicial	Fecha Final
Estación Pitalito	05/02/2018	02/03/2018
Estación San Agustín	05/02/2018	02/03/2018
Estación San José de Isnos	05/02/2018	02/03/2018
Estación Oporapa	05/02/2018	02/03/2018
Estación Salado Blanco	05/02/2018	02/03/2018
Subestación Bruselas	05/02/2018	02/03/2018

DISTRITO I BARAYA	Fecha Inicial	Fecha Final
Estación Baraya	05/03/2018	28/03/2018
Estación Tello	05/03/2018	28/03/2018
Estación Colombia	05/03/2018	28/03/2018
Estación Villavieja	05/03/2018	28/03/2018
Subestación San Alfonso	05/03/2018	28/03/2018

DISTRITO III GARZON	Fecha Inicial	Fecha Final
Estación Garzón	02/04/2018	30/04/2018
Estación Agrado	02/04/2018	30/04/2018
Estación Pital	02/04/2018	30/04/2018
Estación Tarqui	02/04/2018	30/04/2018
Subestación Maito	02/04/2018	30/04/2018
Subestación San Antonio	02/04/2018	30/04/2018
Puesto de Policía Buenavista	02/04/2018	30/04/2018

DISTRITO II CAMPOALEGRE	Fecha Inicial	Fecha Final
Estación Campoalegre	02/05/2018	01/06/2018
Estación Hobo	02/05/2018	01/06/2018
Estación Algeciras	02/05/2018	01/06/2018
Estación Gigante	02/05/2018	01/06/2018
Subestación Silvania	02/05/2018	01/06/2018

DISTRITO IV GUADALUPE	Fecha Inicial	Fecha Final
Estación Guadalupe	03/07/2018	03/08/2018
Estación Altamira	03/07/2018	03/08/2018
Estación Suaza	03/07/2018	03/08/2018
Estación Acevedo	03/07/2018	03/08/2018
Estación Timaná	03/07/2018	03/08/2018
Estación Elías	03/07/2018	03/08/2018

Subestación Naranjal	03/07/2018	03/08/2018
Subestación San Adolfo	03/07/2018	03/08/2018
DISTRITO VI LA PLATA	**Fecha Inicial**	**Fecha Final**
Estación La Plata	03/09/2018	28/09/2018
Estación Nátaga	03/09/2018	28/09/2018
Estación Paicol	03/09/2018	28/09/2018
Estación Tesalia	03/09/2018	28/09/2018
Estación La Argentina	03/09/2018	28/09/2018

DISTRITO VII YAGUARA	**Fecha Inicial**	**Fecha Final**
Estación Yaguara	01/10/2018	31/10/2018
Estación Santa María	01/10/2018	31/10/2018
Estación Teruel	01/10/2018	31/10/2018
Estación Iquira	01/10/2018	31/10/2018

Unidades y procesos	**Fecha Inicial**	**Fecha Final**
Seccional de Tránsito y Transporte	01/11/2018	30/11/2018
Seccional de Protección y Servicios Especiales	01/06/2018	30/06/2018
Seccional de Investigación Criminal	01/11/2018	30/11/2018
Seccional de Inteligencia Policial	01/11/2018	30/11/2018
Proceso Direccionamiento del SGI	01/06/2018	30/06/2018
Proceso de Convivencia y Seguridad Ciudadana	01/11/2018	30/11/2018
Proceso de Prevención	01/06/2018	30/06/2018
Proceso de Gestión Documental	01/11/2018	30/11/2018
Proceso de Integridad Policial	01/11/2018	30/11/2018
Proceso Direccionamiento del Talento Humano	01/06/2018	30/06/2018
Proceso de Actuación Jurídica	01/06/2018	30/06/2018
Proceso Administración Recursos Financieros	01/06/2018	30/06/2018

Paso 2:

Posteriormente se ejecuta las actividades de asesoría, acompañamiento o sensibilización del sistema de seguridad de la información; para lo cual la institución tiene determinado unos factores internos y externos que a medida del tiempo pueden afectar el logro de los objetivos propuestos y la capacidad funcional de la policía, dentro de las verificaciones se presta gran atención a los siguientes factores y elementos:

Factores Externos

- Cambios de políticas
- Cambios normativos

- ❖ Exigencias de la comunidad de seguridad de la información
- ❖ Avances tecnológicos accesibles

Factores Internos

Conceptos del Plan Estratégico Institucional

- ❖ Misión
- ❖ Visión
- ❖ Mega
- ❖ Principios y Valores éticos institucionales
- ❖ Políticas institucionales misionales
- ❖ Gestión humana y calidad de vida optima
- ❖ Servicio de policía
- ❖ Unidad institucional
- ❖ Integridad policial
- ❖ Educación e innovación policial
- ❖ Comunicaciones efectivas
- ❖ Buen uso de los recursos
- ❖ Políticas de sistemas de gestión
- ❖ Sistema de gestión de calidad
- ❖ Sistema de gestión ambiental
- ❖ Sistema de seguridad de la información
- ❖ Sistema de gestión de seguridad y salud en el trabajo
- ❖ Política de gestión del riesgo

Por otra parte, se verifica el cumplimiento de las 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, para lo cual se realiza el seguimiento a las siguientes políticas, así:

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

b) 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.

c) 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.

d) 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.

e) 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.

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

g) 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.

Por consiguiente y como soporte de las actividades realizadas se soporta lo actuado a través de 52 actas de reuniones de trabajo, según las fechas establecidas dentro de la planeación, así:

Acta 023 COMAN DEUIL del 12/02/2018 Estación de Policía Palestina
Acta 026 COMAN DEUIL del 13/02/2018 Estación de Policía San Agustín
Acta 031 COMAN DEUIL del 14/02/2018 Estación de Policía Isnos
Acta 038 COMAN DEUIL del 15/02/2018 Estación de Policía Pitalito
Acta 043 COMAN DEUIL del 16/02/2018 Subestación de Policía Bruselas
Acta 045 COMAN DEUIL del 19/02/2018 Estación de Policía Salado Blanco
Acta 046 COMAN DEUIL del 20/02/2018 Estación de Policía Oporapa
Acta 063 COMAN DEUIL del 12/03/2018 Estación de Policía Colombia

Acta 065 COMAN DEUIL del 13/03/2018 Estación de Policía Baraya
Acta 068 COMAN DEUIL del 14/03/2018 Estación de Policía Tello
Acta 071 COMAN DEUIL del 15/03/2018 Estación de Policía Villavieja
Acta 081 COMAN DEUIL del 16/03/2018 Subestación de Policía San Alfonso
Acta 097 COMAN DEUIL del 16/04/2018 Subestación de Policía Maito
Acta 100 COMAN DEUIL del 17/04/2018 Estación de Policía Tarqui
Acta 103 COMAN DEUIL del 18/04/2018 Estación de Policía Agrado
Acta 106 COMAN DEUIL del 19/04/2018 Estación de Policía Pital
Acta 109 COMAN DEUIL del 20/04/2018 Puesto de Policía Buena Vista
Acta 110 COMAN DEUIL del 23/04/2018 Subestación de San Antonio del Pescado
Acta 112 COMAN DEUIL del 24/04/2018 Estación de Policía Garzón
Acta 131 COMAN DEUIL del 15/05/2018 Estación de Policía Hobo
Acta 135 COMAN DEUIL del 16/05/2018 Subestación de Policía Silvania
Acta 137 COMAN DEUIL del 17/05/2018 Estación de Policía Gigante
Acta 140 COMAN DEUIL del 18/05/2018 Estación de Policía Algeciras
Acta 144 COMAN DEUIL del 21/05/2018 Estación de Policía Campoalegre
Acta 149 COMAN DEUIL del 07/06/2018 Seccional de Protección
Acta 154 COMAN DEUIL del 08/06/2018 Proceso Direccionamiento del SGI
Acta 159 COMAN DEUIL del 13/06/2018 Prevención Ciudadana
Acta 181 COMAN DEUIL del 09/07/2018 Estación de Policía Timana
Acta 184 COMAN DEUIL del 10/07/2018 Estación de Policía Elías
Acta 187 COMAN DEUIL del 11/07/2018 Subestación de Policía Naranjal
Acta 191 COMAN DEUIL del 12/07/2018 Subestación de Policía San Adolfo
Acta 194 COMAN DEUIL del 13/07/2018 Estación de Policía Acevedo
Acta 195 COMAN DEUIL del 16/07/2018 Estación de Policía Suaza
Acta 197 COMAN DEUIL del 17/07/2018 Estación de Policía Altamira
Acta 198 COMAN DEUIL del 18/07/2018 Estación de Policía Guadalupe
Acta 220 COMAN DEUIL del 12/09/2018 Estación de Policía La Argentina
Acta 222 COMAN DEUIL del 13/09/2018 Estación de Policía La Plata
Acta 227 COMAN DEUIL del 14/09/2018 Estación de Policía Natagá
Acta 230 COMAN DEUIL del 17/09/2018 Estación de Policía Paicol
Acta 234 COMAN DEUIL del 18/09/2018 Estación de Policía Tesalia
Acta 257 COMAN DEUIL del 26/10/2018 Estación de Policía Santa María
Acta 259 COMAN DEUIL del 29/10/2018 Estación de Policía Teruel
Acta 262 COMAN DEUIL del 30/10/2018 Estación de Policía Iquira
Acta 263 COMAN DEUIL del 31/10/2018 Estación de Policía Yaguara
Acta 268 COMAN PLANE del 13/11/2018 – Grupo de Gestión Documental
Acta 270 COMAN PLANE del 14/11/2018 – Comando operativo de seguridad
Acta 274 COMAN PLANE del 22/11/2018 – Personal de Integridad Policial

Acta 276 COMAN PLANE del 26/11/2018 – Seccional de Investigación Criminal
Acta No. 279 COMAN PLANE del 27/11/2018 - Seccional de tránsito y transporte
Acta No. 281 COMAN PLANE del 28/11/2018 - Seccional de Inteligencia Policial

Se soporta de manera fotográfica algunas actividades realizadas con el personal que conforma el departamento.

Figura 1. Asesoría Personal perteneciente al Proceso de Prevención.

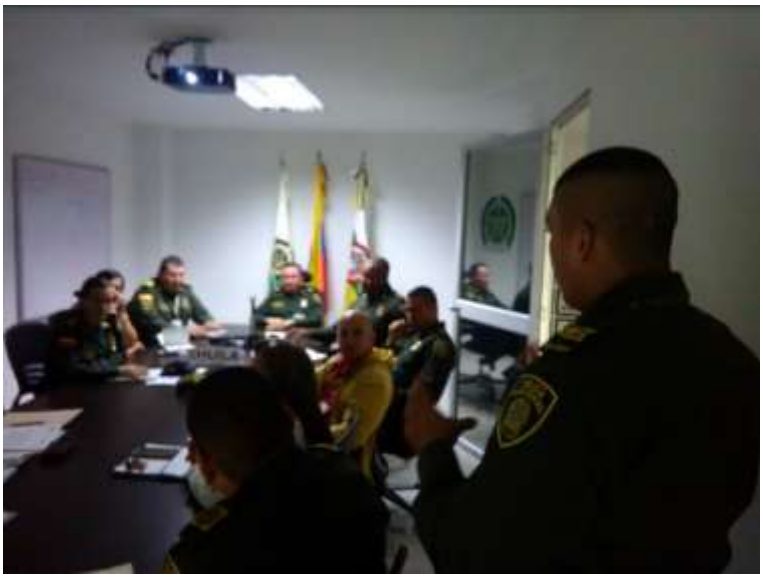


Figura 2. Asesoría Personal perteneciente a la Estación Palestina.

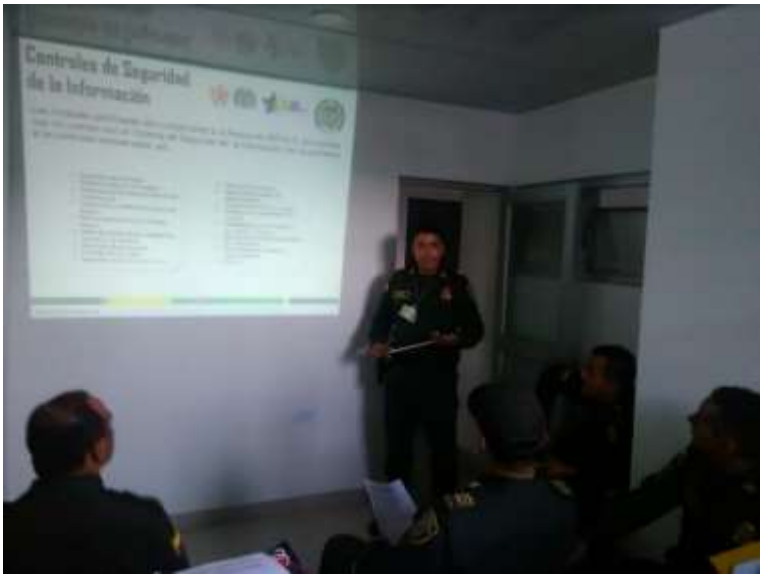


Figura 3. Asesoría Personal perteneciente a la Estación San Agustín.

.

.

Figura 4. Asesoría Personal perteneciente a la Subestación Bruselas

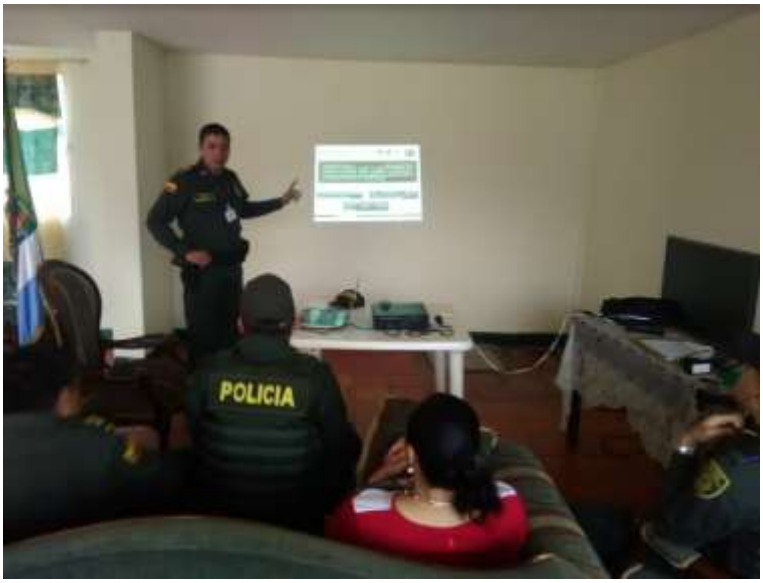


Figura 5. Asesoría Personal perteneciente a la Estación Oporapa

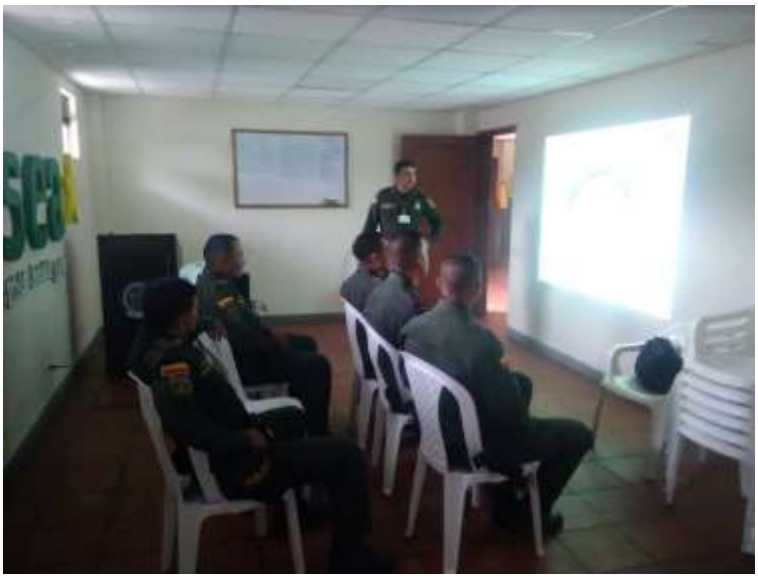
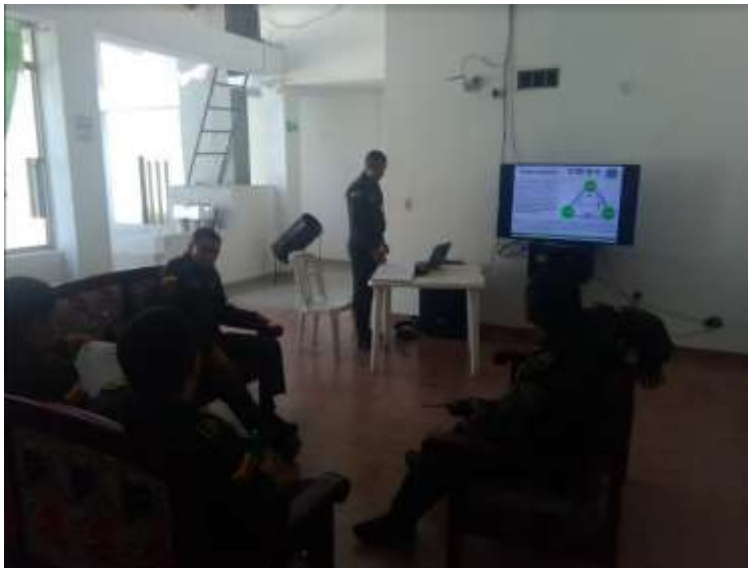


Figura 6. Asesoría Personal perteneciente a la Estación Colombia.



.

CONCLUSIONES

- Se realizó un autoaprendizaje referente a la seguridad de la información aplicable a las políticas, procedimientos y protocolos dispuestos en la Policía Nacional de Colombia.

- Se realizó una efectiva planeación de las actividades las cuales se han ejecutado según lo dispuesto sin ningún contratiempo.

- Se interiorizo los factores de riesgos más frecuentes en la institución, al igual que información relevante para cumplir con los objetivos dispuesto.

- Con los acompañamientos realizados se ha fortalecido la cultura enfocada a lo referente a usuarios de dominios de los equipos de cómputo y la utilización de los formatos establecidos para las entregas de los cargos; Formato 1DT-FR-0010 “Acuerdo para la revelación de información confidencial bajo deber de reserva”.

RECOMENDACIONES

- Para tener un efectivo control con respecto a las políticas, procedimientos y protocolos de la seguridad de la información, se hace necesario dar aplicabilidad a los 38 compromisos dispuestos por la institución.

- Se recomienda aplicar los parámetros establecidos en el documento firmado por todos los funcionarios policiales; formato 1DT-FR-0015 “Declaración de confidencialidad y compromiso con la seguridad de la información servidor público”, especialmente en lo referente a las contraseñas y usuarios que son personales e intransferibles.

- Se recomienda que el personal policial utilice los correos institucionales para el envío y recepción de la información, por tener un carácter confidencial o reservado.

BIBLIOGRAFÍA

[1] Decreto 2364 del 22 noviembre del 2012, firma digital. (22 de 11 de 2012). Obtenido de http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/NOVIEMBRE/22/DECRETO%202364%20DEL%2022%20DE%20NOVIEMBRE%20DE%202012.pdf

[2] Jurídico, A. (15 de 10 de 2018). Ley 1581 del 17 de octubre de 2012, protección de datos. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[3] LEY 527 18 de agosto de 1999 acceso y uso de los mensajes de datos. (18 de 08 de 1999). Obtenido de http://www.hostingred.com/ley_527_1999.pdf

[4] Nacional, P. (28 de 12 de 2016). Resolución 08310 del 28 de diciembre de 2016 “manual del sistema de gestión de seguridad de la información para la Policía Nacional”. Obtenido de http://www.policia.edu.co/sgsi/resolucion%2008310%20de%2028122016-%20manual%20sgsi.pdf

[5] normativa, s. u. (20 de 01 de 2015). Decreto 103 de 2015 del 20 enero de 2015. Obtenido de http://suin.gov.co/viewDocument.asp?ruta=Decretos/30019726

[6] oficial, d. (05 de 01 de 2009). LEY 1273 05 enero del 2009 Delitos informáticos. Obtenido de http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

ANEXO

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DEPARTAMENTO DE POLICIA HUILA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

Fecha:	Salado Blanco, 19 FEB 2018		
Hora de inicio:	07:00 Horas	**Hora de finalización:**	13:00 Horas
Lugar:	Sala de Reuniones Estación de Policía Salado Blanco		

ACTA 045 – COMAN – PLANE – 2.25

QUE TRATA DE LA ASESORÍA, ACOMPAÑAMIENTO Y SENSIBILIZACIÓN SOBRE LO ESTABLECIDO EN LA NORMA ISO 27001:2013 Y RESOLUCIÓN No. 08310 DEL "28122016 MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN"

ORDEN DEL DÍA

1. Verificación de asistentes
2. Socialización: Norma ISO 270012013 y Resolución 08310 del 28/12/2016 Manual de Seguridad de la Información

DESARROLLO

1. Verificación de asistentes

En las instalaciones de la Sala de reuniones de la Estación de policía Salado Blanco, se reúne el señor Intendente Horlid Reina Guzmán Responsable de gestión por Procesos, con el personal que conforma la unidad policial, con el fin de brindar asesoría, acompañamiento y sensibilización de lo dispuesto en la Norma ISO 270012013 y Resolución 08310 del 28/12/2016 "Manual de Seguridad de la Información", verificando la asistencia y disponibilidad del personal.

2. Socialización Norma ISO 27001:2013 y Resolución 08310 del 28/12/2016 Manual de Seguridad de la Información

Se da a conocer algunos apartes de la resolución los cuales son de cumplimiento y ejecución en las unidades que conforman el departamento, así:

Teniendo en cuenta la expedición del Manual de seguridad de la información para la Policía Nacional, el cual busca fortalecer los aspectos de disponibilidad, integridad y confidencialidad de la información al interior de la institución.

Enmarca los lineamientos y parámetros descritos en la norma Técnica de calidad ISO 27001:2013 conformado por 3 Capítulos, 113 artículos y 12 Anexos.

Anexo 1
SEGURIDAD DE LOS RECURSOS HUMANOS

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 la Declaración de Confidencialidad y Compromiso con la Seguridad de la Información Servidor Público al igual que el personal externo o contratista. 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.

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:

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.

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.

Anexo 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. 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.

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:

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

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 SIGMA. A través de IPD cada vez que el funcionario este en una novedad administrativa se cancelará el acceso a los recursos, 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.
Los funcionarios que tienen a cargo usuarios con privilegios y/o administradores deben informar cuando se presente novedad administrativa de vacaciones, retiro, cambio de cargo, licencia y demás novedades.

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.

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 y administra a través del Sistema de Información 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.

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.
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.
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 12. POLÍTICA DISPOSITIVOS MÓVILES Y TELETRABAJO. La Policía Nacional de Colombia aprueba el uso de los dispositivos móviles autorizados por la Institución 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.
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 para la realización de las actividades, se han implementado controles que contribuyen a mitigar la materialización del riesgo de fuga de información, la propagación de software de código malicioso los cuales pueden comprometer la Seguridad de la Información y afectar la 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 4
CONTROLES CRIPTOGRÁFICOS

ARTÍCULO 1. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS. Se utilizan sistemas y técnicas criptográficas con el fin de procurar una adecuada protección de su confidencialidad e integridad de la información. 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.

5. El Grupo de Seguridad de la Información Ofite es quien administra e implementa los controles criptográficos; excepto los Centros de Protección de Datos.

Anexo 5
SEGURIDAD FÍSICA Y DEL ENTORNO

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

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.

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 de 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.
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 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.

Anexo 7
SEGURIDAD DE LAS COMUNICACIONES

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.

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.

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.

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. 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.

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.

Por otra parte se imparte pautas importantes con respecto al manejo de la información a través de confidencialidad, integridad y disponibilidad de la misma; por consiguiente se socializa y verifica la seguridad de las operaciones en:

Control de cambios sobre la plataforma tecnológica
Aprobación, implementación de nuevos productos y servicios tecnológicos
Instalación de nuevas versiones/actualizaciones
Manejo de incidentes y vulnerabilidades
Uso correcto del correo electrónico, usuario empresarial, certificado digital
Administración de identidades
Entrega de información bajo deber de reserva
Protección contra software malicioso
Protección de usuarios contra altos privilegios
Elaboración y recuperación de copias de respaldo
Borrado seguro de información
Eliminación de dispositivos de almacenamiento
Instalación y mantenimiento de equipos de procesamiento y comunicaciones

COMPROMISOS:

Relación de los compromisos adquiridos por los participantes

Actividad	Responsable	Fecha de entrega
1. De manera permanente verificar en la Suite Visión Empresarial los formatos que allí se cargan ante los posibles cambios de los mismos.	Integrantes Estación de Policía	Permanente
2. Solicitar los respectivos permisos ante el jefe de telemática cuando se ausente por vacaciones, comisiones y traslado un funcionario que tenga bajo su responsabilidad dominio de equipo de cómputo, soporte formato 1DT-FR-0010.	Integrantes Estación de Policía	Permanente
3. Promover buenas prácticas de seguridad de la información	Integrantes Estación de Policía	Permanente
4. Dar aplicabilidad a los dispuesto en la Resolución 08310 del 28/12/2016 Manual de Seguridad de la Información	Integrantes Estación de Policía	Permanente
5. Las demás actividades que coadyuven en la mejora continua y fortalecimiento del sistema de gestión de seguridad de la información	Integrantes Estación de Policía	Permanente

Intendente **HORLID REINA GUZMAN**
Responsable Gestión por Procesos

Intendente **ALBEIRO RODRIGUEZ BARRERO**
Comandante Estación de Policía Salado Blanco

Anexo: uno (listado en 1 folios)

Elaborado por: IT. Horlid Reina Guzmán
Revisado por: -OT. Carlos Andrés González Valencia
Fecha de elaboración: 19-02-2018
Ubicación: D:\001B2 ACTAS\2.2\1 Acta de Reuniones de Trabajo

Km 2 Lote G12 Parque Industrial Palermo
Teléfonos 3203046780
deuil.meci@policia.gov.co
www.policia.gov.co

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DEPARTAMENTO DE POLICIA HUILA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

Fecha:	Salado Blanco, 19 FEB 2018		
Hora de inicio:	07:00 Horas	**Hora finalización**	13:00 Horas
Lugar:	Sala de Reuniones Estación de Policía Salado Blanco		

ACTA 045 – COMAN – PLANE – 2.25

QUE TRATA DE LA ASESORÍA, ACOMPAÑAMIENTO Y SENSIBILIZACIÓN SOBRE LO ESTABLECIDO EN LA NORMA ISO 27001:2013 Y RESOLUCIÓN No. 08310 DEL "28122016 MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN"

ASISTENTES

GR.	NOMBRES Y APELLIDOS	UNIDAD O DEPENDENCIA	CARGO	CORREO ELECTRÓNICO	TELÉFONO	FIRMA
IT.	Nelson Morales Ortiz	ESSAL	Gestor	nelson.morales@correo.	3124415169	
IT	JOSE [illegible]	ESSAL	[illegible]	[illegible]	3128741853	
PT	JEAN DE LA ROSA CHAVES	ESSAL	Vigilancia	jean.delarosa[illegible]	3125516735	
PT	MARTIN CALLO CAMPO OSPINA	ESSAL	Vigilancia	martincampo42902@[illegible]	3755866199	
PT	JHONNER VARGAS TAPIAS	ESSAL	Supervisor	jhonner.vargas2463@[illegible]	3102249532	
PT.	Oscar Alexy Calderón	ESSAL	Digitación	oscar.calderón6811@	3123923434	

Km 2 Lote G12 Parque Industrial, Palermo
Teléfonos 3203046780
deuil.plane@policia.gov.co
www.policia.gov.co