DISEÑAR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICABLES AL COMANDO DE LA POLICÍA DE FLORENCIA, BASADAS EN LA NORMA ISO/IEC 27001:2013

WILSON RICARDO ARIAS CARMONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA, CAQUETÁ
2015

DISEÑAR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICABLES AL COMANDO DE LA POLICÍA DE FLORENCIA, BASADAS EN LA NORMA ISO/IEC 27001:2013

WILSON RICARDO ARIAS CARMONA

Tesis de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
Ing. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA, CAQUETÁ
2015

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, lunes 7 de Diciembre de 2015

DEDICATORIA

En primer lugar quiero dedicar con todo mi corazón lleno de alegría por permitirme hacer realidad lograr ser un profesional, con título de especialista en seguridad informática quiero honrar con este trabajo que representa la culminación de un año de esfuerzos y altibajos, a quien merece toda gloria y alabanza, mi Dios. Tú Señor lo hiciste todo posible. A ti te entregué mi carrera, me guiaste de regreso al camino correcto en momentos cuando lo creí todo perdido, me fortaleciste, me renovaste, por esto y mucho más. No quisiera dejar atrás a mi madre Ruby Mónica Quitian Torres que siempre estuvo en contacto conmigo dándome fuerzas para continuar con mi formación de especialista por no permitir que me rindiera en la mitad de mis estudios.

Le dedico este proyecto de grado a todos los que creyeron en mí, a toda la gente que me apoyó, a mis amigos y familiares y ha esta institución que me ha formado con valores propios de un profesional, pero en especial se lo dedico a mi padre que se encuentra un poco mal de salud, a mis amigos que me brindaron su ayuda, su atención y los más importante su amistad.

Dedico este proyecto a mi hermana por ser parte esencial en mi vida, por compartir conmigo en las buenas y en las malas, por permitirme el honor de no solo ser su hermano si no ser su amigo porque sabe que he luchado por este momento, sé que se siente orgullosa de su hermano mayor.

Dedico por supuesto el trabajo, a nuestros docentes en cada Escuela de los rincones más apartados de nuestro estado y nuestra grande Patria, quienes laboran con la materia más valiosa de nuestro país, las mentes, la personalidad, la formación integral de nuestros niños y niñas, y son en definitiva formadores de los hombres y mujeres del mañana sobre la base de valores morales, éticos y de mucho

humanismo, quienes con mucha paciencia estuvieron siempre ahí, asesorando este gran proyecto.

Dedico este gran paso en mi vida a mis abuelos que siempre han estado pendiente del trascurso diario de mi vida, por sus oraciones que siempre hacen ante Dios todo poderoso, por sus enseñanzas a pesar de la distancia.

AGRADECIMIENTOS

Deseamos expresar nuestro más sincero agradecimiento a los ingenieros, Wilson Castaño, Erika Liliana Villamizar, quienes además de transmitirme una parte de su conocimiento, su asesoría y orientaron, nos ayudaron y estimularon constantemente y directamente en todos los aspectos del proyecto de grado. Agradecerles la plena confianza que siempre nos han demostrado, así como la dedicación y la atención que en todo momento nos han ofrecido.

A nuestra Universidad Nacional Abierta y a Distancia del zonal Sur CEAD Florencia por permitirnos realizar nuestros estudios superiores. Por esto, debo agradecer también a todo el cuerpo de docentes de esta universidad por la consideración y comprensión mostrada durante el periodo de estudio y la preparación del proyecto de grado.

Igualmente los autores del presente estudio agradecen muy profundamente a todos los organismos y personas naturales que hicieron posible la realización del mismo como los miembros activos de la Policía Nacional que laboran en el departamento de Policía Caquetá, por permitirnos realzar los diferentes estudios estadísticos y la información básica que dio inicio a la elaboración del trabajo de grado.

A todas y todos quienes de una u otra forma han colocado un granito de arena para el logro de este Trabajo de Grado, agradezco de forma sincera su valiosa colaboración.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

INTRODUCCIÓN

Es de gran importancia que en una organización se implanten o se establezcan políticas para la seguridad de la información, por esto la necesidad de establecerlas. Esto permitirá la fácil administración de la información en una organización, la preservación de la confidencialidad, Integridad y disponibilidad de la misma y garantizar la autenticidad, trazabilidad, no repudio y fiabilidad de la misma.

Las políticas de seguridad de la información tienen por objeto gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del comando policial de Florencia.

En el desarrollo del presente proyecto se diseñarán las políticas de seguridad de la información para el comando de policía de Florencia, ya que dicha entidad requiere la protección de su información tanto en aplicaciones, servicios, personas que forman parte de las herramientas de trabajo. La importancia de diseñar y establecer políticas para la seguridad de la información en una entidad como el comando de policía de Florencia, brindan protección y seguridad frente a las necesidades de seguridad de la información.

1. PLANTEAMIENTO DEL PROBLEMA.

El departamento de policía Caquetá en la actualidad administra la información de forma directa, donde se evidencia un riesgo latente a una gran pérdida de información, pues no se cuenta con unas políticas, normas, directrices, procedimientos, gestión del riesgo, ni con personal profesional para administrar y controlar el uso adecuado de todo el contexto tecnológico del comando, lo que por su puesto conlleva a una falta de concientización en seguridad de la información, con los cuidados y la importancia que se debe tener con el proceso de la información, como lo que tiene que ver con los reglamentos únicos de estricto control.

El comando de policía Florencia, presenta inconsistencias por falta de políticas para gestionar la seguridad de la información, ya que notablemente se requiere de la ayuda de profesionales en la seguridad de la información, con el fin de diseñar políticas de seguridad de la información aplicables según la norma ISO/IEC 27001:2013, de allí nace la idea de disminuir el impacto de los riesgos potenciales, en pro de la seguridad de la información pero a la vez es necesario aplicar controles basados en un cuidadoso análisis de riesgo. Las políticas de seguridad de la información ayudan a mantener el riesgo por debajo del nivel aceptable que se haya determinado a nivel directivo.

Actualmente el comando de policía de Florencia, ha mostrado una serie de debilidades en el manejo de la información tales como: existen vulnerabilidades que pueden ocasionar la fuga de la información; varios usuarios con privilegios para acceder a la información, no se tiene ninguna restricción informática para los dispositivos de almacenamiento de USB, y unidades de DVD, al igual que la captura de pantallazos.

Los requerimientos por parte de los usuarios para la solución de las dificultades que se les presentan, en la necesidad de contar con un servidor de datos donde puedan guardar su información, mas no extraerla, el uso adecuado de las dispositivos de almacenamiento masivo, parámetros establecidos para el uso de contraseñas, que no se utilicen las mismas; situación que genera un desgaste en el tiempo del personal técnico, que en otras condiciones podría estar utilizado para cumplimiento permanente de políticas e innovación de estrategias para el mejoramiento en el uso de la información.

Estas falencias hacen que se sigan presentando fallas en la seguridad de la información, por lo cual se debe tener en cuenta que al diseñar y definir una serie de políticas que sean aplicables para mitigar los problemas con la seguridad de la información en el comando de policía Florencia mejorara esta problemática.

1.1 FORMULACIÓN DEL PROBLEMA

¿Con el fin de preservar la disponibilidad, confidencialidad e integridad de la información en el comando de la policía de Florencia, es necesario contar con políticas de seguridad de la información que ayuden con la solución?

2. JUSTIFICACIÓN

La presente investigación permitirá incrementar el nivel de seguridad de la información del comando de Policía Florencia, es importante saber que uno de los mayores activos de la entidad policial es su información y por ende requiere aplicar lineamientos de seguridad en la manipulación de la información y plataforma tecnológica que es de uso privativo.

El departamento de policía Florencia, requiere definir políticas de seguridad de información que sirvan de insumo para una posterior implantación del Sistema de Gestión de Seguridad de la Información, con el fin de adoptar buenas prácticas y lineamientos para el acceso y tratamiento de la información, bien sea física, magnética y desde los portales web; y que sean eficientes, claras y directas y concienciar a los funcionarios sobre la seguridad de la información.

Con el desarrollo de este proyecto la policía de Florencia obtendrá una serie de beneficios para la protección y seguridad de la información.

Las políticas que se propondrán darán lugar a la confidencialidad, integridad y disponibilidad de la información, generando una serie de restricciones para el usuario y privilegios para el personal técnico de la Unidad policial.

3. OBJETIVOS

3.1 **OBJETIVO GENERAL**

- Diseñar las políticas de seguridad de la información basadas en la norma ISO/IEC 27001:2013 que puedan ser implantadas en el comando de policía de Florencia.

3.2.1 Objetivos Específicos.

- Realizar un análisis del estado actual de la seguridad de la información de acuerdo a los requisitos de la norma ISO27001:2013

- Realizar un análisis de información mediante la utilización de la técnica de investigación tipo encuesta.

- Realizar análisis de vulnerabilidad a la red de datos del comando de policía Florencia, con el fin de identificarlas para así dar inicio con el diseño de políticas de seguridad Informática.

- Definir para el comando de policía Florencia políticas de seguridad de información que permitan incrementar el nivel de seguridad basado en la norma ISO 27001:2013

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Norma ISO 27001:2013; la cual facilita la integración de los sistemas de gestión, debido a que es una estructura de alto nivel, donde los términos y definiciones ayudan a implementar, determina los objetivos de un SGSI, se enfatiza en aplicar el proceso de evaluación de riesgos de seguridad de información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información en el ámbito del sistema de gestión de la seguridad de información.

Sistemas de Gestión de Seguridad de la información (SGSI)[1]

Es el concepto central sobre el que se construye ISO 27001:2013 que se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; la gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización, este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

La gestión de la seguridad de la información:

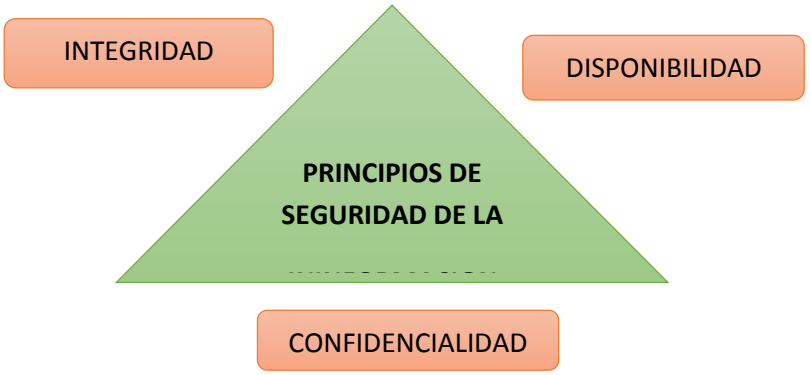
Es la adecuada gestión del riesgo, es el diseño de políticas, normas, líneas bases, guías, procedimientos y educación a los usuarios y propietarios de los activos de información; cuyo objetivo es planificar, diseñar, implementar y mantener un programa de seguridad de la información en concordancia con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

[1] MINISTERIO TIC, 2014 Sistemas de gestión de seguridad de la información Bogotá, edificio Murillo Toro.

teniendo en cuenta el equipo computacional necesario para que el sistema de gestión de seguridad de la información pueda operar, se requiere de un hardware adecuado, un software que haga funcional el hardware y el recurso humano que reconozca y acepte las políticas de seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado, el propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías en las siguientes secciones, se desarrollarán los conceptos fundamentales de unas políticas de seguridad informática bajo la norma ISO 27001:2013

Figura 1. Principios de la seguridad de la información[2]



Fuente: El autor

[2] Alberto Sanglier, Abril 2003, Principios de la seguridad informática, Madrid Cundinamarca

Principio Disponibilidad.

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

Principio Integridad

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

Principio Confidencialidad

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

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo y vulnerabilidad empresarial. Este proceso es el que constituye unas políticas de seguridad informática.

4.2 MARCO LEGAL

✓ ley 23 de 1982 "derechos de autor"[3]

El derecho de autor es una especie dentro de la institución de la propiedad intelectual, en virtud de la cual se otorga la protección a las creaciones inspiradas a través de lo artístico, tiene por objeto las manifestaciones con espíritu, de tal manera que puedan ser captadas.

El Congreso de Colombia expide la lay LEY 23 DE 1982 (enero 28) sobre derechos de autor.

✓ ley 527 de 1999 comercio electrónico y firmas digitales.

Se presentó por parte del Ministro de Transporte, el Ministro de Desarrollo Económico, el Ministro de Comercio Exterior y el Ministro de Justicia el proyecto de ley número 227 de 1998, ante la Honorable Cámara de Representantes, para su respectivo debate y aprobación, con el cual se buscaba definir y reglamentar el acceso y uso del comercio electrónico, de las firmas digitales y se autorizaban las entidades de certificación.

La regulación se proponía brindar un adecuado tratamiento al contenido de las comunicaciones, denominado intercambio electrónico de informaciones o con sus siglas en inglés, aunque no dejaba de lado otros medios conexos de comunicación de datos. Además se centraba en el aspecto probatorio, habida cuenta que hacia futuro, la información presentada por éstos medios sería distinta a la noción tradicional que se tiene de documento.

Se basa exclusivamente para definir lo la seguridad en el Mensaje de datos. La información generada, enviada o recibida, almacenada o comunicada por medios electrónicos, ópticos como pudieran ser, el Intercambio Electrónico de Datos (EDI).

✓ Ley 1273 título "De la protección de la Información y de los datos" [4]

[3] IRAGORRI HORMAZA, 1982, de los derechos de autor, Bogotá D.C

[4] GERMAN VARON COTRINO 2009, de la protección de los datos Bogotá D.C

Esta ley típica los delitos con el manejo de los datos personales, ya que es da gran importancia que las personas utilicen medidas de protección en materia jurídica para evitar realizar uno de estos actos que son penalizados.

Esta ley vincula de forma permanente al código penal su título II denominado de la protección de la información y delos datos, que a su vez se divide en dos capítulos.

Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Segundo: De los atentados informáticos y otras infracciones

- ✓ Ley 1266 del 2008 Habeas Data.

La Corte Constitucional lo definió como el derecho que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, y certificación de los datos, con limitación en las posibilidades de su divulgación o publicación, de conformidad con los principios que regulan el proceso de administración de datos personales.

La persona u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario que le corresponde.

- ✓ Ley Estatutaria 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales.

Preservar el derecho constitucional que todas las personas tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

4.3 MARCO CONTEXTUAL

La Policía Nacional como toda empresa está compuesta por un sistema de gestión integral.

4.3.1 Misión

La misión de la policía nacional está contemplada en el artículo 218 de la carta magna de Colombia la constitución política que a su letra dice:

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

4.3.2 Visión

La policía nacional se consolidara en el 2022 como institución fundamental para la construcción de un país equitativo y en paz, garante y respetuoso de los derechos humanos, afianzando la convivencia y seguridad a través del control del delito, la educación ciudadana, prevención, mediación y articulación institucional e interinstitucional como ejes centrales del servicio.

4.3.3 La Mega

Al 2018 la policía nacional será la institución más reconocida, en virtud de la excelencia profesional de sus integrantes para brindar un servicio policial efectivo basado en el humanismo, solidario y cercano al ciudadano, afianzando la confianza, credibilidad y legitimidad institucional

4.3.4 Política de calidad

La siguiente es la Política de Calidad definida y establecida por la Policía Nacional que hace parte de las Políticas Institucionales:

“En la Policía Nacional nos comprometemos a prestar un servicio respetuoso, efectivo y cercano al ciudadano, para garantizar comunidades seguras, solidarias y en convivencia, a través del mejoramiento de los estándares de eficiencia, eficacia y efectividad del Sistema de Gestión Integral”.

4.3.5 Objetivos de Calidad

Los siguientes, son los objetivos de calidad definidos por la Policía Nacional

- ✓ Garantizar la convivencia y seguridad ciudadana.
- ✓ Lograr el posicionamiento, respeto, credibilidad y apoyo de la comunidad.
- ✓ Garantizar la participación ciudadana como veedor institucional y su corresponsabilidad en la convivencia y seguridad.
- ✓ Contribuir a garantizar la gobernabilidad del país.

Se trabaja en proceso secuencial de desarrollo que permite observar los pasos hacia abajo como en una cascada de agua a través de las fases de análisis de las necesidades, el diseño, implantación, pruebas de validación, la integración y el mantenimiento.

El diseño de la técnica para la selección de la muestra se realizó encuestando el 10% del personal activo que labora en la base del comando de departamento de policía Florencia en el Caquetá.

Analizando cada una de las respuestas donde fue encuestado personas de rangos de edad diferentes de determina estadísticamente que el porcentaje arrojado muestra la necesidad de implantar un sistema de gestión de seguridad de la información.

4.3.6 Reseña Histórica

La Dirección General de la Policía Nacional previo análisis y estudio, consideró necesario crear el Departamento de Policía Caquetá, sede y mando que venía cubriendo el Departamento de Policía Huila como sexto Distrito; Para lo cual el Departamento de Policía Caquetá se creó mediante resolución No. 2600 del 1980, cuando aún el Caquetá políticamente figuraba como intendencia.

Figura 2. Comando de policía Caquetá.

Fuente: Fotografía de perfil tomada por Andrés Meneses.

Reconoció la oportunidad en el sector para crecer, progresar y servir, razón por la cual comprometió el esfuerzo y dedicación de todos sus colaboradores, para diseñar

un plan estratégico, siempre con la visión de satisfacer y superar las necesidades y expectativas de los ciudadanos para tomar acciones encaminadas a prestar un excelente servicio al cliente interno y externo.

Hoy se cuenta con una amplia experiencia de profesionales para el servicio a la ciudadanía, la actitud positiva hace un equipo dinámico, eficiente e innovador, que considera el cambio como un reto permanente.

4.4 LA POBLACIÓN:

En el proceso del análisis para la determinación de la necesidad, podemos identificar, de mayor a menor, tres tipos de poblaciones:

4.4.1 Población de referencia:

Es la cifra de población global, que tomamos como marco de referencia para cálculo, comparación y análisis de la necesidad para contar con un SGSI, que se determina con el personal encuestado, 50 personas que laboran en el área administrativa, de la base del comando de departamento de policía Florencia.

4.4.2 Población afectada:

Es el segmento de la población de referencia que requiere de los servicios del proyecto para satisfacer la necesidad identificada. También llamada población carente, es la parte del personal que no fue encuestada, pero cuentan con una solución sobre el diseño de políticas de seguridad de la información SGSI.

4.4.3 Población objetivo:

Es aquella parte de la población afectada a la que el proyecto, una vez examinados los criterios y restricciones, está en condiciones reales de atender.

Son aquellas personas que perciben algún servicio del proyecto, para el caso del personal total que cumple diversas labores día a día en la base del comando de departamento de policía Caquetá. Según el análisis con la técnica de investigación, la encuesta orienta el proyecto comprobando la hipótesis planteada, con la necesidad de contar con un sistema de gestión de seguridad de la información.

5. RECURSOS DISPONIBLES

5.1 **RECURSOS MATERIALES**.

La base del comando de policía Florencia, consta de una infraestructura tecnológica, que le dan el apoyo necesario y la facilidad para el funcionamiento de implantación de las políticas de seguridad de la información. .

Presenta la certificación de puntos de red en toda la base del comando, un Rack principal ubicado en el tercer piso, en la oficina de Telemática donde se administra la red a la base del comando de policía Caquetá, este Rack consta de los siguientes elementos para el funcionamiento.

5.1.1 Recursos Institucionales.

El proyecto necesitará de los siguientes recursos institucionales:

Por parte de la empresa. El suministro de toda la información necesaria del sistema para conocer cuáles son las vulnerabilidades, amenazas y riegos, el accesos para conocer los procedimientos que se realizan y la disponibilidad del funcionario a fin de poderlos entrevistar y conocer cuáles son las actividades que realiza para la seguridad de la información.

El proyecto tiene el respaldo del cuerpo de docentes como asesores del proyecto para coordinar las labores para definir las políticas de seguridad de la información.

Por parte de la universidad: La asesoría por parte de la ingeniera. Erika Liliana Villamizar como soporte al desarrollo del proyecto.

5.1.2 Recursos Financieros.

El proyecto necesitará de los siguientes recursos financieros:

Los equipos de cómputo que se utilizaran en el proyecto, son equipos propios de la institución.

El tiempo total para el proyecto se determina en varias sesiones de las cual tenemos.

TTPT (Tiempo Total del Proyecto Tradicional): 28 semanas
TPPT (Tiempo de planificación): 12 semanas

TIMT (Tiempo de Implementación): 6 semanas
El TTPA (Tiempo Total de un Proyecto Ágil será:
TTPA: 32-(12+6) + (12/6) = 12 Semanas

12 semanas empleadas para el diseño e implantación forma tradicional comparándolo $1.600.000 mensual, por la cantidad de semanas equivalentes a 3 meses de trabajo real.

1600000x3= 4´800.000 de pesos de horas trabajadas.

La inversión no será muy numerosa, ya que la ventaja de trabajar con software libre, disminuye sustancialmente los costos, como se puede ver en la siguiente tabla:

Tabla 1. Recursos

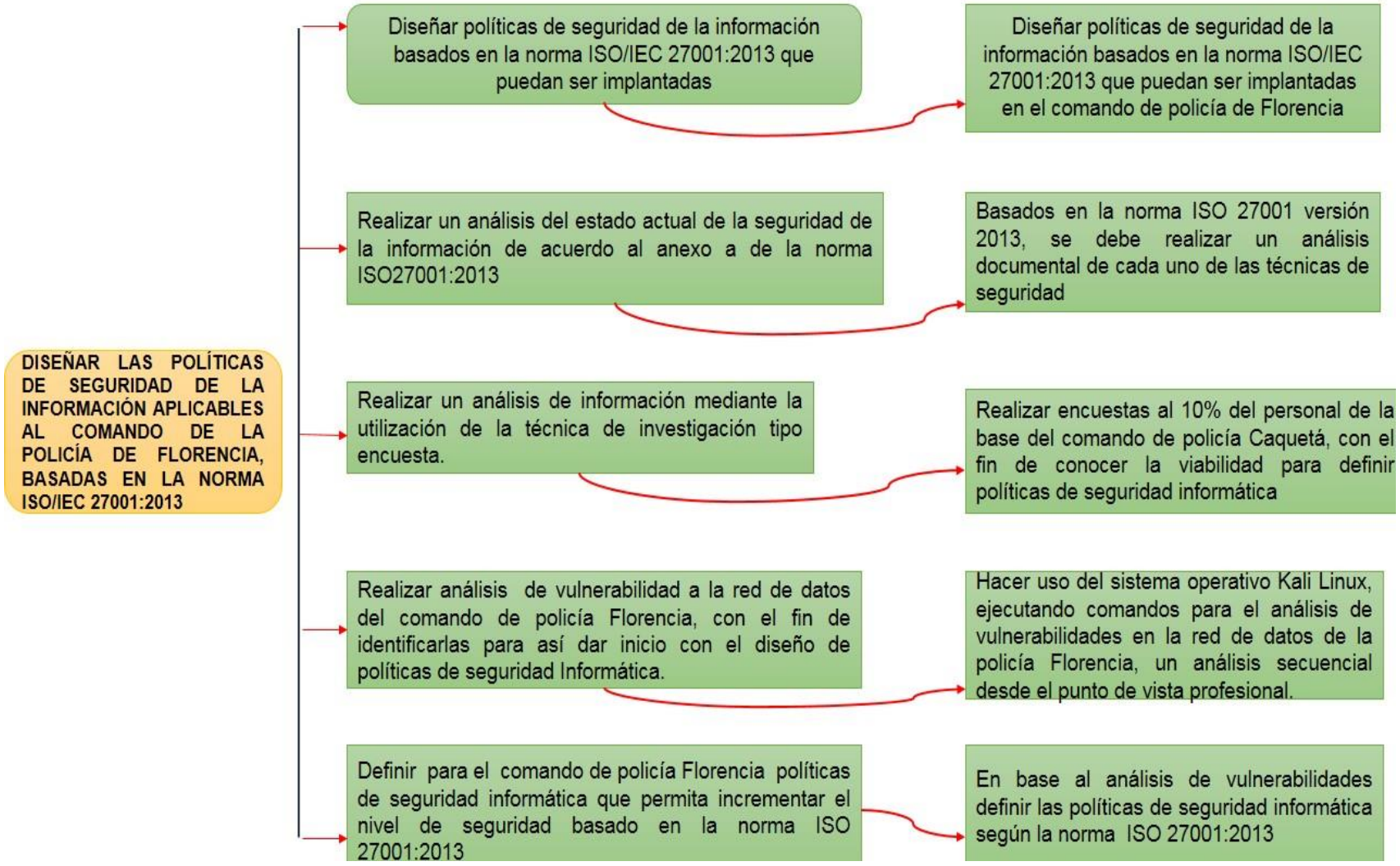
ACTIVIDAD	FUENTE DE FINANCIACIÓN	
	EMPRESA	DISEÑADORES
Adquisición del Equipo de cómputo	propios	
Gastos de personal. Proceso de análisis diseño e implantación del SGSI, con sus políticas definidas		$4’800.000
Adquisición de software para el análisis finas de vulnerabilidades de sitios web		$ 450.000
Análisis y Diseño de Sistemas Papelería Desplazamientos Informe de Diseño		$ 500.00
Desarrollo y programación y definición de las políticas: Tiempo de uso de computador Papelería –CD-ROM Pruebas del sistema Informe de proyecto		$ 800.000
Implantación y capacitación Desplazamientos Capacitación a funcionarios		$ 150.000
Auditoria y correcciones post instalación. Imprevistos (10% del valor proyecto)		$ 500.000
Valor Total		$7’200.000

Fuente. El autor

6. METODOLOGÍA

La metodología que se aplicará para el diseño de las políticas, es un proceso secuencial de desarrollo que permite observar los pasos uno a uno en forma de en una cascada a través de las fases de análisis del estado actual, análisis de la información, pruebas de vulnerabilidad, para una mejor ilustración se utiliza el siguiente diagrama, dando a conocer cada uno de los objetivo y su procedimiento.

Figura 3. Diagrama Metodología del Proyecto.



Fuente: El autor

Tabla 2. Cronograma

CRONOGRAMA	Septiembre				Octubre				Noviembre			
	1	2	3	4	1	2	3	4	1	2	3	4
Aprobación del proyecto												
Identificación del problema												
Análisis de información												
Técnica e investigación												
Clasificación de la información												
Diseño de entradas y salidas												
Realizar un análisis del estado actual de la seguridad de la información en base a la norma ISO27001:2013												
Realizar análisis de vulnerabilidad a la red de datos												
Diseño de Políticas de seguridad informática												
Entrega del informe final												

Fuente: El autor

7. DESARROLLO DEL PROYECTO

7.1 ANÁLISIS DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN DE ACUERDO A LOS REQUISITOS DE LA NORMA ISO27001:2013

Con base a la norma ISO27001:2013, se realiza el siguiente análisis del estado en el que actualmente se encuentra el comando de Policía Florencia Caquetá.

Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información requisitos.

Tabla 3. Análisis de seguridad de la información

REQUISITO	4 CONTEXTO DE LA ORGANIZACIÓN	APLICA	NO APLICA	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
4.1	CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	X		Se tiene el conocimiento de la organización, su contexto, así como la comprensión de su misión, visión y objetivos estratégicos.	Implementar un Gobierno de Tecnología Informática que se ajuste a las necesidades de la organización y que esté acorde a los objetivos estratégicos, capacidades, recursos, sistemas de información y estructura organizacional.
4.2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	X		Se tiene el conocimiento de las partes interesadas en la implementación de un Sistema de Gestión de la Seguridad de la Información (**SGSI**). La oficina de Sistemas y Telecomunicaciones y todas las unidades administrativas que dependen de su correcto funcionamiento para ejercer el desarrollo normal de sus procesos, así como los estudiantes para realizar sus labores académicas.	Capacitar al personal interesado en la seguridad de la información.
4.3	DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	X		Se tienen las herramientas necesarias para la definición y adaptación de un SGSI	Comunicar a los empleados (directores, jefes y operarios de sistemas) la importancia de un SGSI en la institución y establecer un nivel de compromiso, liderazgo y concientización con las políticas de seguridad de la información que allí sean contenidas.

4.4	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		**X**	Actualmente no se tiene implementado un SGSI.	Diseñar y/o planear un SGSI que mediante un proceso sistemático y mejoramiento continuo ayude a establecer los niveles de riesgos aceptables de la institución. La recomendación es el estándar internacional **ISO 27001:2013** aplicable a las organizaciones de cualquier tamaño y actividad.
REQUISITO	**5 LIDERAZGO**	**APLICA**	**NO APLICA**	**¿QUÉ SE TIENE?**	**RECOMENDACIONES A IMPLEMENTAR**
5.1	LIDERAZGO Y COMPROMISO	**X**		La jefa de la oficina de Sistemas y Telecomunicaciones tiene conocimiento de la fase de diseño del SGSI, apoya la investigación e incluso da su aval para una futura implementación y certificación en la norma, comprendiendo así su importancia y beneficios que genera para la institución.	Establecer una comunicación y liderazgo efectivo a los empleados que hagan parte de las unidades (de acuerdo al alcance) sobre la importancia del SGSI.
5.2	POLÍTICA	**x**		No se tiene una política de seguridad de la información documentada.	Redactar las políticas generales y detalladas del SGSI que sean de alcance para la institución y que sean públicamente accesibles a todos los empleados para su conocimiento y aplicación.
5.3	ROLES, RESPONSABILIDADES. Y AUTORIDADES EN LA ORGANIZACIÓN	**X**		Los roles y responsabilidades están asignados.	Documentar los roles y responsabilidades en base a la seguridad de la información.
REQUISITO	**6 PLANIFICACIÓN**	**APLICA**	**NO APLICA**	**¿QUÉ SE TIENE?**	**RECOMENDACIONES A IMPLEMENTAR**
6.1	ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	**x**		Se cuenta con el formato de confidencialidad de la información para los usuarios	Se debe plasmar ciertos controles directo hacia el la seguridad de la información, creando conciencia al funcionario.
6.1.1	Generalidades	**X**		Existen todas las condiciones para diseñar el SGSI. No existen riesgos a gran escala o implicaciones legales que impidan esta fase así como que eviten su mejoramiento continuo.	No Aplica
6.1.2	Valoración de riesgos de la seguridad de la información		**X**	No existe una metodología claramente definida que clasifique, analice, evalúe y gestione los riesgos de la seguridad de la información.	Analizar las distintas metodologías de evaluación de riesgos, escoger la que mejor se adapte a las necesidades de la institución y documentarla.
6.1.3	Tratamiento de los riesgos de seguridad de la información		**X**	No existe un plan para el tratamiento de riesgos.	Determinar los controles necesarios para mitigar los riesgos encontrados en el análisis y documentar el plan de tratamiento para cada uno de ellos justificando su elección.
6.2	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLO		**X**	No están documentados los objetivos de la seguridad de la información.	Definir los objetivos de la seguridad de la información y establecer la forma de alcanzarlos comprometiendo a los empleados en su alcance y logro.
7	**SOPORTE.**	**APLICA**	**NO APLICA**	**¿QUÉ SE TIENE?**	**RECOMENDACIONES A IMPLEMENTAR**

7.1	RECURSOS.	**x**		Se cuenta con el aval y los recursos necesarios para definir un SGSI	Hacer el mejor uso posible de estos recursos con el fin de dar aplicabilidad total al SGSI
7.2	COMPETENCIA	**X**		Se tiene personal profesional en las diferentes áreas administrativas con conocimientos básicos del tema.	Dar la inducción total al personal de la organización, creando perfiles según su competencia para la SGSI
7.3	TOMA DE CONCIENCIA		X	No se tiene el grado de responsabilidad en cuanto al manejo de la información	Se debe tomar el control de las herramientas para el uso y aplicación de un SGSI,
7.4	COMUNICACIÓN		x	No se cuenta con un líder que se encargue de difundir los diferentes cambios y lineamientos sobre el control de la información.	Se es necesario que exista un dinamizador o promotor de seguridad de la información en la organización.
7.5	INFORMACIÓN DOCUMENTADA		X	No existe un historial o protocolo adecuado documentado para el seguimiento y control de un SGSI.	Tomar las medidas necesarias para adoptar soportes documentales que permitan claramente definir la estructura de un SGSI
7.5.1	GENERALIDADES		X	No se cuenta con documentos asociados a un SGSI	Se bebe definir y adoptar controles documentados para el control de un SGSI.
7.5.2	CREACIÓN Y ACTUALIZACIÓN		X	Solo se tiene un formato para la confidencialidad de la información, pero no se ha realizado una actualización masiva.	Es importante tomar acciones en base a la creación y actuación de los documentos asociados al proceso del SGSI
7.5.3	CONTROL DE LA INFORMACIÓN DOCUMENTADA		X	No se lleva un registro de las revistas y supervisión de documentación asociado a un SGSI.	Crear archivo general de la documentación de aplicable al SGSI, realizando planes de trabajo mensual o trimestral.
8	**OPERACIÓN**	**APLICA**	**NO APLICA**	**¿QUÉ SE TIENE?**	**RECOMENDACIONES A IMPLEMENTAR**
8.1	PLANIFICACIÓN Y CONTROL OPERACIONAL		X	No existe un plan de trabajo fijado para el cumplimiento de los requisitos para lograr tener un SGSI.	Se requiere de un planificar e implementar controles en el cumplimiento de las diferentes acciones de un SGSI.
8.2	EVALUACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN	X		Se cuenta con el análisis y evaluación de los riesgos para la seguridad de la información	Mejorar seguimiento a la problemática en cuanto a la gestión del riesgo para su debida evaluación y seguimiento en la seguridad de la información
8.3	TRATAMIENTO DE RIESGOS A LA SEGURIDAD DE LA INFORMACIÓN	x		Existe tratamiento alguno para tratar los riegos debido a que no se lleva un control en el seguimiento y evaluación del riesgo.	Realizar la evaluación del riesgo de forma periódica, con el fin de llevar un control documental sobre el tratamiento de ellos.
9	**EVALUACION DEL DESEMPEÑO**	**APLICA**	**NO APLICA**	**¿QUÉ SE TIENE?**	**RECOMENDACIONES A IMPLEMENTAR**
9.1	SEGUIMIENTO, MEDICIÓN, ANALISIS Y EVALUACIÓN		x	No existe medición en los controles de seguridad informática, ya que no se cuenta con políticas definidas para la unidad.	Es necesario realizar la metodología el seguimiento y medición para obtener resultados validos así asignando responsabilidades.
9.2	AUDITORÍAS INTERNAS	X		Se han realizado auditorías internas a cargo del nivel central en cuanto a la seguridad de la información.	Se necesita mantener definido e implantado un SGSI de forma eficaz.
9.3	REVISIÓN POR LA DIRECCIÓN		x	Se han realizo análisis de los cambios internos y externos para la seguridad de la información pero no se tienen controles algunos.	Llevar un control documental de las auditorias, realizando un análisis de los diferentes cambios en la seguridad de la información para ejecutar acciones preventivas y correctivas

10.	EVALUACION DEL DESEMPEÑO	APLICA	NO APLICA	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
10.1	NO CONFORMIDADES Y ACCIONES CORRECTIVAS	x		Existe no conformidad permanente para la seguridad de la información, debido a la falta de políticas.	Definir de las políticas de seguridad de la información para así determinar con certeza las debilidades existentes.
10.2	MEJORA CONTINUA	X		Existe un plan de mejora mensual en cuanto a lo que se tiene para la seguridad de la información, el cual es muy mínimo ya que solo se lleva el formato de confidencialidad de la información.	Realizar planes de mejora continua con el fin de avanzar de forma directa en la seguridad de la información, ejecutando la implantación de políticas para la misma.

Tabla 4. Vulnerabilidades, amenazas y riesgos

FACTOR	DESCRIPCIÓN	SE PRESENTAN EN
VULNERABILIDAD	**Vulnerabilidad Física:** Teniendo en cuenta que en la unidad se está manejando un servidor de datos en la cual, la mayoría tiene acceso sin ninguna clase de restricción, un equipo de cómputo puede ser manipulado por un tercero, quien puede tener conocimiento de sistemas y aprovecha la ocasión para extraer información	Se presentan en la seguridad física y la red de datos, donde se evidencia de forma permanente el descuido y la falta de control del ingreso al servidor principal de la información. Se presenta en el talento humano, por la falta del perfil necesario en el

	Vulnerabilidad Humana: Las personas que administrar y utilizan el sistema no son solamente una, sino varias que tienen el privilegios de hacer el uso de los sistemas, porque tienen acceso sin ninguna clase de restricciones.	conocimiento adecuado en la seguridad de la información.
AMENAZA	**Amenazas Involuntarias:** Se presenta bastante en las que varios funcionarios utilizan la misma contraseña para el ingreso al equipo, de igual forma utilizan un post-it, dejando su contraseña y su usuario visibles.	Seguridad física y talento humano, por la falta de concienciación en la seguridad de la información en lo que representa un perdida de ella y la necesidad de administrar contraseñas seguras y únicas.
	Riesgos Financieros: Es de tener en cuenta que se	Seguridad física, seguridad en redes de datos y la

RIESGOS	está tratando con el personal administrativo de la policía Florencia, de los cuales la mayoría lleva procesos de ejecución de contratos, administración financiera, es información que se puede representar prácticamente el activo de mayor importancia para la Policía como ente del estado.	configuración esencial del sistema operativo para el bloqueo automático por la ausencia del usuario abierto.

Fuente: el autor

La norma ISO 27001:2013 establece que una fuente de vulnerabilidad se encuentra asociada al fallo en la seguridad de la información al dejarla expuesta y tener el riesgo de ser observada por los empleados si estar autorizados e incluso por terceros, es lo que actualmente se presenta en la Policía de Florencia, lo que puede generar daños en la información sensible de ésta.

Lo que puede venir dado por una falta de protección de la información que se aloja en los servidores y equipos de cómputo locales, puertos de entrada a dispositivos habilitados.

Se pueden dar casos que pongan en evidencia la vulnerabilidad de la organización, ya que la vulnerabilidad no es un concepto estático por lo que nuevas amenazas pueden emerger con el tiempo.

La norma ISO 27001:2013 sugiere que no solo se contemplen las protecciones individuales, sino también las sugeridas por una repentina interrupción del servicio debido a desastres naturales. Las coberturas deberán amparar diferentes riesgos, se deberá tener un plan de contingencia a seguir con el fin de poder salvaguardar la información.

7.2 **INFORME DE LAS PRUEBAS DE VULNERABILIDADES REALIZADO A LA RED DE DATOS**.

7.2.1 Identificación de activos de información para realizar el análisis de vulnerabilidades.

Cuerpo del sistema

Seis (06) PATCH PANEL

Tres (03) Smith de 48 puertos cada uno.

Un (01) Router

Un (01) modem para fibra óptica conexión intranet policial.

Figura 4. Rack principal de red comando de policía Florencia

Fuente: El autor sala de sistemas de policía Florencia

Existen tres servidores con las siguientes especificaciones técnicas.

Marca hp Modelo Proliant Ml350.
Memoria RAM de 8.0 GB
Sistema operativo 64 Bit Windows Server 200
Procesador Intel Xeon 2.000 GH2
Disco duro de 1 TR

Estos servidores están conectados a un switch KVM de cuartos puertos, están constantemente encendidos, cumplen funciones específicas, uno de ellos funciona como servidor de datos para salvaguardar información de vital importancia para cada una de las oficinas o dependencias de la base del comando de policía Caquetá.

El comando de departamento de policía Caquetá posee un servidor Dominio que administra los diferentes usuarios de los quipos de todos los equipos que están unidos al servidor dominio, a su vez este servidor es administrado desde la ciudad de Bogotá por medio de la intranet institucional.

Figura 5. Servidores comando de policía Florencia

Fuente: Sala de sistemas de policía Florencia

Para el funcionamiento permanente del sistema y los servideros, la base del comando cuenta con un planta de marca POWER LINK con una capacidad de 30 Kilo voltio amperios (KVA), se encarga suministrar energía a la sistema integrado de emergencia y seguridad SIES y tiene un enlace de energía para los servidores de la Policía Nacional.

Figura 6. Planta eléctrica comando de policía Caquetá

Fuente: El autor parte externa del comando

7.3.1 Metodología para la detección le vulnerabilidades en la red de datos.

La metodología para la detección de vulnerabilidades en la red datos de la policía de Florencia que se propone en este proyecto, consta de tres fases soportadas por herramientas de software para el análisis, mediante las cuales se busca obtener las vulnerabilidades en los equipos de la red, que normalmente se usa la conexión por cableado y de igual forma en los servidores de datos.

Esta metodología, se describe en la siguiente tabla:

Tabla 5. Fases de análisis de vulnerabilidades

FASE 1 RECONOCIMIENTO	FASE 2 ESCANEO DE PUERTOS Y SERVICIOS	FASE 3 ESCANEO DE VULNERABILIDADES
Busca de información sobre el dominio y subdominios de la Policía de Florencia.	Dependiendo el rango de red se realiza el escaneo de los puertos y sus servicios	Detectar las vulnerabilidades que se presentan según el reconociendo y los puestos.

Fuente: El autor

La primera fase que corresponde al reconocimiento, consiste en obtener tanta información como sea posible de la red, para esto se realizan diferentes tipos de consultas a servidores DNS. Es de aclarar que esta fase no busca obtener alguna vulnerabilidad, solo se obtiene una lista de los equipos con presencia en internet que abarca la red, esta lista se utiliza en la segunda fase llamada escaneo de puertos y servicios.

La segunda fase que corresponde al escaneo de puertos y servicios, allí se evalúan los equipos obtenidos para determinar los puertos y servicios que están activos en cada uno de ellos, en esta fase tampoco pretende encontrar alguna clase de vulnerabilidad, solo seleccionar equipos críticos de la red a los cuales se les aplica el escaneo de vulnerabilidades.

En la fase tercera y última fase correspondiente al escaneo de vulnerabilidades se utiliza la lista de los equipos de la red con presencia en internet y seleccionando los que se encuentran en estado crítico para la red, se procede a la búsqueda de vulnerabilidades.

Para realizar estas pruebas se va a utilizar el sistema operativo Kali-linux en su versión 1.0.

Desarrollo a la primera fase: Se hace el reconocimiento a la red, ubicando la información correspondiente al dominio y subdominios de la Policía de Florencia, con la ejecución de los siguientes comandos así:

Figura 7. Comandos para reconocimiento de red.

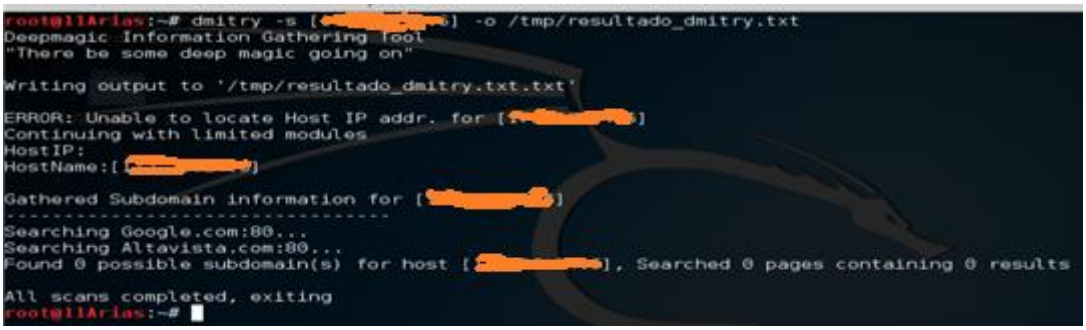
```
# dmitry

# dmitry -w -e -n -s [Dominio] -o /tmp/resultado_dmitry.txt
```

Fuente: el autor instrucciones comandos kali Linux.

La opción -w: Esta permite realizar una consulta whois a la dirección IP de un host.
La opción -e: Esta permite realizar una búsqueda de todas las posibles direcciones de correo electrónico.
La opción -n: Esta intenta obtener información desde netcraft sobre un hot.
La opción -s: Esta permite realizar una búsqueda de posibles subdominios.

Figura 8. Reconocimiento de la red.



Fuente: el autor

Se halla el dominio y subdominio de la red del comando de policía Florencia.

Desarrollo segunda fase: Se escanea los puertos y sus servicios, de la red de datos en la policía de Florencia.

Figura 9. Comandos el escaneo de puertos

```
# nmap [Dirección_IP]
```

Fuente: el autor

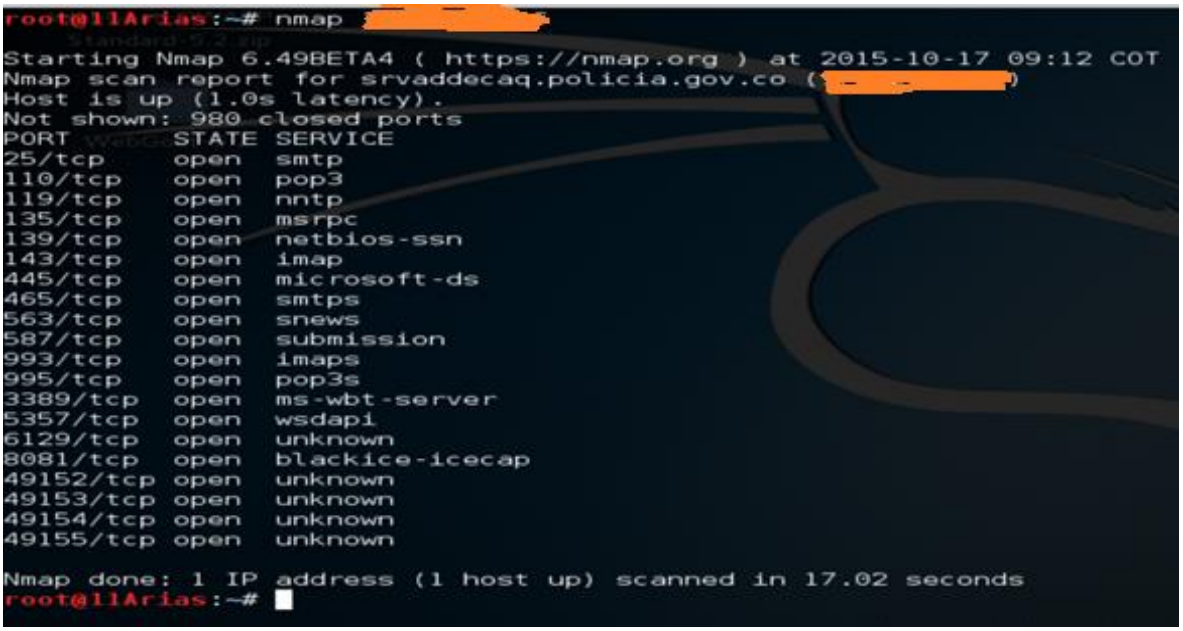
Nmap o conocido como Mapeador de Puertos, es una herramienta de código abierto para la exploración de redes y auditorías de seguridad, el cual ha sido diseñado para escanear velozmente redes y también host únicos.

Teniendo conocimiento del rango de la red y las máquinas activas en el objetivo, es momento de proceder con el escaneo de puertos para obtener los puertos TCP y UDP abiertos.
Existen diversas técnicas para realizar el escaneo de puertos, entre las más comunes se enumeran las siguientes:

Escaneo TCP SYN
Escaneo TCP Connect

Por defecto nmap utiliza un escaneo SYN, que es normalmente para los usuario con privilegios en caso de no, se puede utilizar un escaneo Connect es de aclarar que se escanean los 1,000 puertos más populares, algunos de ellos descritos en el resultado del análisis de escaneo de puertos en la red de datos del policía de Florencia, haciendo el uso de la herramienta. Kali Linux, así:

Figura 10. Escaneo de Puertos



Fuente: El autor escaneo de puertos

Se obtiene los puertos de red y servicios de la base del comando de policía Florencia.

Desarrollo tercera fase: Se detectan las vulnerabilidades de la red según la lista de equipos con los puertos y servicios expuestos.

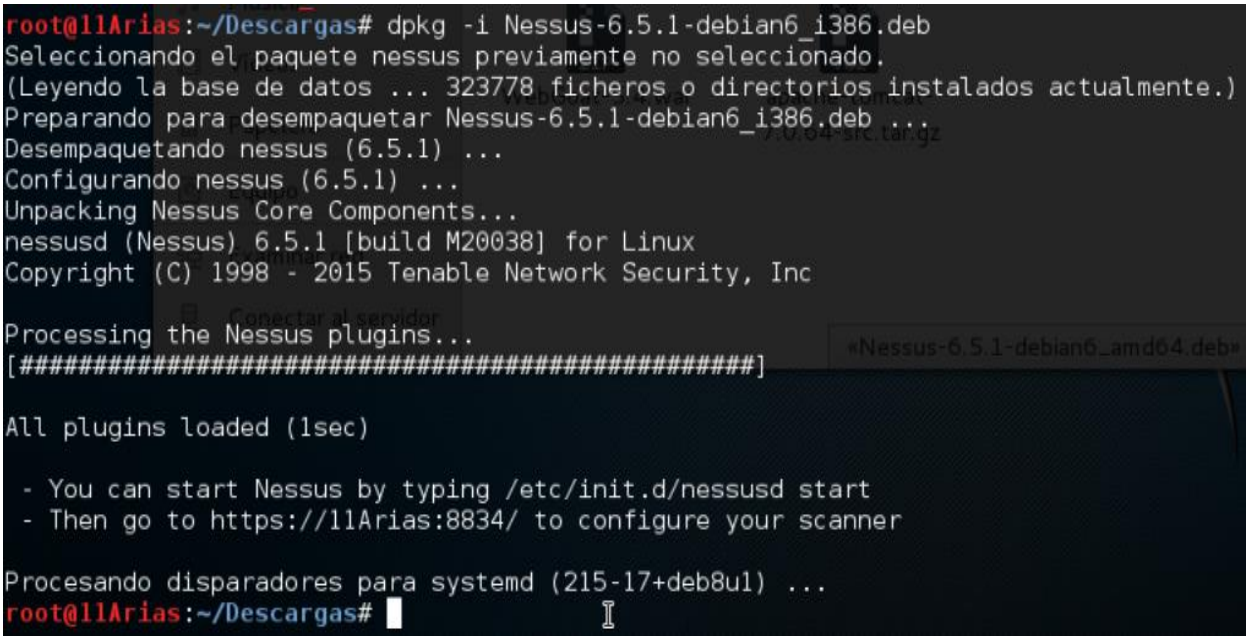
La tarea de mapear vulnerabilidades consiste en identificar y analizar las vulnerabilidades en los sistemas de la red, cuando se ha completado los procedimientos de captura de información, descubrimiento de puertos y servicios, es momento de identificar las vulnerabilidades.

La identificación de vulnerabilidades permite conocer los equipos que son susceptible, y permite realizar un conjunto de ataques que pueden afectar la seguridad de la información.

Para realizar el análisis de las vulnerabilidades se utiliza la aplicación nessus desde comandos con el sistema Operativo kali Linux. También se puede utilizar de forma local a un equipo con sistema operativo Windows.

Nessus: Es la plataforma para el escaneo de vulnerabilidades más confiable para los auditores y especialistas en seguridad informática de allí se puede programar escaneos a través de diversos métodos, Nessus soporta más tecnologías que otros proveedores incluyendo sistemas operativos, y diferentes dispositivos de red.

Figura 11. Proceso de instalación Nessus



Fuente: El autor

Figura 12. Comando iniciar Nessus.

```
# /opt/nessus/sbin/nessus-service -q -D
```

Fuente: El autor

También es autorizado do utilizar el siguiente comando para iniciar Nessus.

Figura 13. Comando dos para iniciar Nessus

```
# /etc/init.d/nessusd start
```

Fuente: El autor

La idea es seguir utilizando la herramienta de Linux. Para ellos se necesita la ejecución de diversos comandos para la aplicación nessus.

Después de haber finalizado la instalación de nessus y la ejecución del servidor, se produce abrir la siguiente URL en un navegador web del sistema operativo Kali Linux. https://127.0.0.1:8834 es la ruta remota a la aplicación para realizar el escaneo de vulnerabilidades.
Durante el proceso de configuración, se crea el nombre de usuario y contraseña, para la interfaz gráfica y utilizar el escáner de vulnerabilidades.

Figura 14. Inicio Nessus

Fuente: El autor

Figura 15. Resultado análisis de vulnerabilidades.

Fuente: Aplicación nessus

7.3.2 Resultado Análisis de Vulnerabilidades

Tabla 6. Sumatoria análisis de vulnerabilidades

SUMATORIA					
CRITICA	ALTO	MEDIO	BAJO	INFORMACION	TOTAL
4	**11**	**38**	**1**	67	**121**

Fuente: Aplicación Nessus

ANÁLISIS DE RESULTADOS

El análisis de los resultados se resalta los más importantes según su clasificación en el grado de vulnerabilidad, critica, alta, media baja e información.

Análisis de vulnerabilidad Crítica. 

- Una de las vulnerabilidades que se presentan es no tener la debida protección al servidor de datos, ya que cualquier usuario puede hace uso de esa información ingresando de forma directa sin alguna clase de restricción.

- La falta de configuración esencial al servidor de datos, la configuración del firewall, restringir el acceso a páginas prohibidas para el funcionario.

- No existe un procedimiento adecuado para realizar el borrado seguro de la información de los discos duros que son dados de baja o reasignados.

Análisis de vulnerabilidad Alta 

- El uso inadecuado de las contraseñas para el inicio de sesión en cada uno de los equipos de cómputo.

- Los funcionarios tienen privilegios para ingresar su usuario a cualquier equipo de cómputo, sin importar su dependencia.

- Se tiene habilitados los puertos USB Y DVD, cualquiera puede hacer uso de estos dispositivos de almacenamiento con el fin de extraer información importante.

- Según el análisis de vulnerabilidades con el uso de las herramientas nessus se evidencia que el uso exclusivo de la captura de pantallazos es vulnerable para transportar información vital de los equipos e incluso de las tareas administrativas.

- Los equipos de cómputo no tiene una protección adecuada para la seguridad de la información ya que varios tiene diferente software de antivirus instalados.

- Se tiene una débil protección de respaldo eléctrico y es un factor de riesgo tanta para la información como los equipos de cómputo.

- No existe el seguimiento ni la ejecución de copias de respaldo para evitar la pérdida de información.

Análisis de vulnerabilidad Media

- No existe un responsable del monitoreo de la red, para la seguridad de la información.

- No existen instrucciones básicas para los funcionarios para conservar los lugares de trabajo limpios.

- Se evidencia una débil estructura en la instalación del cableado estructurado, además posee una categoría obsoleta 5e.

- No posee un sector adecuado para conservar os equipos principales de la red, ya que se ingresan personas que no son autorizadas.

- Se evidencia la instalación de programas de uso comercial que no son necesarios para el debido funcionamiento de los equipos de cómputo.

- No se cuenta con una protección secuencial para la protección de la infraestructura tecnológica en caso de desastres naturales.

- No existe la protección válida para los sistemas Operativos, ya que se tienes copias para ser licenciadas con software utilitarios.

- El nivel de seguridad de la red está sin una configuración radical desde el servidor.

Análisis de vulnerabilidad Baja 

- Se presenta soportes documentales para los usuarios de la red, de igual forma evidencia la falta de soporte documental para tener el control de acceso a terceros o proveedores de diferentes servicios públicos.

Análisis de vulnerabilidad Baja 

a. En la organización se utilizan correos electrónicos personales, dejando a un lado los institucionales.

b. Se necesita la orientación profesional, en la seguridad de la información para mitigar los riesgos y vulnerabilidades en la red.

7.3 ANÁLISIS DE INVESTIGACIÓN, RESULTADO DE LAS ENCUESTAS REALIZADAS.

Para el cumplimiento de este objetivo en la selección de la muestra se encuesto el 10% del personal activo que labora en la base del comando de departamento de policía Caquetá.

Analizando cada una de las respuestas donde fue encuestado personas de rangos de edad diferentes de determina estadísticamente que el porcentaje arrojado muestra la necesidad de implementar un sistema de registro y control para el ingreso del personal ajeno a la base del comando de departamento de policía Caquetá.

7.3.1 Análisis de la información

Para recolectar la información, el tipo de estudio y la técnica a emplear, es necesario realizar la encuesta como instrumento de recolección de información. La encuesta se aplicada a los miembros activos de la Policía Nacional, quienes laboran diariamente en la base del comando de departamento de Policía Caquetá, con la idea de investigar y obtener muestras sobre la necesidad de elaborar y definir políticas de Seguridad de la Información.

La investigación inició encuestando a 50 funcionarios que representan el 10% de los Funcionarios que laboran en el área administrativa en los diferentes bloques del comando de la policía de Florencia Caquetá.

A continuación se muestra el diseño de la encuesta aplicada:

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión sobre la necesidad de adoptar políticas de seguridad de la información, como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo
2. De acuerdo
3. Totalmente en desacuerdo
4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1 Totalmente de acuerdo
2 De acuerdo
3 Totalmente en desacuerdo
4 En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo.
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

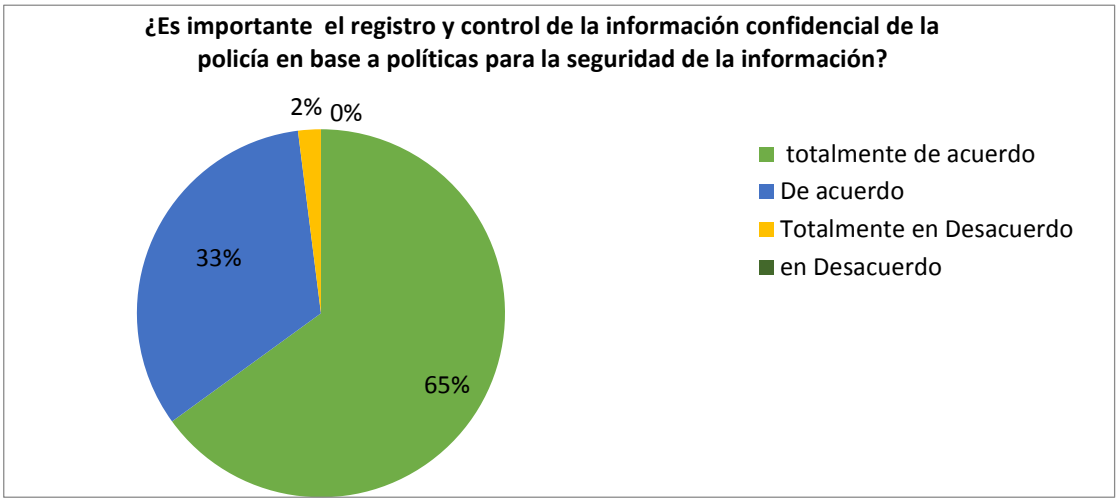
SI NO

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información. Se ha presentado la pérdida de información importante en memorias USB.

a) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
b) Se ha presentado daño en la información por ataques de virus injustificados.
c) El personal permanece mucho tiempo en sitios web no permitidos.

d) Resultados estadísticos de la técnica investigación realizada con la encuesta al 10% del personal, equivalente a 50 personas adscritos a la base del comando de departamento de policía Florencia.

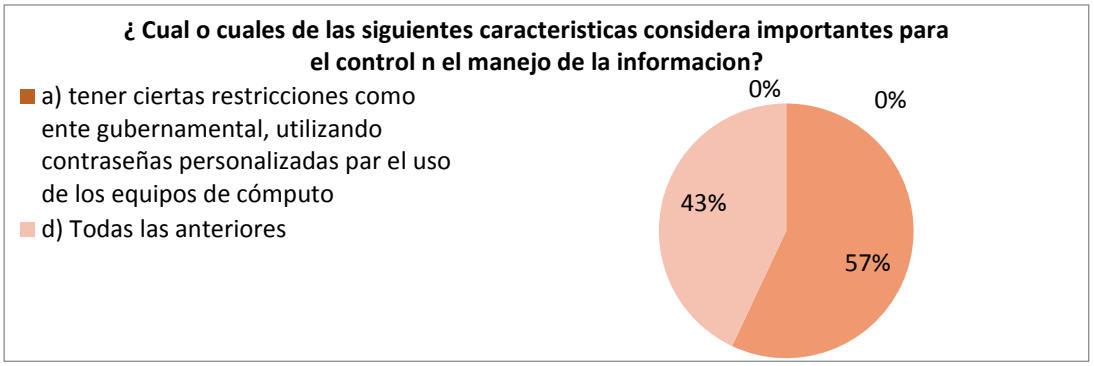
Figura 16. Pregunta 1 del análisis de la información.



Fuente: el autor análisis de información

Estadísticamente el personal del comando de policía Florencia ha contestado la encuesta lanzando el siguiente análisis. Con un 65% el personal se encuentra totalmente de acuerdo que se tenga un control de la información confidencial, un 33% se encuentra de acuerdo, tenemos un 2% que se encuentran totalmente en desacuerdo con este control.

Figura 17. Pregunta 2 del análisis de la información

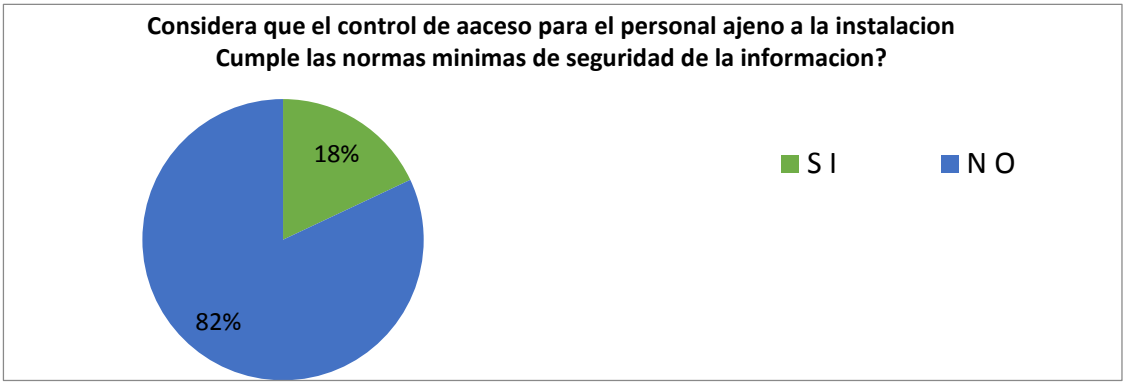


Fuente: el autor análisis de información

Analizando la gráfica se observa una reacción positiva de los encuestados arrojando el siguiente resultado. Con un 57% el comando de policía Florencia

requiere definir un SGSI con sus políticas debidamente controladas, y con el 43% restante mencionan que todas las respuestas son lógicas y necesarias para implantar políticas de seguridad informática.

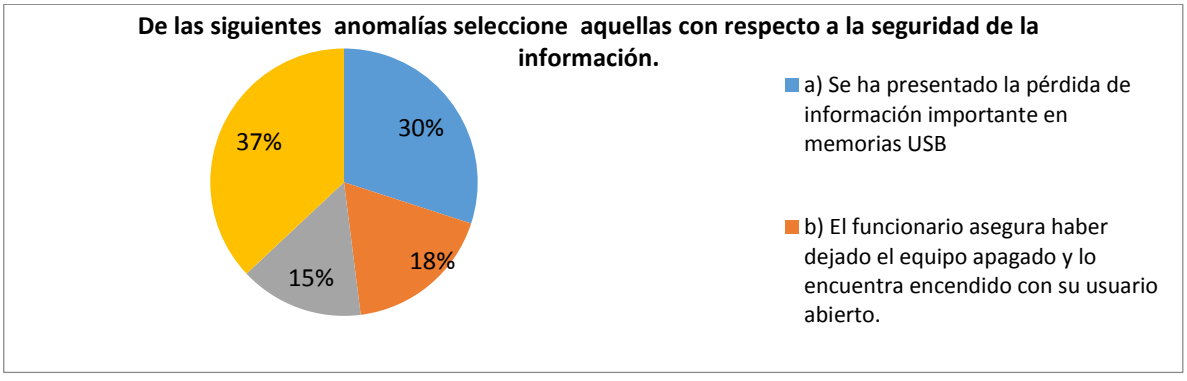
Figura 18. Pregunta 3 análisis de la información



Fuente: el autor análisis de información

Se considera que en un 82% del personal encuestado consideran que el control de acceso para el personal ajeno a la base del comando de departamento de policía Florencia NO cumple con las normas mínimas de seguridad para la información confidencial, por el contrario el 18% consideran que se están aplicando las nomas adecuadas de seguridad para la información.

Figura 19. Pregunta 4 análisis de la información



Fuente: el autor análisis de información

Se considera que para un 37% del personal asegura que el personal permanece mucho tiempo en sitios web no permitidos.

Para el 30% tienen la versión de la perdida de información en memorias USB.

Según el 18% del personal aseguran haber dejado el equipo apagado, y lo encuentran encendido con su usuario abierto.

Para el 15% restante manifiestan que se ha presentado daños en la información por ataques de virus injustificados.

Según el análisis realizado con la encuesta para el personal de la base del comando de policía Florencia, se observa que esta entidad requiere la implantación de un sistema de gestión de seguridad de la información, definiendo políticas para la administración de la información.

7.3.2 Entrada de Información: [5]

Es el proceso mediante el cual define las políticas de seguridad de seguridad informática toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas.

Los manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos.

7.3.3 Almacenamiento de información:

El almacenamiento es una de las actividades o capacidades más importantes que tiene el sistema de información, ya que a través de esta propiedad el sistema puede recordar la información.

[5] LARA BEDOYA Adriana, 2014 Enfoque práctico de la Auditoría Informática, UNIVERSIDAD DEL VALLE.

Para el almacenamiento de la información se podrá hacer únicamente mediante carpetas compartidas en red, no se permitirá el uso de las memorias USB, unidades de DVD.

Dichas debilidades han sido obtenidas como resultado de una encuesta realizada a los diferentes funcionarios del comando de policía Caquetá; dichas debilidades se presentan en las dependencias que procesan información que merece tener un alto grado de confidencialidad.

Al no contar con los parámetros establecidos para el desarrollo y aplicación de políticas de Seguridad de la Información, se tiene la dificultad de para llevar un control estricto en la reserva de la información, siendo vulnerables y visibles en los diferentes para personal terceros.

Para el uso de los equipos de cómputo este funciona a través de un usuario Dominio, sin llevar un control documental dando a conocer cada una de las políticas de la seguridad de la información.

En vista de lo anterior se hace necesario el diseño, desarrollo e implementación de un Sistema de gestión de seguridad de la información que permita subsanar los inconvenientes que se presentan al momento de tener acceso a la información de uso privativo del comando de policía Caquetá.

A continuación se anexa la un formato de la encuesta que se aplica al personal del comando de policía Florencia en el Caquetá.

Figura 20. Formato encuesta.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo ✓	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo. ✓
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	✓

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos. ✓

Fuente: El autor

8. POLÍTICAS DE SEGURIDAD APLICABLES AL COMANDO DE POLICÍA

8.1 DEFINICIONES

Para los propósitos de este documento se aplican los siguientes términos y definiciones en pro de la seguridad de la información para el comando de policía Florencia.

- **Activo**: Cualquier bien que tenga valor para la organización.

- **Acuerdo de Confidencialidad:** Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de la Policía de Florencia

- **Administradores:** Usuarios a quienes la Policía de Florencia ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la Policía de Florencia quienes estarán bajo la dirección de la Vicepresidencia de tecnología y soluciones de información de la Policía nacional.

- **Amenaza**: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

- **Backup**: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

- **Coordinación de Planeación e Innovación:** Es el responsable de velar por el cumplimiento de esta Política, documentar el Manual de Seguridad de la Información, los procesos, procedimientos, instructivos y formatos específicos alineados al estándar internacional ISO 27001 y sus normas derivadas además de los otros marcos generalmente aceptados como: COBIT, ITIL, NIST, ASNZ y DRII, así como liderar la implementación de los controles exigidos por la Ley y la Regulación Vigente.

- **Comité de Seguridad:** Equipo de trabajo conformado por el Vicepresidente Ejecutivo. Gerente del RUES, Gerente de Servicios Camerales, Director de Desarrollo y Jefe de Servicios Tecnológicos.

- **Contraseña:** Clave de acceso a un recurso informático, sistema de información, bases de datos, usuarios empresariales.

- **Control**: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- **Directrices**: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

- **Servicios de procesamiento de información**: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

- **Seguridad de la Información**: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

- **Evento de seguridad de la información**: Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

- **Firewall**: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.

- **Incidente de seguridad de la información**: Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información confidencial:** Información generada por la Policía de Florencia que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Policía nacional. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

- **Información privada (USO INTERNO):** Información generada por la Policía de Florencia que operan a través de la Policía de Florencia, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Policía nacional y es accesible por todos los usuarios.

- **Información pública:** Es la información administrada por la Policía de Florencia que operan a través de la Policía de Florencia que está a disposición del público en general; por ejemplo la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES.

- **LAN:** Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio ó una oficina).

- **Licencia de Software:** Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.[6]

- **Copyright:** Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.

- **Propiedad Intelectual**: Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.

- **Derechos patrimoniales**: Los derechos patrimoniales de una obra referencia a la forma en cómo se puede utilizar, o recibir algún tipo de beneficio de la obra. Es un derecho temporal, expropiable disponible, renunciable, y embargable.
- **Derecho moral**: Es la relación intangible que une al creador de una obra y su obra, es un derecho inalienable, nadie puede expropiar ese derecho.

[6] LA DIAN, DICIEMBRE 2013 Ley 603 del 2000 Bogotá

- **Open Source (Fuente Abierta)**: Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.

- **Software Libre**: Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.

- **Software pirata:** Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.

- **Software de Dominio Público:** Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.

- **Freeware:** Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.

- **Shareware:** Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. para adquirir el software de manera completa es necesario un pago económico.

- **Módem (Modulador - Demodulador de señales):** Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.

- **Monitoreo**: Verificación de las actividades de un usuario con respecto a los recursos informáticos de la Policía de Florencia.

- **OTP (One Time Password):** Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

- **Plan de contingencia**: Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de la Policía de Florencia en casos de desastres y otros casos que impidan el funcionamiento normal.

- **Política**: Toda intención y directriz expresada formalmente por la dirección.
- **Protector de pantalla**: Programa que se activa a voluntad del usuario, ó

automáticamente después de un tiempo en el que no ha habido actividad.

- **Proxy**: Servidor que actúa como puerta de entrada a la Red Internet.

- **Recursos informáticos**: Son aquellos elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.

- **Riesgo**: Combinación de la probabilidad de un evento y sus consecuencias.

- **Análisis de Riesgos**: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

- **Evaluación de Riesgos**: Todo proceso de análisis y valoración del riesgo.

- **Valoración del riesgo**: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- **Router**: Equipo que permite la comunicación entre dos o más redes de computadores.

- **Sesión**: Conexión establecida por un usuario con un Sistema de Información.

- **Sistema de control de acceso**: Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.

- **Sistema de detección de intrusos (IDS)**: Es un conjunto de hardware y software que ayuda en la detección de accesos ó intentos de acceso no autorizados a los recursos informáticos de la Policía de Florencia.

- **Sistema de encriptación**: Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.

- **Sistema multiusuario**: Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.

- **Sistema operativo**: Software que controla los recursos físicos de un

computador.

- **Sistema sensible:** Es aquel que administra información confidencial ó de uso interno que no debe ser conocida por el público en general.

- **Tercera parte**: Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.

- **Usuario**: toda persona que pueda tener acceso a un recurso informático de la Policía de Florencia.

- **Usuarios de red y correo**: Usuarios a los cuales la Policía de Florencia les entrega un identificador de cliente para acceso a sus recursos informáticos.

- **Usuarios externos**: Son aquellos clientes externos que utilizan los recursos informáticos de la Policía de Florencia a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.

- **Usuarios externos con contrato**: Usuarios externos con los cuales la Policía de Florencia establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.

- **Vulnerabilidad**: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

Responsabilidades de los diferentes involucrados para el cumplimiento de las políticas

Compromiso de la Dirección

La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información:

Mediante el establecimiento de una política de seguridad de la información; asegurando que se establezcan objetivos y planes de seguridad de la información;

Estableciendo funciones y responsabilidades de la seguridad de la información.

Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y la necesidades de la mejora continua; Asegurando que se realizan auditorías internas.

Gestión de los Recursos

- Asegurar que las políticas de seguridad de la información brindan apoyo a los requisitos del negocio.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados.
- Asegurar que todo el personal tiene conciencia de la importancia de la seguridad de la información.

Procedimiento

Los miembros del Comité de Seguridad, conscientes que los recursos de información son utilizados de manera permanente por los usuarios de la Policía de Florencia que implementen el servicio de identificación biométrica., definidos en este documento, han considerado oportuno transmitir a los mismos las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos y de información.

Las políticas de seguridad informática tienen como objetivo reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo, principalmente la ocurrencia.

8.2 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION EN LA POLICÍA DE FLORENCIA.

Nombre del documento:	**POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION EN LA POLICÍA DE FLORENCIA** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUAR MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

En la Policía de Florencia se reconoce abiertamente la importancia de la seguridad de la información así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

Se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la Policía de Florencia con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia de la compañía, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

8.3 POLÍTICAS ESPECÍFICAS DE SEGURIDAD INFORMÁTICA

Nombre del documento:	**POLÍTICAS ESPECÍFICAS DE SEGURIDAD INFORMÁTICA** 
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUAR MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en:

- ✓ Políticas de Cumplimiento y Sanciones
- ✓ Políticas de uso de recursos informáticos.
- ✓ Políticas de contraseñas.
- ✓ Políticas de uso de la información.
- ✓ Políticas del uso de Internet y correo electrónico.
- ✓ Políticas de uso de la Intranet y Sitio Web de la Policía de Florencia
- ✓ Políticas Generales de la Presidencia.
- ✓ Políticas para Desarrolladores de Software.
- ✓ Políticas para Administradores de Sistemas.
- ✓ Políticas de Copias de respaldo.
- ✓ Políticas de Uso de Firewall.
- ✓ Políticas para Usuarios Externos.
- ✓ Políticas de Acceso Físico.

8.4 POLÍTICA DE CUMPLIMIENTO Y SANCIONES

Nombre del documento:	**POLÍTICA DE CUMPLIMIENTO Y SANCIONES** 
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUAR MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política hace relevancia al uso indebido de la información confidencial para el comando de Policía de Florencia, y debe ser de estricto cumplimiento.

Uso indebido de la información confidencial

El personal que labora en el comando de policía Florencia debe tener presente esta política dando estricto cumplimiento a los parámetros establecidos en esta política para el uso de la información confidencial por ningún motivo se puede divulgar información no autorizada desde los correos institucionales a los personales, El uso de los dispositivos masivo como los CD, DVD memorias USB, con el fin de extraer información relevante de la empresa sin la debida autorización del gestor de seguridad de la información.

Alcance de Cumplimiento con la seguridad de la información:

Todos los funcionarios activos, contratistas, deben cumplir y acatar las políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia de la Policía de Florencia y al comité de seguridad.

Aplicable

Esta política debe ser dar cumplimiento por todos los funcionarios desde el inicio del contrato hasta el término de la mismo.

RESPONSABILIDADES

De la dirección:

Garantizar la toma de conciencia de los funcionarios en relación a la seguridad de la información y los lineamientos de recurso humano y el buen uso de cada parámetro de la seguridad informática.

Promover la educación y formación de la Seguridad de la Información, para tomar las medidas disciplinarias cuando sea requerido.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, se deben ceñir a la presente política en pro de la seguridad de la información.

Responsabilidades de los empleados, y demás incluidos en el alcance:

El personal que no tenga funciones administrativas, o contacto con algún sistema informático, no deben manipular de alguno de estos, ya que esta política los acogerá aun desconociendo la norma.

Medidas Disciplinarias por Incumplimiento de Políticas de Seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en una sede, Policía de Florencia podrá suspender la prestación del servicio de identificación biométrica.

Cumplimiento con la seguridad de la información

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Presidencia de la Policía de Florencia y al comité de seguridad.

Medidas Disciplinarias por Incumplimiento de Políticas de Seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en una sede, Policía de Florencia podrá suspender la prestación del servicio de identificación biométrica.

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial del contenido de este sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado.

8.5 POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

Nombre del documento:	**POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS**
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUAR MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política nombra el uso adecuado que se le debe tener a los recursos informáticos, sin alterar su estado normal, la no instalación de programas no autorizados para la institución.

Alcance de cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Le Corresponde velar por su estricto cumplimiento al comandante Policía de Florencia y al comité de seguridad.

Aplicable

Para todos los funcionarios activos, contratistas desde el inicio de la actividad hasta el término de la misma aun estando en la ejecución de sus actividades extraordinarias.

Responsabilidades de la dirección:

Dar a conocer a todo el personal adscrito a la base del comando de policía Florencia esta política con el fin de ser aplicada y adoptar las políticas para seguridad de la información a los recursos informáticos.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, se deben ceñir a la presente política en pro de la seguridad de la información, con el fin de conocer las diferentes acciones disciplinarias que da lugar el incumplimiento de esta política.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma acoge al responsable del medio o recurso informático, ya que por ningún motivo lo debe dejar en estado de abandono, exponiendo a la manipulación de personal sin el debido conocimiento.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Si el incumplimiento se origina en una sede, Policía de Florencia podrá suspender la prestación del servicio de identificación biométrica.

Instrucciones para el uso de recursos informáticos.

El uso del computador personal y demás recursos informáticos por parte del empleado, trabajadores o usuarios del sistema de autenticación biométrica en línea, debe someterse a todas las instrucciones técnicas, que imparta el comité de seguridad.

Uso personal de los recursos

Los recursos informáticos del comando de Policía de Florencia, solo deben ser usados para fines laborales, entre los cuales, se resalta la prestación del servicio de autenticación biométrica en línea a los usuarios de Policía de Florencia. El producto del uso de dichos recursos tecnológicos será de propiedad de la Policía nacional y estará catalogado como lo consagran las políticas de la Policía nacional. Cualquier otro uso está sujeto a previa autorización de la Presidencia.

Uso del aplicativo entregado.

Policía de Florencia ha suscrito con los fabricantes y proveedores un contrato de "LICENCIA DE USO" para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Policía nacional, esto se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que maneje información de uso restringido a Policía de Florencia Adicional a esto cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un perfil limitado, de esta forma es controlado el acceso.

El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien fue otorgada dicha identificación. Los usuarios no deben permitir que otros usuarios realicen labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la Policía de Florencia.

Declaración de reserva de derechos de policía de Florencia

Policía de Florencia usa controles de acceso para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos del comando de Policía de Florencia, se reservan el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier usuario; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la Policía de Florencia**.** Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del comité de seguridad siempre con el concurso de la Presidencia o de quién él delegue esta función.

Recursos compartidos.

Está terminantemente prohibido compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización previa y restringir por Dominio, y debido conocimiento del gestor o coordinador de la seguridad de la información de la Policía Florencia

Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.

Un usuario puede ser monitoreado bajo previa autorización del comité de seguridad, donde se hará el respectivo seguimiento de los diferentes movimientos informáticos del usuario.

Acceso no autorizado a los sistemas de información de la policía nacional.

Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de encriptación y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.

Posibilidad de acceso no implica permiso de uso.

Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.

Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos.

A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso.

En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al comité de seguridad y lideradas por el gestor de seguridad de la información.

Dejar sistemas sensibles desatendidos.

Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada, durante su ausencia se debe y por requisito.

Notificación de sospecha de pérdida, divulgación ó uso indebido de información sensible.

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del comité de seguridad.

Etiquetado y presentación de información de tipo confidencial a los usuarios de los equipos de cómputo.

Toda la información que sea crítica para la organización debe ser etiquetada de acuerdo a los niveles establecidos en el presente documento: **USO INTERNO** y **CONFIDENCIAL.**

Traslado de equipos debe estar autorizado.

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones del comando de Policía de Florencia sin previa autorización. Así mismo, ningún equipo de cómputo asignado. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado.

Control de recursos informáticos entregados a los usuarios.

Cuando un usuario inicie su relación laboral con Policía de Florencia se debe diligenciar el documento de entrega de inventario, dando a conocer los cuidados y responsabilidades con los medios informáticos.

Cuando un empleado termine su vinculación laboral con la Policía nacional, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario (Firmado). El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

Cuando un funcionario de Policía de Florencia inicie su relación laboral se debe diligenciar el documento de entrega de inventario.

Configuración de sistema operativo de las estaciones de trabajo.

Solamente los funcionarios del área técnica de sistemas están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios, por ningún motivo por extrema necesidad los usuarios alternos podrán realizar cambios con ayuda de técnicos de otras entidades.

Uso restringido de módems en las estaciones de trabajo.

Queda prohibido el uso de módems en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación escrita por parte de Presidencia, para su configuración

como acceso desde PVN.

Protección por defecto de copyright

Todos los colaboradores de Policía de Florencia deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito con el fin de asegurar el cumplimiento de las leyes que aplican para este tipo de información.

Regularmente se deben realizar actividades de monitoreo sobre el software instalado en cada uno de los equipos de la organización, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la empresa a nivel nacional.

Custodia de licencias de software

Las licencias deben ser custodiadas y controladas por el área de tecnología o des sistemas de la unidad policial en este caso la oficina de telemática. Esta área debe realizar auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal y autorizado por los coordinados o gestor de la seguridad de la información.

Apagado de equipos por ausencia de usuarios.

Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina al medio día y/o en la noche.

Tiempo limitado de conexión en aplicaciones de alto riesgo

Si el usuario está conectado a un sistema que contiene información sensible, y este presenta un tiempo de inactividad corto no más de cinco minutos la aplicación deberá cerrar la sesión iniciada por el usuario.

ACUERDO DE CONFIDENCIALIDAD

Para el uso de los recursos tecnológicos de la Policía de Florencia, todo usuario debe firmar un acuerdo de confidencialidad y un acuerdo de Seguridad de los sistemas de información antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación de las soluciones de autenticación biométrica en línea con su respectivo kit de hardware

- Prohibición de instalación de software y hardware en los computadores de la Policía de Florencia

La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios de sistemas autorizados por la Policía de Florencia.

8.6 POLÍTICAS DE USO DE LAS CONTRASEÑAS

Nombre del documento:	**POLÍTICAS DE USO DE LAS CONTRASEÑAS**
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política nombra y estipula el correcto uso de las contraseñas que usan para acceder a los diferentes recursos informáticos

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Le Corresponde velar por su estricto cumplimiento al comandante Policía de Florencia y al comité de seguridad.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que empieza a ejecutar actividades que le implique el uso contraseña para el acceso a los recursos informáticos.

Responsabilidades de la dirección:

Dar a conocer a todo el personal adscrito a la base del comando de policía Florencia esta política, es de vital importancia la autoprotección delos datos personal y los medios informáticos.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, se deben ceñir a la presente política con el ánimo de no ser víctima del vulneración de los medios informáticos asignados por el mal uso de la contraseña.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa ya que cada uno posee un correo electrónico para uso institucional.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Confidencialidad de las contraseñas.

La contraseña que cada usuario asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

Uso de diferentes contraseñas para diferentes recursos informáticos.

Para impedir el compromiso de múltiples recursos informáticos, cada usuario

deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso. Esto involucra así mismo a los equipos de comunicación (firewall, routers, servidores de control de acceso) y a los administradores de los mismos.

Identificación única para cada usuario.

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso, acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores.

Esta política rige para aplicativos implementados hasta la fecha de liberación de este documento. En caso del sistema de autenticación biométrica en línea, el acceso al sistema se realizará mediante un cotejo biométrico, los funcionarios contarán con una identificación única personal y su respectiva contraseña asignada por el encargado por el área de tecnología de Policía de Florencia

Cambios periódicos de contraseñas.

Todos los usuarios deben ser automáticamente forzados a cambiar su contraseña por lo menos una vez cada 45 días.

Longitud mínima de contraseñas.

Todas las contraseñas deben tener una longitud mínima de diez (10) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales. Este tamaño debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.

Contraseñas fuertes.

Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números, letras mayúsculas, minúsculas y caracteres especiales.

Prohibición de contraseñas cíclicas.

No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es “Noviembre-2015” que según la política “Contraseñas fuertes”, es una contraseña válida, pero al mes siguiente pasa a ser “Diciembre-2015” y así sucesivamente, el usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente

Almacenamiento de contraseñas.

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, en post-it, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas.

Ningún usuario bajo ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso.

Sospechas de compromiso deben forzar cambios de contraseña.

Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

Revelación de contraseñas prohibida.

Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Policía nacional. Ningún usuario deberá intentar obtener contraseñas de otros usuarios, excluyendo lo contemplado en la política “Auditoria periódica a las contraseñas de los usuarios”.

Bloqueo estación de trabajo.

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo

automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 5 min. Por otra parte el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.

Reporte de cambio en las responsabilidades de los usuarios al administrador del sistema.

El ingeniero en soporte y web master debe reportar por medio de un correo electrónico, de manera oportuna al área de sistemas grupo de telemática, todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral, de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad de la información.

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

8.7 POLÍTICAS DE USO DE LA INFORMACIÓN

Nombre del documento:	**POLÍTICAS DE USO DE LA INFORMACIÓN** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política se enfatiza de forma directa al uso adecuado y la reserva de la información confidencial para la Policía de Florencia como ente del estado.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Le Corresponde velar por su estricto cumplimiento al comandante Policía de Florencia y al comité de seguridad.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que empieza a ejecutar actividades donde tenga acceso a la información pública de la policía de Florencia para el acceso a los recursos informáticos.

Responsabilidades De la dirección:

Dar a conocer a todo el personal adscrito a la base del comando de policía Florencia esta política, que tiene que ver con la reserva y protección de la información.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, deben velar por la protección de la información confidencial, teniendo en cuenta que su uso es diariamente controlado por esta política.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Divulgación de la información manejada por los usuarios del comando policía de Florencia

Policía de Florencia podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal, por solicitud de autoridad judicial o administrativa salvo las excepciones indicadas en este documento y las disposiciones legales de protección de datos personales.

Transferencia de datos solo a organizaciones con suficientes controles.

El comando de Policía de Florencia puede transmitir información privada solamente a terceros que por escrito se comprometan a mantener dicha información bajo controles adecuados de protección. Se da una excepción en casos en los que la divulgación de información es forzada por la ley.

Registro de las compañías que reciben información privada.

El personal de Policía de Florencia que liberó información privada a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

Transferencia de la custodia de información de un funcionario que deja el comando de policía de Florencia.

Cuando un empleado se retira de la Policía de Florencia, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

Transporte de datos sensibles en medios legibles.

Si se transporta información sensible en medios legibles por el computador (disquetes, cintas magnéticas, CD´s, memorias USB), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados. Para equipos portátiles este tipo de información es asegurada mediante una aplicación de cifrado.

Datos sensibles enviados a través de redes externas deben estar encriptados.

Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptado, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

Clasificación de la información

Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.

Toda la información y los activos asociados con los servicios de procesamiento de la información deben ser "propiedad"[7] de una parte designada por el comando de Policía de Florencia. Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

Cualquier uso de servicio de procesamiento de información debe ser autorizado por el coordinador o gestor de la seguridad de la información según el caso, por lo anterior cualquier acceso a un servicio no autorizado es prohibido y de esto deben tener conocimiento todos los usuarios involucrados.

Uso de dispositivos de almacenamiento masivo y captura de pantallazos

No debe hacer uso de las dispositivos de almacenamiento masivo como Discos duros extraíbles, USB, unidad de CD, y la captura de pantallazos, sin la debida autorización del coordinador o gestor de seguridad de la información, dejando el debido registro de las acciones con estas herramientas, los dispositivos almacenamiento solo podrán leer información mas no extraer de los equipos de cómputo.

Eliminación segura de la información en medios informáticos

Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por Policía de Florencia, antes de su entrega se les realizara un proceso de borrado seguro en la información.

Eliminación segura de la información en medios físicos

Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel.

[7] El término "propietario" identifica a un individuo o una Policía Nacional que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "propietario" no implica que la persona tenga realmente derechos de propiedad de los activos.

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

8.8 POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

Nombre del documento:	**POLÍTICAS DEL USO DEL INTERNET Y CORREO ELECTRONICO** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política es aplicada para el comando de policía Florencia, donde se específica de forma directa las responsabilidades que se debe tener en el uso del internet y los correos electrónicos siguiendo al margen las instrucciones allí descritas.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas en el uso del internet para la protección y seguridad de la información.

Aplicable

Para todos los funcionarios activos, contratistas desde el inicio de sus prestaciones a la institución hasta que sea desvinculado de la misma ya que a partir de su nombramiento tendrá derecho a navegar sobre la red del comando de policía Florencia.

Responsabilidades de la dirección:

Dar las instrucciones pertinentes a todo el personal que comprenden la base del comando de policía Florencia, con el fin de dar aplicabilidad de forma permanente sobre el uso controlado del internet.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, deben acatar las líneas enmarcadas sobre las políticas de la protección de la información confidencial, haciendo un uso adecuado del internet y los correos electrónicos.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Prohibición de uso de Internet para propósitos personales.

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. Esta política se complementa con la política “Instrucciones para el uso de recursos informáticos”.

Formalidad del correo electrónico.

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.

Preferencia por el uso del correo electrónico.

Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.

Uso de correo electrónico.

La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.

Revisión del correo electrónico.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos tres veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

Mensajes Prohibidos.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros ó que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

Acciones para frenar el SPAM.

En el caso de recibir un correo no deseado y no solicitado (también conocido

como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de sistemas de la oficina de Telemática.

Todo buzón de correo debe tener un responsable.

Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.

Enviando software e información sensible a través de Internet.

Software e información sensible del comando de Policía de Florencia que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

Intercambio de información a través de Internet.

La información interna puede ser intercambiada a través de Internet pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida el uso de las redes comerciales y el uso de correos no institucionales sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

8.9 POLÍTICAS DE LA INTRANET Y SITIOS WEB DE POLICÍA DE FLORENCIA

Nombre del documento:	**POLÍTICAS DE LA INTRANET Y SITIOS WEB DE LA POLICIA FLORENCIA** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Es tomarla relación del empleado con las funciones administrativas u operativa con el uso de la intranet policial Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados para seguir su uso estandarizo según la norma.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos para la actualización y el uso de la intranet policial para la protección y seguridad de la información. Le Corresponde velar por su estricto cumplimiento al comandante Policía de Florencia y al comité de seguridad.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que inician su contrato con la entidad policial hasta el término de la misma.

Responsabilidades De la dirección:

Instruir al personal de la base del comando de policía Florencia, con el ánimo de generar un grado de sensibilización para el uso de la intranet policial y la actualización de los documentos que se generan para ser utilizados en su versión actual.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, deben actualizarse y seguir el uso legal de la intranet policial con el fin de brindar protección de la información confidencial, teniendo en cuenta que su uso es diariamente controlado por esta política.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el uso de la intranet policial.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Reglas de uso de la intranet.

El comando de Policía de Florencia utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y el empleado o trabajador. Por lo tanto, el empleado debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

Prohibición de publicitar la imagen de la policía en sitios diferentes a los institucionales.

La publicación de logos, marcas o cualquier tipo de información sobre la Policía o sus actividades en Internet solo podrá ser realizada a través de las páginas institucionales de la misma y previa autorización del gestor de la seguridad de la Información. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los empleados.

Prohibición establecer conexiones a los sitios web de policía de Florencia

Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios Web de la Policía de Florencia por parte de los empleados y de sus sitios Web o páginas particulares, salvo previa autorización del gestor de seguridad de la información, dependiendo del caso. Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la Policía Nacional en sitios diferentes a los institucionales o como meta-etiquetas.

Prohibición de anuncios en sitios web particulares.

Está terminantemente prohibido anunciarse en los sitios Web particulares como empleados del comando Policía de Florencia o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio Web a pensar que existe algún vínculo con Policía de Florencia.

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

8.10 POLÍTICAS GENERALES DEL GESTOR DE SEGURIDAD DE LA INFORMACION

Nombre del documento:	**POLÍTICAS GENERALES DEL GESTOR DE SEGURIDAD DE LA INFORMACIÓN** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política busca enfatizar a todos los funcionarios de la base del comando de policía Florencia, la definición de cada una de las políticas de la seguridad de la información por parte del gestor de seguridad de la información.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Le Corresponde velar por su estricto cumplimiento al comandante Policía de Florencia y al comité de seguridad.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que empieza a ejecutar actividades donde tenga acceso a la información pública de la policía de Florencia para el acceso a los recursos informáticos.

Responsabilidades De la dirección:

Dar a conocer a todo el personal adscrito a la base del comando de policía Florencia esta política, que tiene que ver con la reserva y protección de la información, siguiendo y cumpliendo cada uno de los parámetros establecidos en cumplimiento a la aplicación de políticas para la seguridad de la información, estipuladas por el gestor de seguridad de la información.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes en toda la base del comando de policía Florencia, los cuales deben velar por el estricto cumplimento en cada uno de las políticas para la protección de la información confidencial.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información, recursos informáticos y uso exclusivo de la red e intranet policial.

Medidas disciplinarias por incumplimiento de políticas de seguridad:

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Evaluación y tratamiento del riesgo

La evaluación de riesgos debería identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deberían guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

El alcance de la evaluación de riesgos puede abarcar a toda la organización,

partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil.

Se debe realizar una evaluación de riesgos a los recursos informáticos del comando de Policía de Florencia por lo menos una vez al año utilizando el procedimiento Interno: “Análisis de riesgos”

Restricción por acceso telefónico e internet sobre recursos tecnológicos de uso interno a clientes externos.

No se otorgarán privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Presidencia.

Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados.

Todos los computadores multiusuario, equipos de comunicaciones, otros equipos que contengan información sensible y el software licenciado de propiedad de la Policía Nacional deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

Entrenamiento compartido para labores técnicas críticas.

Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de la Policía de Florencia

Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.

Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que

sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor.

Personal competente en el centro de cómputo para dar pronta solución a problemas.

Con el fin de garantizar la continuidad de los sistemas de información, el comando de Policía de Florencia debe contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

Chequeo de virus en archivos recibidos en correo electrónico.

El comando de Policía de Florencia debe procurar y disponer de los medios para que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

Contacto con grupos especializados en seguridad informática

El personal involucrado con la seguridad de la información deberá tener contacto con grupos especializados o foros relacionados con la seguridad de la información. Esto con el objetivo de conocer y actualizar en conocimientos sobre las nuevas medidas en cuanto a seguridad de la información se van presentando.

comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado.

8.11 POLÍTICAS PARA DESARROLLADORES DE SOFTWARE

Nombre del documento:	**POLÍTICAS PARA DESARROLLADORES DE SOFTWARE** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política es directamente para los diseñadores de software cumpliendo los las políticas de seguridad informática para la adquisición y diseño de software.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, el personal que tenga el perfil necesario para el desarrollo de software en la policía de Florencia, deben cumplir y acatar el manual de políticas y los procedimientos adecuados para el desarrollo de software aplicable para el comando de policía Florencia.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que empieza a ejecutar actividades y tengan las posibilidades de realizar el diseño, desarrollo y adquisición de software para el comando de policía Florencia.

Responsabilidades de la dirección:

Mediante instructivos legales enmarcados en la ley 603 del 2000 del uso y desarrollo de software.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, deben propender que se el diseño de software para el comando de policía Florencia se haga siguiendo los diferentes las normas vigentes, teniendo en cuenta la lay de derechos de autor.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad:

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Ambientes separados de producción y desarrollo.

Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. Así mismo para la realización de pruebas no se deben utilizar datos de producción.

Cumplimiento del procedimiento para cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, serán evaluadas en ambientes de prueba cuya función es determinar el correcto funcionamiento y compatibilidad con las herramientas base. Una vez determinado el correcto funcionamiento y compatibilidad con las herramientas base se debe crear un plan de trabajo para la migración del ambiente de producción a la nueva versión.

Documentación de cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe tener la documentación respectiva.

Catalogación de programas.

Debe cumplirse con el procedimiento establecido para pasar programas del ambiente de desarrollo al ambiente de producción previa prueba por parte del área encargada.

Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.

Todos los controles de seguridad para los sistemas de información deben ser implantados y probados sobre ambientes de pruebas o desarrollo y antes que dicho sistema entre en operación.

Dependencia de la autenticación de usuario en el sistema operativo.

Los desarrolladores de aplicaciones no deberán crear su propio sistema de control de acceso a la aplicación en desarrollo, esta labor deberá recaer en el sistema operativo o en un sistema de control de acceso que mejora las capacidades del sistema operativo. Esta política debe empezar a cumplirse desde la liberación de este documento.

Incorporación de Contraseñas en el Software.

Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por el comando de Policía de Florencia o sus proveedores, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política “Cambios periódicos de contraseñas”.

Acceso del usuario a los comandos del sistema operativo.

Después de haber iniciado una sesión, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

Se requieren registros de auditoria en sistemas que manejan información sensible.

Todo sistema que maneje información sensible para la Policía de Florencia debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

Registros para los usuarios privilegiados en los sistemas en producción que lo permitan.

Toda actividad realizada en los sistemas por usuarios con privilegios de administración debe ser registrada, si los mismos lo permiten, o de lo contrario debe existir un procedimiento alterno de control.

Los registros del sistema deben incluir eventos relevantes para la seguridad.

Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad relevantes son: intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

Resistencia de los registros contra desactivación, modificación y eliminación.

Los mecanismos para detectar y registrar eventos de seguridad informática significativos deben ser resistentes a ataques, en los sistemas que permitan dicha configuración. Estos ataques incluyen intentos por desactivar, modificar o eliminar el software de registro y/o los registros mismos.

Procesos controlados para la modificación de información del negocio en producción.

La modificación de información en producción debe darse únicamente mediante procesos con privilegios dentro de la aplicación que maneja dicha información. Esto con el fin de evitar que la información pueda ser modificada por medios diferentes a los canales establecidos. Se excluyen los casos de emergencia, previa autorización de la Presidencia.

Validación de entradas en los desarrollos.

El desarrollador debe tener en cuenta durante la elaboración de la aplicación, la validación de las entradas de código con el objeto de evitar la ejecución de comandos que pongan en riesgo la seguridad de los sistemas.

Diseño de seguridad para aplicaciones.

El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para el comando de Policía de Florencia.

Personas autorizadas para leer los registros de auditoria.

Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado. Personal no autorizado es aquel que no pertenece a auditoria interna, personal de seguridad informática, personal de administración de sistemas o administradores de bases de datos.

Archivo histórico de contraseñas.

En todo sistema multiusuario, software del sistema o software desarrollado localmente se debe mantener un archivo histórico encriptado de las contraseñas anteriores. Este archivo deberá ser usado para prevenir que un usuario seleccione una contraseña ya usada (ver política “Las contraseñas creadas por usuarios no deben ser reutilizadas”) y debe contener como mínimo las últimas cinco (5) contraseñas de cada usuario.

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

9. POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

10. Nombre del documento:	**POLÍTICAS PARA ADMINITRADORES DE SISTEMAS** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política es aplicable directamente para los administradores de los sistemas, ya que se deben realizar los procedimientos de actualización y difusión de las políticas de seguridad para el comando de policía Florencia.

Alcance de Cumplimiento con la seguridad de la información:

Todos los administradores del sistema que deben hacer cumplir las políticas de seguridad de la información, además deben tener actualizado el sistema sin obtener alguna clase de perjuicios para los funcionarios beneficiaros del sistema.

Aplicable

Para todos los funcionarios activos, que laboran en área de telemática de la base del comando de policía Florencio quienes tienen los privilegios para realizar acciones sobre el sistema activo y directivo del sistema.

Responsabilidades de la dirección:

Dar a conocer a todo el personal adscrito al área de telemática de la base del comando de policía Florencia esta política, que tiene que ver con la reserva y protección de la información.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes del área de Telemática del comando de policía Florencia, deben velar por la protección de la información confidencial, teniendo en cuenta que su uso es diariamente en cambio por las actualizaciones obligatorias del sistema.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos administradores del sistema en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Soporte para usuarios con privilegios especiales.

Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.

Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la policía nacional.

Todos los privilegios sobre los recursos informáticos de Policía de Florencia otorgados a un usuario deben eliminarse en el momento que éste abandone la Policía Nacional y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

Cuando y como pueden asignar contraseñas los administradores

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el sistema debe obligar al usuario a cambiar su contraseña.

Límite de intentos consecutivos de ingreso al sistema.

El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados:

1) ser suspendido hasta nueva reactivación por parte del administrador;

2) ser temporalmente bloqueado (no menos de 5 minutos);

3) ser desconectado si se trata de una conexión telefónica.

Cambio de Contraseñas Por Defecto.

Todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización siguiendo los lineamientos de la política “Contraseñas fuertes”.

Cambio de contraseñas después de compromiso detectado en un sistema multiusuario.

Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema debe asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata si se conoce evidencia de que el sistema ha sido comprometido. En este caso los usuarios deben ser advertidos de cambiar su contraseña en otros sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

Administración de los buzones de correo.

Los administradores deben establecer y mantener un proceso sistemático para la creación y mantenimiento de los buzones de correo electrónico, mensualmente se realizará una revisión de control sobre cada uno de los buzones creados para determinar cuáles requieren una depuración para que no alcancen su límite de espacio asignado.

Brindar acceso a personal externo.

El ingeniero de soporte y web master velará porque individuos que no sean empleados, contratistas o consultores del comando de Policía de Florencia no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Policía Nacional a menos que exista una aprobación escrita de la Presidencia o el comité de seguridad.

Acceso a terceros a los sistemas de la policía nacional requiere de un contrato firmado.

Antes de otorgarle acceso a un tercero a los recursos tecnológicos en el comando de Policía de Florencia se requiere la firma de un formato, acuerdo o autorización de comandante del departamento de policía Caquetá. Es obligatoria la firma del acuerdo de confidencialidad.

Restricción de administración remota a través de Internet.

La administración remota desde Internet no es permitida a menos que se utilicen mecanismos para encriptación del canal de comunicaciones.

Dos usuarios requeridos para todos los administradores.

Administradores de sistemas multiusuarios deben tener dos identificaciones de usuario: una con privilegios de administración y otra con privilegios de usuario normal.

Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.

Sin o con autorización escrita, los administradores no deben otorgarle privilegios de administración a ningún usuario, para evitar cambios no Autorizados en la red.

Las herramientas de detección de vulnerabilidades usadas por los administradores se deben desinstalar cuando no estén operativas o implementar un mecanismo de control de acceso especial basado en contraseñas o en encriptación del software como tal.

Manejo administrativo de Seguridad Para Todos los Componentes de la Red.

Los parámetros de configuración de todos los dispositivos conectados a la red del comando de Policía de Florencia deben cumplir con las políticas y estándares internos de seguridad.

Información a Capturar Cuando un Crimen Informático O Abuso es Sospechado.

Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea. La información a recolectar

incluye configuración actual del sistema, copias de backup y todos los archivos potencialmente involucrados.

Sincronización de relojes para un registro exacto de eventos en la red.

Los dispositivos multiusuario conectados a la red interna de Policía de Florencia deben tener sus relojes sincronizados con la hora oficial.

Revisión regular de los registros del sistema.

El área de sistemas de la oficina de Telemática debe revisar regularmente los registros de cada uno de los diferentes sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

Confidencialidad en la información relacionada con investigaciones internas.

Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del empleado.

Software de identificación de vulnerabilidades.

Para asegurar que el equipo técnico de la oficina de telemática del comando de Policía de Florencia han tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet se les debe correr un software de identificación de vulnerabilidades por lo menos una vez al año; adicionalmente en las estaciones de trabajo se cuenta con un software de Cortafuegos y Antivirus que cuente con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades. A nivel Corporativo se cuenta con un firewall que proporciona un software de IDS (Instrusion Detection System), sistema detección de intrusos, detección de virus y bloqueo de correo no deseado.

En dónde usar controles de acceso para sistemas informáticos.

Todo computador que almacene información sensible de la Policía de Florencia, debe tener un sistema de control de acceso para garantizar que esta información no sea modificada, borrada o divulgada.

Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales

Se debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo.

Habilitación de logs en sistemas y aplicaciones

Se debe habilitar la gestión de logs (archivos de transacción) en los sistemas y aplicaciones críticas de Policía de Florencia.

Monitoreo de sistemas

Se debe mantener una adecuada aplicación de monitoreo configurada que identifique el mal funcionamiento de los sistemas controlados.

Mantenimiento de los sistemas

Se debe realizar periódicamente el mantenimiento en las bases de datos, antivirus, servidores de correo y servicios del comando de Policía de Florencia

Verificación física de equipos críticos

Se debe verificar periódicamente el estado físico de los equipos de cómputo críticos.

Servicios de red

Se debe garantizar que el servicio de red utilizado por el comando de Policía de Florencia, se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por el comité de seguridad puede efectuar escaneos de la red con la finalidad de: resolver problemas de servicio, como parte de las operaciones normales del sistema y del mantenimiento, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

Revisión de accesos de usuarios

Se debe realizar por control de auditoría la revisión de los accesos de los usuarios a las aplicaciones utilizadas, por lo menos dos veces por año.

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

9.1 POLÍTICAS DE BACKUP

Nombre del documento:	**POLÍTICAS DE BACKUP** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política se centra en difundir la forma correcta, para dar inicio al procedimiento en al realizar BACKUP de información, para evitar la pedida masiva de la misma y se conserven los principios de la seguridad de la información.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar los requisitos de esta política.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que empieza a ejecutar actividades donde se tenga acceso a la información pública de la policía de Florencia, aplicando la reserva y confidencialidad de la información.

Responsabilidades De la dirección:

Cada procedimiento en cuanto al BACKUP de la información, es de pleno conocimiento de la dirección Comandante de Policía, a su vez instruir al personal bajo su mando en cada uno de los parámetros establecidos en cumplimiento de esta política.

Responsabilidades del área de recurso humano:

Deben seguir las instrucciones impartidas por esta política sin salirse del marco legal, para la ejecución y realizar el BACKUP de la información según la política.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Período de almacenamiento de registros de auditoria.

Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.

Tipo de datos a los que se les debe hacer backup y con qué frecuencia.

A toda información sensible y software crítico del comando de Policía de Florencia residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por el procedimiento de copias de respaldo. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

Copias de información sensible.

Se deben elaborar una copia de cada backup con el fin de minimizar el riesgo por daño del medio de almacenamiento en disco y cinta, según procedimiento de copias de respaldo.

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

9.2 POLÍTICAS DE USO DE FIREWALL

Nombre del documento:	**POLÍTICAS DE USO DE FIREWALL** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Establece los lineamientos de seguridad y protección que se deben conservar para el uso de la red de datos en la base del comando de policía Florencia.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar esta política y los procedimientos en materia de protección y seguridad de la información del firewall para la red del comando de policía Florencia.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que empieza a hacer uso de algunos de los recursos informáticos y de la red de datos de la base del comando de policía Florencia.

Responsabilidades De la dirección:

Establecer ciertos parámetros para el debido conocimiento del personal que labora en el comando de policía Florencia, con el fin de concientizar a todos los funcionarios sobre la política del uso de firewall.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias deberá hacer cumplir los requisitos de esta política según lo estipulado en ella para así conservar los principios de la seguridad de la información.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad:

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Detección de intrusos.

Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.

Toda conexión externa debe estar protegida por el firewall.

Toda conexión a los servidores del comando de Policía de Florencia proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

Toda conexión hacia Internet debe pasar por el Firewall.

El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

Firewall debe correr sobre un computador dedicado o appliance.

Todo firewall debe correr sobre un computador dedicado o modelo appliance para estos fines. Por razones de desempeño y seguridad no debe correr otro tipo de aplicaciones.

Inventario de conexiones.

Se debe mantener un registro de las conexiones a redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización, lo anterior se cumple con el diagrama de red.

El sistema interno de direccionamiento de red no debe ser público.

Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

Revisión Periódica y Reautorización de Privilegios de Usuarios.

Los privilegios otorgados a un usuario deben ser reevaluados una vez al año con el fin de analizar sí los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por el área de sistemas de la oficina de telemática con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios al comandante de Policía Caquetá.

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

9.3 POLÍTICAS PARA USUARIOS EXTERNOS

Nombre del documento:	**POLÍTICAS PARA USUARIOS EXTERNOS** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRO EDURDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política establece los requisitos y parámetros para usuarios externos, con el fin de optimizar el control para la seguridad de la información.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, personal externo deben acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Le Corresponde velar por su estricto cumplimiento al comandante Policía de Florencia y al comité de seguridad.

Aplicable

Para todos los usuarios externos, que por situaciones laborales, en el momento que empieza a ejecutar actividades donde tenga acceso a la información pública de la policía de Florencia para el acceso a los recursos informáticos.

Responsabilidades de la dirección:

Dar a conocer a todo el personal externo a la base del comando de policía Florencia esta política, que tiene que ver con la reserva y protección de la información.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, deben velar por la protección de la información confidencial, para el uso de personal externo.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad:

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Términos y Condiciones Para Clientes de Internet.

El comando de Policía de Florencia asumen que todos los clientes que usan Internet para establecer relación con la Policía de Florencia o realizar operaciones aceptan los términos y condiciones impuestos por Policía de Florencia en sus términos y condiciones de uso del portal de internet, antes de realizarse cualquier transacción.

Acuerdos con terceros que manejan información o cualquier recurso informático de Policía de Florencia.

Todos los acuerdos relacionados con el manejo de información o de recursos de informática del comando de Policía de Florencia por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a Policía de Florencia ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de la Policía de Florencia.

Definición clara de las responsabilidades de seguridad informática de terceros.

Socios de negocios, proveedores, clientes y otros asociados a los negocios del comando de Policía de Florencia deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos con la Policía y verificada por el comandante de Policía Caquetá , el responsable del manejo de estos terceros deberá realizar un acompañamiento controlado durante su estadía en las instalaciones del comando de Policía de Florencia, y de esta manera podrá verificar la calidad en la entrega de los servicios contratados.

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

9.4 POLÍTICAS DE ACCESO FÍSICO

Nombre del documento:	**POLÍTICAS DE ACDESO FISICO** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	Ing. ERIKA VILLAMIZAR
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política trata de las consignas y cuidados que se deben tener diariamente en el ingreso de personal a las instalaciones policiales, conservando consigo su debida identificación al ingreso físico al comando de policía Florencia.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad física.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que empieza su contrato de prestación de servicio hasta el término de la misma ejecutar actividades donde tenga acceso a la información pública de la policía de Florencia para el acceso a los recursos informáticos.

Responsabilidades de la dirección:

Dar a conocer a todo el personal adscrito a la base del comando de policía Florencia esta política, que tiene que ver con la reserva y protección de la información.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, deben velar por la protección de la información confidencial, teniendo en cuenta que su uso es diariamente controlado por esta política.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad:

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

Reporte de pérdida o robo de identificación.

Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones.

Orden de salida para equipos electrónicos.

Ningún equipo electrónico podrá salir de las instalaciones del comando de Policía de Florencia sin una orden de salida otorgada por el personal adecuado o sin haber sido

registrado en el momento de su ingreso.

Orden de salida de activos

Todos los activos que afecten la seguridad de la información del comando de Policía de Florencia como medios de almacenamiento, CDs, DVDs., entre otros, y que necesiten ser retirados de la Policía Nacional, se debe realizar la autorización de salida por medio del formato de Autorización de salida de activos dispuesto para estos casos.

Cuando se da una terminación laboral, los privilegios de acceso a la sede de policía de Florencia deben ser revocados.

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnés, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados enviando (funcionarios autorizados) correo electrónico del laboratorio Sistemas de la oficina de telemática de policía Florencia (decaq.telem-lab@policia.gov.co)

Ingreso de equipos de grabación y fotografías al cuarto de servidores.

Cualquier miembro del comando Policía de Florencia y/o tercero debe estar autorizado por el área de seguridad de la información para ingresar con equipos, mas no hacer uso de ellos sin la debida autorización equipos donde puedan obtener información, estos pueden ser (video cámaras, celulares, cámaras fotográficas.

NOTA DE CONFIDENCIALIDAD

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

9.5 POLITICA DE USO DE PORTATILES

Nombre del documento:	**POLÍTICAS DE USO DE PORTATILES** POLICÍA NACIONAL
Elaborado por:	WILSON RICARDO ARIAS CARMONA
Revisado por:	JAIRDO EDUARDO MOLINA VIVAS
Elaborado para la empresa:	COMANDO DE LA POLICÍA DE FLORENCIA CAQUETÁ, COLOMBIA
Fecha:	18/11/2015

Descripción de la política:

Esta política está directamente enfocada en la prohibición total del uso de portátil personal al interior de la base del comando de departamento de policía Florencia.

Alcance de Cumplimiento con la seguridad de la información:

Todos los colaboradores de la organización, así como los contratistas, deben cumplir y acatar esta política y los procedimientos en materia de protección y seguridad de la información.

Aplicable

Para todos los funcionarios activos, contratistas desde el momento que empieza a ejecutar actividades donde tenga acceso a la información pública de la policía de Florencia para el uso de portátiles al interior del comando de policía Florencia.

Responsabilidades de la dirección:

Dar a conocer a todo el personal adscrito a la base del comando de policía Florencia esta política, que tiene que ver con la reserva y protección de la información.

Responsabilidades del área de recurso humano:

Cada uno de los integrantes de las diferentes dependencias del comando de policía Florencia, deben velar por la protección de la información confidencial, teniendo en cuenta que su uso es diariamente controlado por esta política.

Responsabilidades de los empleados, y demás incluidos en el alcance:

Esta norma es de estricto cumplimiento por todos los empleados de la empresa en el cuidado u buen uso de la información.

Medidas disciplinarias por incumplimiento de políticas de seguridad:

Cualquier incumplimiento de una política de seguridad de la información por parte de un funcionario de contratistas, así como de la Policía de Florencia, estándar, o procedimiento es causa para iniciar acciones disciplinarias, las cuales de acuerdo a su gravedad pueden suponer la terminación de la vinculación laboral del empleado o contratista.

9.6.1 PROTECCIÓN DE LA INFORMACIÓN

El antivirus siempre debe estar activo y actualizado

No permitir que personas extrañas lo observen mientras trabaja en el equipo portátil, especialmente si esta fuera de las instalaciones del comando de Policía de Florencia, seguir las políticas de acceso remoto, toda la información que es confidencial debe ir cifrada.

Cuando el equipo deba ser devuelto a Policía de Florencia para reparación, mantenimiento. La información confidencial deberá ser borrada y respectivamente guardada en una copia de respaldo

De la información de usuario debe generarse copia de respaldo, por solicitud del usuario al área de sistemas.

Actualización, mantenimiento y divulgación de las políticas de seguridad de la información.

Las políticas se deben revisar a intervalos planificados o cuando se produzcan cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

El Jefe de Riesgos debe aprobar el documento de actualización, es responsable por su publicación y comunicación a todos los empleados y partes externas pertinentes. El mecanismo de notificación y divulgación de los cambios realizados a la política de seguridad de la información será mediante correo electrónico.

NOTA DE CONFIDENCIALIDAD PARA LA SEGURIDAD LA INFORMACION

Este documento es de propiedad única y exclusivamente del comando de Policía Florencia y su uso debe estar regido a lo dispuesto en la clasificación del mismo, quedando totalmente prohibida la divulgación y/o reproducción total o parcial de las contraseñas personal e institucional sin la debida autorización por parte del comité de seguridad de la información. Su uso y distribución solo está autorizado al interior de comando de Policía y por parte del personal debidamente habilitado

10 COMITÉ DE SEGURIDAD

El Comité de Seguridad de la información está conformado por un equipo de trabajo interdisciplinario encargado de garantizar una dirección clara y brindar apoyo visible a la Presidencia con respecto al programa de seguridad de la información dentro del comando de policía.

El comité debe estar a cargo de promover la seguridad de la organización por medio de un compromiso apropiado y contar con los recursos adecuados.

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad De la información, dentro de la Policía Nacional:

- Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar al interior del comando de Policía de Florencia.
- Revisión y valoración de la Política de Seguridad de la Información, dando a conocer cada uno de los puntos básicos para su estricto cumplimiento.
- Alineación e integración de la seguridad a los objetivos de la organización en la oficina de telemática como área de sistemas de la unidad policial.
- Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización en cada una de las unidades desconcentradas a nivel Nacional, como lo son las metropolitanas y departamentos.
- Establecer las funciones y responsabilidades específicas de seguridad de la información para toda la Organización.
- Reportar, a través de reuniones semestrales al comandante del departamento de policía Caquetá, el estado de la seguridad y protección de la información en la Organización y la necesidad de nuevos proyectos en temas de seguridad de la información.
- Establecer y respaldar los programas de concientización de la compañía en materia de seguridad y protección de la información

- Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información para ser utilizado de forma directa en el comando de Policía Caquetá.

- Evalúa la adecuación y coordina la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.

- Promueve explícitamente el apoyo institucional a la seguridad de la información en toda la organización.

- Supervisión y control de los cambios significativos en la exposición de los activos de información a las principales amenazas.

- Revisión y seguimiento a los incidentes de seguridad de la información, para la toma de decisiones en cuanto a la mejora continua.

- Analizar y autorizar cualquier tipo de movimiento o traslado de equipos de misión crítica para la Organización.

Adicionalmente, el comité tiene la responsabilidad de tratar los siguientes temas (por demanda):

- Mejoras en las actividades inherentes a la Seguridad de Policía de Florencia y sus procesos.

- Seguimiento a la aplicación de las políticas, programas y planes adoptados para la protección de los sistemas, recursos informáticos y servidores de la Red Interna y Centro de Cómputo del comando de Policía de Florencia

- Decisiones de carácter preventivo y proactivo que apunten a la optimización de la seguridad de los procesos y sus procedimientos.

- Participación activa en la revisión, evaluación, mantenimiento, recomendaciones, mejoras y actualizaciones de la presente política de seguridad de la información. El jefe del área de sistemas con el Gestor de seguridad de la información, convocan al comité de seguridad con el propósito de evaluar los cambios a la presente política y autorizar su publicación. De este comité se deja Acta como constancia de su evaluación y aprobación.

Las decisiones del comité de seguridad son protocolizadas mediante un Acta de Comité de Seguridad firmada por los miembros, así:

- Comandante del departamento de policía Caquetá.
- Jefe de planeación
- Jefe del área administrativo
- Jefe Grupo de telemática
- Coordinador o gestor de seguridad de la información.

Las Actas de comité de seguridad podrán ser Anuladas por el comité de Seguridad mediante el uso de un Acta que invalide el contenido siempre y cuando no se haya ejecutado acciones relacionadas con la seguridad de la información.

CONCLUSIONES

- Con base al a los requisitos para la seguridad de la información tipificados en la norma ISO27001:2013, se realiza el análisis del estado actual en la que funciona la seguridad de la información en el comando de Policía Caquetá.

- Se acude a la encuesta como técnica de investigación al 10% del personal en el comando de Policía Caquetá, con el fin de observar el grado de factibilidad para el diseño y la definición de políticas para la seguridad de la información.

- Haciendo del sistema operativo Kali linux y la aplicación nessus como herramientas exclusivas para la hallar vulnerabilidades en la red, con base en ello se realiza un escaneo profundo en búsqueda de vulnerabilidades en la red del comando de Policía Florencia.

- Siguiendo los parámetros, requisitos y el anexo A de la norma ISO27001 en su versión 2013, de se diseña y se definen las políticas para seguridad de la información, que serán aplicadas en el comando de Policía Florencia en el departamento del Caquetá.

11 BIBLIOGRAFÍA

Norma ISO versión 2014 [El SGSI Sistema de Gestión de Seguridad de la Información]" es el concepto central sobre el que se construye ISO 27001. http://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

Guía para la elaboración de [políticas de seguridad 2003] "universidad nacional de Colombia, políticas con estándares mejores prácticas y guías.

La seguridad de la información, según [ISO 27001], consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. http://www.iso27000.es/sgsi.html

Conceptos básicos de seguridad de la información [INTECO 2010], Protección de activos de una Organización https://www.youtube.com/watch?v=zV2sfyvfqik

Avance en la apropiación y concepción filosófica de los [SGSI 2014] http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

Octubre de 2005, el estándar fue adoptado por el International Organización por estandarización (ISO). Como resultado, la implantación de BS 7799 – ahora ISO http://www.iso27000.es/download/KeyStrategiesforImplementingISO27001.pdf

ISO 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos.

Toro, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.

Moreno, F. 2009. La ISO/IEC 27005 en la búsqueda de información más segura Normas y Calidad. ICONTEC. Cuarta edición. P 28 – 32.

ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

12 ANEXOS

ANEXO 1. CONFIGURACIÓN AL SERVIDOR DE DOMINO.

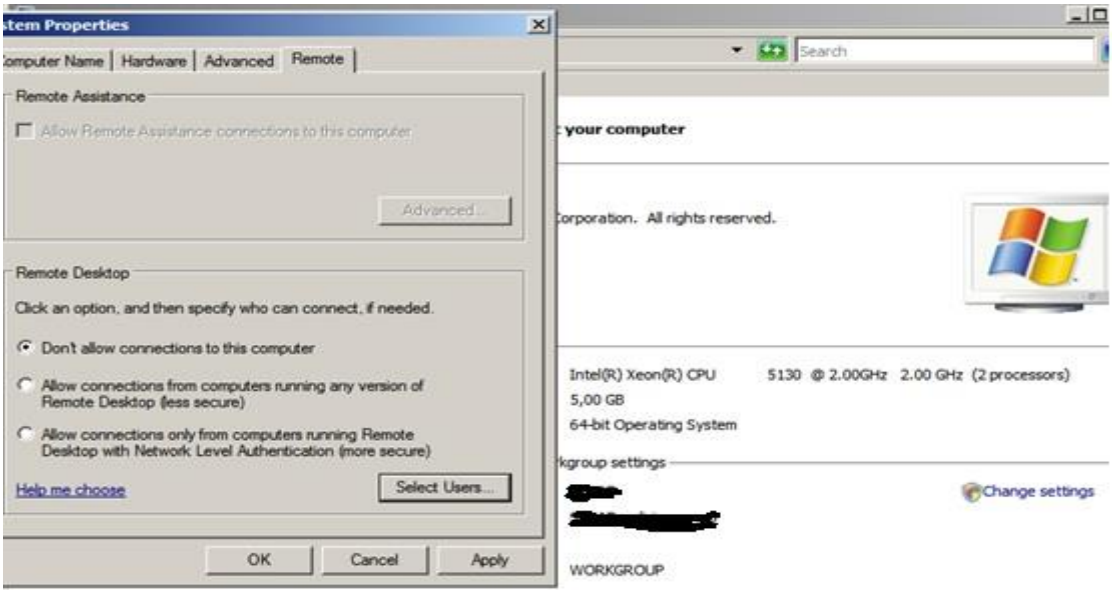
Para que los equipos que tengan conexión con el servidor este con dirección IP dinámica, protocolo de configuración dinámica de host (DHCP).

Figura 21. Conexión servidor policía.gov.co

Fuente: El autor

Se configurara el firewall para el servidor de la policía, primero lo ingresamos al dominio y le configuramos el control de acceso remoto de forma segura.

Figura 22. Configuración acceso remoto.

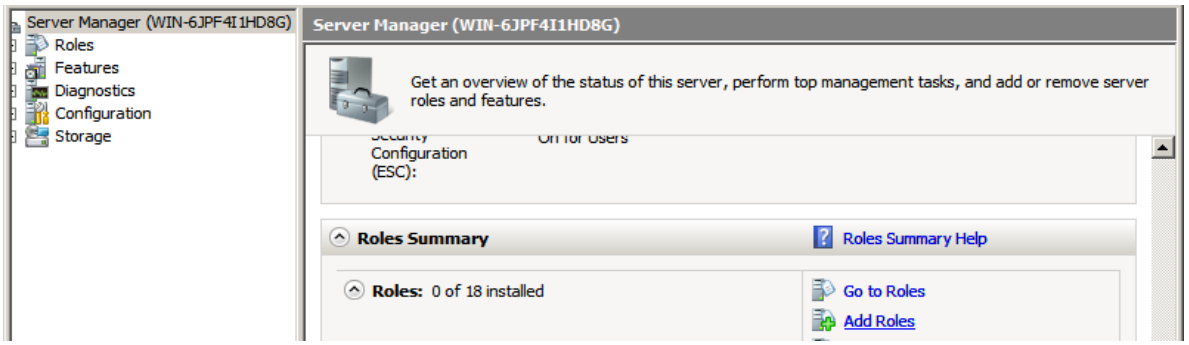


Fuente: El autor

Con el fin de habilitar las características y propiedades básicas del servidor para el trabajo real ROUTER y así aplicar las políticas a los equipos que se una a esta red del sistema.

Vamos a agregar roles - ADD ROLES para el servidor de la policía de Florencia

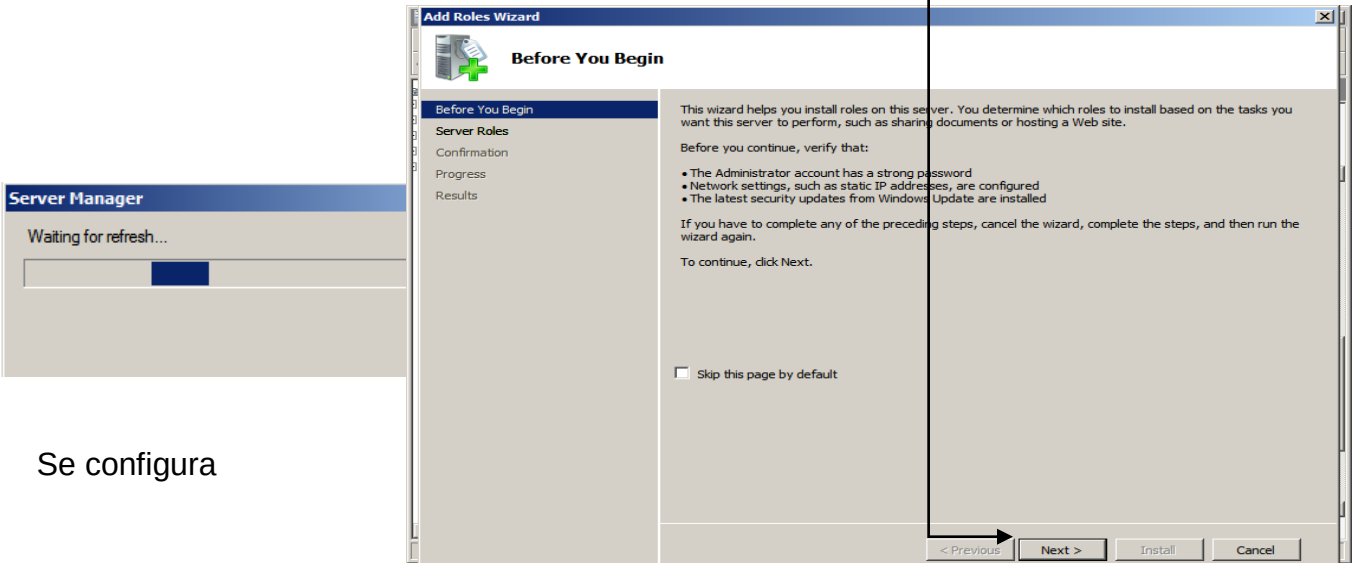
Figura 23. Server manager adicionar roles



Fuente: El autor

Continuamos con los pasos sugeridos para llegar a la configuración esencial y damos clic en siguiente.

Figura 24 . Secuencia configuración

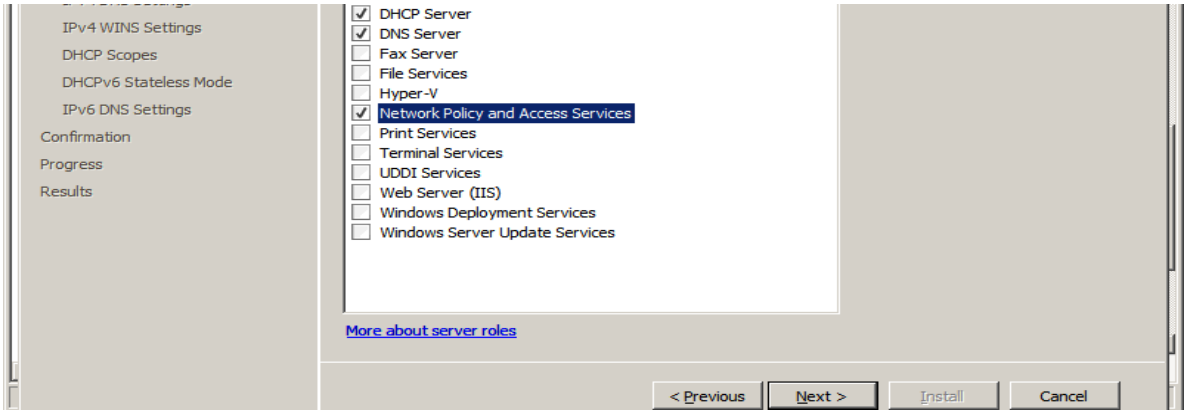


Se configura

Fuente: El autor

El servidor con características de router y así asociar los usuarios seleccionando el servicio de acceso y las directivas de redes, NETWORK POLICY AND ACCESS SERVICE, damos clic en next o siguiente.

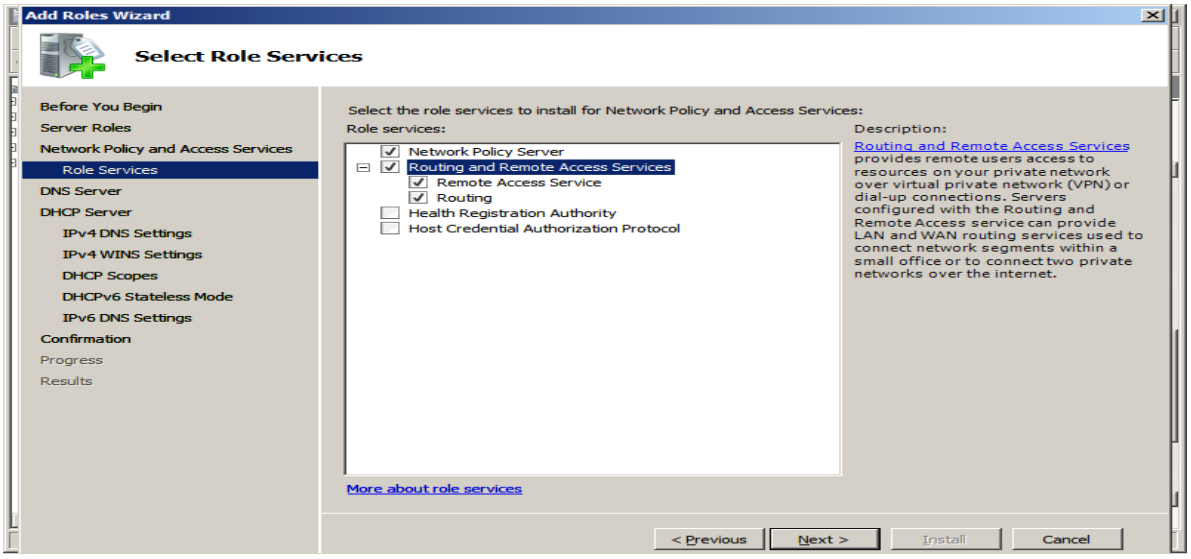
Figura 25. Aplicación de Políticas



Fuente: El autor

Luego ingresamos a los servicios del rol y selecciona los servicios adecuados para la debida configuración del servidor con propiedades de RUOTER. CLIC EN NEXT.

Figura 26. Selección roles y servicios.



Fuente: El autor

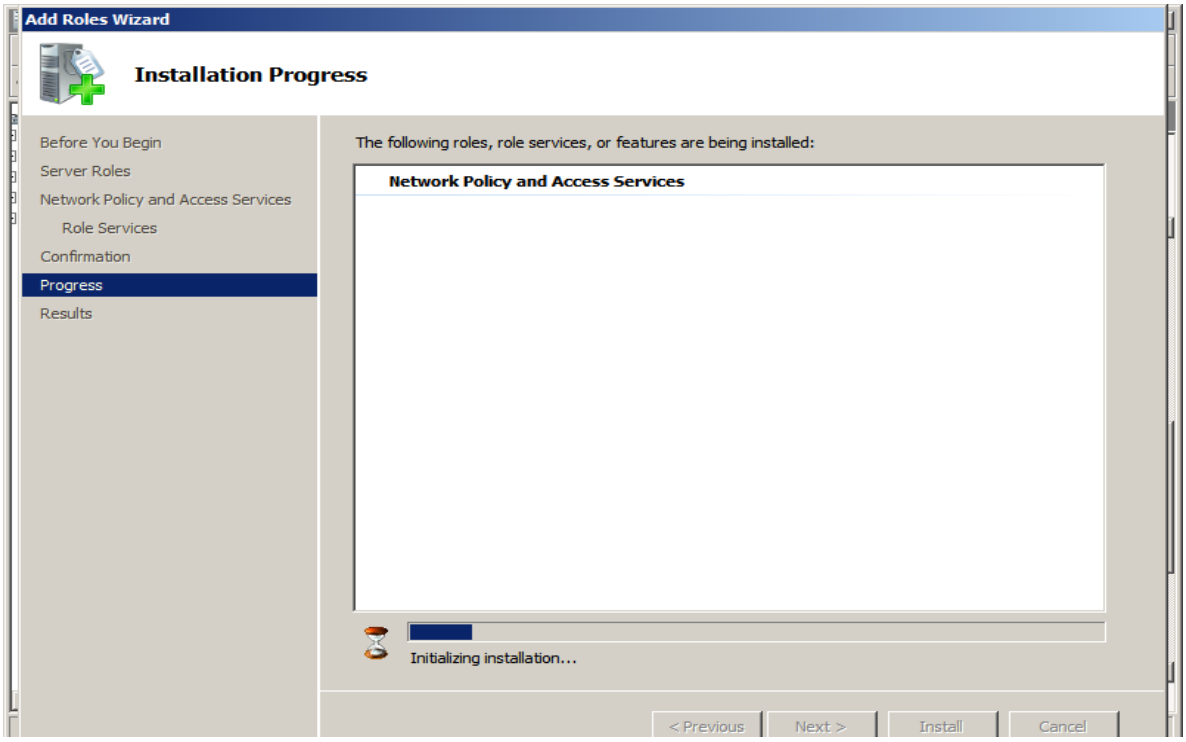
Después de esta configuración el servidor avisa que posiblemente se necesite reinar para guardar cambios, bueno continuamos con la configuración NEXT.

Figura 27. Confirmación de la instalación de las Políticas.

Fuente: El autor

Inicia el progreso de instalación de esta configuración esta lista para tomar el control del servidor y dar inicio a la creación las reglas de entrada y salida.

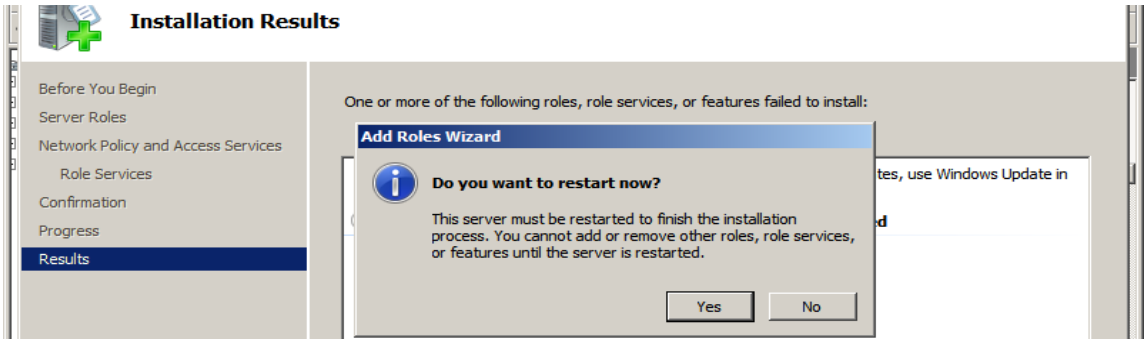
Figura 28. Progreso instalación de políticas



Fuente: El autor

Ya terminado la instalación me pide reiniciar el servidor para guardar los cambios.

Figura 29. Reiniciar el sistema.



Fuente: El autor

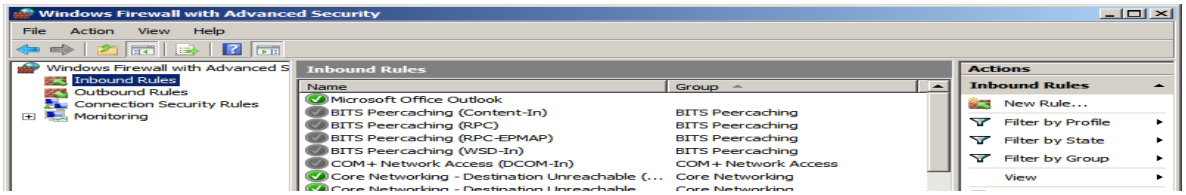
Configuración del firewall del servidor

Bueno, ahora se va a configurar el firewall del servidor para la protección de navegación interna de los usuarios y equipos adicionados al servidor dominio.

Esto es teniendo en cuenta que la red del servidor está funcionando, por lo tanto se requiere la configuración de las reglas de entrada y salida para el flujo de información entre los equipos del servidor.

Para las reglas de entrada, es para la configuración esencial y protección en caso de que alguien externo quiera entrar a mi red, en este caso un cracker, o intruso no autorizado.

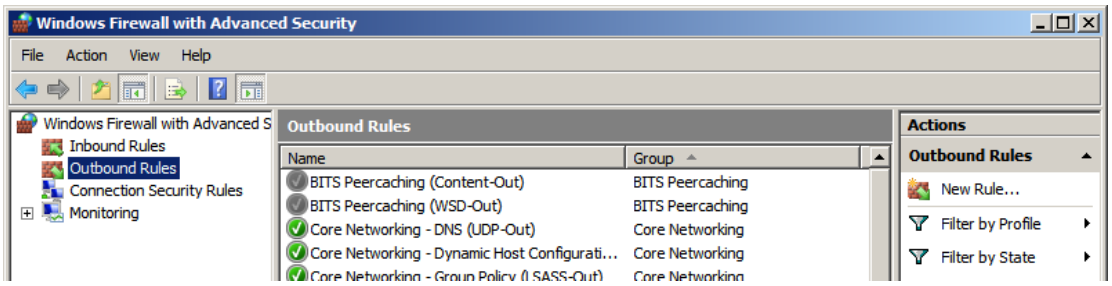
Figura 30. Reglas de entrada y salida.



Fuente: El autor

Para las reglas de salida es para monitorear y controlar a los usuarios de nuestra propia red, en caso de querer salir de los parámetros autorizados definidos por el servidor.

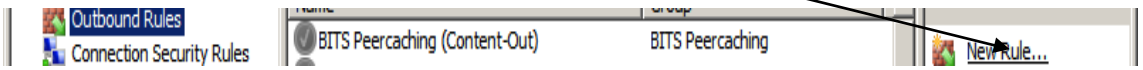
Figura 31. Configuración reglas de entrada



Fuente: El autor

Como crear reglas de salida para los equipos en mi red, es de conocer la ubicación general del acceso a nueva regla.

Figura 32. Inicio regla nueva



Fuente: El autor

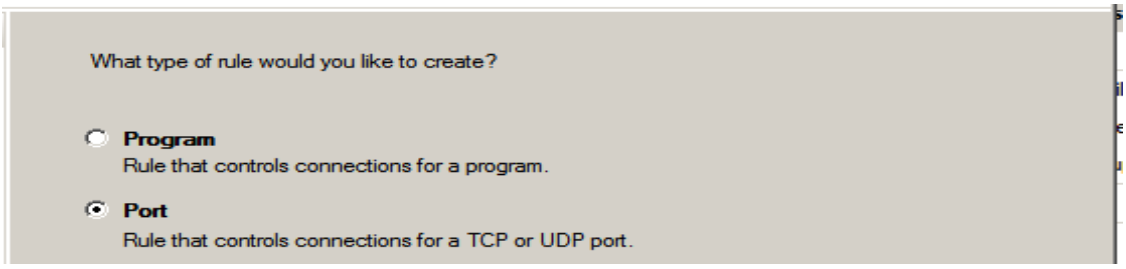
Bueno, allí se puede bloquear un programa, un puerto de red, predefinida y personalizada.

Bloqueo de Programa: Es conocer la ruta de instalación donde se ejecuta esta Programa y así poderlo bloquear, se puede para todas las maquinas o en su defecto para las que decida el administrador por sus funciones.

Bloqueo de Puerto: Es para tener el control medido del tráfico de red, evitar que fluya ciertas páginas por el firewall del servidor. o dejar los equipos sin internet, e incluso seleccionados. Dejar de funcionar el puerto 80, navegación por http:// o el puerto 443, el puerto https:// el puerto 25 para bloqueo de envió de mensajes a correo electrónicos, en fin un sin número de bloqueo para más los más de 150

puerto de red existentes. Ahora se configurar una regla de salida sobre un puerto de red ejemplo el 80 y el 443. Veamos.

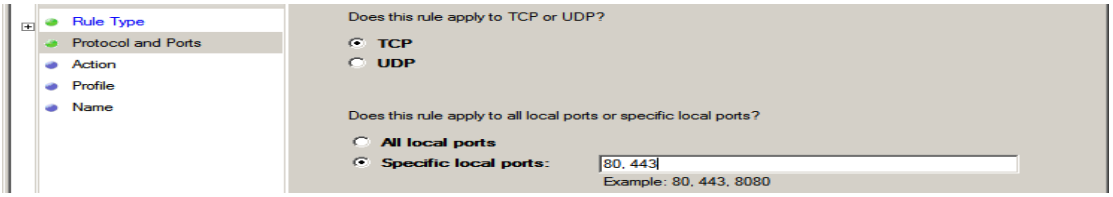
Figura 33. Configuración regla puerto de red.



Fuente: El autor

Especificar el puerto para ser bloqueado en los equipos.

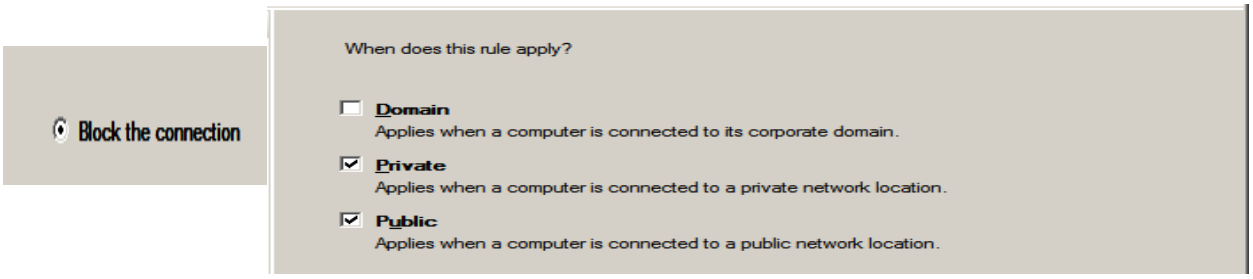
Figura 34. Ejemplo configuración puerto.



Fuente: El autor

Allí seleccionamos el parámetro de bloquear conexión, y seleccionado bloquear las máquinas de la red, privado y público, incluso dominio que también es considerable.

Figura 35. Sector Aplicación de la regla.



Fuente: El autor

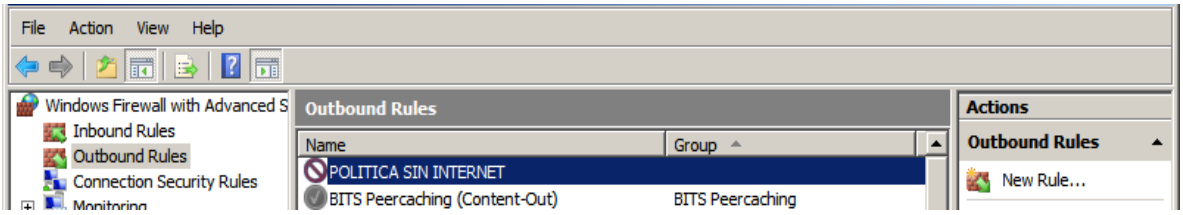
Se le nombra a la política según se quiera, para tener un control seguro de la red de forma temporal o permanente según sea, para la protección de la red en la Policía de Florencia.

Figura 36. Política SIN INTERNET

Fuente: El autor

Observamos ya aparecerá en la lista de los reglas de salida.

Figura 37. Creación política sin internet.



Fuente: El autor

Configuración Tomada En El Sistema para los usuarios.

Los equipos en general quedan con la restricción de ser tomados en acceso remoto, de esta manera estamos protegiendo los equipos de la policía de Florencia, ya con su nemotecnia definida decaq-telem1, es el primer equipo de la oficina de Telemática de la Unidad Policial.

ANEXO 2. ENCUESTA APLICADA

Acontinuacion se anexa la encuesta realizada por 15 de las 50 personas que laboran al intererior del comando de Policia Florencia.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo X	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo.
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores X

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto. X
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo X	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo.
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores X

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto. X
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo X	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo.
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores X

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto. X
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo	X	2	De acuerdo
3	Totalmente en desacuerdo		4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo.
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores X

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB. X
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo ✓	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo. ✓
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	✓

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB. ✓
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo X	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo X
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB. X
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo X	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo. X
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB. X
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo X	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo X
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos. X

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo ✓	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo. ✓
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	✓

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos. ✓

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo ✓	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo. ✓
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	✓

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos. ✓

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo	2	De acuerdo X
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo. X
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos. X

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo	2	De acuerdo X
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo. X
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI		NO	X

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos. X

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo	2	De acuerdo X
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo. X
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI	X	NO	

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados.
d) El personal permanece mucho tiempo en sitios web no permitidos. X

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo	2	De acuerdo X
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo.
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores X

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI	X	NO	

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados. X
d) El personal permanece mucho tiempo en sitios web no permitidos.

NOMBRE DEL ENCUESTADOR: WILSON RICARDO ARIAS CARMONA

Cordial saludo Estamos interesados en conocer su opinión como miembro activo de la Policía Nacional, por favor, ¿sería tan amable de contestar el siguiente cuestionario? La información que nos proporcione será utilizada para conocer la viabilidad de desarrollar políticas de seguridad de la información para el comando de policía Caquetá gracias.

1.- En la siguiente escala de 1 al 4, dónde.

1. Totalmente de acuerdo	2. De acuerdo
3.Totalmente en desacuerdo	4. En desacuerdo

¿Es importante el registro y control de la información confidencial de la policía en base a políticas para la seguridad de la información?

1	Totalmente de acuerdo	2	De acuerdo
3	Totalmente en desacuerdo	4	En desacuerdo

2.- ¿Cuál o cuáles de las siguientes características considera importantes para el control en el manejo de la información?

a) tener ciertas restricciones como ente gubernamental, utilizando contraseñas personalizadas par el uso de los equipos de cómputo.
b) prohibirse el acceso a páginas web no autorizadas para la Policía.
c) Tener definido un SGSI con sus políticas definidas y debidamente controladas.
d) Todas las anteriores X

3.- Considera que el control de acceso para el personal ajeno a la instalación Cumple las normas mínimas de seguridad de la información confidencial?

SI	X	NO	

4. De las siguientes anomalías seleccione aquellas con respecto a la seguridad de la información.

a) Se ha presentado la pérdida de información importante en memorias USB.
b) El funcionario asegura haber dejado el equipo apagado y lo encuentra encendido con su usuario abierto.
c) Se ha presentado daño en la información por ataques de virus injustificados. X
d) El personal permanece mucho tiempo en sitios web no permitidos.

RESUMEN ANALITICO EDUCATIVO
RAE

Título del texto	DISEÑAR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICABLES AL COMANDO DE LA POLICÍA DE FLORENCIA, BASADAS EN LA NORMA ISO/IEC 27001:2013
Nombres y Apellidos del Autor	WILSON RICARDO ARIAS CARMONA
Año de la publicación	**2016**
Resumen del texto:	
Palabras Claves	Análisis de la Información, diseño políticas, escaneo red, Políticas, reconocimiento, seguridad Informática, vulnerabilidades.
Problema que aborda el texto: El departamento de policía Caquetá no cuenta con unas políticas, normas, directrices, procedimientos, gestión del riesgo, ni con personal profesional para administrar y controlar el uso adecuado de todo el contexto tecnológico del comando, lo que por su puesto conlleva a una falta de concientización en seguridad de la información, con los cuidados y la importancia que se debe tener con el proceso de la información, como lo que tiene que ver con los reglamentos únicos de estricto control	

Objetivos del texto:

General

Diseñar las políticas de seguridad de la información basadas en la norma ISO/IEC 27001:2013 que puedan ser implantadas en el comando de policía de Florencia

Específicos

Realizar un análisis del estado actual de la seguridad de la información de acuerdo a los requisitos de la norma ISO 27001:2013

Realizar un análisis de información mediante la utilización de la técnica de investigación tipo encuesta.

Realizar análisis de vulnerabilidad a la red de datos del comando de policía Florencia, con el fin de identificarlas para así dar inicio con el diseño de políticas de seguridad Informática.

Definir para el comando de policía Florencia políticas de seguridad de información que permitan incrementar el nivel de seguridad basado en la norma ISO 27001:2013

Hipótesis planteada por el autor:

Se intenta llevar un control mediante el uso de formatos para la confidencialidad de la información, pero no se cuenta con un sistema de gestión del riesgo para la seguridad de la información que respalde dichos formatos.

Tesis principal del autor:

Se necesita realizar un Escaneo total a la red de datos de la policía Florencia,

con el fin de hallar las vulnerabilidades.

Argumentos expuestos por el autor:

La política de Florencia es un ente estatal de lo cual**,** se necesita diseñar políticas de seguridad informática que permita controlar y proteger los activos de información de esta entidad Gubernamental.

Conclusiones del texto:

Con base al a los requisitos para la seguridad de la información tipificados en la norma ISO27001:2013.

Se acude a la encuesta como técnica de investigación al 10% del personal en el comando de Policía Caquetá.

Mediante el uso del sistema operativo KALI LINUX y la aplicación NESSUS como herramientas exclusivas para la hallar vulnerabilidades en la red.

Siguiendo los parámetros, requisitos y el anexo A de la norma ISO27001 en su versión 2013 se diseñan las políticas.

Bibliografía citada por el autor:

Guía para la elaboración de [políticas de seguridad 2003] “universidad nacional de Colombia, políticas con estándares mejores prácticas y guías.

ISO 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos.

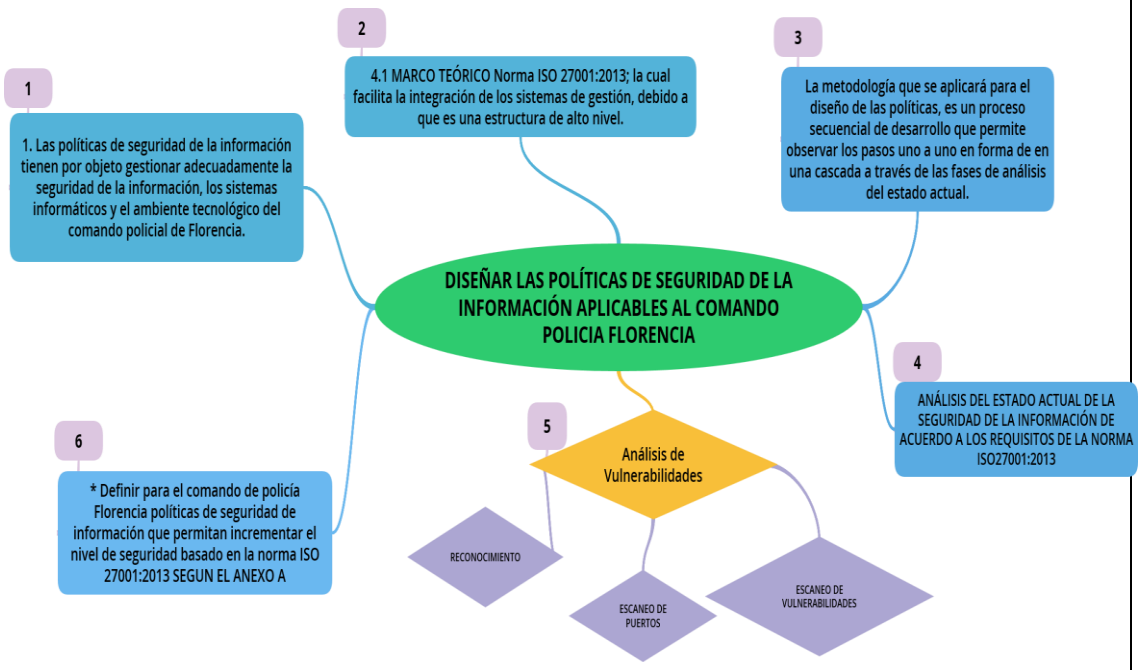
Toro, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.

Moreno, F. 2009. La ISO/IEC 27005 en la búsqueda de información más

segura Normas y Calidad. ICONTEC. Cuarta edición. P 28 – 32.

Nombre y apellidos de quien elaboró este RAE	**WILSON RICARDO ARIAS CARMONA**
Fecha en que se elaboró este RAE	18 DE ABRIL DE 2016

Imagen (mapa conceptual) que resume e interconecta los principales conceptos encontrados en el texto:



Comentarios finales:

Este proyecto es de gran y vital importancia para el comando de policía de Florencia, ya que los altos mandos de esta entidad están de acuerdo y probaron que se realizaran los estudios pertinentes para su ejecución.

UNAD Universidad Nacional Abierta y a Distancia	FORMATO CONCEPTO ASESOR O JURADO	CODIGO: FI-PF-VIACI-004-003
		VERSION. 000-21-10-2009
	PROCEDIMIENTO RELACIONADO: TRABAJO DE GRADO	PAGINAS 1

Fecha: **13 de Abril de 2016**	CEAD: **José Acevedo y Gómez**	Escuela: **Escuela de Ciencias Básicas Tecnología e Ingeniería**

DE: **SALOMON GONZALEZ GARCIA**
PARA: Comité de Investigación Formativa

Asunto: Aval de proyecto para: Asesor /O/ Jurado ☐ Sustentación ☒ de Trabajo de Grado Periodo académico 2016.

En cumplimiento de las funciones del Reglamento Académico **apruebo** ☒ **apruebo con correcciones** ☐ **rechazo** ☐ el proyecto **DISEÑAR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN APLICABLES AL COMANDO DE LA POLICÍA DE FLORENCIA, BASADAS EN LA NORMA ISO/IEC 27001:2013** para ser presentado ante Jurado ☐ para Sustentación ☒.

Los integrantes del proyecto son:

PRIMER INTEGRANTE

Identificación		**93.062.246 de Fresno- Tolima**
Nombre Completo		**Wilson Ricardo arias Carmona**
Programa del que se graduará		**Especialización en seguridad informática**
Celular	**3212082823**	Correo Electrónico: **wrariasc@unadvirtual.edu.co**

Atentamente,

Asesor

Salomón González García

Jurado