REDISEÑO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA PARA LA GOBERNACIÓN DE NARIÑO.

JORGE DANIEL ÁLVAREZ GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2018

REDISEÑO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA PARA LA GOBERNACIÓN DE NARIÑO.

PRESENTADO POR:
JORGE DANIEL ÁLVAREZ GARCÍA

Proyecto de Grado presentado como requisito para optar al título de Especialista en Seguridad Informática

TUTOR:
LUIS FERNANDO ZAMBRANO
233006A_360

ASESOR:
MARTIN CANCELADO

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2018

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

San Juan de Pasto, noviembre de 2018

Dedicatoria

Dedico este trabajo a todas
las personas que han tenido que ver con mi formación
personal y profesional, aquellas personas que siempre han
estado conmigo en momentos importantes o ‘aquellas que
también han estado por determinado tiempo, todos son
importantes, dedico especialmente este trabajo a mi familia,
padres e hijo Samuel

AGRADECIMIENTOS

Quiero agradecer este trabajo a la gobernación de Nariño que me facilito los insumos para poder practicar y trabajar conjunto con ellos , en especial a la secretaria Tic Innovación y Gobierno Abierto, tambien a la UNAD por ser parte de mi formación Profesional.

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

ACCIÓN CORRECTORA: acción adoptada para eliminar las causas de una condición existente indeseable con objeto de minimizar o evitar su reaparición.

ACTIVO: con respecto a la informática, hace referencia a toda información o sistema que la contenga y que sea de importancia para la continuidad del negocio. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

ALERTA: con respecto a la seguridad informática, hace referencia a un aviso de manera formal con el cual se indica que se ha producido un evento adverso relacionado con la seguridad informática, el cual puede desarrollarse hasta que se convierta en un desastre.

AMENAZA: de acuerdo [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

ANÁLISIS DE RIESGOS: de acuerdo [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

ANALIZADOR DE REDES: es **un** aparato electrónico que ofrece la posibilidad de medir, graficar y analizar de las variaciones de voltaje en cada una de las fases, el amperaje y el nivel de armónicos de un sistema eléctrico, además permite bajar la información a un computador a través de un puerto, para su posterior estudio.

ARMÓNICOS: distorsiones de las ondas de tensión y/o corriente de los sistemas eléctricos, debido al uso de cargas con impedancia no lineal, a materiales ferromagnéticos, y en general al uso de equipos que necesiten realizar conmutaciones o switcheo en su operación normal. La aparición de corrientes y/o tensiones armónicas en el sistema eléctrico crea problemas tales como, el aumento de pérdidas de potencia activa, sobretensiones en los condensadores, errores de medición, mal funcionamiento de protecciones, daño en los aislamientos, deterioro de dieléctricos, disminución de la vida útil de los equipos, entre otros.

AISLANTE: material que impide la propagación de algún fenómeno o agente físico. Material de tan baja conductividad eléctrica, que puede ser utilizado como no conductor.

AUDITADO: persona u organización que se audita.

AUDITOR: persona cualificada para realizar auditorías de la calidad; para llevar cabo una auditoría de la calidad el auditor debe estar autorizado para esta auditoría en particular.

AVISO DE SEGURIDAD: advertencia de prevención o actuación, fácilmente visible, utilizada con el propósito de informar, exigir, restringir o prohibir una actuación.

BACKUP: véase Copia de respaldo.

CARACTERÍSTICA: cualquier propiedad distintiva de un elemento o actividad que se puede describir y medir.

CERTIFICACIÓN DE AUDITORES: acto de determinar, verificar y atestiguar las cualificaciones de una persona para realizar auditorías de acuerdo con los requisitos aplicables; la certificación puede ser interna (por la propia organización a la que pertenece el auditor) o externa (por una sociedad autorizada).

CERTIFICACIÓN: procedimiento mediante el cual un organismo expide por escrito o por un sello de conformidad, que un producto, un proceso o servicio cumple un reglamento técnico o una(s) norma(s) de fabricación.

COBIT (Objetivos de Control de las Tecnologías de la Información y Tecnologías Relacionadas) creado en 1992 por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y por el Instituto de Administración de las Tecnologías de la Información (ITGI). Su objetivo promover el desarrollo de políticas y optimas prácticas de la Tecnología de Información.

COPIA DE RESPALDO: copia de los datos de un archivo electrónico en un soporte que posibilite su recuperación. El procedimiento de copia de respaldo tiene como propósito garantizar la reconstrucción en el estado en que se encontraban los datos al tiempo de producirse la pérdida o destrucción a fin de mantener la disponibilidad de la información.

COPIA DE SEGURIDAD: véase Copia de respaldo.

DIRECCIÓN IP: Dirección numérica obligatoria de un dominio 'Internet', que identifica de manera organizada la interfaz de red de un dispositivo que utilice el protocolo IP. Está conformada por una serie cuatro cifras (de 0 a 255) decimales separadas por puntos.

EQUIPO AUDITOR: grupo de personas que realizan una auditoría bajo la dirección de un auditor jefe.

ESPECIFICACIÓN: conjunto de requisitos que tiene que satisfacer un producto o

servicio.

ESPECIFICACIÓN TÉCNICA: documentó que establece características técnicas mínimas de un producto o servicio.

ESTIMACIÓN: una forma de auditoría del sistema de calidad, realizada normalmente para examinar la eficacia del programa de calidad total y su puesta en práctica; la evaluación la realiza normalmente una tercera parte e informa de ella a la alta dirección de la organización.

EVALUACIÓN: acto de examinar un proceso o grupo con respecto a alguna norma y obtener, en consecuencia, ciertas conclusiones.

EVIDENCIA: soporte de una información. La evidencia surge cuando un acontecimiento empírico o los vestigios del mismo la respalden.

EVIDENCIA OBJETIVA: datos que respaldan la existencia o veracidad de algo y que pueden obtenerse por medio de la medición, observación, ensayo/prueba u otros medios.

INDEPENDIENTE: no responsable directamente de la calidad, del coste y/o de la fabricación de los bienes y servicios que se examinan.

INFORME DE AUDITORÍA: es esencialmente un instrumento de comunicación. A través del informe de auditoría el auditor expresa, en forma resumida, su dictamen profesional y las recomendaciones acerca del área auditada.

INSPECCIÓN: conjunto de actividades tales como medir, examinar, ensayar o comparar con requisitos establecidos, una o varias características de un producto o instalación eléctrica, para determinar su conformidad.

LOG: es un registro oficial de eventos durante un periodo de tiempo en particular, es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación. La mayoría de los logs son almacenados o desplegados en el formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. De esta forma cada log generado por un dispositivo en particular puede ser leído y desplegado en otro diferente.

MANTENIMIENTO: conjunto de acciones o procedimientos tendientes a preservar o restablecer un bien, a un estado tal que le permita garantizar la máxima confiabilidad

MÉTODO: modo de hacer con orden una actividad.

NIVEL DE RIESGO: valoración conjunta de la probabilidad de ocurrencia de los accidentes, de la gravedad de sus efectos y de la vulnerabilidad del medio.
NO CONFORMIDAD: falta de cumplimiento de los requisitos especificados; esta definición comprende el término «desviaciones» o la ausencia de una o varias de las características de la calidad o de elementos del sistema de la calidad respecto a los requisitos especificados.

NORMA: documento aprobado por una institución reconocida, que prevé, para un uso común y repetido, reglas, directrices o características para los productos o los procesos y métodos de producción conexos, servicios o procesos, cuya observancia no es obligatoria.

NORMA DE SEGURIDAD: toda acción encaminada a evitar un accidente.

NORMA TÉCNICA COLOMBIANA (NTC): norma técnica aprobada o adoptada como tal por el organismo nacional de normalización.

OBSERVACIÓN: constatación de hechos, realizada en el marco del proceso de auditoría y justificada por evidencias objetivas. Es una conclusión de una auditoría que identifica un punto débil de un sistema de calidad, bien en la definición o en la puesta en práctica; una observación de una auditoría identifica una condición que todavía no está causando una degradación grave de la calidad.

PAPELES DE TRABAJO: son los registros que el auditor mantiene de las técnicas y de los procedimientos seguidos, las pruebas efectuadas, la información obtenida y las conclusiones alcanzadas durante la ejecución de la labor de auditoría.

PROGRAMA DE AUDITORÍA: conjunto de instructivos o procedimientos, lógicamente encadenados que aplicados al examen de un hecho sirve para obtener una conclusión demostrable.

PROCEDIMIENTO DE AUDITORÍA: concepto elemental técnico que, en auditoría, orienta una acción encaminada a determinar una evidencia.

REGLAMENTO TÉCNICO: documentó en el que se establecen las características de un producto, servicio o los procesos y métodos de producción, con inclusión de las disposiciones administrativas aplicables y cuya observancia es obligatoria.

REQUISITO: precepto, condición o prescripción que debe ser cumplida, es decir que su cumplimiento es obligatorio.

RESGUARDO: medio de protección que impide o dificulta el acceso de las personas o sus extremidades, a una zona de peligro.

RETIE O Retie: acrónimo del Reglamento Técnico de Instalaciones Eléctricas adoptado por Colombia. Es un el Reglamento Técnico de Instalaciones Eléctricas - RETIE, que fija las condiciones técnicas que garantizan la seguridad en los procesos de Generación Transmisión, trasformación, Distribución y Utilización de la energía eléctrica. Además, este Reglamento tiene el propósito de prevenir riegos para la vida, la salud, eliminar prácticas que puedan inducir a errores a los consumidores y facilitar la adaptación de las normas técnicas, en referencia, al futuro progreso tecnológico.

RIESGO: condición ambiental o humana cuya presencia o modificación puede producir un accidente o una enfermedad ocupacional. Posibilidad de consecuencias nocivas o perjudiciales vinculadas a exposiciones reales o potenciales.

SEÑALIZACIÓN: conjunto de actuaciones y medios dispuestos para reflejar las advertencias de seguridad en una instalación.

SISTEMA ININTERRUPIDO DE POTENCIA (UPS): sistema que provee energía a cargas críticas unos milisegundos después del corte de la alimentación normal. Durante ese tiempo, normalmente no debe salir de servicio ninguno de los equipos que alimenta.

STORAGE: es una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

TECNOLOGÍA: conjunto de elementos técnicos, herramientas y procedimientos específicos mediante los cuales se puede realizar con eficiencia y eficacia una especialidad o una actividad productiva.

TEST DE PENETRACIÓN o **PENETRATION TESTING:** es un procedimiento de tipo metódico y sistemático con el cual se pretende un ataque real a una red o sistema informático, con el fin de descubrir vulnerabilidades, amenazas y riesgos, con el fin de mitigar los problemas de seguridad existentes.

VERIFICACIÓN: acto de revisar, inspeccionar, ensayar, comprobar, auditar o establecer y documentar de cualquier otro modo si los artículos, procesos, servicios o documentos son conformes con los requisitos especificados.

RESUMEN

El presente proyecto de grado pretende hacer un diagnostico al estado de la seguridad informática en la Gobernación de Nariño , evaluando aspectos que tiene que ver con la norma ISO 27002 que nos dará un marco para poder complementar las actuales políticas de seguridad de la entidad y por ultimo nos permitirá realizar un informe ejecutivo que permita una mejor implementación de políticas de seguridad internas.

Este procesos empieza con unas entrevistas a la secretaria Tic de la gobernación, las cuales nos dan una vista previa de como son los lineamientos de seguridad en este lugar ya que la SECTIC de la gobernación de Nariño es líder en este proceso, allí nos encontramos con el problema inicial , existen unas políticas pero no se aplican además son algo deficientes ya que no cubren todos los aspectos de la normal ISO 27000.

Después se realiza un diagnostico basado en la norma ISO 27000 con todos los integrantes de la secretaria y por ultimo se realiza un levantamiento de activos y su respectiva estimación de impacto, riesgo y amenazas. Con el anterior insumo se establece las respectivas amenazas a la que se encuentra expuesta la gobernación, con lo cual se propone un nuevo documento de políticas de seguridad.

INTRODUCCIÓN

Con la aparición de la computación digital, inició el periodo de más desarrollo tecnológico jamás visto por la humanidad, donde la información se ha convertido en un activo de gran valor para las organizaciones, es primordial garantizar que este activo esté siempre bien custodiado, garantizando su integridad, confidencialidad y disponibilidad en todo momento y lo más resguardado posible de todas las amenazas que hay alrededor, por lo anterior es importante la seguridad informática, pues trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Esta visión de la seguridad informática implica la necesidad de gestión, fundamentalmente gestión del riesgo, donde se implantan medidas preventivas y correctivas que ayuden a eliminar los riesgos asociados o en su caso reducirlos al máximo garantizando así que los servicios informáticos ofrecidos por las empresas e instituciones sean preservados, seguros y confiables.

La seguridad informática en una empresa, consiste en un análisis exhaustivo de todos los sistemas de información, los datos e infraestructura tecnológica que los soporta, lo cual permite dictaminar el estado real de la seguridad informática dentro de la empresa, en el proceso se van a diseñar las pruebas para determinar las vulnerabilidades y amenazas existentes que permitirá evaluar el estado actual en que se encuentra la organización.

Para la realización de este análisis existe una serie de normas ISO/IEC 27000 desarrolladas por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier organización grande o pequeña, pública o privada.

El objetivo de este proyecto es hacer un estudio sobre los aspectos de seguridad informática dentro de la Gobernación de Nariño donde existe una infraestructura tecnológica bastante compleja de datos y redes, por lo cual se propone mediante una auditoria inicial rediseñar las políticas de seguridad informática de la entidad y estudiar cualquier aspecto que se enmarque dentro de las normas ISO 2700-1, para generar un informe de hallazgos después de su debido estudio.

Siendo esta una necesidad vigente de la entidad se cuenta con una aprobación previa para poder realizar esta práctica.

1. TEMA

1.1 TITULO

Rediseño de Políticas y procedimientos de Seguridad Informática para la Gobernación de Nariño.

1.2 LÍNEA DE INVESTIGACIÓN

Gestión Seguridad y control. Esta línea tiene como objetivo, planificar, analizar, diseñar, implantar sistemas de control de información, con el propósito de brindar seguridad de la información en las organizaciones.

1.3 ALCANCE Y DE LIMITACIÓN

Los aspectos que serán evaluados en cuanto a la seguridad informática serán los siguientes:

- -Acceso
- -Cifrado
- -Telecomunicaciones

Estos Aspectos se evaluarán únicamente en el edificio central de la Gobernación en la secretaria Tic Innovación y Gobierno Abierto Ubicada en Calle 19 No. 23-78 - Pasto Nariño Colombia, aunque muchas de las políticas diseñadas y evaluadas pueden ser aplicadas en cualquier sede de la entidad.

1.4 MODALIDAD

Este anteproyecto de trabajo de grado corresponderá a la Modalidad de Trabajo de Aplicado.

2. DESCRIPCIÓN DEL PROBLEMA

2.1. PLANTEAMIENTO DEL PROBLEMA.

La Gobernación de Nariño tiene definido un documento de Políticas de Seguridad de la Información pero estas políticas no han sido difundidas e implementadas lo que ocasiona que los funcionarios de esta entidad realicen acciones inseguras, como por ejemplo:

No cambiar las claves de acceso, no tener un registro de las personas que entran a la Gobernación a excepción de aquellas que llevan portátil, en cuanto a la seguridad en la red de datos los nodos ya están por encima del límite permitido, el edificio por ser patrimonio arquitectónico no permite hacer la adecuación del cableado de acuerdo a normas ISO o ICONTEC, el cableado estructurado del edificio en algunos casos no tiene protección, no cuenta contar con un firewall físico para protección y aseguramiento de la red, en ocasiones los equipos sufren de calentamiento por no encontrarse ubicados en áreas con temperaturas adecuada. Con respecto a los aplicativos web se han presentado ataques de varios tipos entre los cuales encontramos ataques de denegación de servicio a las páginas de la gobernación, suplantación de usuarios en servidores internos en aquellos servicios y aquellos que dan su cara a la nube, para poder plantear un nuevo documento de Políticas de Seguridad Informática en la Gobernación de Nariño, debido a que el actual se queda corto en controles , casi nadie conoce su existencia y no esta implementado.

2.2. FORMULACIÓN DEL PROBLEMA.

- ¿Cómo el rediseño de las políticas y procedimientos basados en el análisis y diagnóstico de la situación actual permitirán mejorar la seguridad informática en la Gobernación de Nariño?

2.3. SISTEMATIZACIÓN DEL PROBLEMA.

- ¿Cuáles son las Políticas y procedimientos de seguridad informática definida y aplicada actualmente en la Gobernación de Nariño?

- ¿Cuál es el estado actual de la Gobernación en cuanto a seguridad informática y que cambios se requieren en las políticas de seguridad informática?

- ¿Cuáles son las vulnerabilidades, amenazas y riesgos en la seguridad informática a que se ve expuesta la gobernación de Nariño?

- ¿Cómo el plan de pruebas ejecutado permitirán evidenciar los riesgos

existentes en seguridad informática de la entidad?

- ¿Cómo diseñar las nuevas políticas de seguridad a partir de los hallazgos confirmados y los controles definidos en cada dominio evaluado?

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Mejorar la seguridad informática mediante el rediseño de las políticas y procedimientos basados en el análisis y diagnóstico de la situación actual en la Gobernación de Nariño

3.2. OBJETIVOS ESPECÍFICOS

- ✓ Conocer la documentación de procesos y procedimientos de manejo de la información, la documentación de políticas de seguridad y determinar los activos tecnológicos y sistemas de información que funcionan en la gobernación de Nariño en la secretaria TIC.

- ✓ Realizar el proceso de análisis y evaluación de riesgos identificando mediante pruebas las vulnerabilidades y amenazas de seguridad a que está expuesta la gobernación de Nariño en la secretaria TIC.

- ✓ Verificar la existencia de controles de seguridad informática y de la información de acuerdo a la norma ISO/IEC 27002 de control interno de seguridad informática

- ✓ Diseñar las nuevas políticas y procedimientos de seguridad informática de acuerdo a los resultados obtenidos del proceso aplicado anteriormente.

4. JUSTIFICACIÓN

La Gobernación de Nariño siendo la más importante entidad administrativa en el departamento, actualmente cuenta con una infraestructura tecnológica amplia conformada por software, hardware, sistemas de información, comunicaciones, tecnologías de la información y plataformas tecnológicas en línea entre otros, se considera necesario que la entidad establezca acciones que garanticen la seguridad física y lógica de sus activos informáticos y que le permita valorar los riesgos informáticos que han sido identificados mediante el análisis de seguridad en toda su infraestructura tecnológica.

Teniendo en cuenta lo anterior, es importante realizar este proyecto ya que , las actuales políticas se quedan cortas en controles, casi nadie las conoce y no se encuentra en uso por parte de la entidad, con el Rediseño de Políticas y procedimientos de seguridad, los funcionarios conocerán la importancia y la sensibilidad de la información y sobre los métodos para asegurar el buen uso de los recursos informáticos, manteniéndolos libre de peligros, daños y riesgos, además tanto los usuarios internos como externos contarán con una información confidencial, integra y disponible al acceder a los sistemas de información y a las páginas web de la gobernación, dicho esto es necesario tener unas políticas de seguridad informática bien concebidas y efectivas que puedan proteger la inversión y los recursos de información de la entidad.

Con este proyecto la Gobernación de Nariño podrá mejorar la eficiencia gubernamental, minimizar los riesgos asociados a daños y asegurar que se cumplan las funciones misionales de la entidad estableciendo políticas de seguridad y procedimientos de seguridad informática dando cumplimiento a la Estrategia de Gobierno en Línea (GEL) en cuanto al Componente TIC para Seguridad y Privacidad de la información.

6. MARCO DE REFERENCIAL

6.1 MARCO CONTEXTUAL

El Palacio de la Gobernación de Nariño se encuentra ubicado:

Calle 19 No. 23-78 - Pasto-Nariño-Colombia.

Ubicación Georeferencial: Latitud:1°12N Altitud:2527msnm

Horario de Atención: Lunes a Viernes 8:00am - 12:00m y 2:00pm - 6:00pm.

Línea gratuita de Atención: 018000949898

Pbx: (57)2 7235003- (57)2 7233600- (57)2 7232916- (57)2 7235329- (57)2 7235004- (57)2 7223846- (57)2 7235005.

Contáctenos (Correo Electrónico): contactenos@narino.gov.co

MISIÓN

La Gobernación de Nariño, como institución pública, está comprometida con el desarrollo regional bajo los principios de justicia social, democracia política, desarrollo humano sostenible, equidad de género, reconocimiento y protección de la diversidad étnica, respeto por derechos humanos y participación ciudadana; propiciando la concurrencia, complementariedad y subsidiaridad con las entidades territoriales de su jurisdicción y la Nación, coordinando esfuerzos con el sector público, privado y sociedad civil.

VISIÓN

En el año 2019, El departamento de Nariño es un referente mundial de Nuevo Gobierno que se fundamenta en la participación, colaboración e innovación y avanza en la construcción de la Paz Territorial. el Cierre de Brechas Sociales y la Sostenibilidad Ambiental. Es un territorio integrado a nivel regional, nacional e internacional que trabaja por el logro de propósitos comunes y genera una gobernanza multinivel para la construcción corresponsable de derecho Humano Sostenible.

Figura 1. Foto

Fuente: "http://www.flickr.com/photos/udenardigitalfotos/5184278187/"

HISTORIA DEL PALACIO DE GOBIERNO DE NARIÑO

El lugar que hoy ocupa el edificio del PALACIO DE GOBIERNO DE NARIÑO, presenta históricamente la presencia de diferentes construcciones con diferente función social.

Hasta 1581 fue la base de una vivienda particular de propiedad del presbítero Andrés Moreno Zúñiga quien la dono con el fin de convertirla en la sede del Convento de Las Conceptas, según lo refiere el historiador Sergio Elías Ortiz:

“Una vez decididos los vecinos de San Juan de Pasto a tomar la fundación del convento de Concepcionistas a su cargo, en lo primero en que pensaron fue en la ampliación y reconstrucción de una casa que para efecto dono el presbítero prebendano Andrés Moreno Zúñiga, a quien es preciso señalar como el verdadero fundador de dicho convento…”.

A continuación la comunidad de vecinos de Pasto se dispone a interponer sus propios recursos para contar con un Convento de Religiosas:

“La necesidad de la obra no daba espera, sino antes bien urgía darles principio, pues que las doncellas principales por su falta de dote no podían casarse como su calidad lo requería y que lo que la prudencia aconsejaba en tal emergencia era meterlas a un Convento”.

Durante un año, la vivienda destinada para el Convento de religiosas de clausura sufrió remodelación y adaptación en estructura arquitectónica. Su extensión era considerable si se tiene en cuenta que para aquel entonces la construcción ocupaba más “De dos tercios de la manzana en que hoy se encuentra el edificio de la Gobernación.”

La historia lo sostiene así: “La obra de reparaciones y adaptación del edificio que dicho sea de paso, era una fábrica de construcción pesada en parte de mampostería y en parte de tierra apisonada y que ocupaba más de dos tercios de la manzana en que actualmente se levanta el edificio de la Gobernación del Departamento, quedo concluida en menos de un año, pues principalmente los trabajos en 1987 estuvo terminada a fines de septiembre de 1588, menos la ermita, que debía servir para uso público y para actos religiosos del convento la cual se concluyó 4 meses más tarde”

El 3 de octubre de 1588, se fundó el Ministerio de la Pura y Limpia Concepción de Nuestra Señora, contando por aquel entonces con 7 damas, 6 doncellas y 1 viuda. La ceremonia de clausura todavía la recuerda la historia; “El Vicario de Bracamonte puso cerrojo a las puertas y se guardó las llaves a la vista del numeroso concurro de habitantes que presencio la ceremonia en señal de que las monjas se quedaban enclaustradas”

Es en febrero de 1864, cuando en aplicación del decreto de desamortización de bienes de manos muertas, las conceptas fueron obligadas por acciones de facto, a cambiar de domicilio, porque se había por orden superior que la edificación que ocupaban pasaría ahora a formar parte del patrimonio de la Republica”. (S.E. ORTIZ: 1929: 6L-62). Del paso de las Conceptas, quedo el recuerdo y el nombre de la calle, conocida popularmente como “La calle de las Monjas”. La construcción o el local sirvió a partir de entonces para diferentes fines. Al respecto dice Silvia Narváez que desde 1881, se había previsto que allí se levantaría un colegio, que siempre quedó solo como un proyecto.

“Como proyecto pendiente estaba el de levantar una construcción para que sirviera de sede de un colegio de señoritas. Para tal fin el gobierno tenía cedido el lote que contiene los vestigios del antiguo Convento de las Monjas”.

A finales del Siglo XIX y principios de XX, en el lote en mención, se formó una

pequeña plaza de mercado con toldos y fogones al aire libre, lugar de encuentro y reunión, anexa a la Plaza de la Constitución.

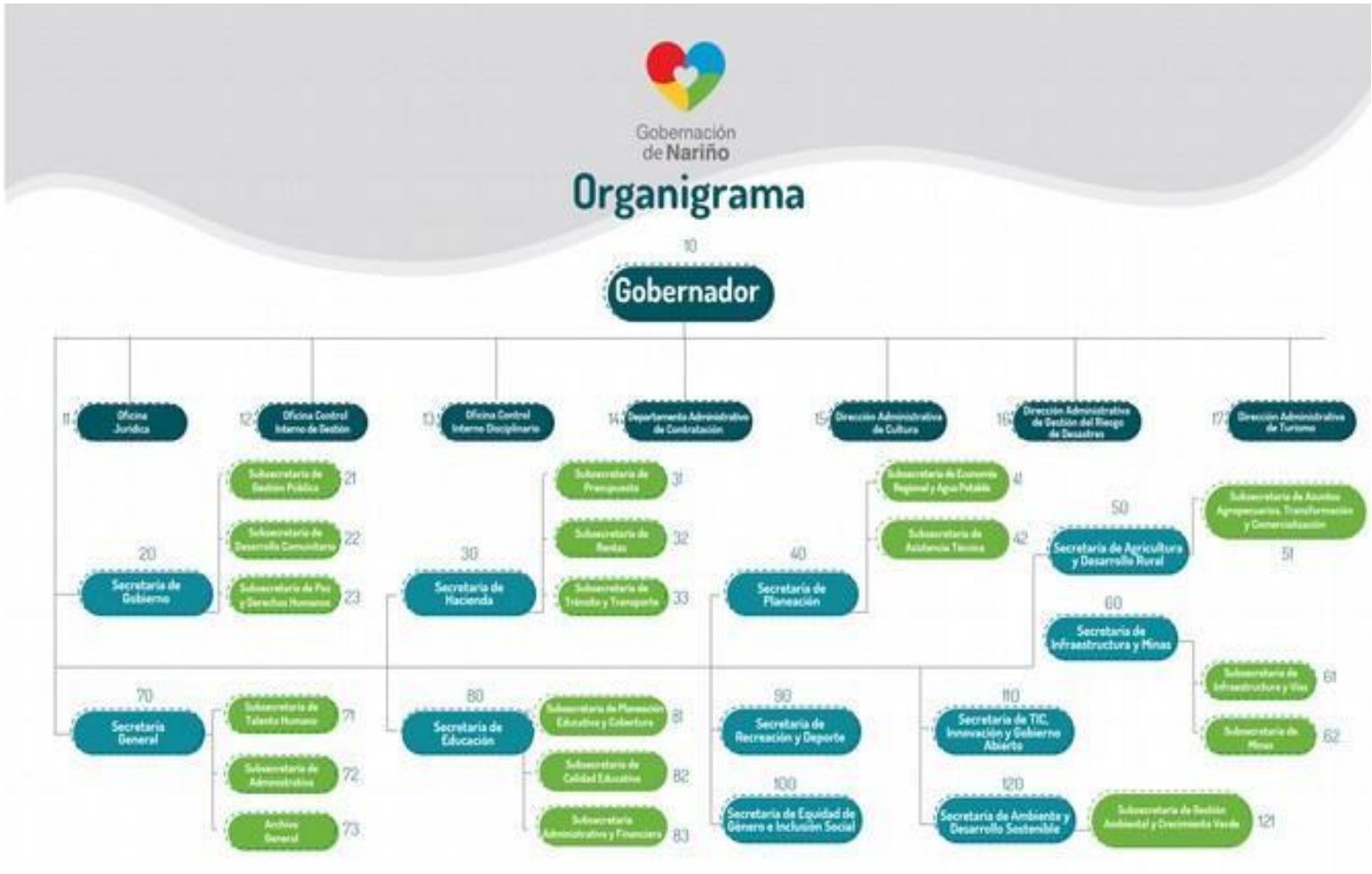
En la plaza mayor de la Colonia, todavía se podía apreciar, hacia 1884, que las viviendas que enmarcaban el entorno eran: “casas porticadas” poseedoras de amplios aleros y corredores”.

En 1904, bajo la presidencia del General Rafael Reyes se erige el noveno departamento NARIÑO, en homenaje al precursor de la independencia Antonio Nariño y por efectos de la ley 1 del mes de agosto del mismo año en segregación del antiguo departamento del Cauca. El primer gobernador de Nariño fue Julián Buchely Ayerbe, quien tomo posesión del cargo ante el doctor José Maria Navarrete en su calidad de Presidente del Tribunal del Sur, en la Casa de la calle 19 con carera 26, sede actual de la Casa de Cultura de Nariño, ante la situación presente de no contar en la fecha con sede propia del Gobierno Departamental.

Figura 2. Gobernación De Nariño

Fuente: Gobernacion de Nariño, www.narino.gov.co

Figura 3. Organigrama Gobernación de Nariño



6.2 MARCO CONCEPTUAL

Dentro de las variables que se va a medir con el desarrollo del proyecto se encuentran las características de la información que se contemplan en la ISO 27001, las cuales son:

Confidencialidad

Es la propiedad de la información que nos dice que los datos deben estar disponibles y no ser divulgada a personal no autorizado.

Integridad

Es la propiedad de la información que consiste en la salvaguardia, exactitud e integridad de los datos contenidos en cualquier medio de almacenamiento

Disponibilidad

Es la propiedad de la información la cual dice que siempre debe estar disponible y utilizable cuando sea requerido

Según Magerit agrega estas dos características a la información:

Autenticidad

Propiedad que consiste en que una organización u empresa es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Trazabilidad

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia.

6.3 MARCO LEGAL

Colombia ha sido uno de los pioneros en Latinoamérica en cuanto a la legislación de seguridad informática se refiere con la puesta en marcha de la ley 1273 del 5 de enero de 2009.

“Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"• y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". 1.

Con la ley 1273 del 5 de enero del 2009, se crea una norma encaminada a proteger uno de los activos más importantes de las empresas como son los datos informáticos y sistemas de información, entre los delitos que tipifica se encuentra los siguientes:

Artículo 269A: Acceso abusivo a un sistema informático toda persona que acceda a un sistema informático y permanezca en el sin autorización.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación incurrir en este delito toda persona que sin estar autorizado no permita el acceso a una red, sistema informático o los datos informáticos.

Artículo 269C: Interceptación de datos informáticos incurrirá en este delito toda persona que sin tener orden judicial intercepte ya sea en su origen, trasmisión, destino o al interior de un sistema informático los datos informáticos.

Artículo 269D: Daño Informático este delito contempla que toda persona quien no tenga la debida autorización que borre, altere, suprima o modifique datos informáticos o dentro de un sistema sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso aquí se contempla como delito la producción, tráfico, venta, distribución importación o exportación de software considerado como dañino o malicioso

Artículo 269F: Violación de datos personales, incurrirá en este delito toda persona que obtenga beneficio para sí mismo o para terceros de información personal contenida en bases de datos, ficheros.

Artículo 269G: Suplantación de sitios web para capturar datos personales, este delito contempla el diseño, creación distribución o venta de sitios web, enlaces o ventanas emergentes diseñados para capturar ilegalmente datos personales.

Artículo 269I: Hurto por medios informáticos y semejantes, incurrirá en este delito toda persona que a través de un sistema informático, red de un sistema electrónico o telemático cometa hurto.

Artículo 269J: Transferencia no consentida de activos. Este delito contempla la trasferencia no autorizada de activos en perjuicio de otra persona, mediante manipulaciones de tipo informático.

Entre los delitos más comunes en Colombia se encuentran:

- Hurto por medios informáticos y semejantes.
- Uso de software malicioso

- Violación de datos personales
- Acceso abusivo a un sistema informático

Ley 1150 de2007

Medios y Sistemas Electrónicos

Introduce modificaciones a la Ley 80 de 1993, y dicta disposiciones generales aplicables a toda contratación con recursos públicos. Establece que las actuaciones, la expedición de los actos administrativos, los documentos, contratos y en general los actos derivados de la actividad precontractual y contractual, podrán tener lugar por medios electrónicos.

Ley 1341 de 2009

Establece que la Comisión de Regulación de Telecomunicaciones -CRT, de que trata la Ley 142 de 1994, se denominará Comisión de Regulación de Comunicaciones (CRC), Unidad Administrativa Especial, con independencia administrativa, técnica y patrimonial, sin personería jurídica adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones.

Ley 527 de 1999

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

COMERCIO ELECTRÓNICO

Reglamentación

Aplicación jurídica de los mensajes de datos, art. 6 a 14. Comunicación de mensajes de datos, art. 14 a 25.

Firmas Digitales

Concepto, Características y Uso

Ámbito de aplicación, art. 1. Definiciones, art. 2. Firmas digitales, certificados y entidades de certificación, art. 28 a 42.

Mensajes De Datos

Reglamentación

Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación. Dicta disposiciones sobre la aplicación de los requisitos jurídicos de los mensajes de datos y comunicación de los mensajes de datos.

Telecomunicaciones

Mensajes de Datos y Documentos Electrónicos

Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación. Dicta disposiciones sobre la aplicación de los requisitos jurídicos de los mensajes de datos y comunicación de los mensajes de datos.

Ley 37 De 1993

ARTÍCULO 5. INVERSIÓN EXTRANJERA EN TELECOMUNICACIONES.

La inversión extranjera, en las materias reguladas por la presente ley, valor agregado, servicio e infraestructura satelital, se regirá por la Ley 9a de 1991 (Por la cual se dictan normas generales a las que deberá sujetarse el Gobierno Nacional para regular los cambios internacionales y se adoptan medidas complementarias) y las normas que la modifiquen o complementen y no tendrán más limitaciones que las señaladas en esas disposiciones.

LEY 72 DE 1989

Por la cual se definen nuevos conceptos y principios sobre la organización de las telecomunicaciones en Colombia y sobre el régimen de concesión

6.4 MARCO REFERENCIAL METODOLOGICOANTECEDENTES

Para el proyecto se tendrán en cuenta los siguientes antecedentes:

El proyecto titulado [1] DISEÑO DE POLÍTICAS Y CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN EN PEQUEÑAS EMPRESAS CON REDES SOHO EN EL SECTOR TRANSPORTE DE BOGOTÁ. Presentado por ANDREA MARCELA PULIDO CHADID, PAULO CÉSAR RINCÓN ALBARRACÍN, OSCAR MAURICIO VELÁSQUEZ ACOSTA en la UNIVERSIDAD DE SAN

BUENAVENTURA en el año 2010. [1]

El proyecto se centra en el diseño de políticas y controles para las empresas del sector transporte con redes SOHO en Bogotá: es por esto que se realiza un estudio técnico que establece normas, políticas y controles de seguridad de la información en el sector de transporte de las pequeñas empresas con redes SOHO en Bogotá, surge de la necesidad de que estas empresas adquieran una protección para su información que pueda estar almacenada en bases de datos o sea transmitida mediante redes de comunicación.

El proyecto titulado [2] MODELO PARA LA IMPLEMENTACIÓN DEL SISTEMA GENERAL DE SEGURIDAD INFORMATICA Y PROTOCOLOS DE SEGURIDAD INFORMÁTICA EN LA OFICINA TIC DE LA ALCALDÍA MUNICIPAL DE FUSAGASUGÁ, BASADOS EN LA GESTIÓN DEL RIESGO INFORMÁTICO. Presentado por ANA MILENA PULIDO BARRETO, JENITH MARSELLA MANTILLA RODRIGUEZ en la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA en el año 2016.[2]

Este proyecto se considera importante y prioritario ya que contribuye al fortalecimiento de los procesos, actividades y servicios que realiza la Oficina TIC de la Alcaldía de Fusagasugá, así como el cumplimiento de lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Modelo de Seguridad y Privacidad de la Información (MSPI) que busca una vez implementado y con índice de madurez alto que la entidad inicie con el requerimiento del Sistema Administrativo de Seguridad de la Información para Gobierno en línea (SASIGEL), de esta manera se dará cumplimiento de los principios definidos en la Ley 1341 de 2009 y en la Estrategia de Gobierno en línea, que corresponden a la protección de la información del individuo y la credibilidad y confianza en Gobierno en línea. La Alcaldía Municipal de Fusagasugá contará con protocolos de seguridad y un Modelo para la implementación del Sistema Gestión de Seguridad de la información (SGSI), que estará alineado a la metodología del ciclo PHVA para realizar la implementación de

[1] PULIDO, Ana y MANTILLA, Jenith. Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. Tesis previa a la obtención del título de Especialización de Seguridad en Informática. Fusagasugá. Colombia: Universidad Nacional Abierta y a Distancia, 2016.

[2] PATIÑO, Luis. Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR. Tesis previa a la obtención del título de Especialización de Seguridad en Informática. San Juan de Pasto. Colombia: Universidad Nacional Abierta y a Distancia, 2014.

un Sistema de Gestión de Seguridad de la Información que ha sido señalado en el manual de la estrategia de Gobierno en Línea (GEL) en su versión 3.0.

El proyecto titulado [3] PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA CORPORATIVA, PROPOLSINECOR. Presentado por LUIS OLMEDO PATIÑO ALPALA en la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD" en el año 2014. [3]

Este proyecto se realiza con el fin de valorar los activos informáticos, analizar las vulnerabilidades, amenazas y riesgos existentes en la seguridad informática, que puedan afectar los recursos y prestigio de la compañía; para contrarrestar y mitigar los riesgos en seguridad informática, se diseña una propuesta de actualización, apropiación e implementación de Políticas claras de Seguridad de la Información, acordes al negocio y actividades de la compañía, para ser aprobadas por la alta gerencia, difundidas e implementación por PROPOLSINECOR. En este orden de ideas, con el presente proyecto se pretende actualizar, apropiarse y establecer políticas de seguridad de la información, que protejan los activos de información, teniendo en cuenta la infraestructura y los últimos aplicativos o procesos de manejo de información implementados en la compañía, para ello se estudiará el marco teórico referente al tema, se identificarán activos de información, vulnerabilidades y amenazas en la seguridad informática, para estructurar una matriz de riesgos que permitirá determinar acciones de solución a corto, mediano y largo plazo, con el propósito de eliminar o mitigar el riesgo informático y salvaguardar activos de información que son el eje principal de toda gestión de seguridad de la información.

El proyecto titulado [4] EVALUACIÓN DE SEGURIDAD A SISTEMAS DE INFORMACIÓN EN CUANTO A ATAQUES MALICIOSOS CON BASE EN NORMATIVIDAD, TENDENCIAS, IMPACTO Y TÉCNICAS VIGENTES PARA AMBIENTES EMPRESARIALES A NIVEL NACIONAL. Presentado por DAVID HERNANDO ALONSO TORRES en la UNIVERSIDAD DE LA SABANA en al año 2014. [4]

En este proyecto se quieren compilar procedimientos consolidados en una

---

[3] PROPUESTA DE ACTUALIZACIÓN, APROPIACIÓN Y APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN UNA EMPRESA CORPORATIVA, PROPOLSINECOR. Presentado por LUIS OLMEDO PATIÑO ALPALA en la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD" en el año 2014

[4] ALONSO, David. Evaluación de seguridad a sistemas de información en cuanto a ataques maliciosos con base en normatividad, tendencias, impacto y técnicas vigentes para ambientes empresariales a nivel nacional. Tesis previa a la obtención del título de Ingeniero en Informática modalidad independiente. Chía-Cundinamarca. Colombia: Universidad de la Sabana, 2014

metodología, apoyados con técnicas y herramientas de Ethical Hacking específicas, que sirva como guía para las empresas en el desarrollo e implementación de sistemas seguros, y así contrarrestar dichas vulnerabilidades; contribuir para que los ambientes informáticos en las empresas públicas y privadas en el país, cuenten con lo necesario de acuerdo a la normatividad y legislación vigente, para lograr un adecuado nivel de seguridad informática. El resultado será una investigación con el estado actual de los ataques maliciosos más comunes y el impacto que generan en las organizaciones en cuanto a robo o fuga de información, clasificación que será de acuerdo a unos criterios definidos a lo largo de la misma, apoyados en la legislación nacional. De esta forma, como valor agregado, generar una guía metodológica apoyada en las técnicas y procedimientos de Ethical Hacking y Pruebas de Penetración bajo software libre, para la prevención, detección corrección y buenas prácticas del Top. 5 de Vulnerabilidades clasificadas previamente, junto a una campaña de sensibilización que le dará relevancia social a la misma, todo aplicable a cualquier empresa sin importar el sector económico a nivel nacional.

6.5 METODOLOGÍAS DE GESTIÓN DE RIESGOS

6.5.1 ISO/IEC 27001:2013. La norma ISO 27001 hace parte de la familia de normas ISO27000, la cual da lineamientos acerca de como se implementa las políticas de seguridad en una entidad, por ejemplo que documentos se requieren inicialmente, procesos que se deben de tener en cuenta y los debidos procesos de auditoria continua para su cumplimiento

6.5.2 ISO/IEC 27002:2013. Su nombre completo es ISO/IEC 27002:2013, es una norma internacional emitida por la ISO (Organización Internacional de Normalización) en conjunto con IEC (Comisión Electrotécnica Internacional. Esta norma se divide en 14 dominios de la seguridad de la información y establece controles para cada uno, Es compatible con la norma ISO/IEC 27001 y fue diseñada para servir de soporte para la implementación de un SGSI con perfil de gestión de riesgos.

Su versión más reciente fue publicada en el año 2011 y la primera versión se publicó en el año 2008, antiguamente era conocida como la norma ISO13335-2 Gestión de seguridad de la información y la tecnología de las comunicaciones.

6.5.3 Metodología Magerit. En esta metodología se tiene en cuenta, los riesgos que se derivan del uso de las tecnologías de la información, todas las tecnologías buscan el análisis de riesgos para saber qué tan seguros son o el grado de inseguridad que presentan, por eso es necesaria una aproximación metódica fiable que no dependa solamente del analista.

Se puede encontrar los siguientes objetivos en esta fase

- Tomar conciencia de los riesgos a los que se está expuesto y a las necesidades de aportar una solución confiable.

- Verificar el mejor método analizando los riesgos que nos ofrece el uso de las TIC'S.

- Desarrollar un control para mantener los riesgos bajo nuestro control sin la necesidad de depender de la persona encargada del análisis.

- Siempre se tiene que tener presente los procesos que se hagan y deben conllevar a un proceso de evaluación, auditoria, certificación dependiendo de le caso que se esté manejando, brindando buenos informes dependiendo de los hallazgos y conclusiones de las actividades todos esto representa de un gran

valor para los activos de la empresa para lo que se debe tener en cuenta las salvaguardas existentes en relación al riesgo que se pueda afrontar todo esto para proteger al sistema de posibles amenazas.

En la actualidad, todas las empresas se han venido incluyendo en el mundo de la tecnología , todo esto para no quedarse atrás en el ámbito competitivo laboral para esto se hace necesario que todas las empresas tengan una buena organización y que utilice la tecnología para tener comunicación en un sistema en red de datos obteniéndola mejor administración de los recursos de la empresa, para todo este proceso de manejo de la red la empresa necesita ser auditada y obtener una evaluación eficiente y eficaz tanto en la parte física como lógica en todo el diseño de la red , instalaciones, cableado estructurado, ups, cuartos de comunicaciones, centros y equipos de cómputo , teniendo en cuenta lo mencionado anteriormente se hace necesario tener un plan estratégico y corporativo que genere a la empresa seguridad y confiabilidad en todo el entorno que se maneja

7. METODOLOGÍA

7.1 METODOLOGÍA DE INVESTIGACIÓN

El proyecto que se va a desarrollar es de enfoque cuantitativo, ya que se pretende medir las variables de seguridad Informática.

El proyecto tendrá los siguientes tipos de investigación:

- Exploratoria por cuanto se pretende descubrir las vulnerabilidades amenazas y riesgos en la seguridad informática de la Gobernación.

- Descriptiva porque el proyecto presenta medir confiabilidad, disponibilidad y confidencialidad de la información en cuanto a la seguridad.

Universo y muestra

El universo lo conforman alrededor de 400 usuarios internos que integran la planta de trabajo, distribuido entre personal de planta y contratistas, para la muestra se seleccionarán los usuarios que tengan mayor experiencia en el manejo y el estado de seguridad informática de la Gobernación los cuales son los funcionarios de La secretaria Tic de la Gobernación que son alrededor de 25 personas para algunas encuestas y algunos usurios específicos como se me mencionan a continuación:

- Profesional Universitario Secretaria TIC

- Administrador web.

- Encargado de Servidores

- Área soporte y mantenimiento

Fuentes de Recolección de la Información

- Libros

- Artículos

- Páginas web

Técnicas e instrumentos

- Entrevistas, se aplicaran entrevistas al coordinador de la Secretaria Tic en su

división de Soluciones TI

- Cuestionarios para confirmar la existencia de riesgos en la red, aplicativos web, base de datos.

- Listas de chequeo para determinar que controles existen dentro de la seguridad informática.

- Pruebas para confirmar el estado de la infraestructura tecnológica.

7.2. METODOLOGÍA DE DESARROLLO

- **Objetivo 1:** Conocer la infraestructura tecnológica de la gobernación para verificar las vulnerabilidades, riesgos y amenazas existentes.

Actividades:

- Realizar una visita de campo para conocer los aspectos a evaluar

- Solicitar la documentación de los procesos y procedimientos de manejo de información que se llevan a cabo en la entidad.

- **Objetivo 2:** Generar documentos de Políticas de Seguridad Iniciales así como sus respectivos anexos conjunto a la constitución del comité Tic que tendrá dentro un comité específico para los temas de Seguridad de La Información

Actividades:

- Estudio de Actuales Políticas
- Estudio de Referentes de Políticas de Seguridad Informática
- Normas ISO 27000
- MAGERIT
- COBIT
- Rediseño de Políticas Actuales
- Creación de Nuevos Anexos a políticas de Seguridad Informática

- **Objetivo 3**: Elaborar el plan de auditoría, diseñar los instrumentos y el plan de pruebas que se ejecutará sobre los activos informáticos.

Actividades:

- Determinar los puntos que serán evaluados.
- Identificar y seleccionar los métodos, pruebas y procedimientos necesarios.

- **Objetivo 4:** Ejecutar las pruebas y aplicar los instrumentos que permitan

evidenciar las vulnerabilidades y confirmar los hallazgos de seguridad existentes.

Actividades

- Ejecutar las acciones programadas.
- Aplicar las pruebas e instrumentos seleccionados.
- Elaborar el dictamen preliminar.
- Organizar los papeles de trabajo de la auditoria

- **Objetivo 5:** Mostrar los resultados en el informe final.

Actividades

- Examinar la información y los resultados obtenidos en las pruebas.
- Preparar el dictamen final
- Presentar el informe de rediseño de políticas de seguridad informática a la dirección de la Gobernación.

8. DESARROLLO DE PROYECTO

8.1 CRONOGRAMA

Cuadro 1. Cronograma Actual Planteado

ACTIVIDAD	ENERO				FEBRERO				MARZO				ABRIL				MAYO			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Vista preliminar al área que será evaluada.																				
Evaluación de Documentos de Seguridad de la Gobernación																				
Entrevistas de Seguridad al Área TIC'S de la Gobernación																				
Determinación de Aspectos más relevantes y estudio de falla de seguridad de la Gobernación																				
Identificar Metidos Necesarios para las pruebas a ejecutar en los aspectos anteriormente establecidos																				
Levantamiento de Información Inicial en Dependencias																				
Ejecución de Plan de Trabajo y Pruebas																				
Elaboración de Informe Técnico Elaboración de Informe Ejecutivo																				

8.2 LEVANTAMIENTO INICIAL DE INFORMACIÓN

Este proyecto inicia en noviembre del 2017 donde se hace una investigación previa en la gobernación de Nariño acerca de la información relacionada con la seguridad de la información, inicialmente se plantean algunas entrevistas con el personal de la secretaria Tic Innovación y gobierno abierto quienes son los encargados de la infraestructura tecnológica de la Gobernación, en estas entrevistas realizadas en la Gobernación de Nariño, se entrevistó a la ingeniera Ana Julia Cárdenas quien nos suministra la información actual referente a políticas de Seguridad de la Información que incluye 3 ítems

- Políticas de la Seguridad de la Información(Ver Anexo A)
- Inventario de Activos de la Información 2015 (Ver Anexo B)
- Manuales de Procesos de la Secretaria Tic (Ver Anexo C)
- Mapas de Red Desactualizados (Ver Anexo D)

Este primer acercamiento a la secretaria Tic nos llevó a identificar los elementos iniciales sobre los cuales se pueden partir para realizar una auditoría a la Gobernación como aspecto Inicial se hizo algunas entrevistas a los funcionarios de la Gobernación, entre ellos están

1. Funcionario Encargado de Pagina web y plataformas
2. Funcionarios Encargados de Soporte Técnico y Redes

8.3 ANALISIS INICIAL ENTREVISTAS

8.3.1 seguridad física y lógica

SITUACIÓN ACTUAL: Durante la revisión, hemos observado lo siguiente:

- No existe una vigilancia estricta en la secretaria TIC de la GOBERNACIÓN DE NARIÑO por personal de seguridad dedicado a este sector.
- No existe un puesto o cargo específico para la función de seguridad Informática.
- Falta de alarmas de seguridad.

SUGERENCIAS

A los efectos de minimizar los riesgos descritos, se sugiere:

- Establecer guardia de seguridad, durante horarios no habilitados para el ingreso en la secretaría Tic de la Gobernación De Nariño

- Instalar alarmas como sugerencia de seguridad.

EFECTOS Y/O IMPLICACIONES PROBABLES POR LAS DEFICIENCIAS

- Si no hay un guardia de seguridad en el área informática en horarios inhabilitados personas con mala intención podría infiltrarse y robar información muy valiosa incluyendo los equipos de cómputo también.

- Si no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las amenazas esta se ve afectada a estar en riesgo de pérdida de información procesada causado por infiltración de manos terceras.

- Por falta de alarmas de seguridad la persona que intente infiltrarse y tomar lo ajeno lo hará de una forma más segura en el momento que intente robar el Área de Proceso de Gestión TIC de la Gobernación De Nariño

8.3.2 Plan de prevención y contingencias

SITUACION ACTUAL: En el transcurso de nuestro trabajo hemos observado lo siguiente:

- Ausencia de un Plan de Contingencia debidamente formalizado en la secretaria Tic de la Gobernación De Nariño

- No existen normas y procedimientos que indiquen las tareas manuales e informáticas que son necesarias para realizar y recuperar la capacidad de procesamiento ante un eventual problema (desperfectos de equipos, incendios, cortes de energía con más de una hora), y que determinen los niveles de participación y responsabilidades del área de sistemas y de los usuarios.

- Ausencia de un plan de prevención en desastres en la secretaría Tic de la Gobernación De Nariño.

SUGERENCIAS

- Establecer un plan de contingencia escrito, en donde se establezcan los procedimientos manuales e informáticos para restablecer la operatoria normal de la organización y establecer los responsables de cada sistema.

- Efectuar pruebas simuladas en forma periódica a efectos de monitorear el desempeño de los funcionarios responsables ante eventuales desastres.

8.4 VISITAS PARA LEVANTAMIENTO DE INFORMACIÓN

Una vez hecha esta entrevista se hace una análisis a los activos de la información entregados por la Gobernación de Nariño(Ver Anexo B) y se llega a la conclusión de que ya son dos años desde el ultimo levantamiento de información inclusive cuando se realizó este levantamiento de activos en el 2015 la secretaria Tic no estaba creada sino que era en ese momento la Oficina de Sistemas la que realizo ese inventario. Por lo tanto se entra en la necesidad de actualizarlo, paralelo a este proceso también la entidad entra a realizar el Plan Estratégico de Tic o PETIC el cual se adjudica a un tercero cuya finalidad es hacer un inventario del parque informático de la entidad, aprovechando este levantamiento de información nos unimos a este proceso que tiene el siguiente cronograma y que se publicó en la intranet de la gobernación de Nariño

Tabla 1. Levantamiento de Activos 2015

Nombre del Procedimiento	Nombre del Activo	Descripción / Observaciones
Talento Humano	MANUAL DE FUNCIONESS	Coordinar y velar por el desarrollo integral del talento humano de los servidores públicos del nivel central de la gobernación
	CERTIFICACIONES LABORALES	
	BONOS PENSIONALES	
	DERECHOS DE PETICION	
	SYSMAN	
	MODULO DESPRENDIBLES DE PAGO DE NOMINA	
	CORREPONDENCIA ENVIADA Y RECIBIDA PROPIA	

	DE LA OFICINA (Oficios Internos, Memorandos entre otros)	
ADMINISTRATIVA	PLAN DE COMPRAS	Realizar la adquisición, suministro y control de los elementos necesarios para el funcionamiento administrativo de las dependencias de la Gobernación.
	SECOP	
	AUTORIZACIONES	
	CORREPONDENCIA ENVIADA Y RECIBIDA PROPIA DE LA OFICINA (Oficios Internos, Memorandos entre otros)	
ARCHIVO	TODA LA CODUMENTACION GENERADA POR LAS DEPENDENCIAS DE LA GOBERNACION	Dirigir la actividad del Archivo Departamental, con eficiente aplicación de los sistemas, normas y procedimientos archivísticos para la administración de los documentos.
	DOCUMENTACION DE LAS ENTIDADES QUE SE HAN LIQUIDADO: IDATT, LICORERA	
	HISTORIAS LABORALES	
	BASE DE DATOS	
	CORREPONDENCIA ENVIADA Y RECIBIDA PROPIA DE LA OFICINA (Oficios Internos, Memorandos entre otros)	
OFICINA TICS	SERVIDORES	Administrar la Red de Datos, Sistemas de Información, elementos y servicios de tecnología implementados en la entidad, mediante la utilización de herramientas y estrategias adecuadas, para garantizar que los
	CENTROS DE CABLEADO	

	SWITCHES	recursos informáticos sean productivos y capaces de satisfacer las necesidades de procesamiento, almacenamiento y transmisión de información, de man era eficiente y segura, con una planeación adecuada. [5]
	CORREPONDENCIA ENVIADA Y RECIBIDA PROPIA DE LA OFICINA (Oficios Internos, Memorandos entre otros)	

Donde podemos evidenciar que la secretaria Tic todavía no estaba creada, y que los activos no fueron debidamente evaluados, hay que tener en cuenta que centro de cableado y equipos de red actualmente no hacen parte de secretaria tic sino de Secretaria general.

[5]

Figura 4. Banner Levantamiento de información

Fuente: Gobernación de Nariño tomada de http://intranet.nariño.gov.co/index.php/2014-01-31-17-55-57/circulares/1821-levantamiento-de-informacion-para-creacion-de-plan-estrategico-de-tic-petic

Cuadro 2. Cronograma de Visitas Levantamiento de Activos de la Información Gobernación de Nariño

DEPENDENCIA	FECHA	DIRECCION
DESPACHO DEL GOBERNADOR	14 de Febrero	PRINCIPAL
OFICINA DE PRENSA Y COMUNICACIONES	14 de Febrero	PRINCIPAL
OFICINA SECCIÓN DE COOPERACIÓN INTERNACIONAL	14 de Febrero	AMA PASTO
OFICINA DE CENTRO DE INNOVACIÓN SOCIAL - CISNA	14 de Febrero	CASONA TAMINANGO
PROGRAMA SEGURIDAD ALIMENTARIA	14 de Febrero	PRINCIPAL
DEPARTAMENTO ADMINISTRATIVO CONTRATACION	15 de Febrero	EDIFICIO LOTERIA
DIRECCION ADMINISTRATIVA JUNIN BARBACOAS	16 de Febrero	SEGIS
DIRECCIÓN ADMINISTRATIVA DE CULTURA	16 de Febrero	CASONA TAMINANGO
PINACOTECA	16 de Febrero	CRA 25 CON 19
BANDA	16 de Febrero	CONCHA ACUSTICA
DIRECCION ADMINISTRATIVA DE GESTION DEL RIESGO	19 de Febrero	PRINCIPAL
DIRECCIÓN ADMINISTRATIVA DE TURISMO	19 de Febrero	CALLE 17
OFICINA CONTROL INTERNO DE GESTIÓN	19 de Febrero	PRINCIPAL
OFICINA CONTROL INTERNO DISCIPLINARIO	19 de Febrero	PRINCIPAL

DEPENDENCIA	FECHA	DIRECCION
OFICINA ASESORA JURIDICA	19 de Febrero	PRINCIPAL
SECRETARIA GENERAL	20 de Febrero	PRINCIPAL
SUBSECRETARIA DE TALENTO HUMANO	20 de Febrero	PRINCIPAL
SUBSECRETARIA ADMINISTRATIVA	20 de Febrero	PRINCIPAL
ALMACEN GENERAL	20 de Febrero	PRINCIPAL
ARCHIVO GENERAL	20 de Febrero	PRINCIPAL
SECRETARIA DE AGRICULTURA Y DESARROLLO RURAL	21 de Febrero	PRINCIPAL
SUBSECRETARIA DE ASUNTOS AGROPECUARIOS,	21 de Febrero	PRINCIPAL
SECRETARIA DE AMBIENTE Y DESARROLLO SOSTENIBLE	21 de Febrero	PRINCIPAL
SUBSECRETARIA DE GESTIÓN AMBIENTAL Y CRECIMIENTO VERDE	21de Febrero	PRINCIPAL
SECRETARIA DE EQUIDAD DE GÉNERO E INCLUSIÓN SOCIAL	21 de Febrero	SEGIS
SECRETARIA DE GOBIERNO	22 de Febrero	PRINCIPAL
SUBSECRETARIA DE GESTIÓN PÚBLICA	22 de Febrero	PRINCIPAL
SUBSECRETARIA DE DESARROLLO COMUNITARIO	22 de Febrero	AMA PASTO
SUBSECRETARIA DE PAZ Y DERECHOS HUMANOS	22 de Febrero	PRINCIPAL
SECRETARIA DE HACIENDA	23 de Febrero	PRINCIPAL
SUBSECRETARIA DE RENTAS	24 de Febrero	PRINCIPAL
IMPUESTO VEHICULOS Y REGISTRO	24 de Febrero	PANAMERICANA
AGUARDIENTE NARIÑO	24 de Febrero	SAN MIGUEL
SUBSECRETARIA DE PRESUPUESTO	23 de Febrero	PRINCIPAL
SUBSECRETARIA DE TRANSITO Y TRANSPORTE	26 de Febrero	PANAMERICANA
TESORERIA GENERAL	23 de Febrero	PRINCIPAL
CONTADURÍA GENERAL	23 de Febrero	PRINCIPAL
SECRETARIA DE INFRAESTRUCTURA Y MINAS	27 de Febrero	PRINCIPAL
SUBSECRETARIA DE MINAS	27 de Febrero	PRINCIPAL
SUBSECRETARIA DE VIAS	27 de Febrero	PRINCIPAL
SECRETARIA DE PLANEACION	28 de Febrero	PASTO PLAZA
SUBSECRETARIA DE ASISTENCIA TÉCNICA	28 de Febrero	PASTO PLAZA
SUBSECRETARIA DE ECONOMÍA REGIONAL Y AGUA POTABLE	28 de Febrero	AMA PASTO
SECRETARIA DE RECREACIÓN Y DEPORTES	28 de Febrero	CALLE 17 ENTRE 26 Y 27

La metodología para levantamiento de Información se hizo por medio del formato de entrevistas, la gobernación proveyó los contactos de los integrantes del comité Tic quienes eran los encargados de suministrar la información en cada oficina, se llamaba previamente con un día anterioridad al encargado de la oficina y se programaba su visita, se hacía un levantamiento previo de información y luego se iba equipo por equipo preguntando información. Mediante las siguientes preguntas además de las ya propuestas para el levantamiento de inventario que se hace en paralelo

8.5 ANALISIS DE ACTIVOS

Definición y valoración de Activos de Información a proteger

Se formalizó un inventario de activos de información, en la Tabla 2 se encuentra el inventario en el que se definen y valoran los principales activos de información que conforman el Área de Soporte Técnico y Proceso de gestión TIC

.

Cuadro 3. Inventario Área de Soporte Técnico y Proceso de Gestión TIC

ID	ACTIVO	CANT	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
PGT-01	Soporte Técnico	1	P	Uso Interno	Normal	Muy Alta	**Alto**	**5**	Jefe Proceso de Gestión TIC	…
PGT-02	Servidor NS1	1	HW	Confidencial	Sensible	Muy Alta	**Alto**	**5**	Jefe Proceso de Gestión TIC	Soporte Técnico
PGT-03	Código fuente Portal Web de la Gobernación de Nariño, Portales.		D	Confidencial	Sensible	Muy Alta	**Alto**	**5**	Jefe Proceso de Gestión TIC	Administrador Portal Web
PGT-04	Portal Web de la Gobernación de Nariño	1	SI	Uso Público	Sensible	Muy Alta	**Bajo**	**4**	I Jefe Proceso de Gestión TIC	Administrador Portal Web
PGT-06	Servidor NS2	1	HW	Confidencial	Sensible	Muy Alta	**Alto**	**5**	Jefe Proceso de Gestión TIC	Soporte Técnico
PGT-07	Correo Electrónico institucional		S	Uso Interno	Sensible	Alta	**Alto**	**5**	Jefe Proceso de Gestión TIC	Soporte Técnico
PGT-08	Base de datos Correo Electrónico Institucional		D	Confidencial	Sensible	Alta	**Alto**	**5**	Jefe Proceso de Gestión TIC	Soporte Técnico
PGT-13	Computadores de Escritorio	10	HW	Uso Interno	Sensible	Alta	**Medio**	**4**	I Jefe Proceso de Gestión TIC	Soporte Técnico
PGT-14	Computadores Portátiles	5	HW	Uso Interno	Sensible	Alta	**Medio**	**4**	I Jefe Proceso de Gestión TIC	Soporte Técnico
PGT-15	Impresoras	4	HW	Uso Interno	Normal	Media Baja	**Bajo**	**3**	Jefe Proceso de Gestión TIC	Soporte Técnico
PGT-16	Escáner	2	HW	Uso Interno	Normal	Media Baja	**Bajo**	**3**	Jefe Proceso de Gestión TIC	Soporte Técnico

Para obtener esta valoración, se realizaron conversaciones con el personal de Proceso de Gestión TIC de la Gobernación de Nariño; quienes conocen la importancia de cada activo dentro de la unidad, se revisó la información y documentación suministrada, para así determinar los niveles de confidencialidad, integridad y disponibilidad requeridos para cada procedimiento, que permitan cumplir con las operaciones normales de la Unidad.

8.6 ESTIMACIÓN DE AMENAZAS

En este caso específico usaremos el método de investigación de riesgos denominado Magerit, la cual nos recomendará las medidas apropiadas para controlar los activos.

La metodología Magerit nos muestra el grado de protección que tienen los activos con respecto al ambiente en que se encuentran y cómo interactúan con este, con el cual se podrá evaluar y posteriormente determinar la vulnerabilidad de estos equipos. Además de la implantación de controles para mejorar la manipulación y en lo posible tratar de disminuir la ocurrencia de los factores maliciosos, los cuales se podrían transformar en un impacto desfavorable para la organización.

Permite a la organización, identificar los riesgos en el entorno ya sean existentes o latentes y determina la vulnerabilidad a las que están expuestos recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, y controlar los riesgos identificados y así reducir el mínimo sus perjuicios. Está compuesta de cuatro etapas, que nos aclara la forma de trabajar en este ámbito que son:

- La Planificación se considera como el comienzo del proyecto y es donde se define lo que se va a cumplir.

- En el análisis de riesgos, se identifican y se cuantifica los activos, obteniendo una estimación deseable que se pueda controlar.

- La Gestión de riesgos identifica las funciones y servicios de salvaguardas que sirven para reducir el riesgo e implantar restricciones para el uso de los activos.

- Seleccionar las salvaguardas que incluyen el plan de implantación y los procedimientos de seguimiento, y se obtienen los resultados finales a diversos niveles.

Identificación de amenazas a que están expuestos los Activos de Información

MAGERIT facilita mucho esta actividad, debido a que indica que tipos de activos se pueden ver afectados por determinadas amenazas. A continuación se presenta

un ejemplo:

Cuadro 4. Amenazas por tipo de activos

[N.1] Fuego	
Tipos de activos afectados:	Descripción:
[HW] Hardware	Incendios: Posibilidad de que el fuego acabe con recursos del sistema.
[Media] Soportes de información	
[AUX] Equipamiento auxiliar	
[L] Instalaciones	

De esta forma se definieron las principales amenazas que se podrían presentar sobre cada uno de los activos de información del Proceso de Gestión TIC de la Gobernación de Nariño.

A continuación se dan a conocer las amenazas definidas de los principales activos de información del Proceso de Gestión TIC de la Gobernación de Nariño.

Cuadro 5. Amenazas servidor NS1

Activo PGT-02		**PGT-02 Servidor NS1**
Administrador		**Soporte Técnico**
Tipo activo		**Hardware**
Tipo	**ID**	**Amenaza**
Desastres naturales	N1	Fuego
	N2	Daños por agua
	N*	Desastres naturales
De origen industrial	I1	Fuego
	I2	Daños por agua
	I*	Desastres industriales
	I3	Contaminación mecánica
	I4	Contaminación electromagnética
	I5	Avería de origen físico o lógico
	I6	Corte del suministro eléctrico
	I7	Condiciones inadecuadas de temperatura o humedad
	I11	Emanaciones electromagnéticas
E	E2	Errores del administrador
	E23	Errores de mantenimiento/actualización de equipos
	E24	Caídas del sistema por agotamiento de recursos
	E25	Perdida de equipos

Ataques intencionados	A6	Abuso de privilegios de acceso
	A7	Uso no previsto
	A11	Acceso no autorizado
	A23	Manipulación de equipos
	A24	Denegación de servicio
	A25	Robo

Cuadro 6. Amenazas portal web de la Gobernación de Nariño

Activo PGT-04	**PGT-04 Portal Web Gobernación de Nariño**	
Administrador	**Administrador Portal Web**	
Tipo activo	**Sistema de Información**	
Tipo	**ID**	**Amenaza**
–	I5	Avería de origen físico o lógico
Errores y fallos no intencionados	E2	Errores del administrador
	E8	Difusión de software dañino
	E9	Errores de [re-] encaminamiento
	E10	Errores de secuencia
	E15	Alteración accidental de la información
	E18	Destrucción de información
	E19	Fugas de información
	E20	Vulnerabilidades de los programas
	E21	Errores de mantenimiento/actualización de programas
Ataques intencionados	A5	Suplantación de la identidad del usuario
	A6	Abuso de privilegios de acceso
	A7	Uso no previsto
	A8	Difusión de software dañino
	A9	[Re-] encaminamiento de mensajes
	A10	Alteración de secuencia
	A11	Acceso no autorizado
	A15	Modificación deliberada de la información
	A18	Destrucción de información
	A22	Manipulación de programas

8.7 ANÁLISIS DE VULNERABILIDADES

En el siguiente informe se realizó la Identificación de Vulnerabilidades, La cual se realizó mediante una visita a las instalaciones para realizar una inspección visual de los activos, entrevistas con el personal encargado del manejo de los recursos informáticos, luego de haber identificado las vulnerabilidades realizamos la Estimación del Impacto el objetivo conocer el alcance del daño producido en el Proceso de Gestión TIC de la Gobernación de Nariño derivado de la

materialización de las amenazas sobre los activos de información, también se realizó la Estimación de la Probabilidad el objetivo consiste en estimar la frecuencia de materialización de una amenaza en función de la cantidad de veces que esta pueda ocurrir, por último se realizó la Estimación del Riesgo con el objetivo de levantar la información sobre la identificación de los peligros, el análisis de las condiciones de vulnerabilidad y cálculo del riesgo con la finalidad de recomendar las medidas de prevención, todo lo anterior se realizó para cada uno de los activos que se encuentran en el Proceso de Gestión TIC de la Gobernación de Nariño.

Cuadro 7. Vulnerabilidades Servidor NS1

Activo PGT-02		**PGT-02 Servidor NS1**	
Administrador		**Soporte Técnico**	
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. no posee un solo extintor en la sala de servidores
	N2	Daños por agua	Hay buenas tuberias que tratan el agua lluvia por lo cual no se estima una posible inundacion o posibles daños por agua lluvia
	N*	Desastres naturales	El Proceso de Gestión TIC se encuentra en zona media de riesgo de desastre natural de origen de inundación debido a su mala ubicación en el primer piso
De origen industrial	I1	Fuego	No existe sistema de alarma contra incendios.
	I2	Daños por agua	No hay redes hidricas en esta zona
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.
	I3	Contaminación mecánica	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.
	I4	Contaminación electromagnética	Los racks no cuentan con aisladores.
	I5	Avería de origen físico o lógico	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.
	I6	Corte del suministro eléctrico	No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.
	I7	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.
	I11	Emanaciones electromagnéticas	Los racks no cuentan con aisladores.
E	E2	Errores del administrador	Falta de conocimiento del administrador.
	E23	Errores de mantenimiento/ actualización de equipos	No existe hoja de vida del servidor NS1 Falta de conocimiento del administrador.
	E24	Caídas del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio
	E25	Perdida de equipos	No existen la suficiente cámaras de seguridad en la organización

Ataques intencionados	A6	Abuso de privilegios de acceso	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Proceso de Gestión TIC, y luego por la oficina de Soporte Técnico; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio, donde cada puerta cuenta con una sola chapa de seguridad
	A11	Acceso no autorizado	Cualquier persona puede entrar a la sala de servidores no existe un control
	A23	Manipulación de equipos	Falta de controles para el ingreso a la sala de servidores
	A24	Denegación de servicio	Falta de recursos necesarios. Falta de planes de continuidad del negocio
	A25	Robo	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Proceso de Gestión TIC, y luego por la oficina de Soporte Técnico; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio, donde cada puerta cuenta con una sola chapa de seguridad.

Cuadro 8. Vulnerabilidades Portal Web de la Gobernación de Nariño

Activo PGT-04		**PGT-04 Portal Web Gobernación de Nariño**	
Administrador		**Administrador Portal Web**	
Tipo activo		**Sistema de Información**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y fallos no intencionados	E2	Errores del administrador	Un error del administrador puede conllevar a la disponibilidad de las aplicaciones los servicios que ellos soportan se vería seriamente afectado
	E8	Difusión de software dañino	Hay poca capacitación para los empleados que manejan software de la organización
	E15	Alteración accidental de la información	No existe medidas de control
	E18	Destrucción de información	No existe un protocolo para la limpieza del sitio web y un procedimiento de mantenimiento
	E19	Fugas de información	No existe medidas de control esta información puede ser modificada o usada para beneficios propios
	E20	Vulnerabilidades de los programas	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento
	E21	Errores de mantenimiento/actualización de programas	No existe un protocolo para la actualización de las diferentes aplicaciones

Ataques intencionados	A5	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios
	A8	Difusión de software dañino	No existe un procedimiento para la actualización de software
	A9	[Re-] encaminamiento de mensajes	Falta de controles, esta falla permite desplegar en el navegador datos no confiables proporcionados por usuarios, generalmente inyectando código javascript malicioso. Estos datos pueden secuestrar tu sitio web, permitiendo que tus usuarios sean re direccionados a sitios maliciosos o descarguen malware.
	A15	Modificación deliberada de la información	Falta de controles, afectara directamente la dimensión de integridad en un nivel muy alto, porque de presentarse ataques de modificación de información se va a ver alterados los datos almacenados, causando un caos informático y arrojando datos erróneos a la hora de las consultas transacciones en cada uno de los procesos normalizados dentro de las labores de la organización
	A18	Destrucción de información	No existe un control para la información importante, sería muy grave destruir información importante de la organización

Cuadro 9. Vulnerabilidades Soporte Técnico

Activo PGT-01		**PGT-01 Soporte Técnico**	
Administrador		**Administrador de Sistemas**	
Tipo activo		**Personal**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
E	E19	Fugas de información	Falta de controles, al haber fuga de información esta puede ser modificada o usada para beneficios propios llevando a pérdida de confianza de la organización
	E28	Indisponibilidad del personal	Falta de controles, al haber indisponibilidad del personal pueden dejar ausentes sus puestos de trabajo dejando así al no desarrollo de sus labores
A	A28	Indisponibilidad del personal	Falta de controles, ejecutar información importante para la organización si el personal esta indispuesto
	A29	Extorsión	Mediante amenazas pueden sacar información importante para la organización
	A30	Ingeniería social	Falta de concientización del personal en las mejores prácticas de seguridad informática. Llevando a un afectación alta en la dimensión de confidencialidad

Cuadro 10. Vulnerabilidades Base de Datos Correo Electrónico Institucional

Activo PGT-08		PGT-08 **Base de Datos Correo Electrónico Institucional**	
Administrador		**Administrador de Sistemas**	
Tipo activo		**Datos / Información**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Errores y fallos no intencionados	E1	Errores de los usuarios	Los usuarios no cuentan con capacitación para el manejo del activo
	E2	Errores del administrador	Algunos equipos del Proceso de Gestión TIC No están actualizados por software de protección y reparación de virus
	E3	Errores de monitorización	No se realizan correctamente los mantenimientos
	E18	Destrucción de la información	No existe un protocolo para la clasificación de la información
	E19	Fugas de información	Falta de interés por aplicar las políticas de seguridad
Ataques intencionados	A3	Manipulación de los registros de actividad	Falta de controles
	A5	Suplantación de la identidad del usuario	No existe una implementación de procesos rigurosos para actualizar las contraseñas
	A6	Abuso de privilegios de acceso	No existe mecanismos de control
	A15	Modificación deliberada de la información	No realizan copias de seguridad periódicamente
	A19	Divulgación de información	No hay mayor seguridad para la información

Cuadro 11. Vulnerabilidades Código Fuente Portal Web de la Gobernación de Nariño, Portales.

Activo PGT-03	**PGT-03 Código Fuente Portal Web de la Gobernación de Nariño, Portales.**		
Administrador	**Administrador Portal Web**		
Tipo activo	**Datos/información**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
De origen industrial	I8	Fuego	No existe sistema de alarma contra incendios.
E	E2	Errores del administrador	La actualización del antivirus no se actualiza diariamente
	E4	Errores de configuración	No cuenta con una protección segura a los ataques al sitio web
	E19	Fugas de información	Los datos no son correctamente protegidos
Ataques intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido
	A7	Uso no previsto	Autorización insuficiente
	A24	Denegación de servicio	No cuenta con la suficiente protección a los Ataques maliciosos
	A26	Ataque destructivo	No se cuenta con la suficiente protección

Cuadro 12. Vulnerabilidades Correo Electrónico Institucional

Activo PGT-07		**PGT-07 Correo Electrónico Institucional**	
Administrador		**Administrador Portal Web**	
Tipo activo		**Sistema de Información**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente alterna de corriente eléctrica
	I8	Fallo de servicio de comunicaciones	Baja capacidad de respuesta
E	E2	Errores del administrador	No existe un análisis de seguridad para todos los correos spam que llegan
	E21	Errores de mantenimiento / actualización de programas (Software)	No se mantienen actualizados los parches de seguridad.

Cuadro 13. Vulnerabilidades Computadores de Escritorio

Activo PGT-13		**PGT-13 Computadores de Escritorio**	
Administrador		**Soporte Técnico**	
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. No poseen extintor en la oficina de Proceso de Gestión TIC
	N2	Daños por agua	Los computadores de escritorio se encuentra ubicados sin ninguna precaución
	N*	Desastres naturales	El Proceso de Gestión TIC se encuentra en zona media de riesgo de desastre natural de origen de inundación debido a su mala ubicación en el primer piso
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente de energía alterna
	I7	Condiciones inadecuadas de temperatura o humedad	No cuentan con aire acondicionado en la oficina de Proceso de Gestión TIC
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
E	E1	Errores de los usuarios	No existe un manual para el uso de las diferentes aplicaciones
	E2	Errores del administrador	No existe un protocolo para la instalación de las diferentes aplicaciones
	E4	Errores de configuración	No existe un manual para la debida configuración de los equipos de computo
	E21	Errores de mantenimiento / actualización de programas (hardware)	No cuentan con una política de mantenimiento
	E25	Perdida de equipos	No existen las suficientes cámaras de seguridad en la oficina de Proceso de Gestión TIC
Ataques intencionados	A6	Difusión de software dañino	Debido a la gran cantidad de equipos de cómputo que están destinados para los usuarios y la falta de asesoría puede causar daños
	A11	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios
	A3	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones

Cuadro 14. Vulnerabilidades Computadores Portátiles

Activo PGT-14		**PGT-14 Computadores Portátiles**	
Administrador		**Soporte Técnico**	
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. No poseen extintor en la oficina de Proceso de Gestión TIC
	N2	Daños por agua	Los computadores portátiles se encuentra ubicados sin ninguna precaución
	N*	Desastres naturales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente de energía alterna
	I7	Condiciones inadecuadas de temperatura o humedad	No cuentan con aire acondicionado en la oficina de Proceso de Gestión TIC
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
E	E1	Errores de los usuarios	No existe un manual para el uso de las diferentes aplicaciones
	E2	Errores del administrador	No existe un protocolo para la instalación de las diferentes aplicaciones
	E4	Errores de configuración	No existe un manual para la debida configuración de los equipos de computo
	E21	Errores de mantenimiento / actualización de programas (hardware)	No cuentan con una política de mantenimiento
	E25	Perdida de equipos	No existen las suficientes cámaras de seguridad en la oficina de Proceso de Gestión TIC
Ataques intencionados	A6	Difusión de software dañino	Debido a la gran cantidad de equipos de cómputo que están destinados para los usuarios y la falta de asesoría puede causar daños
	A11	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios
	A3	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones

Cuadro 15. Vulnerabilidades Impresoras

Activo PGT-15		**PGT-15 Impresoras**	
Administrador		**Soporte Técnico**	
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**
Desastres naturales	N1	Fuego	Falta de protección contra fuego
	N2	Daños por agua	Falta de protección física adecuada
	N*	Desastres naturales	Condiciones de los locales donde los recursos son fácilmente afectados por desastres
De origen industrial	I1	Fuego	No poseen extintor en la oficina de Proceso de Gestión TIC
	I2	Daños por agua	Falta de protección física adecuada
	I*	Desastres industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
	I5	Avería de origen físico o lógico	Mal ubicación de las impresoras
E	E1	Errores de los usuarios	Falta de conocimiento para el uso de la aplicación
	E4	Errores de configuración	Falta de control
	E25	Perdida de equipos	Falta de protección física
Ataques intencionados	A4	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones

Cuadro 16. Vulnerabilidades Escáner

Activo PGT-16		**PGT-16 Escáner**	
Administrador		**Soporte Técnico**	
Tipo activo		**Hardware**	
Tipo	**ID**	**Amenaza**	**Exposición /Vulnerabilidad**
Desastres naturales	N1	Fuego	Falta de protección contra fuego
	N2	Daños por agua	Falta de protección física adecuada
	N*	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
De origen industrial	I1	Fuego	No poseen extintor en la oficina de Proceso de Gestión TIC
	I2	Daños por agua	Falta de protección física adecuada
	I*	Desastres industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.
	I5	Avería de origen físico o lógico	Mala ubicación del escáner
E	E1	Errores de los usuarios	Falta de conocimiento para el uso de la aplicación
	E4	Errores de configuración	Falta de control
	E25	Perdida de equipos	Falta de protección física
Ataques intencionados	A4	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones
	A25	Robo	Falta de protección física

8.8 ESTIMACIÓN DEL IMPACTO

Mediante el uso de tablas de doble entrada, en donde:

Impacto = Valor del activo x Degradación

El objetivo es conocer el alcance del daño producido en el Proceso de Gestión TIC de la Gobernación de Nariño derivado de la materialización de las amenazas sobre los activos de información, mediante el uso de tablas de doble entrada para la obtención de resultados. A partir de los datos obtenidos en las fases anteriores, se procede a estimar el impacto.

El primer dato requerido es el “Nivel del activo” valorado cuantitativa y/o cualitativamente:

Cuadro 17. Valor del activo Servidor NS1

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-02	Servidor NS1	1	HW	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**

El segundo dato necesario para la valoración del impacto es la “Degradación”, el cual nos indica que tan perjudicado resulta el valor del activo de información (1%, 50%, 100%), como resultado de la materialización de las amenazas:

- 90% a 100%: Degradación muy considerable del activo
- 25% a 89%: Degradación medianamente considerable del activo
- 1% a 24%: Degradación poco considerable del activo

Para el caso de Servidor NS1 con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%**, puesto que al ser de tipo hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres industriales y robo; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla , el valor del impacto obtenido es 8 equivalentes a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información

Tabla 2 Impacto de Activo Servidor NS1.

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

Mayor (5): Impacta en la operatividad de los procesos.

Moderado (3): Impacta en la operatividad del macro proceso.

Menor (2): Impacta en la operatividad del proceso.

Insignificante (1): Impacta levemente en la operatividad del proceso

Cuadro 18. Valor del activo Soporte Técnico

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-01	Soporte Técnico	1	P	Uso Interno	Normal	Muy Alta	**Alto**	**4**

Para el caso de Soporte Técnico con nivel **Alto** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de tipo Personal, las principales amenazas que recaen sobre esta clase de activos son fugas de información, extorción, ingeniería social; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 2, el valor del impacto obtenido es 3 equivalente a Moderado, lo que quiere decir que en caso de materialización de amenaza(s), impacta Moderadamente en la operatividad del macro proceso en los que participa este activo de información

Tabla 3. Impacto del activo Soporte Técnico

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	**3**	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Moderado (3): Impacta en la operatividad del macro proceso.

Cuadro 19. Valor del activo Código fuente portal Web de la Gobernación de Nariño , portales

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-03	Código fuente Portal Web de la Gobernación de Nariño, Portales.		D	Confidencial	Sensible	Muy Alta	**Muy Alto**	**5**

Para el caso de Código fuente Portal Web de la Gobernación de Nariño, Portales con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%**, puesto que al ser de tipo Datos/Información, las principales amenazas que recaen sobre esta clase de activos son errores y fallas no intencionadas, ataques intencionados, fugas de información; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 3, el valor del impacto obtenido es 8 equivalentes a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información

Tabla 4. Impacto activo Código fuente portal Web de la Gobernación de Nariño , portales

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

Cuadro 20. Valor del activo Portal web de la gobernación de Nariño

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-04	Portal Web de la Gobernación de Nariño	1	SI	Uso Público	Sensible	Muy Alta	**Alto**	**4**

Para el caso de Portal Web de la Gobernación de Nariño con nivel **Alto** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de Sistema de Información, las principales amenazas que recaen sobre esta clase de activos son fugas de información, extorción, ingeniería social; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 4, el valor del impacto obtenido es 3 equivalente a Moderado, lo que quiere decir que en caso de materialización de amenaza(s), el impacto es moderado en la en la operatividad del macro proceso en los que participa este activo de información

Tabla 5.Impacto del activo Portal web de la gobernación de Nariño

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	Muy Alto	3	5	8
	Alto	2	**3**	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Moderado (3): Impacta en la operatividad del macro proceso.

Cuadro 21. Valor del activo Servidor NS2

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-06	Servidor NS2	1	HW	Confidencial	Sensible	Alta	**Muy Alto**	**5**

Para el caso de Servidor NS2 R810 con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%**, puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres industriales y robo; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 5, el valor del impacto obtenido es 8 equivalentes a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información

Tabla 6. Impacto activo Servidor NS2

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

Cuadro 22. Valor del activo Correo Electrónico institucional

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-07	Correo Electrónico institucional		S	Uso Interno	Sensible	Alta	**Muy Alto**	**5**

Para el caso de Correo Electrónico institucional con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%**, puesto que al ser de tipo Servicios, las principales amenazas que recaen sobre esta clase de activos desastres industriales, errores y fallos no intencionados, ataques intencionados, fugas de información; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 6 el valor del impacto obtenido es 8 equivalentes a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información

Tabla 7. Impacto del activo Correo Electrónico institucional

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

Cuadro 23. Valor del activo Base de datos correo Electronico Institucional

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-08	Base de datos Correo Electrónico Institucional		D	Confidencial	Sensible	Alta	Muy Alto	5

Para el caso de Base de datos Correo Electrónico Institucional con nivel **Muy Alto** y un porcentaje estimado de degradación de **90% - 100%**, puesto que al ser de tipo Datos/Información, ataques intencionados, errores fallos no intencionados, fugas de información; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 7, el valor del impacto obtenido es 8 equivalentes a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información

Tabla 8. Impacto del activo Base de datos correo Electronico Institucional

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	**8**
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

Cuadro 24. Valor del activo Computadores de escritorio

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-13	Computadores de Escritorio	10	HW	Uso Interno	Sensible	Alta	**Alto**	**4**

Para el caso de Computadores de Escritorio con nivel **Alto** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, errores fallos no intencionados, robo; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 8, el valor del impacto obtenido es 3 equivalente a Moderado, lo que quiere decir que en caso de materialización de amenaza(s), el impacto es moderado impacta levemente en la operatividad del proceso en los que participa este activo de información

Tabla 9.Impacto del activo Computadores de escritorio

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	**3**	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Moderado (3): Impacta en la operatividad del macro proceso.

Cuadro 25. Valor del activo Computadores Portatiles

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-14	Computadores Portátiles	5	HW	Uso Interno	Sensible	Alta	**Alto**	**4**

Para el caso de Computadores Portátiles con nivel **Alto** y un porcentaje estimado de degradación de **25% a 89%**, puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, errores fallos no intencionados, robo; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 9, el valor del impacto obtenido es 3 equivalente a Moderado, lo que quiere decir que en caso de materialización de amenaza(s), el impacto es moderado impacta levemente en la operatividad del proceso en los que participa este activo de información

Tabla 10. Impacto del activo Computadores Portatiles

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	**3**	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Moderado (3): Impacta en la operatividad del macro proceso.

.

Cuadro 26. Valor del activo impresora

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor
PGT-15	Impresoras	4	HW	Uso Interno	Normal	Media Baja	**Medio**	**3**

Para el caso de Impresoras con nivel **Medio** y un porcentaje estimado de degradación de **1% a 24%**, puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, errores fallos no intencionados, robo; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla 10, el valor del impacto obtenido es 1 equivalente a Insignificante, lo que quiere decir que en caso de materialización de amenaza(s), impacta levemente en la operatividad de los

procesos en los que participa este activo de información
Tabla 11.Impacto del activo impresora

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	**1**	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Insignificante (1): Impacta levemente en la operatividad del proceso

Cuadro 27. Valor del activo Escaner

ID	**ACTIVO**	**CANT**	**TIPO ACTIVO**	**CLASIFICACION INFORMACION**			**VALORACION DEL ACTIVO**	
				Confidencialidad	**Integridad**	**Disponibilidad**	**Nivel**	**Valor**
PGT-16	Escáner	2	HW	Uso Interno	Normal	Media Baja	**Bajo**	**2**

Para el caso de Escáner con nivel **Bajo** y un porcentaje estimado de degradación de **1% a 24%:** puesto que al ser de tipo Hardware, las principales amenazas que recaen sobre esta clase de activos son desastres naturales, desastres de origen industrial, errores fallos no intencionados, robo; que lo afectarían considerablemente o afectarían a Proceso de Gestión TIC considerablemente.

Al realizar el producto de ambos datos en la tabla X, el valor del impacto obtenido es 1 equivalente a Menor, lo que quiere decir que en caso de materialización de amenaza(s), impacta levemente en la operatividad de los procesos en los que participa este activo de información.

Tabla 12.Impacto de del activo Escaner

IMPACTO		***Degradación***		
		1%	50%	**100%**
Valor del activo	**Muy Alto**	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	**1**	1	2
	Muy Bajo	1	1	1

Insignificante (1): Impacta levemente en la operatividad del proceso

1	Raro	Puede ocurrir una vez cada 2 años.
2	Muy baja	Al año.
3	Baja	En 6 meses.
4	Media	Al mes.
5	Alta	A la semana.

8.9 ESTIMACIÓN DE LA PROBABILIDAD

El objetivo consiste en estimar la frecuencia de materialización de una amenaza en función de la cantidad de veces que esta pueda ocurrir (a mayor número de vulnerabilidades, mayor probabilidad de ocurrencia de las amenazas) y se utilizó la siguiente escala:

Se visualiza el impacto y la frecuencia de materialización cada una de las amenazas sobre el Servidor NS1:

Cuadro 28. Impacto y frecuencia Servidor NS1

Activo PGT-02		PGT-02 Servitor NS1			
Administrador		**Soporte Técnico**			
Degradación		**100%**			
Impacto		**8**	**Desastroso**		
Tipo activo		**Hardware / equipos**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. no posee un solo extintor en la sala de servidores	Muy baja	2
	N2	Daños por agua		Raro	1
De origen industrial	N*	Desastres naturales	El Proceso de Gestión TIC se encuentra en zona media de riesgo de desastre natural de origen de inundación debido a su mala ubicación en el primer piso	Muy baja	2
	I1	Fuego	No existe sistema de alarma contra incendios.	Muy baja	2
	I2	Daños por agua		Raro	1
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de	Media	4

De origen industrial			temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.		
	I3	Contaminación mecánica	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3
	I4	Contaminación electromagnética	Los racks no cuentan con aisladores.	Muy baja	2
	I5	Avería de origen físico o lógico	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3
	I6	Corte del suministro eléctrico	No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.	Muy baja	2
	I7	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	Baja	3
E	I11	Emanaciones electromagnéticas	Los racks no cuentan con aisladores.	Baja	3
	E2	Errores del administrador	Falta de conocimiento del administrador.	Muy baja	2
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida del servidor NS1 Falta de conocimiento del administrador.	Baja	3
	E24	Caídas del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3
Ataques intencionados	E25	Perdida de equipos	No existen la suficiente cámaras de seguridad en la organización	Muy baja	2
	A6	Abuso de privilegios de acceso	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Proceso de Gestión	Baja	3

Ataques intencionados			TIC, y luego por la oficina de Soporte Técnico; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio, donde cada puerta cuenta con una sola chapa de seguridad		
	A11	Acceso no autorizado	Cualquier persona puede entrar a la sala de servidores no existe un control	Baja	3
	A23	Manipulación de equipos	Falta de controles para el ingreso a la sala de servidores	Baja	3
	A24	Denegación de servicio	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3
	A25	Robo	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Proceso de Gestión TIC, y luego por la oficina de Soporte Técnico; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio, donde cada puerta cuenta con una sola chapa de seguridad.	Baja	3

Cuadro 29. Impacto y frecuencia Portal Web de la Gobernación de Nariño

Activo	**PGT-04 Portal Web Gobernación de Nariño**				
Administrador	**Administrador Portal Web**				
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Sistema de Información**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y fallos no intencionados	E2	Errores del administrador	Un error del administrador puede conllevar a la disponibilidad de las aplicaciones los servicios que ellos soportan se vería seriamente afectado	Media	4
	E8	Difusión de software dañino	Hay poca capacitación para los empleados que manejan software de la organización	Baja	3
	E15	Alteración accidental de la información	No existe medidas de control	Baja	3
	E18	Destrucción de información	No existe un protocolo para la limpieza del sitio web y un procedimiento de mantenimiento	Baja	3
	E19	Fugas de información	No existe medidas de control esta información puede ser modificada o usada para beneficios propios	Baja	3
	E20	Vulnerabilidades de los programas	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento	Media	4
	E21	Errores de mantenimiento/ actualización de programas	No existe un protocolo para la actualización de las diferentes aplicaciones	Baja	3

Ataques intencionados	A5	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3
	A8	Difusión de software dañino	No existe un procedimiento para la actualización de software	Baja	3
	A9	[Re-] encaminamiento de mensajes	Falta de controles, esta falla permite desplegar en el navegador datos no confiables proporcionados por usuarios, generalmente inyectando código javascript malicioso. Estos datos pueden secuestrar tu sitio web, permitiendo que tus usuarios sean re direccionados a sitios maliciosos o descarguen malware.	Baja	3
	A15	Modificación deliberada de la información	Falta de controles, afectara directamente la dimensión de integridad en un nivel muy alto, porque de presentarse ataques de modificación de información se va a ver alterados los datos almacenados, causando un caos informático y arrojando datos erróneos a la hora de las consultas transacciones en cada uno de los procesos normalizados dentro de las labores de la organización	Media	4
	A18	Destrucción de información	No existe un control para la información importante, sería muy grave destruir información importante de la organización	Media	4

Cuadro 30. Impacto y frecuencia Soporte Técnico

Activo		**PGT-01 Soporte Técnico**			
Administr		**Administrador de Sistemas**			
Degradac		**100%**			
Impacto		**8**	**Desastroso**		
Tipo		**Personal**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
E	E19	Fugas de información	Falta de controles, al haber fuga de información esta puede ser modificada o usada para beneficios propios llevando a pérdida de confianza de la organización	Baja	3
	E28	Indisponibilidad del personal	Falta de controles, al haber indisponibilidad del personal pueden dejar ausentes sus puestos de trabajo dejando así al no desarrollo de sus labores	Muy baja	2
A	A28	Indisponibilidad del personal	Falta de controles, ejecutar información importante para la organización si el personal esta indispuesto	Muy baja	2
	A29	Extorsión	Mediante amenazas pueden sacar información importante para la organización	Baja	3
	A30	Ingeniería social	Falta de concientización del personal en las mejores prácticas de seguridad informática. Llevando a un afectación alta en la dimensión de confidencialidad	Baja	3

Cuadro 31. Impacto y frecuencia Base de Datos Correo Electrónico Institucional

Activo PGT-08		**PGT-08 Base de Datos Correo Electrónico Institucional**			
Administrador		**Administrador de Sistemas**			
Degradación		**100%**			
Impacto		**8**	**Desastroso**		
Tipo activo		**Datos / Información**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Errores y fallos no intencionados	E1	Errores de los usuarios	Los usuarios no cuentan con capacitación para el manejo del activo	Media	4
	E2	Errores del administrador	Algunos equipos del Proceso de Gestión TIC No están actualizados por software de protección y reparación de virus	Media	4
	E3	Errores de monitorización	No se realizan correctamente los mantenimientos	Baja	3
	E18	Destrucción de la información	No existe un protocolo para la clasificación de la información	Baja	3
	E19	Fugas de información	Falta de interés por aplicar las políticas de seguridad	Muy baja	2
	A3	Manipulación de los registros de actividad	Falta de controles	Media	4
	A5	Suplantación de la identidad del usuario	No existe una implementación de procesos rigurosos para actualizar las contraseñas	Muy baja	2
Ataques intencionados	A6	Abuso de privilegios de acceso	No existe mecanismos de control	Baja	3
	A15	Modificación deliberada de la información	No realizan copias de seguridad periódicamente	Muy baja	2
	A19	Divulgación de información	No hay mayor seguridad para la información	Muy baja	2
	E1	Errores de los usuarios	Los usuarios no cuentan con capacitación para el manejo del activo	Baja	3
	E2	Errores del administrador	Algunos equipos del Proceso de Gestión TIC No están actualizados por software de protección y reparación de virus	Muy baja	2
	E3	Errores de monitorización	No se realizan correctamente los mantenimientos	Baja	3
	E18	Destrucción de la información	No existe un protocolo para la clasificación de la información	Baja	3

Cuadro 32. Impacto y frecuencia Código Fuente Portal Web de la Gobernación de Nariño, Portales.

Activo PGT-03		**PGT-03 Código Fuente Portal Web de la Gobernación de Nariño, Portales.**			
Administrador		**Administrador Portal Web**			
Degradación		**100%**			
Impacto		**8**	**Desastroso**		
Tipo activo		**Datos/información**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
De origen industrial	I8	Fuego	No existe sistema de alarma contra incendios.	Muy baja	2
E	E2	Errores del administrador	La actualización del antivirus no se actualiza diariamente	Media	4
	E4	Errores de configuración	No cuenta con una protección segura a los ataques al sitio web	Media	4
	E19	Fugas de información	Los datos no son correctamente protegidos	Media	4
Ataques intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido	Muy baja	2
	A7	Uso no previsto	Autorización insuficiente	Baja	3
	A24	Denegación de servicio	No cuenta con la suficiente protección a los Ataques maliciosos	Media	4
	A26	Ataque destructivo	No se cuenta con la suficiente protección	Media	4

Cuadro 33. Impacto y frecuencia Correo Electrónico Institucional

Activo PGT-07		**PGT-07 Correo Electrónico Institucional**			
Administrador		**Administrador Portal Web**			
Degradación		**100%**			
Impacto		**8**	**Desastroso**		
Tipo activo		**Sistema de Información**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente alterna de corriente eléctrica	Muy baja	2
	I8	Fallo de servicio de comunicaciones	Baja capacidad de respuesta	Baja	3
E	E2	Errores del administrador	No existe un análisis de seguridad para todos los correos spam que llegan	Media	4
	E21	Errores de mantenimiento / actualización de programas (Software)	No se mantienen actualizados los parches de seguridad.	Baja	3

Cuadro 34. Impacto y frecuencia Computadores de Escritorio

Activo PGT-13	**PGT-13 Computadores de Escritorio**				
Administrador	**Soporte Técnico**				
Degradación	**50%**				
Impacto	**3**	**Moderado**			
Tipo activo	**Hardware**				
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. No poseen extintor en la oficina de Proceso de Gestión TIC	Baja	3
	N2	Daños por agua	Los computadores de escritorio se encuentra ubicados sin ninguna precaución	Bajo	3
	N*	Desastres naturales	El Proceso de Gestión TIC se encuentra en zona media de riesgo de desastre natural de origen de inundación debido a su mala ubicación en el primer piso	Baja	3
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente de energía alterna	Baja	3
	I7	Condiciones inadecuadas de temperatura o humedad	No cuentan con aire acondicionado en la oficina de Proceso de Gestión TIC	Baja	3
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3
E	E1	Errores de los usuarios	No existe un manual para el uso de las diferentes aplicaciones	Baja	3
	E2	Errores del administrador	No existe un protocolo para la instalación de las diferentes aplicaciones	Baja	3
	E4	Errores de configuración	No existe un manual para la debida configuración de los equipos de computo	Baja	3
	E21	Errores de mantenimiento / actualización de programas (hardware)	No cuentan con una política de mantenimiento	Baja	3
	E25	Perdida de equipos	No existen las suficientes cámaras de seguridad en la oficina de Proceso de Gestión TIC	Baja	3
Ataques intencionados	A6	Difusión de software dañino	Debido a la gran cantidad de equipos de cómputo que están destinados para los usuarios y la falta de asesoría puede causar daños	Baja	3
	A11	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3
	A3	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3

Cuadro 35. Impacto y frecuencia Computadores Portátiles

Activo PGT-14		**PGT-14 Computadores Portátiles**			
Administrador		**Soporte Técnico**			
Degradación		**50%**			
Impacto		**3**	**Moderado**		
Tipo activo		**Hardware**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. No poseen extintor en la oficina de Proceso de Gestión TIC	Muy baja	2
	N2	Daños por agua	Los computadores portátiles se encuentra ubicados sin ninguna precaución	Raro	1
	N*	Desastres naturales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente de energía alterna	Muy baja	2
	I7	Condiciones inadecuadas de temperatura o humedad	No cuentan con aire acondicionado en la oficina de Proceso de Gestión TIC	Baja	3
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3
E	E1	Errores de los usuarios	No existe un manual para el uso de las diferentes aplicaciones	Baja	3
	E2	Errores del administrador	No existe un protocolo para la instalación de las diferentes aplicaciones	Baja	3
	E4	Errores de configuración	No existe un manual para la debida configuración de los equipos de computo	Muy baja	2
	E21	Errores de mantenimiento / actualización de programas (hardware)	No cuentan con una política de mantenimiento	Baja	3
	E25	Perdida de equipos	No existen las suficientes cámaras de seguridad en la oficina de Proceso de Gestión TIC	Muy baja	2
Ataques intencionados	A6	Difusión de software dañino	Debido a la gran cantidad de equipos de cómputo que están destinados para los usuarios y la falta de asesoría puede causar daños	Muy baja	2
	A11	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3
	A3	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3

Cuadro 36. Impacto y frecuencia Impresoras

Activo PGT-15		**PGT-15 Impresoras**			
Administrador		**Soporte Técnico**			
Degradación		**1%**			
Impacto		**1**	**Insignificante**		
Tipo activo		**Hardware**			
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de protección contra fuego	Muy baja	2
	N2	Daños por agua	Falta de protección física adecuada	Raro	1
	N*	Desastres naturales	Condiciones de los locales donde los recursos son fácilmente afectados por desastres	Muy baja	2
De origen industrial	I1	Fuego	No poseen extintor en la oficina de Proceso de Gestión TIC	Muy baja	2
	I2	Daños por agua	Falta de protección física adecuada	Raro	1
	I*	Desastres industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2
	I5	Avería de origen físico o lógico	Mal ubicación de las impresoras	Muy baja	2
E	E1	Errores de los usuarios	Falta de conocimiento para el uso de la aplicación	Baja	3
	E4	Errores de configuración	Falta de control	Baja	3
	E25	Perdida de equipos	Falta de protección física	Baja	3
Ataques intencionados	A4	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3

Cuadro 37. Impacto y frecuencia Escáner

Activo PGT-16		**PGT-16 Escáner**			
Administrador		**Soporte Técnico**			
Degradación		**1%**			
Impacto		**1**	**Insignificante**		
Tipo activo		**Hardware**			
Tipo	**ID**	**Amenaza**	**Exposición /Vulnerabilidad**	**Frecuencia (F)**	
Desastres naturales	N1	Fuego	Falta de protección contra fuego	Muy baja	2
	N2	Daños por agua	Falta de protección física adecuada	Raro	1
	N*	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Muy baja	2
De origen industrial	I1	Fuego	No poseen extintor en la oficina de Proceso de Gestión TIC	Muy baja	2
	I2	Daños por agua	Falta de protección física adecuada	Raro	1
	I*	Desastres industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2
	I5	Avería de origen físico o lógico	Mala ubicación del escáner	Muy baja	2
E	E1	Errores de los usuarios	Falta de conocimiento para el uso de la aplicación	Baja	3
	E4	Errores de configuración	Falta de control	Baja	3
	E25	Perdida de equipos	Falta de protección física	Baja	3
Ataques intencionados	A4	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3
	A25	Robo	Falta de protección física	Muy baja	2

8.10 ESTIMACIÓN DEL RIESGO

Este valor se obtiene como resultado de la siguiente fórmula:

Riesgo (R)= Probabilidad (F) x Impacto

Cuadro 38. Estimación del Riesgo Servidor NS1

Activo PGT-02		PGT-02 Servidor NS1						
Administrador		**Soporte Técnico**						
Degradación		**100%**						
Impacto		**8**	**Desastroso**					
Tipo activo		**Hardware / equipos**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							3.91	Intolerable
				Frecuencia (F)		**R**	**NR**	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. no posee un solo extintor en la sala de servidores	Muy baja	2	16	4	Extremo
	N2	Daños por agua		Raro	1	8	3	Intolerable
De origen industrial	N*	Desastres naturales	El Proceso de Gestión TIC se encuentra en zona media de riesgo de desastre natural de origen de inundación debido a su mala ubicación en el primer piso	Muy baja	2	16	4	Extremo
	I1	Fuego	No existe sistema de alarma contra incendios.	Muy baja	2	16	4	Extremo
	I2	Daños por agua		Raro	1	8	3	Intolerable
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.	Media	4	32	4	Extremo

De origen industrial	I3	Contaminación mecánica	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3	24	4	Extremo
	I4	Contaminación electromagnética	Los racks no cuentan con aisladores.	Muy baja	2	16	4	Extremo
	I5	Avería de origen físico o lógico	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3	24	4	Extremo
	I6	Corte del suministro eléctrico	No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.	Muy baja	2	16	4	Extremo
	I7	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	Baja	3	24	4	Extremo
E	I11	Emanaciones electromagnéticas	Los racks no cuentan con aisladores.	Baja	3	24	4	Extremo
	E2	Errores del administrador	Falta de conocimiento del administrador.	Muy baja	2	16	4	Extremo
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida del servidor NS1 Falta de conocimiento del administrador.	Baja	3	24	4	Extremo
	E24	Caídas del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3	24	4	Extremo
Ataques intencionados	E25	Perdida de equipos	No existen la suficiente cámaras de seguridad en la organización	Muy baja	2	16	4	Extremo
	A6	Abuso de privilegios de acceso	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Proceso de Gestión TIC, y luego por la oficina de Soporte Técnico; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio, donde cada puerta cuenta con una sola chapa de seguridad	Baja	3	24	4	Extremo

	A11	Acceso no autorizado	Cualquier persona puede entrar a la sala de servidores no existe un control	Baja	3	24	4	Extremo
	A23	Manipulación de equipos	Falta de controles para el ingreso a la sala de servidores	Baja	3	24	4	Extremo
	A24	Denegación de servicio	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3	24	4	Extremo
	A25	Robo	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Proceso de Gestión TIC, y luego por la oficina de Soporte Técnico; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio, donde cada puerta cuenta con una sola chapa de seguridad.	Baja	3	24	4	Extremo

Tabla 13. El valor **NR** (Nivel de Riesgo) obedece al Mapa de Riesgos :

Riesgo = Probabilidad * Impacto								
	Probabilidad	**5**	**5**	10	15	25	40	
		4	4	8	12	20	32	
		3	3	6	9	15	24	
		2	2	4	6	10	16	
		1	1	2	3	**5**	8	
			1	**2**	**3**	**5**	**8**	
			Impacto					

Nivel de Riesgo	
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para el Servidor NS1 es de 3.91, es decir, intolerable y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Cuadro 39. Estimación del Riesgo Portal Web de la Gobernación de Nariño

Activo PGT-04		**PGT-04 Portal Web Gobernación de Nariño**							
Administrador		**Administrador Portal Web**							
Degradación		**50%**							
Impacto		**3**	**Moderado**						
Tipo activo		**Sistema de Información**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
							3	Intolerable	
				Frecuencia (F)		**R**	**NR**		
Errores y fallos no intencionados	E2	Errores del administrador	Un error del administrador puede conllevar a la disponibilidad de las aplicaciones los servicios que ellos soportan se vería seriamente afectado	Media	4	12	3	Intolerable	
	E8	Difusión de software dañino	Hay poca capacitación para los empleados que manejan software de la organización	Baja	3	9	3	Intolerable	
	E15	Alteración accidental de la información	No existe medidas de control	Baja	3	9	3	Intolerable	
	E18	Destrucción de información	No existe un protocolo para la limpieza del sitio web y un procedimiento de mantenimiento	Baja	3	9	3	Intolerable	
	E19	Fugas de información	No existe medidas de control esta información puede ser modificada o usada para beneficios propios	Baja	3	9	3	Intolerable	
	E20	Vulnerabilidades de los programas	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento	Media	4	12	3	Intolerable	
	E21	Errores de mantenimiento/actualización de programas	No existe un protocolo para la actualización de las diferentes aplicaciones	Baja	3	9	3	Intolerable	

Ataques intencionados	A5	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	9	3	Intolerable
	A8	Difusión de software dañino	No existe un procedimiento para la actualización de software	Baja	3	9	3	Intolerable
	A9	[Re-] encaminamiento de mensajes	Falta de controles, esta falla permite desplegar en el navegador datos no confiables proporcionados por usuarios, generalmente inyectando código javascript malicioso. Estos datos pueden secuestrar tu sitio web, permitiendo que tus usuarios sean re direccionados a sitios maliciosos o descarguen malware.	Baja	3	9	3	Intolerable
	A15	Modificación deliberada de la información	Falta de controles, afectara directamente la dimensión de integridad en un nivel muy alto, porque de presentarse ataques de modificación de información se va a ver alterados los datos almacenados, causando un caos informático y arrojando datos erróneos a la hora de las consultas transacciones en cada uno de los procesos normalizados dentro de las labores de la organización	Media	4	12	3	Intolerable
	A18	Destrucción de información	No existe un control para la información importante, sería muy grave destruir información importante de la organización	Media	4	12	3	Intolerable

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para el Portal Web de la Gobernación de Nariño es de 3, es decir, intolerable y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Cuadro 40. Estimación del Riesgo Soporte Técnico

Activo PGT-01		**PGT-01 Soporte Técnico**		
Administrador		**Administrador de Sistemas**		
Degradación		**50%**		
Impacto		**3**	**Moderado**	
Tipo activo		**Personal**		
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**

							2.6	Tolerable
				Frecuencia (F)		R	NR	
E	E19	Fugas de información	Falta de controles, al haber fuga de información esta puede ser modificada o usada para beneficios propios llevando a pérdida de confianza de la organización	Baja	3	9	3	Intolerable
	E28	Indisponibilidad del personal	Falta de controles, al haber indisponibilidad del personal pueden dejar ausentes sus puestos de trabajo dejando así al no desarrollo de sus labores	Muy baja	2	6	2	Tolerable
A	A28	Indisponibilidad del personal	Falta de controles, ejecutar información importante para la organización si el personal esta indispuesto	Muy baja	2	6	2	Tolerable
	A29	Extorsión	Mediante amenazas pueden sacar información importante para la organización	Baja	3	9	3	Intolerable
	A30	Ingeniería social	Falta de concientización del personal en las mejores prácticas de seguridad informática. Llevando a un afectación alta en la dimensión de confidencialidad	Baja	3	9	3	Intolerable

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para Soporte Técnico es de 2.6, es decir, Tolerable y por lo tanto no se requiere de atención inmediata.

Cuadro 41. Estimación del Riesgo Base de Datos Correo Electrónico Institucional

Activo PGT-08		**PGT-08 Base de Datos Correo Electrónico Institucional**						
Administrador		**Administrador de Sistemas**						
Degradación		**100%**						
Impacto		**8**	**Desastroso**					
Tipo activo		**Datos / Información**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
Errores y fallos no intencionados	E1	Errores de los usuarios	Los usuarios no cuentan con capacitación para el manejo del activo	Media	4	32	4	Extremo
	E2	Errores del administrador	Algunos equipos del Proceso de Gestión TIC No están actualizados por software de protección y reparación de virus	Media	4	32	4	Extremo
	E3	Errores de monitorización	No se realizan correctamente los mantenimientos	Baja	3	24	4	Extremo
	E18	Destrucción de la información	No existe un protocolo para la clasificación de la información	Baja	3	24	4	Extremo
	E19	Fugas de información	Falta de interés por aplicar las políticas de seguridad	Muy baja	2	16	4	Extremo
	A3	Manipulación de los registros de actividad	Falta de controles	Media	4	32	4	Extremo
	A5	Suplantación de la identidad del usuario	No existe una implementación de procesos rigurosos para actualizar las contraseñas	Muy baja	2	16	4	Extremo
Ataques intencionados	A6	Abuso de privilegios de acceso	No existe mecanismos de control	Baja	3	24	4	Extremo
	A15	Modificación deliberada de la información	No realizan copias de seguridad periódicamente	Muy baja	2	16	4	Extremo
	A19	Divulgación de información	No hay mayor seguridad para la información	Muy baja	2	16	4	Extremo
	E1	Errores de los usuarios	Los usuarios no cuentan con capacitación para el manejo del activo	Baja	3	24	4	Extremo
	E2	Errores del administrador	Algunos equipos del Proceso de Gestión TIC No están actualizados por software de protección y reparación de virus	Muy baja	2	16	4	Extremo
	E3	Errores de monitorización	No se realizan correctamente los mantenimientos	Baja	3	24	4	Extremo
	E18	Destrucción de la información	No existe un protocolo para la clasificación de la información	Baja	3	24	4	Extremo

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para la Base de Datos Correo Electrónico Institucional es de 4, es decir, extremo y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Cuadro 42. Estimación del Riesgo Código Fuente Portal Web de la Gobernación de Nariño, Portales.

Activo PGT-03		**PGT-03 Código Fuente Portal Web de la Gobernación de Nariño, Portales.**						
Administrador		**Administrador Portal Web**						
Degradación		**100%**						
Impacto		**8**	**Desastroso**					
Tipo activo		**Datos/información**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
De origen industrial	I8	Fuego	No existe sistema de alarma contra incendios.	Muy baja	2	16	4	Extremo
E	E2	Errores del administrador	La actualización del antivirus no se actualiza diariamente	Media	4	32	4	Extremo
	E4	Errores de configuración	No cuenta con una protección segura a los ataques al sitio web	Media	4	32	4	Extremo
	E19	Fugas de información	Los datos no son correctamente protegidos	Media	4	32	4	Extremo
Ataques intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido	Muy baja	2	16	4	Extremo
	A7	Uso no previsto	Autorización insuficiente	Baja	3	24	4	Extremo
	A24	Denegación de servicio	No cuenta con la suficiente protección a los Ataques maliciosos	Media	4	32	4	Extremo
	A26	Ataque destructivo	No se cuenta con la suficiente protección	Media	4	32	4	Extremo

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para el Código fuente Portal Web de la Gobernación de Nariño, Portales es de 4, es decir, extremo y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Cuadro 43. Estimación del Riesgo Correo Electrónico Institucional

Activo PGT-07	**PGT-07 Correo Electrónico Institucional**	
Administrador	**Administrador Portal Web**	
Degradación	**100%**	
Impacto	**8**	**Desastroso**

Tipo activo		Sistema de Información						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							4	Extremo
				Frecuencia (F)		**R**	**NR**	
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente alterna de corriente eléctrica	Muy baja	2	16	4	Extremo
	I8	Fallo de servicio de comunicaciones	Baja capacidad de respuesta	Baja	3	24	4	Extremo
E	E2	Errores del administrador	No existe un análisis de seguridad para todos los correos spam que llegan	Media	4	32	4	Extremo
	E21	Errores de mantenimiento / actualización de programas (Software)	No se mantienen actualizados los parches de seguridad.	Media	4	32	4	Extremo

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para el Correo Electrónico Institucional es de 4, es decir, extremo y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Cuadro 44. Estimación del Riesgo Computadores de Escritorio

Activo PGT-13		**PGT-13 Computadores de Escritorio**						
Administrador		**Soporte Técnico**						
Degradación		**50%**						
Impacto		**3**	**Moderado**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**				
							3	Intolerable
				Frecuencia (F)		**R**	**NR**	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. No poseen extintor en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable
	N2	Daños por agua	Los computadores de escritorio se encuentra ubicados sin ninguna precaución	Bajo	3	9	3	Intolerable
	N*	Desastres naturales	El Proceso de Gestión TIC se encuentra en zona media de riesgo de desastre natural de origen de inundación debido a su mala ubicación en el primer piso	Baja	3	9	3	Intolerable
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente de energía alterna	Baja	3	9	3	Intolerable
	I7	Condiciones inadecuadas de temperatura o humedad	No cuentan con aire acondicionado en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3	9	3	Intolerable
E	E1	Errores de los usuarios	No existe un manual para el uso de las diferentes aplicaciones	Baja	3	9	3	Intolerable
	E2	Errores del administrador	No existe un protocolo para la instalación de las diferentes aplicaciones	Baja	3	9	3	Intolerable
	E4	Errores de configuración	No existe un manual para la debida configuración de los equipos de computo	Baja	3	9	3	Intolerable
	E21	Errores de mantenimiento / actualización de programas (hardware)	No cuentan con una política de mantenimiento	Baja	3	9	3	Intolerable
	E25	Perdida de equipos	No existen las suficientes cámaras de seguridad en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable

Ataques intencionados	A6	Difusión de software dañino	Debido a la gran cantidad de equipos de cómputo que están destinados para los usuarios y la falta de asesoría puede causar daños	Baja	3	9	3	Intolerable
	A11	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	9	3	Intolerable
	A3	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3	9	3	Intolerable

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para los Computadores de Escritorio es de 3, es decir, intolerable y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Cuadro 45. Estimación del Riesgo Computadores Portátiles

Activo PGT-14		**PGT-14 Computadores Portátiles**							
Administrador		**Soporte Técnico**							
Degradación		**50%**							
Impacto		**3**	**Moderado**						
Tipo activo		**Hardware**							
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					
							3	Intolerable	
				Frecuencia (F)		**R**	**NR**		
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. No poseen extintor en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable	
	N2	Daños por agua	Los computadores portátiles se encuentra ubicados sin ninguna precaución	Bajo	3	9	3	Intolerable	
	N*	Desastres naturales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3	9	3	Intolerable	
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente de energía alterna	Baja	3	9	3	Intolerable	
	I7	Condiciones inadecuadas de temperatura o humedad	No cuentan con aire acondicionado en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable	
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3	9	3	Intolerable	
E	E1	Errores de los usuarios	No existe un manual para el uso de las diferentes aplicaciones	Baja	3	9	3	Intolerable	
	E2	Errores del administrador	No existe un protocolo para la instalación de las diferentes aplicaciones	Baja	3	9	3	Intolerable	
	E4	Errores de configuración	No existe un manual para la debida configuración de los equipos de computo	Baja	3	9	3	Intolerable	
	E21	Errores de mantenimiento / actualización de programas (hardware)	No cuentan con una política de mantenimiento	Baja	3	9	3	Intolerable	
	E25	Perdida de equipos	No existen las suficientes cámaras de seguridad en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable	

Ataques intencionados	A6	Difusión de software dañino	Debido a la gran cantidad de equipos de cómputo que están destinados para los usuarios y la falta de asesoría puede causar daños	Baja	3	9	3	Intolerable
	A11	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	9	3	Intolerable
	A3	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3	9	3	Intolerable

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para los Computadores Portátiles es de 3, es decir, intolerable y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Cuadro 46. Estimación del Riesgo Impresoras

Activo PGT-15	**PGT-15 Impresoras**		
Administrador	**Soporte Técnico**		
Degradación	**1%**		
Impacto	**1**	**Insignificante**	
Tipo activo	**Hardware**		

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				
							1.4	Aceptable
				Frecuencia (F)		R	NR	
Desastres naturales	N1	Fuego	Falta de protección contra fuego	Muy baja	2	2	1	Aceptable
	N2	Daños por agua	Falta de protección física adecuada	Raro	1	1	1	Aceptable
	N*	Desastres naturales	Condiciones de los locales donde los recursos son fácilmente afectados por desastres	Muy baja	2	2	1	Aceptable
De origen industrial	I1	Fuego	No poseen extintor en la oficina de Proceso de Gestión TIC	Muy baja	2	2	1	Aceptable
	I2	Daños por agua	Falta de protección física adecuada	Raro	1	1	1	Aceptable
	I*	Desastres industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2	2	1	Aceptable
	I5	Avería de origen físico o lógico	Mal ubicación de las impresoras	Muy baja	2	2	1	Aceptable
E	E1	Errores de los usuarios	Falta de conocimiento para el uso de la aplicación	Baja	3	3	2	Aceptable
	E4	Errores de configuración	Falta de control	Baja	3	3	2	Aceptable
	E25	Perdida de equipos	Falta de protección física	Baja	3	3	2	Aceptable
Ataques intencionados	A4	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3	3	2	Aceptable

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para las Impresoras es de 1.4, es decir, aceptable y por lo tanto no se requiere de atención inmediata.

Cuadro 47. Estimación del Riesgo Escáner

Activo PGT-16		**PGT-16 Escáner**						
Administrador		**Soporte Técnico**						
Degradación		**1%**						
Impacto		**1**	**Insignificante**					
Tipo activo		**Hardware**						
Tipo	**ID**	**Amenaza**	**Exposición /Vulnerabilidad**	**Riesgo Actual**				
							1.33	Aceptable
				Frecuencia (F)		**R**	**NR**	
Desastres naturales	N1	Fuego	Falta de protección contra fuego	Muy baja	2	2	1	Aceptable
	N2	Daños por agua	Falta de protección física adecuada	Raro	1	1	1	Aceptable
	N*	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Muy baja	2	2	1	Aceptable
De origen industrial	I1	Fuego	No poseen extintor en la oficina de Proceso de Gestión TIC	Muy baja	2	2	1	Aceptable
	I2	Daños por agua	Falta de protección física adecuada	Raro	1	1	1	Aceptable
	I*	Desastres industriales	No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Muy baja	2	2	1	Aceptable
	I5	Avería de origen físico o lógico	Mala ubicación del escáner	Muy baja	2	2	1	Aceptable
E	E1	Errores de los usuarios	Falta de conocimiento para el uso de la aplicación	Baja	3	3	2	Aceptable
	E4	Errores de configuración	Falta de control	Baja	3	3	2	Aceptable
	E25	Perdida de equipos	Falta de protección física	Baja	3	3	2	Aceptable
Ataques intencionados	A4	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3	3	2	Aceptable
	A25	Robo	Falta de protección física	Muy baja	2	2	1	Aceptable

Por último, con ayuda de la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para los Escáner es de 1.33, es decir, aceptable y por lo tanto no se requiere de atención inmediata.

Con los resultados obtenidos en este análisis se procede a la evaluación de riesgos.

Para cada activo de información, el proceso concluye si el Nivel de Riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles necesarios.

Para el Servidor NS1 como el Nivel de Riesgo es Intolerable; es necesario definir el tratamiento a seguir.

Primeramente se descarta la opción de evitar el riesgo, ya que este es un activo de muy alto valor y el retiro del mismo no permitiría la prestación de muchos servicios fundamentales para la unidad de Proceso de Gestión Tic de la Gobernación de Nariño.

La opción de transferir el riesgo por medio de la adquisición de un seguro tampoco es la adecuada, puesto que los costos de las pólizas en la mayoría de los casos son muy elevados y el Proceso de Gestión Tic no cuenta con los recursos necesarios para adquirirlos.

No obstante, el tratamiento a seguir consiste en la definición de nuevos controles de tipo preventivo y/o correctivo que permitan reducir los niveles de riesgo del Servidor NS1 pase de un nivel Intolerable a un nivel tolerable, o en el mejor de los casos a un nivel aceptable de ser posible; que es lo que se espera que suceda con los demás activos de información que tienen un nivel de riesgo similar o peor. Por lo tanto, se procede a realizar el diagnostico o Análisis de Brecha para verificar los controles existentes en la unidad de Proceso de Gestión Tic de la Gobernación de Nariño con respecto al estándar ISO/IEC 27002:2005 y así poder determinar con mayor claridad el tratamiento a seguir para cada uno de los activos con nivel de riesgo tolerable, intolerable o extremo.

8.10 LISTA DE CHEQUEO

Cuadro 48. Lista de chequeo

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
1	A.5.Políticas de seguridad	A.5.1. Directrices de la Dirección en seguridad de la información	A.5.1.1. Políticas para la seguridad de la información	¿La empresa posee un conjunto de políticas para la seguridad de la información?	5	8	38	Repetible
			A.5.1.2. Revisión de las políticas para seguridad de la información	¿Se cuenta con un plan de revisión y cumplimiento de las políticas de la seguridad de la información?	2	10	17	Inexistente
2	A.6. Aspectos organizativos de la SI	A.6.1. Organización interna	A.6.1.1. Roles y responsabilidades para la seguridad de la información	¿Se cuenta con un equipo líder del proceso de seguridad informática?	3	9	25	Repetible
			A.6.1.2. Separación de deberes	¿Se realizan verificaciones a las tareas asignadas al equipo encargado?	3	10	23	Repetible
			A.6.1.3. Contacto con las autoridades	¿Se cuenta con un protocolo de alerta en caso de la presentación de emergencias (robos, pérdidas, personas a las cuales se debe acudir)?	6	9	40	Definido
			A.6.1.4. Contacto con grupos de interés especial	¿Se realizar asignación de responsabilidades para la seguridad de la información?	4	8	33	Repetible
			A.6.1.5. Seguridad de la información en la gestión de proyectos	¿Existe contacto con las autoridades?	4	6	40	Definido

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
		A.6.2. Dispositivos para movilidad y teletrabajo	A.6.2.1. Política para dispositivos móviles	¿La empresa tiene una política de uso de dispositivos para movilidad?	6	8	43	Definido
			A.6.2.2. Teletrabajo	¿La empresa implementa el teletrabajo?	0	14	0	Inexistente
3	A.7. Seguridad ligada a los recursos humanos	A.7.1. Antes de la contratación	A.7.1.1. Selección	¿Se realiza Investigación de antecedentes?	7	4	64	Definido
			A.7.1.2. Términos y condiciones del empleo	¿En los acuerdos contractuales en donde se especifiquen las responsabilidades y las de la organización en cuanto a la seguridad la información?	3	5	38	Repetible
		A.7.2. Durante la contratación	A.7.2.1. Responsabilidad de la dirección	¿Se encuentra contratado un profesional específicamente para la realización del tema?	2	7	22	Repetible
			A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	¿la empresa capacita a sus funcionarios en cuanto a la seguridad de la información?	4	12	25	Repetible
			A.7.2.3. Proceso disciplinario	¿Se realizan socializaciones para actualizar a los empleados en los diferentes cambios generados?	9	6	60	Definido
		A.7.3. Terminación o cambio de puesto de trabajo	A.7.3.1. Terminación o cambio de responsabilidades de empleo	¿Se tienen definidos las responsabilidades y deberes de seguridad de la información una vez el empleado termine su contratación o se le realice un cambio de puesto?	5	4	56	Definido

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
4	A.8. Gestión de Activos	A.8.1. Responsabilidad sobre los activos	A.8.1.1. Inventario de activos	¿Se cuenta con un inventario de activos actualizado?	4	7	36	Repetible
			A.8.1.2. Propiedad de los activos	¿Se cuenta con un procedimiento para la solicitud de algún equipo faltante y necesario para el desempeño?	12	4	75	Gestionado
			A.8.1.3. Uso aceptable de los activos	¿Los funcionarios de la empresa hacen buen uso de los activos informáticos?	6	5	55	Definido
			A.8.1.4. Devolución de activos	¿Los empleados de la entidad al terminar su contrato hacen devolución de los activos?	14	1	93	Optimizado
		A.8.2. Clasificación de la información	A.8.2.1. Clasificación de la información	¿Se cuenta con un sistema de etiquetado de los equipos para verificar su propiedad?	12	2	86	Gestionado
			A.8.2.2. Etiquetado de la información	¿Se tienen implementado un procedimiento para el etiquetado de la información?	8	3	73	Gestionado
			A.8.2.3. Manejo de activos	¿Se manejan los activos de acuerdo al procedimiento implementado?	6	3	67	Definido
5	A.9. Control de Acceso	A.9.1. Requisitos de negocio para el control de accesos	A.9.1.1. Política de control de acceso	¿Se tiene control sobre los accesos a las redes por parte personas internas a la compañía?	7	1	88	Gestionado
			A.9.1.2. Política sobre el uso de los servicios de red	¿La empresa posee una política de control de accesos?	5	5	50	Definido

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
				¿Se tiene control sobre los accesos a las redes por parte personas externas a la compañía?	6	6	50	Definido
		A.9.2. Gestión de acceso de usuario	A.9.2.1. Registro y cancelación del registro de usuarios	¿Se lleva un control sobre los usuarios de los sistemas de información?	5	4	56	Definido
			A.9.2.2. Suministro de acceso a usuarios	¿Se tiene un reporte de los procesos realizados por cada usuario en los Sistemas de información?	1	6	14	Inexistente
			A.9.2.3. Gestión de derechos de acceso privilegiado	¿La empresa realiza gestión de altas/bajas en el registro de usuarios?	9	4	69	Definido
			A.9.2.4. Gestión de información de autenticación secreta de usuarios	¿Cuenta la empresa con un procedimiento que identifique los diferentes niveles de seguridad de acceso a las herramientas o sistemas de información?	4	5	44	Definido
			A.9.2.5. Revisión de los derechos de acceso de usuarios	¿Se realiza una revisión periódica de los logs de acceso a las diferentes herramientas o sistemas de información?	2	5	29	Repetible
			A.9.2.6. Retiro o ajuste de los derechos de acceso	¿Se realiza una revisión periódica de los derechos de acceso, realizando de esta manera la eliminación de los usuarios que ya no trabajan en la empresa?	4	2	67	Definido
		A.9.3. Responsabilidad de los usuarios	A.9.3.1. Uso de la información de autenticación secreta	¿Los usuarios cumplen a cabalidad con el buen uso de la información secreta (No divulgación)?	11	1	92	Optimizado

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
		A.9.4. Control de acceso a sistemas y aplicaciones	A.9.4.1. Restricción de acceso de la información	¿Se cuenta con la decisión de niveles de acceso con relación a cada usuario?	8	2	80	Gestionado
			A.9.4.2. Procedimiento de ingreso seguro	¿Se cuenta con la asignación de contraseñas para el acceso a la información?	12	1	92	Optimizado
			A.9.4.3. Sistema de gestión de contraseñas	¿Se cuenta con un administrador de la base de datos y el código de aplicaciones?	10	1	91	Optimizado
			A.9.4.4. Uso de programas utilitarios privilegiados	¿La empresa hace uso de herramientas de administración de sistemas?	6	3	67	Definido
			A.9.4.5. Control de acceso a códigos fuente de programas	¿Se tiene definido los roles de las personas que tienen acceso al código fuente y se encuentra esta información en lugares seguros?	3	4	43	Definido
6	A.10. Criptografía	A.10.1. Controles criptográficos	A.10.1.1. Política sobre el uso de controles criptográficos	¿Se tiene una política sobre el uso de controles criptográficos para la protección de la información?	0	8	0	Inexistente
			A.10.1.2. Gestión de llaves	¿Se tiene una política con la cual se conoce el uso, protección y tiempo de vida de las llaves criptográficas?	0	8	0	Inexistente
7	A.11. Seguridad física y del entorno	A.11.1. Áreas seguras	A.11.1.1 Perímetro de seguridad física	¿Los servidores y puntos de conexión se encuentran ubicados en un lugar seguro?	10	2	83	Gestionado

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.11.1.2. Controles físicos de entrada	¿Las entradas a los lugares prohibidos se encuentran con algún mecanismo de seguridad, por ejemplo biométricos?	5	6	45	Definido
			A.11.1.3. Seguridad de oficinas, recintos e instalaciones	¿Las oficinas, recintos e instalaciones cuentan con algún tipo de seguridad? Por ejemplo Vigilantes, cámaras.	11	2	85	Gestionado
			A.11.1.4. Protección contra amenazas externas y ambientales	¿El lugar donde se encuentran los servidores cuenta con las medidas de seguridad apropiadas (Extintores, aire acondicionado, entre otros)?	11	2	85	Gestionado
			A.11.1.5. Trabajo en áreas seguras	¿Se tiene establecido un procedimiento que indique como se debe realizar el trabajo en las áreas seguras?	1	9	10	Inexistente
			A.11.1.6. Áreas de despacho y carga	¿El lugar donde se realiza el despacho y carga de herramientas (computadores, teclados, entre otros), cuenta con medidas de seguridad?	5	8	38	Repetible
		A.11.2. Seguridad de los equipos	A.11.2.1. Ubicación y protección de los equipos	¿La infraestructura eléctrica se encuentra bien instalada y sin riesgos?	7	7	50	Definido
			A.11.2.2. Servicios de suministro	¿Los equipos informáticos y accesos de red, están seguros?	5	9	36	Repetible
			A.11.2.3. Seguridad del cableado	¿Se realiza mantenimiento a los equipos periódicamente?	10	4	71	Gestionado

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.11.2.4. Mantenimiento de equipos	¿Se cuenta con puestos de trabajos agradables y seguros?	11	3	79	Gestionado
			A.11.2.5. Retiro de activos	¿Cuándo se va a realizar un cambio de algún computador a otro puesto de trabajo, se tiene un conducto regular para realizar dicho proceso?	10	2	83	Gestionado
			A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	¿Cuándo un activo es sacado de la empresa, este cuenta con las medidas de seguridad en caso de tener pérdida?	5	5	50	Definido
			A.11.2.7. Disposición segura o reutilización de equipos	¿Se realiza un backup y limpieza de los equipos de cómputo antes de entregarlo a otra persona?	11	1	92	Optimizado
			A.11.2.8. Equipos de usuario desatendidos	¿Los equipos que no tienen personal asignado se les dá una protección adecuada?	4	6	40	Definido
			A.11.2.9. Política de escritorio limpio y pantalla limpia	¿Se tiene una política de escritorio limpio para los papeles y medios de almacenamiento removibles?	7	7	50	Definido
8	A.12. Seguridad en las operaciones	A.12.1. Procedimientos operacionales y responsabilidades	A.12.1.1. Procedimientos de operación documentados	¿Se documentan los procedimientos de operación y se ponen a disposición de los usuarios?	4	5	44	Definido
			A.12.1.2. Gestión de cambios	¿Se tiene un procedimiento de gestión de cambios en el área de desarrollo de los aplicativos?	3	5	38	Repetible

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.12.1.3. Gestión de capacidad	¿Se realiza periódicamente revisión de los recursos, espacio de los diferentes servidores de la empresa?	4	4	50	Definido
			A.12.1.4. Separación de los ambientes de desarrollo, pruebas y operación	¿Se cuenta con ambientes de desarrollo, pruebas y producción separados?	2	4	33	Repetible
		A.12.2. Protección contra códigos maliciosos	A.12.2.1. Controles contra códigos maliciosos	¿Se cuenta con antivirus activo en todos los equipos de la compañía?	6	6	50	Definido
				¿Se cuenta con antivirus activo en todos los equipos de la compañía?	6	7	46	Definido
				¿Se realizan monitoreo en prevención a ataques que se generan al sistema?	4	5	44	Definido
		A.12.3. Copias de seguridad	A.12.3.1. Respaldo de información	¿Se realizan periódicamente copias de seguridad de la información?	8	2	80	Gestionado
		A.12.4. Registro y seguimiento	A.12.4.1. Registro de eventos	¿Se realiza revisión periódica de los logs de las diferentes herramientas con el fin de verificar las fallas y eventos de seguridad de la información?	1	2	33	Repetible
			A.12.4.2. Protección de la información de registro	¿Se tiene un control de acceso no autorizado, con el fin de proteger la información de algún tipo de modificación?	11	1	92	Optimizado

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.12.4.3. Registros del administrador y del operador	¿Las actividades realizadas por los administradores de las diferentes herramientas son monitoreadas?	1	6	14	Inexistente
			A.12.4.4. Sincronización de relojes	¿Los relojes de los equipos de cómputo, servidores y demás sistemas, se encuentran sincronizados?	6	3	67	Definido
		A.12.5. Control de software operacional	A.12.5.1. Instalación de software en sistemas operativos	¿Se tiene alguna regla que impida a los usuarios finales realizar la instalación de software?	10	2	83	Gestionado
		A.12.6. Gestión de la vulnerabilidad técnica	A.12.6.1. Gestión de las vulnerabilidades técnicas	¿Se realizan pruebas de penetración para encontrar vulnerabilidades en los sistemas y así prevenirlas?	1	8	11	Inexistente
			A.12.6.2. Restricciones sobre la instalación de software	¿Se tiene un procedimiento definido para las personas de soporte sobre la instalación del software que se puede realizar en los equipos?	6	2	75	Gestionado
		A.12.7. Consideraciones sobre auditorias de sistemas de información	A.12.7.1. Información de controles de auditoría de sistemas	¿Los sistemas de información de la entidad, como las Bases de Datos cuentan con un sistema de auditoria activo?	3	5	38	Repetible
9		A.13.1. Gestión de la seguridad de las redes	A.13.1.1. Controles de redes	¿Se tiene un reporte de las transacciones realizadas en las redes de la compañía?	1	5	17	Inexistente
			A.13.1.2. Seguridad de los servicios de red	¿En la empresa existen mecanismos de seguridad asociados a servicios de red?	3	5	38	Repetible

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.13.1.3. Separación en las redes	¿Se tiene algún procedimiento sobre el acceso a las redes?	3	5	38	Repetible
		A.13.2. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información	¿Se cuenta con protocolos de intercambio de información con externos?	2	5	29	Repetible
			A.13.2.2. Acuerdos sobre transferencia de información	¿Se cuenta con servicio de email dentro del dominio de la compañía?	11	1	92	Optimizado
			A.13.2.3. Mensajería electrónica	¿La información contenida en los correos cuenta con mecanismos de seguridad, como por ejemplo antivirus, protección por contraseña?	8	2	80	Gestionado
			A.13.2.4. Acuerdos de confidencialidad o de no divulgación	¿Se realiza revisión y actualización de los acuerdos de confidencialidad?	0	7	0	Inexistente
10	A.14. Adquisición, desarrollo y mantenimiento de sistemas	A.14.1. Requisitos de seguridad de los sistemas de información	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	Se han implementado protocolos de seguridad en los sistemas de información	4	3	57	Definido
			A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas	Se cuenta con control de las transacciones realizadas a nivel externo por medio del SI	1	5	17	Inexistente

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.14.1.3. Protección de transacciones de los servicios de las aplicaciones	¿Se realiza la protección de la información involucrada en las transacciones de los servicios de las aplicaciones, por ejemplo certificados digitales?	2	5	29	Repetible
		A.14.2. Seguridad en los procesos de desarrollo y soporte	A.14.2.1. Política de desarrollo seguro	Se cuenta con un procedimiento para la solicitud de desarrollo de software	3	3	50	Definido
			A.14.2.2. Procedimientos de control de cambios en sistemas	Se lleva un control de las versiones de las aplicaciones desarrolladas	3	3	50	Definido
			A.14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Se cuenta con un protocolo para la aplicación de pruebas a los SI desarrollados	0	6	0	Inexistente
			A.14.2.4. Restricciones en los cambios a los paquetes software	Se cuenta con un procedimiento para la puesta en producción de un desarrollo en SI	0	5	0	Inexistente
			A.14.2.5. Principios de construcción de sistemas seguros	Se tienen en cuenta principios de seguridad en un entorno de desarrollo	1	5	17	Inexistente
			A.14.2.6. Ambiente de desarrollo seguro	¿El lugar en donde se encuentra el código y las aplicaciones desarrolladas es seguro?	4	1	80	Gestionado
			A.14.2.7. Desarrollo contratado externamente	¿Cuenta la empresa con un hosting tercerizado?	7	1	88	Gestionado

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.14.2.8. Pruebas de seguridad de sistemas	¿Se realizan pruebas de funcionalidad a las aplicaciones desarrolladas?	6	1	86	Gestionado
			A.14.2.9. Pruebas de aceptación de sistemas	¿Cuándo se realizan actualizaciones a los desarrollos de aplicaciones, se hacen pruebas de aceptación?	3	3	50	Definido
		A.14.3. Datos de prueba	A.14.3.1. Protección de datos de prueba	¿Cuándo se realizan las pruebas se trabajan con datos falsos?	4	2	67	Definido
11	A.15. Relación con los proveedores	A.15.1. Seguridad de la información en las relaciones con los proveedores	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores	¿Se cuenta con una política de seguridad de la información asociada a terceros?	2	8	20	Repetible
			A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	¿Se tienen establecidos los requisitos y procedimientos de acceso a las instalaciones por parte de terceros?	4	7	36	Repetible
			A.15.1.3. Cadena de suministro de tecnología de información y comunicación	¿Se tiene acuerdos con terceros que incluyan los requisitos para tratar los riesgos de seguridad de la información asociados a la cadena de suministro?	0	8	0	Inexistente
		A.15.2. Gestión de la prestación de servicios con los proveedores	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores	¿Se hace un seguimiento de la prestación del servicio de terceros?	8	1	89	Gestionado

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.15.2.2. Gestión de cambios en los servicios de proveedores	¿Se tiene una gestión de cambios en el suministro de servicios por parte de terceros?	4	5	44	Definido
12	A.16. Gestión de incidentes en la seguridad de la información	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1. Responsabilidad y procedimientos	¿Se cuenta con un procedimiento para la identificación de un incidente de seguridad de la información?	2	7	22	Repetible
			A.16.1.2. Reporte de eventos de seguridad de la información	¿Se cuenta con un procedimiento para el reporte de un incidente de seguridad de la información?	2	7	22	Repetible
			A.16.1.3. Reporte de debilidades de seguridad de la información	¿Se cuenta con un procedimiento para el trámite de un incidente de seguridad de la información?	1	8	11	Inexistente
			A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones de la información	¿Se tiene identificado un responsable para la gestión de los incidentes de seguridad de la información?	4	5	44	Definido
			A.16.1.5. Respuesta a incidentes de seguridad de la información	¿Los incidentes informáticos son tratados y solucionados a tiempo?	6	1	86	Gestionado
			A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información	¿Se solicitan evidencias de los incidentes de seguridad de información identificados?	3	5	38	Repetible

#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
			A.16.1.7. Recolección de evidencia	¿Se tiene definido un procedimiento en donde se especifique como debe realizarse la identificación, recolección, adquisición y preservación de información que es tomada como evidencia?	1	7	13	Inexistente
13	A.17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	A.17.1. Continuidad de la seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información	¿Se hace seguimiento a la seguridad de la información?	4	4	50	Definido
			A.17.1.2. Implementación de la continuidad de la seguridad de la información	¿Se tiene un plan de continuidad?	1	6	14	Inexistente
			A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se realiza regularmente la verificación del plan de continuidad?	0	6	0	Inexistente
		A.17.2. Redundancias	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información	¿Las instalaciones de procesamiento de información se implementan con redundancia suficiente para cumplir los requisitos de disponibilidad?	0	5	0	Inexistente

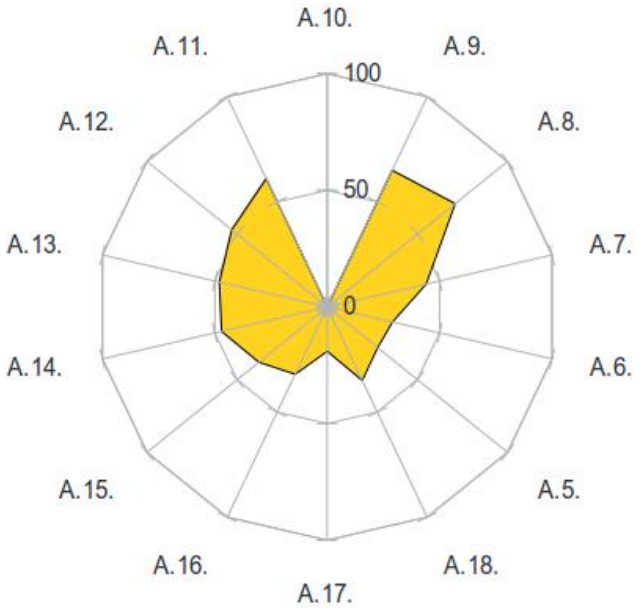
#	Dominio	Objetivo de Control	Controles	Pregunta existencia control	TOTAL SI	TOTAL NO	% DE CUMPLIMIENTO	ESTADO
14	A.18. Cumplimiento	A.18.1. Cumplimiento de requisitos legales y contractuales	A.18.1.1. Identificación de requisitos legales y contractuales	¿Se realizan auditorías internas para verificar el cumplimiento de la norma?	3	9	25	Repetible
			A.18.1.2. Derechos de propiedad intelectual	¿Se cuenta con mecanismos de protección de la información?	7	7	50	Definido
			A.18.1.3. Protección de registros	¿Se tiene documentado todo el proceso de seguridad y protección de la información?	3	9	25	Repetible
			A.18.1.4. Privacidad y protección de datos personales	¿Se asegura la privacidad y la protección de la información de datos personales?	7	5	58	Definido
		A.18.2. Revisiones de la seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información	¿Se cumple con las políticas y normas de seguridad?	3	9	25	Repetible
			A.18.2.2. Cumplimiento con las políticas y normas de seguridad	¿Se realizan comités de seguridad con los altos directivos en donde se revisen con regularidad el cumplimiento de las políticas de seguridad en todas las áreas?	3	8	27	Repetible
			A.18.2.3. Revisión del cumplimiento técnico	¿Se realiza revisión periódica de los sistemas con el fin de verificar el cumplimiento de las políticas de seguridad de la información?	3	7	30	Repetible

8.11 NIVEL DE MADUREZ

Tabla 14 de la gobernacion de Nariño por ISO 27002

	Data			
DOMINIO	**Sum – TOTAL SI**	**Sum – TOTAL NO**	**% DE CUMPLIMIENTO**	**Estado**
A.10.Cifrado	0	16	0	Inexistente
A.11.Fisica y Ambiental	113	73	61	Definido
A.12.Operativas	76	67	53	Definido
A.13.Telecomunicaciones	28	30	48	Definido
A.14.Adquisicion Desarrollo y mantenimiento de sistemas de información	38	43	47	Definido
A.15.Suministradores	18	29	38	Repetible
A.16.Incidentes	19	40	32	Repetible
A.17.Continuidad Negocio	5	21	19	Inexistente
A.18.Cumplimiento	29	54	35	Repetible
A.5.Politicas	7	18	28	Repetible
A.6.Organizacion	26	64	29	Repetible
A.7.Recursos humanos	30	38	44	Definido
A.8.Activos	62	25	71	Gestionado
A.9.Accesos	93	50	65	Definido
Total Resultados	**544**	**568**		

Figura 5.Nivel de Madurez


A.10.
A.9.
A.8.
A.7.
A.6.
A.5.
A.18.
A.17.
A.16.
A.15.
A.14.
A.13.
A.12.
A.11.
100
50
0

8.12 PLAN DE TRATAMIENTO

Cuadro 49. Análisis y evaluación de riesgos Servidor NS1

Activo PGT-02		PGT-02 NS1				Tipo		Hardware / equipos											
Administrador		Soporte Técnico				Degradación		100%											
Impacto		8	Desastroso			Ubicación		Proceso de Gestión TIC Gobernación de Nariño											
Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado									
							3.91	Intolerable						2.61	Tolerable				
				Frecuencia (F)		R	NR			Frecuencia (F')		R'	NR'						
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios. No posee un solo extintor en la sala de servidores	Muy baja	2	16	4	Extremo	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable					
	N2	Daños por agua		Raro	1	8	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable					
	N*	Desastres naturales	El Proceso de Gestión TIC se encuentra en zona media de riesgo de desastre natural de origen de inundación debido a su mala ubicación en el primer piso	Muy baja	2	16	4	Extremo	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable					

De origen industrial	I1	Fuego	No existe sistema de alarma contra incendios.	Muy baja	2	16	4	Extremo	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano. 9.2.3 - Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Raro	1	3	2	Tolerable
	I2	Daños por agua		Raro	1	8	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable
	I3	Contaminación mecánica	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3	24	4	Extremo	9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.2.1 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable
	I4	Contaminación electromagnética	Los racks no cuentan con aisladores.	Muy baja	2	16	4	Extremo	9.2.1 - El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Muy baja	2	6	2	Tolerable
	I5	Avería de origen físico o lógico	En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad.	Baja	3	24	4	Extremo	9.2.1 - El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Raro	1	3	2	Tolerable

	I6	Corte del suministro eléctrico	No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la unidad no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.	Muy baja	2	16	4	Extremo	9.2.3 - Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable
	I7	Condiciones inadecuadas de temperatura o humedad	No existe sistema de alarma de control de temperatura y humedad.	Baja	3	24	4	Extremo	9.2.1 - El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable

	I11	Emanaciones electromagnéticas	Los racks no cuentan con aisladores.	Baja	3	24	4	Extremo	9.2.1 El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Muy baja	2	6	2	Tolerable
E	E2	Errores del administrador	Falta de conocimiento del administrador.	Muy baja	2	16	4	Extremo	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes. 8.1.1 Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable
	E23	Errores de mantenimiento/actualización de equipos	No existe hoja de vida del servidor NS1 Falta de conocimiento del administrador.	Baja	3	24	4	Extremo	8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 12.5.1 Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.	Raro	1	3	2	Tolerable

	E24	Caídas del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Baja	3	24	4	Extremo	9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 14.1.3 -Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requeridos, tras la interrupción o fallo de los procesos críticos de negocio.	Raro	1	3	2	Tolerable
	E25	Perdida de equipos	No existen la suficiente cámaras de seguridad en la organización	Muy baja	2	16	4	Extremo	9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Raro	1	3	2	Tolerable

Ataques intencionados	A6	Abuso de privilegios de acceso	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Proceso de Gestión TIC, y luego por la oficina de Soporte Técnico; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio, donde cada puerta cuenta con una sola chapa de seguridad	Baja	3	24	4	Extremo	8.2.3 - Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización. 11.2.2 - Se debería restringir y controlar la asignación y uso de los privilegios.	Raro	1	3	2	Tolerable

	A7	Uso no previsto	No cuenta con una hoja dej vida	Baja	3	24	4	Extremo	8.2.3 - Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad. 9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Raro	1	3	2	Tolerable

	A11	Acceso no autorizado	Cualquier persona puede entrar a la sala de servidores no existe un control	Baja	3	24	4	Extremo	9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Raro	1	3	2	Tolerable
	A23	Manipulación de equipos	Falta de controles para el ingreso a la sala de servidores	Baja	3	24	4	Extremo	9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Raro	1	3	2	Tolerable

	A24	Denegación de servicio	Falta de recursos necesarios. Falta de pljanes de continuidad del negocio	Baja	3	24	4	Extremo	9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 14.1.3 - Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requerido, tras la interrupción o fallo de los procesos críticos de negocio.	Raro	1	3	2	Tolerable
	A25	Robo	Como medida de control de acceso a la sala de servidores en la puerta no se cuenta con un control biométrico, sino con una cerradura de llave la cual no garantiza un control de quienes tienen los privilegios de entrar al sitio, ni manera de identificarlos. Para ingresar a la sala de servidores primeramente se debe pasar por la oficina del Proceso de Gestión TIC, y luego por la oficina de Soporte Técnico; cuyos controles de ingreso son únicamente puertas de madera con ventanas de vidrio, donde cada puerta cuenta con una sola chapa de seguridad.	Baja	3	24	4	Extremo	6.1.6 - Se deberían mantener los contactos apropiados con las autoridades pertinentes. 6.2.1 - Se deberían identificar los riesgos a la información y a las instalaciones del procesamiento que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso. 8.2.3 - Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad. 8.3.3 - Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios a la información y a las instalaciones del procesamiento a la finalización del empleo, contrato o acuerdo, o ser revisada en caso de cambio. 9.1.1 - Los perímetros de seguridad deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos fuera de las instalaciones sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad	Raro	1	3	2	Tolerable

Cuadro 50 Análisis y evaluación de riesgos de Portal web Gobernación de Nariño

Activo TI		PGT-04 Portal Web Gobernación de Nariño				Tipo		Sistema de Información									
Administrador		Administrador Portal Web				Degradación		50%									
Impacto		3	Moderado			Ubicación		Proceso de Gestión TIC									
Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado							
							3	Intolerable					2	Tolerable			
				Frecuencia (F)		R	NR			Frecuencia (F')		R'	NR'				
Errores y fallos no intencionados	E2	Errores del administrador	Un error del administrador puede conllevar a la disponibilidad de las aplicaciones los servicios que ellos soportan se verá seriamente afectado	Media	4	12	3	Intolerable	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes. 8.1.1 Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable
	E8	Difusión de software dañino	Hay poca capacitación para los empleados que manejan software de la organización	Baja	3	9	3	Intolerable	12.6 Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados.	Raro	1	3	2	Tolerable			

	E15	Alteración accidental de la información	No existe mediadas de control	Baja	3	9	3	Intolerable	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes. 5.1.2 La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.	Raro	1	3	2	Tolerable
	E18	Destrucción de información	No existe un protocolo para la limpieza del sitio web y un procedimiento de mantenimiento	Baja	3	9	3	Intolerable	10.7.3 Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados. 12.3.1 Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	Raro	1	3	2	Tolerable
	E19	Fugas de información	No existe medidas de control esta información puede ser modificada o usada para beneficios propios	Baja	3	9	3	Intolerable	6.1.1 Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización. 6.1.2 Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización.	Raro	1	3	2	Tolerable

	E20	Vulnerabilidades de los programas	No existe un procedimiento para llevar a cabo las pruebas de los programas antes de ponerlos en funcionamiento	Media	4	12	3	Intolerable	10.5.1 Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación	Muy baja	2	6	2	Tolerable
	E21	Errores de mantenimiento/ actualización de programas	No existe un protocolo para la actualización de las diferentes aplicaciones	Baja	3	9	3	Intolerable	9.2.4 Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 10.4.1 Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios. 11.3.2 Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada.	Muy baja	2	6	2	Tolerable
	A5	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	9	3	Intolerable	11.2.2 Se debería restringir y controlar la asignación y uso de los privilegios. 11.3.1 Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas. 11.3.2 Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada.	Raro	1	3	2	Tolerable
	A8	Difusión de software dañino	No existe un procedimiento para la actualización de software	Baja	3	9	3	Intolerable	10.4.1 Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.	Raro	1	3	2	Tolerable

Ataques intencionados	A9	[Re-] encaminamiento de mensajes	Falta de controles, esta falla permite desplegar en el navegador datos no confiables proporcionados por usuarios, generalmente inyectando código javascript malicioso. Estos datos pueden Secuestrar tu sitio web, permitiendo que tus usuarios sean re direccionados a sitios maliciosos o descarguen malware.	Baja	3	9	3	Intolerable	6.1.3 Se deberían definir claramente todas las responsabilidades para la seguridad de la información. 10.5.1 Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación 10.10.4 Se deberían registrar las actividades del administrador y de los operadores del sistema.	Raro	1	3	2	Tolerable
	A15	Modificación deliberada de la información	Falta de controles, afectara directamente la dimensión de integridad en un nivel muy alto, porque de presentarse ataques de modificación de información se va a ver alterados los datos almacenados, causando un caos informático y arrojando datos erróneos a la hora de las consultas transacciones en cada uno de los procesos normalizados dentro de las labores de la organización	Media	4	12	3	Intolerable	6.1.3 Se deberían definir claramente todas las responsabilidades para la seguridad de la información. 6.1.5 Se deberían identificar y revisar regularmente en los acuerdos aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la Organización. 7.2.1 La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización	Raro	1	3	2	Tolerable
	A18	Destrucción de información	No existe un control para la información importante sería muy grave destruir información importante de la organización	Media	4	12	3	Intolerable	10.7.3 Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados. 12.3.1 Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	Raro	1	3	2	Tolerable

Cuadro 51. Análisis y evaluación de riesgos de Soporte Tecnico

Activo PGT-01		PGT-01 Soporte Técnico				**Tipo**		Personal											
Administrador		Administrador de Sistemas				**Degradación**		50%											
Impacto		3	Moderado			**Ubicación**		Proceso de Gestión TIC											
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					**Control recomendado**	**Riesgo Residual Esperado**									
							2.6	**Tolerable**						**2**	**Tolerable**				
				Frecuencia (F)		**R**	**NR**			**Frecuencia (F')**		**R'**	**NR'**						
E	E19	Fugas de información	Falta de controles, al haber fuga de información esta puede ser modificada o usada para beneficios propios llevando a pérdida de confianza de la organización	Baja	3	9	3	Intolerable	6.1.1 Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización. 6.1.2 Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización.	Raro	1	3	2	Tolerable					
	E28	Indisponibilidad del personal	Falta de controles, al haber indisponibilidad del personal pueden dejar ausentes sus puestos de trabajo dejando así al no desarrollo de sus labores	Muy baja	2	6	2	Tolerable	6.1.1 Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización. 11.3.2 Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada.	Raro	1	3	2	Tolerable					

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Frecuencia (F)		R	NR		Control recomendado	Frecuencia (F')		R'	NR'	
	A28	Indisponibilidad del personal	Falta de controles, ejecutar información importante para la organización si el personal esta indispuesto	Muy baja	2	6	2	Tolerable	6.1.1 Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización. 11.3.2 Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada.	Raro	1	3	2	Tolerable
A	A29	Extorsión	Mediante amenazas pueden sacar información importante para la organización	Baja	3	9	3	Intolerable	13.1.1 Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados. 13.1.2 Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos. 13.2.1 Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.	Raro	1	3	2	Tolerable
Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Frecuencia (F)**		**R**	**NR**		**Control recomendado**	**Frecuencia (F')**		**R'**	**NR'**	
A	A30	Ingeniería social	Falta de concientización del personal en las mejores prácticas de seguridad informática. Llevando a un afectación alta en la dimensión de confidencialidad	Baja	3	9	3	Intolerable	8.2.1 La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo. 8.2.3 Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.	Raro	1	3	2	Tolerable

Cuadro 52. Análisis y evaluación de riesgos de Base de Datos Correo Electronico Institucional

Activo PGT-08	**PGT-08 Base de Datos Correo Electrónico Institucional**			**Tipo**	**Datos / Información**		
Administrador	**Administrador de Sistemas**			**Degradación**	**100%**		
Impacto	**8**	**Desastroso**		**Ubicación**	**Proceso de Gestión TIC**		

Tipo	**ID**	**Amenaza**	**Exposición / Vulnerabilidad**	**Riesgo Actual**					**Control recomendado**	**Riesgo Residual Esperado**				
							4	Extremo					2	Tolerable
				Frecuencia (F)		**R**	**NR**			**Frecuencia (F')**		**R'**	**NR'**	
Errores y fallos no intencionados	E1	Errores de los usuarios	Los usuarios no cuentan con capacitación para el manejo del activo	Media	4	32	4	Extremo	8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable
	E2	Errores del administrador	Algunos equipos del Proceso de Gestión TIC no están actualizados por software de protección y reparación de virus	Media	4	32	4	Extremo	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes. 8.1.1 Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Frecuencia (F)		R	NR		Control recomendado	Frecuencia (F)		R	NR	
Errores y fallos no intencionados	E3	Errores de monitorización	No se realizan correctamente los mantenimientos	Baja	3	24	4	Extremo	10.3.1 Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema. 10.3.2 Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.	Raro	1	3	2	Tolerable
	E4	Errores de configuración	No se tiene un Anti spam para controlar el ingreso de correos no deseados propagación de virus	Baja	3	24	4	Extremo	12.4.1 Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos. 12.4.3 Se debería restringir el acceso al código fuente de los programas. 12.5.4 Se debería prevenir las posibilidades de fuga de información.	Raro	1	3	2	Tolerable
	E18	Destrucción de la información	No existe un protocolo para la clasificación de la información	Media	4	32	4	Extremo	10.7.3 Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados. 12.3.1 Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	Raro	1	3	2	Tolerable

	E19	Fugas de información	Falta de interés por aplicar las políticas de seguridad	Muy baja	2	16	4	Extremo	6.1.1 Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización. 6.1.2 Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización.	Raro	1	3	2	Tolerable
	A3	Manipulación de los registros de actividad	Falta de controles	Baja	3	24	4	Extremo	7.2.1 La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización. 7.2.2 Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización. 10.7.3 Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados.	Raro	1	3	2	Tolerable

	A4	Manipulación de la configuración [D.log]	Falta de controles	Muy baja	2	16	4	Extremo	7.2.2 Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización. 10.7.3 Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados. 10.10.2 Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.3 Se deberían proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados.	Raro	1	3	2	Tolerable
Ataques intencionados	A5	Suplantación de la identidad del usuario	No existe una implementación de procesos rigurosos para actualizar las contraseñas	Muy baja	2	16	4	Extremo	11.2.1 Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información. 11.2.2 Se debería restringir y controlar la asignación y uso de los privilegios. 11.2.3 Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal. 11.2.4 El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.	Raro	1	3	2	Tolerable

	A6	Abuso de privilegios de acceso	No existe mecanismos de control	Baja	3	24	4	Extremo	11.4.2 Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios. 11.4.4 Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico. 11.4.5 Se deberían segregar los grupos de usuarios, servicios y sistemas de información en las redes.	Raro	1	3	2	Tolerable
	A11	Acceso no autorizado	Falta de controles	Muy baja	2	16	4	Extremo	9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Raro	1	3	2	Tolerable

	A15	Modificación deliberada de la información	No realizan copias de seguridad periódicamente	Baja	3	24	4	Extremo	13.2.1 Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información. 10.5.1 Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación	Raro	1	3	2	Tolerable
	A19	Divulgación de información	No hay mayor seguridad para la información	Baja	3	24	4	Extremo	6.1.1 Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización. 6.1.2 Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización. 6.1.3 Se deberían definir claramente todas las responsabilidades para la seguridad de la información.	Raro	1	3	2	Tolerable

Cuadro 53. Análisis y evaluación de riesgos de Codigo fuente Portal Web

Activo PGT-03		PGT-03 Código Fuente Portal Web de la Gobernación de Nariño, Portales.				Tipo	Datos/información												
Administrador		Administrador Portal Web				Degradación	100%												
Impacto		8	Desastroso			Ubicación	Proceso de Gestión TIC												
Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
							4	Extremo					2	Tolerable
				Frecuencia (F)		R	NR			Frecuencia (F')		R'	NR'	
De origen industrial	I8	Fuego	No existe sistema de alarma contra incendios.	Muy baja	2	16	4	Extremo	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable
E	E2	Errores del administrador	La actualización del antivirus no se actualiza diariamente	Media	4	32	4	Extremo	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes 8.1.1 Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable

	E4	Errores de configuración	No cuenta con una protección segura a los ataques al sitio web	Media	4	32	4	Extremo	12.4.1 Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos. 12.4.3 Se debería restringir el acceso al código fuente de los programas. 12.5.4 Se debería prevenir las posibilidades de fuga de información.	Raro	1	3	2	Tolerable
	E19	Fugas de información	Los datos no son correctamente protegidos	Media	4	32	4	Extremo	6.1.1 Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización. 6.1.2 Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización.	Raro	1	3	2	Tolerable
Ataques intencionados	A3	Manipulación de los registros de actividad	Suplantación de contenido	Muy baja	2	16	4	Extremo	7.2.1 La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización. 7.2.2 Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización. 10.7.4 Se debería proteger la documentación de los sistemas contra accesos no autorizados.	Raro	1	3	2	Tolerable
	A7	Uso no previsto	Autorización insuficiente	Baja	3	24	4	Extremo	10.10.2 Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.3 Se deberían proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados.	Raro	1	3	2	Tolerable

	A24	Denegación de servicio	No cuenta con la suficiente protección a los Ataques maliciosos	Media	4	32	4	Extremo	10.4.1 Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios. 10.9.3 Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas.	Raro	1	3	2	Tolerable
	A26	Ataque destructivo	No se cuenta con la suficiente protección	Media	4	32	4	Extremo	10.7.3 Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados. 12.3.1 Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	Raro	1	3	2	Tolerable

Cuadro 54. Análisis y evaluación de riesgos de Correo Institucional

Activo PGT-07		PGT-07 Correo Electrónico Institucional				Tipo	Sistema de Información												
Administrador		Administrador Portal Web				Degradación	100%												
Impacto		8	Desastroso			Ubicación	Proceso de Gestión TIC												
Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
							4	Extremo					2	Tolerable
				Frecuencia (F)		R	NR			Frecuencia (F')		R'	NR'	
De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente alterna de corriente eléctrica	Muy baja	2	16	4	Extremo	9.2.3 - Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable
	I8	Fallo de servicio de comunicaciones	Baja capacidad de respuesta	Baja	3	24	4	Extremo	13.1.1 Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados. 13.1.2 Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable

E	E2	Errores del administrador	No existe un análisis de seguridad para todos los correos spam que llegan	Media	4	32	4	Extremo	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes. 8.1.1 Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable
	E21	Errores de mantenimiento / actualización de programas (Software)	No se mantienen actualizados los parches de seguridad.	Media	4	32	4	Extremo	9.2.4 Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 9.2.6 Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación 10.3.2 Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación. Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación 10.4.1 Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios. 12.4.1 Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos.	Raro	1	3	2	Tolerable

Cuadro 55. Análisis y evaluación de riesgos de Computadores de Escritorio

Activo PGT-13		PGT-13 Computadores de Escritorio				Tipo	Hardware												
Administrador		Soporte Técnico				Degradación	50%												
Impacto		3	Moderado			Ubicación	Proceso de Gestión TIC												
Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
							3	Intolerable					2	Tolerable
				Frecuencia (F)		R	NR			Frecuencia (F')		R'	NR'	
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios.	Baja	3	9	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable
	N2	Daños por agua	Los computadores de escritorio se encuentra ubicados sin ninguna precaución	Bajo	3	9	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable
	N*	Desastres naturales	El Proceso de Gestión TIC se encuentra en zona media de riesgo de desastre natural de origen de inundación debido a su mala ubicación en el primer piso	Baja	3	9	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable

De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente de energía alterna	Baja	3	9	3	Intolerable	9.2.3 - Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable
	I7	Condiciones inadecuadas de temperatura o humedad	No cuentan con aire acondicionado en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable	9.2.1 - El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3	9	3	Intolerable	9.1.1 Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.3 Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos. 9.2.2 Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo. 9.2.3 Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.	Raro	1	3	2	Tolerable

	E1	Errores de los usuarios	No existe un manual para el uso de las diferentes aplicaciones	Baja	3	9	3	Intolerable	8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable
E	E2	Errores del administrador	No existe un protocolo para la instalación de las diferentes aplicaciones	Baja	3	9	3	Intolerable	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes. 8.1.1 Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable
	E4	Errores de configuración	No existe un manual para la debida configuración de los equipos de computo	Baja	3	9	3	Intolerable	12.4.1 Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos. 12.4.3 Se debería restringir el acceso al código fuente de los programas. 12.5.4 Se debería prevenir las posibilidades de fuga de información.	Raro	1	3	2	Tolerable

	E21	Errores de mantenimiento / actualización de programas (hardware)	No cuentan con una política de mantenimiento	Baja	3	9	3	Intolerable	8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 12.5.1 Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.	Raro	1	3	2	Tolerable
	E25	Perdida de equipos	No existen las suficientes cámaras de seguridad en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable	9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Raro	1	3	2	Tolerable
Ataques intencionados	A6	Difusión de software dañino	Debido a la gran cantidad de equipos de cómputo que están destinados para los usuarios y la falta de asesoría puede causar daños	Baja	3	9	3	Intolerable	10.4.1 Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios	Raro	1	3	2	Tolerable

	A11	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	9	3	Intolerable	11.2.1 Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información. 11.2.2 Se debería restringir y controlar la asignación y uso de los privilegios. 11.2.3 Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal. 11.2.4 El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.	Raro	1	3	2	Tolerable
	A3	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3	9	3	Intolerable	6.1.3 Se deberían definir claramente todas las responsabilidades para la seguridad de la información. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo. 8.2.3 Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad. 11.3.1 Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas. 13.2.1 Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.	Raro	1	3	2	Tolerable

Cuadro 56. Análisis y evaluación de riesgos de Computadores Portátiles

Activo PGT-14	PGT-14 Computadores Portátiles					Tipo	Hardware											
Administrador	Soporte Técnico					Degradación	50%											
Impacto	3	Moderado				Ubicación	Proceso de Gestión TIC											
Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Esperado					Residual			
							3	Intolerable							2			
				Frecuencia (F)		R	NR		Frecuencia (F')		R'		NR'					
Desastres naturales	N1	Fuego	No existe sistema de alarma contra incendios.	Baja	3	9	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable				
	N2	Daños por agua	Los computadores portátiles se encuentra ubicados sin ninguna precaución	Bajo	3	9	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable				
	N*	Desastres naturales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3	9	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable				

De origen industrial	I6	Corte del suministro eléctrico	No existe una fuente de energía alterna	Baja	3	9	3	Intolerable	9.2.3 - Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable
	I7	Condiciones inadecuadas de temperatura o humedad	No cuentan con aire acondicionado en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable	9.2.1 - El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable
	I*	Desastres industriales	No se utilizan paneles de obturación para el cableado. No existe sistema de alarma de control de temperatura y humedad. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.	Baja	3	9	3	Intolerable	9.1.1 Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.3 Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos. 9.2.2 Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo. 9.2.3 Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.	Raro	1	3	2	Tolerable

	E1	Errores de los usuarios	No existe un manual para el uso de las diferentes aplicaciones	Baja	3	9	3	Intolerable	8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable
E	E2	Errores del administrador	No existe un protocolo para la instalación de las diferentes aplicaciones	Baja	3	9	3	Intolerable	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes. 8.1.1 Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable
	E4	Errores de configuración	No existe un manual para la debida configuración de los equipos de computo	Baja	3	9	3	Intolerable	12.4.1 Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos. 12.4.3 Se debería restringir el acceso al código fuente de los programas. 12.5.4 Se debería prevenir las posibilidades de fuga de información.	Raro	1	3	2	Tolerable
	E21	Errores de mantenimiento / actualización de programas (hardware)	No cuentan con una política de mantenimiento	Baja	3	9	3	Intolerable	8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 12.5.1 Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.	Raro	1	3	2	Tolerable

	E25	Perdida de equipos	No existen las suficientes cámaras de seguridad en la oficina de Proceso de Gestión TIC	Baja	3	9	3	Intolerable	9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Raro	1	3	2	Tolerable
Ataques intencionados	A6	Difusión de software dañino	Debido a la gran cantidad de equipos de cómputo que están destinados para los usuarios y la falta de asesoría puede causar daños	Baja	3	9	3	Intolerable	10.4.1 Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.	Raro	1	3	2	Tolerable
	A11	Suplantación de la identidad del usuario	No se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios	Baja	3	9	3	Intolerable	11.2.1 Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información. 11.2.2 Se debería restringir y controlar la asignación y uso de los privilegios. 11.2.3 Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal. 11.2.4 El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.	Raro	1	3	2	Tolerable

	A3	Manipulación de la configuración	No se ha tomado medidas o políticas de seguridad que asesore a los usuarios de la manipulación de las aplicaciones	Baja	3	9	3	Intolerable	6.1.3 Se deberían definir claramente todas las responsabilidades para la seguridad de la información. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo. 8.2.3 Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad. 11.3.1 Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas. 13.2.1 Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.	Raro	1	3	2	Tolerable

8.13 PRUEBAS REALIZADAS

Se hizo un proceso denominado ethical hacking que expone los problemas de seguridad que existen en los sistemas informáticos. Para ello hemos trabajado con las principales herramientas de seguridad y tratado algunas vulnerabilidades importantes. Este proceso se realizó con el sistema operativo Kali Linux, dimitry para recolección de información del servicio DNS, zenmap, la interfaz gráfica de nmap, la herramienta por preferencia para realizar escaneo de vulnerabilidades a servidores, subgraph vega, una de las mejores herramientas para escaneo de vulnerabilidades en las aplicaciones web, y también se utilizó sqlmap para la explotación de vulnerabilidades de inyección SQL.

Kali Linux: Es una distribución de Linux, su propósito es la auditoria y seguridad informática. Kali Linux persigue tener la mejor colección de herramientas de código abierto destinadas a pruebas de penetración, bajo un análisis y con el uso de diferentes herramientas que cumplen este propósito, así que se buscaran nombres de domino, direcciones IP, posibles nombres de usuario, bases de datos públicas, se buscaran las versiones de los sistemas operativos, los parches de seguridad, etc.

dmitry: Para obtener todos los subdominios relacionados al dominio nariño.gov.co se realizó una exploración minuciosa de la página institucional y se utilizó herramienta dmitry, esta es una herramienta que permite obtener toda la información posible sobre un host, esta incluye lo relacionado con los servidores DNS incluyendo nombre de la empresa a la que está registrado el dominio, el nombre las personas encargadas de este host, los correos electrónicos de las mismas y los subdominios asociados y sus respectivas direcciones IP.

Nmap: Es una herramienta de escaneo de redes que permite identificar qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls, entre otros.

Zenmap: Es **multiplataforma, libre y gratuito,** Zenmap es la interfaz gráfica oficial de Nmap, el conocido programa de código abierto para hacer escaneo de puertos a fondo de cualquier equipo conectado. Zenmap proporciona una interfaz gráfica para ejecutar los diferentes tipos de análisis de puertos.

Vega: es una herramienta de análisis de vulnerabilidades open source desarrollada por Subgraph y una plataforma para testear la seguridad de aplicaciones web.

Es una aplicación de escritorio desarrollada en Java que funciona en Linux, OS X y Windows. Incluye un escáner automático y un proxy que intercepta peticiones. Además proporciona funciones Javascript para la integración con otras

aplicaciones. Vega proporciona, entre otras, las siguientes funcionalidades:

Puede funcionar en modo proxy, interceptando las peticiones que se realizan durante la navegación y analizándolas para obtener información. Permite establecer puntos de ruptura y criterios de interceptación de peticiones salientes (desde el navegador) o entrantes (desde el servidor).

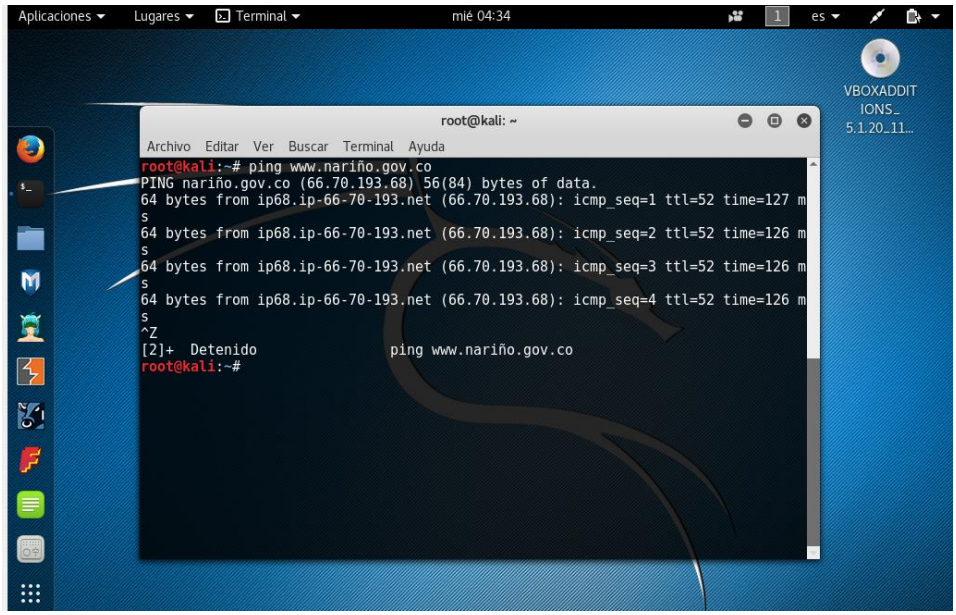
Con todas estas herramientas se realizó las Pruebas Penetración Testing obteniendo los siguientes resultados.

Utilizamos una máquina virtual en la cual instalamos el sistema operativo Kali Linux, ejecutamos la terminal de Kali Linux en la cual utilizamos el comando ping al dominio de la gobernacion de nariño www.nariño.gov.co el cual nos arrogo la siguiente dirección IP

ping www.nariño.gov.co

IP 66.70.193.68

Figura 6. Resultado de ejecutar ping en la terminal de Kali Linux



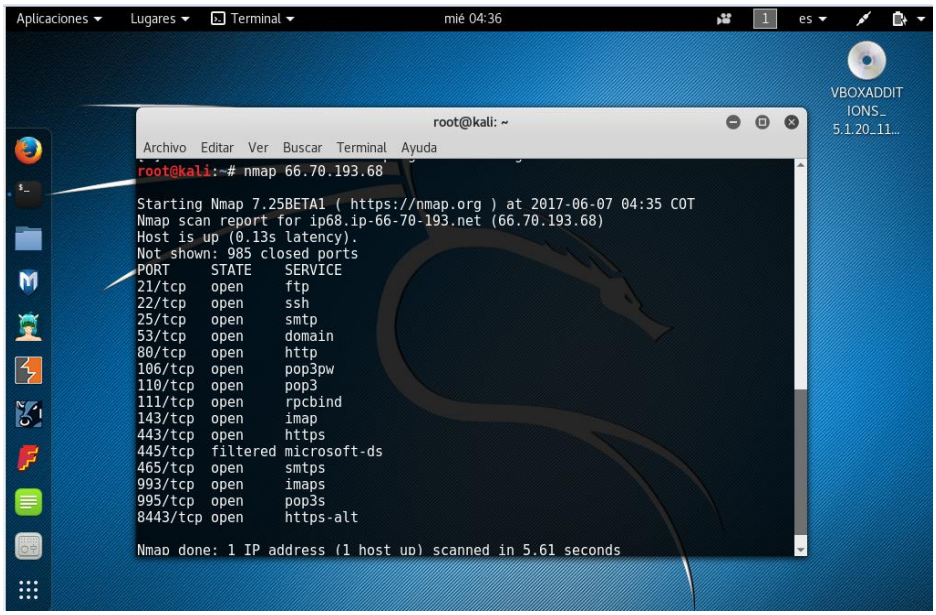
Fuente: Autoria Propia

Con la dirección IP obtenida utilizamos la herramienta nmap que se encuentra en Kali Linux y ejecutamos el comando nmap en la terminal obteniendo el siguiente resultado.

nmap 66.70.193.68

Se puede observar que tenemos puertos abiertos. El único puerto que esta filtrado es el puerto 445/tcp que corresponde al servicio de microsoft-ds, el filtrado puede provenir de un dispositivo de cortafuegos dedicado, de las reglas de un enrutador, o por una aplicación de cortafuegos instalada en el propio equipo. Estos puertos suelen frustrar a los atacantes, porque proporcionan muy poca información

Figura 7. Resultado de ejecutar nmap en la terminal de Kali Linux



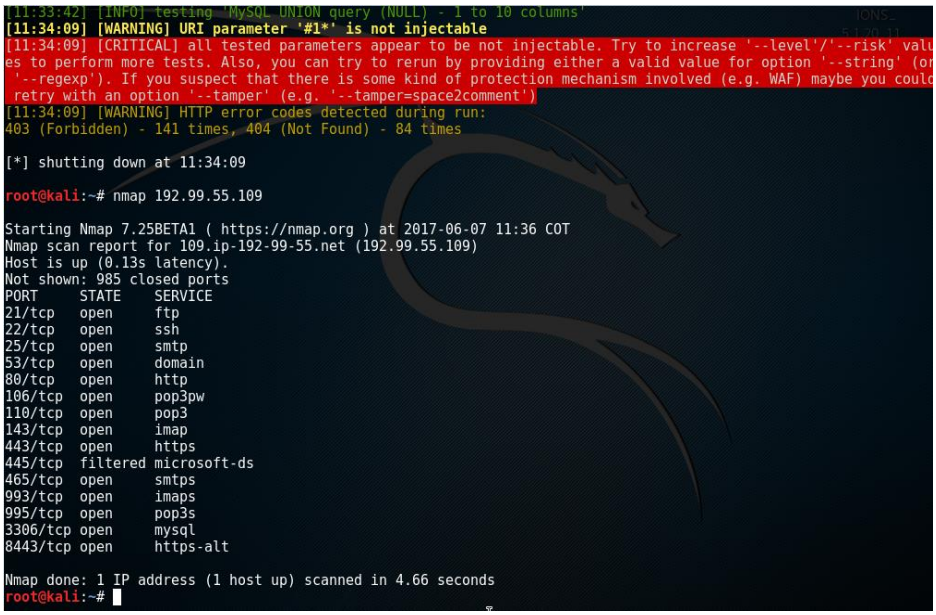
Fuente: Autoria Propia

Con la siguiente IP se encontró el siguiente resultado

nmap 192.99.55.109

nmap informa que el servidor tiene 14 puertos abiertos y también informa cuales son los servicios ofrecidos**,** son los puertos de conexión remota segura (ssh) por el puerto 22, el servicio web por el puerto 80 y el servicio de webseguro por el puerto 443. El puerto 445/tcp microsoft-ds se encuentra cerrado.

Figura 8. Resultado de ejecutar nmap en la terminal de Kali Linux



Fuente: Autoria Propia

En la terminal de Kali Linux utilizamos el comando dmitry para obtener todos los subdominios relacionados al dominio nariño.gov.co

 # dmitry –w –e –n –s www.narino.gov.co

Encontrando el siguiente resultado nos permite obtener toda la información posible sobre un host, esta incluye lo relacionado con los servidores DNS incluyendo nombre de la empresa a la que está registrado el dominio, el nombre las personas encargadas de este host, los correos electrónicos de las mismas y los subdominios asociados y sus respectivas direcciones IP. También encontramos los siguientes hosts con sus respectivas IP

HostName: www.narino.gov.co

Host IP: 66.70.193.68

HostName: datos.narino.gov.co

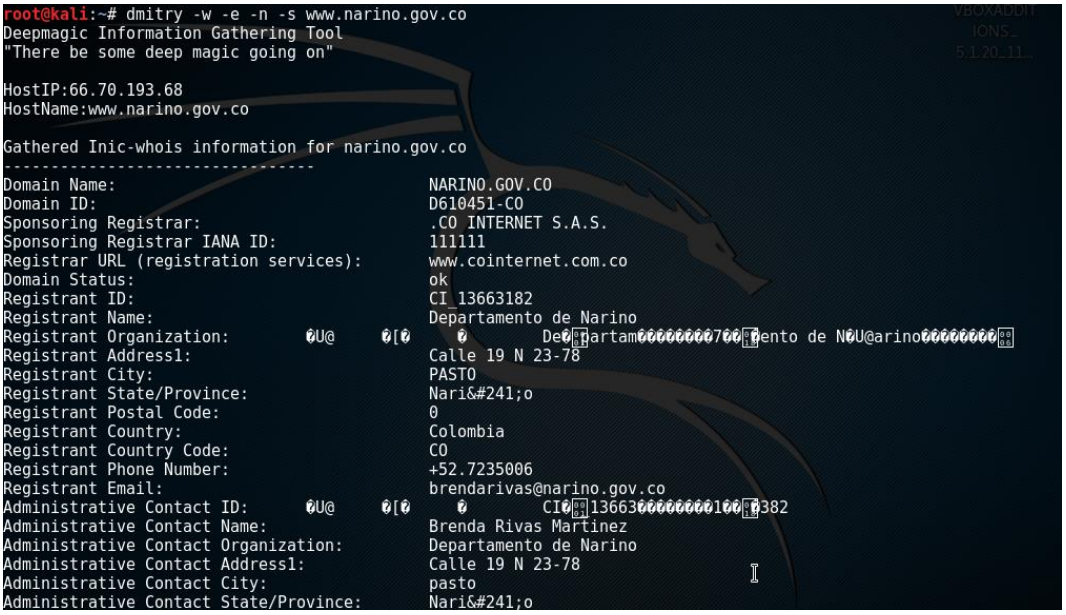
Host IP: 198.100.153.250

HostName: ganadatos.narino.gov.co

Host IP: 198.100.153.250

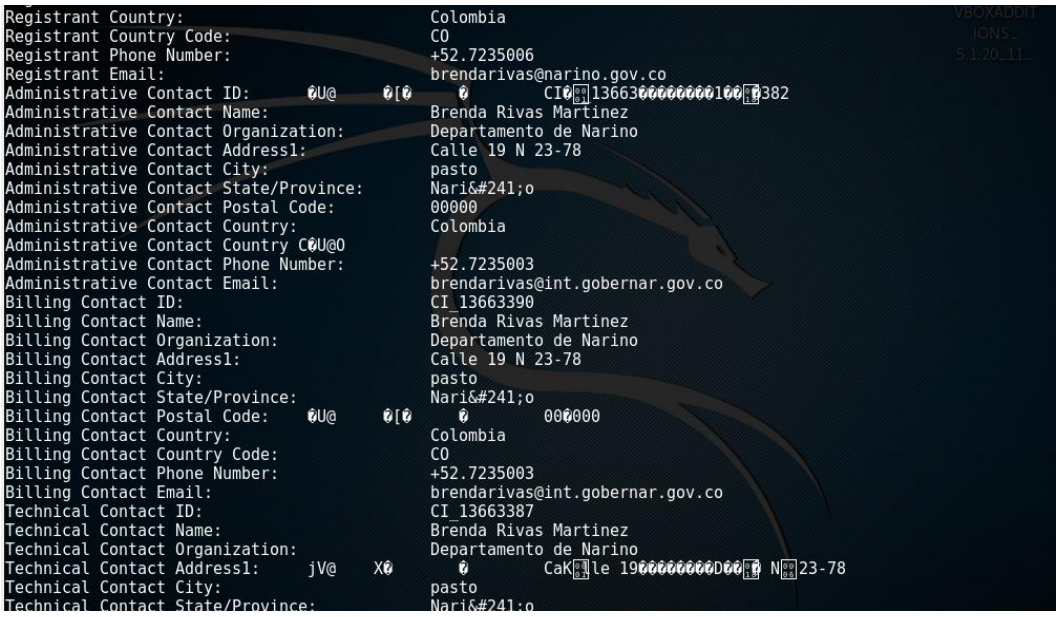
HostName: aplicaciones.narino.gov.co
Host IP: 190.14.247.68

Figura 9. Resultado de ejecutar dmitry en la terminal de Kali Linux



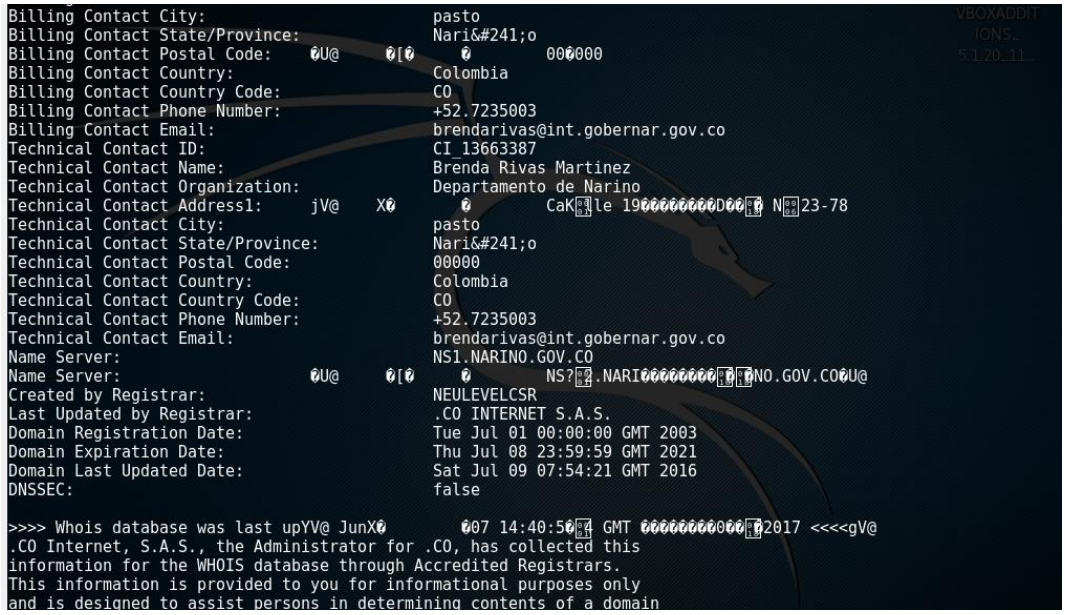
Fuente: Autoria Propia

Figura 10. Resultado de ejecutar dmitry en la terminal de Kali Linux



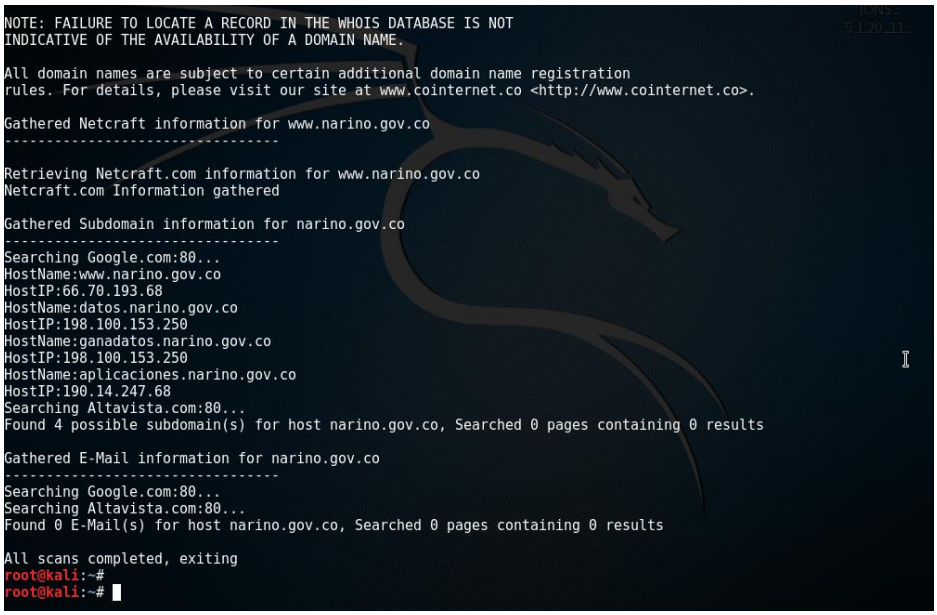
Fuente: Autoria Propia

Figura 11. Resultado de ejecutar dmitry en la terminal de Kali Linux



Fuente: Autoria Propia

Figura 12. Resultado de ejecutar dmitry en la terminal de Kali Linux

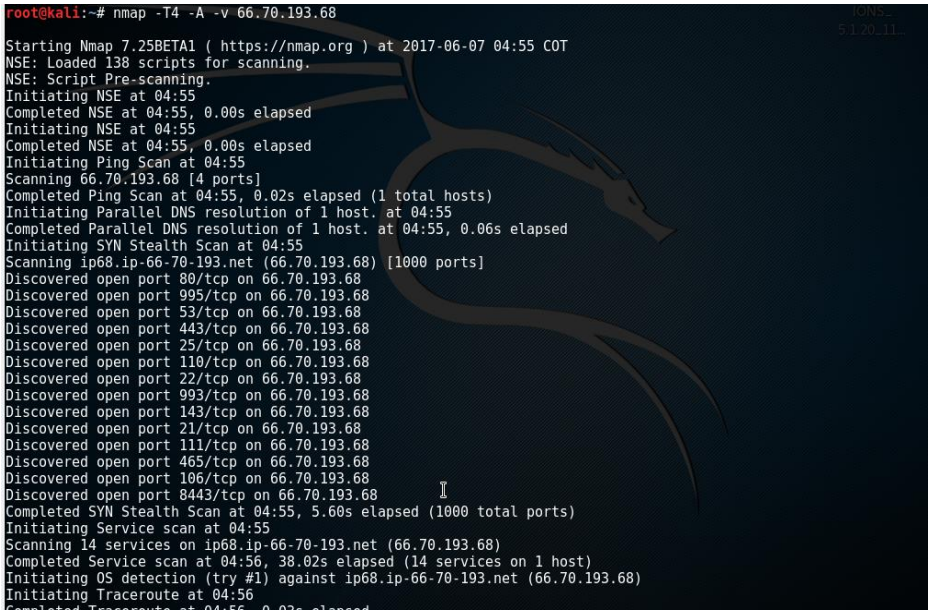


Fuente: Autoria Propia

En la terminal de Kali Linux ejecutamos el siguiente comando las opción –T4 del comando nmap acelera el proceso de búsqueda y escaneo, mientras que la opción –A permite identificar el sistema operativo de los servidores atacados y la opción –v arroja la versión de los servicios instalados en el mismo.

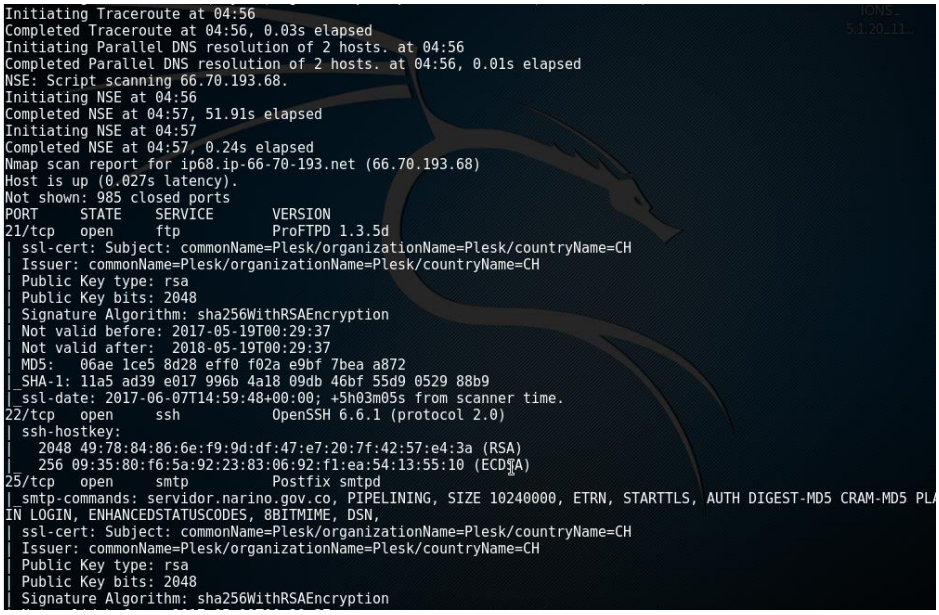
#nmap –T4 –A –v 66.70.193.68
Nos dio como resultado lo siguiente nos muestra el estado, el servicio y la versión de los puertos

Figura 13. Resultado de ejecutar nmap en la terminal de Kali Linux



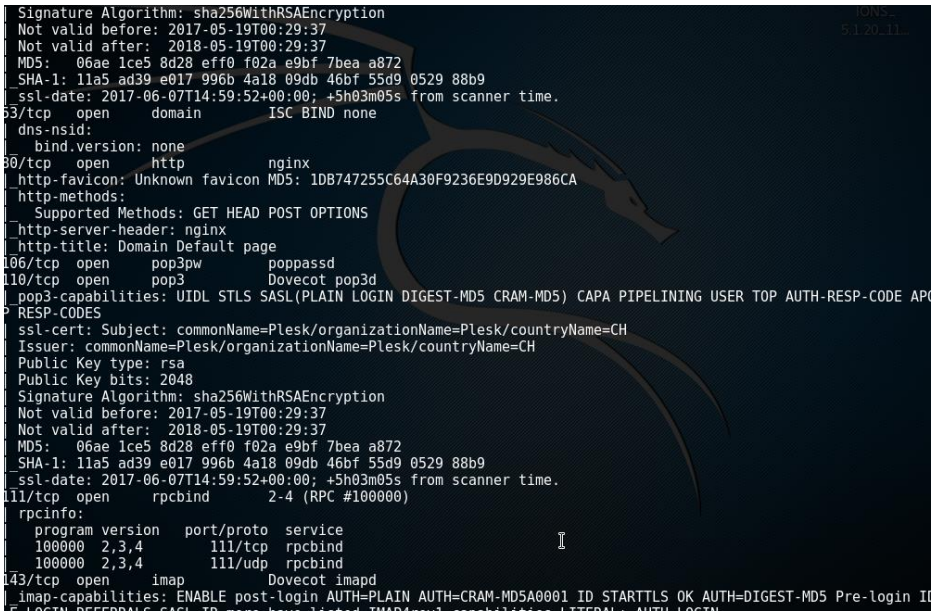
Fuente: Autoria Propia

Figura 14. Resultado de ejecutar nmap en la terminal de Kali Linux



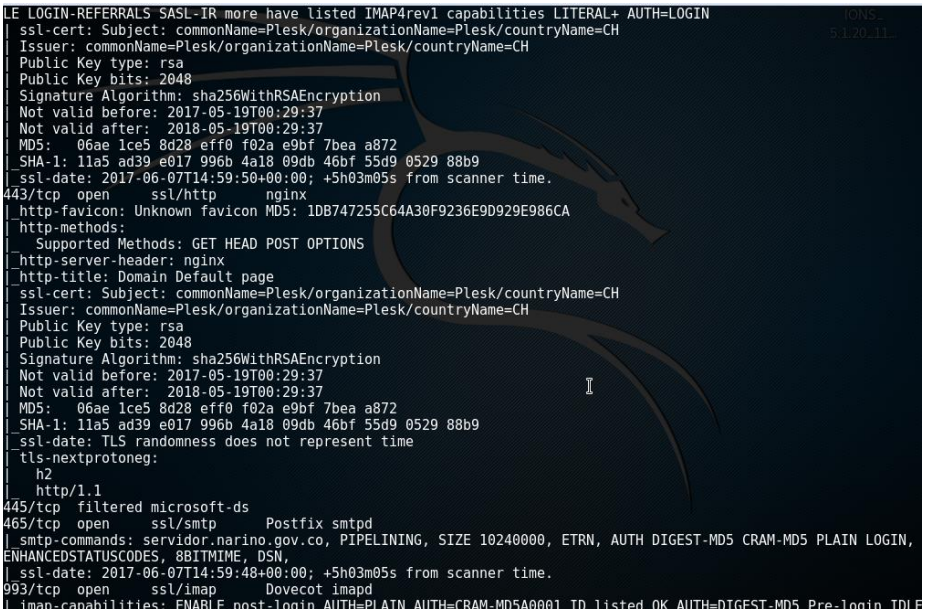
Fuente: Autoria Propia

Figura 15. Resultado de ejecutar nmap en la terminal de Kali Linux



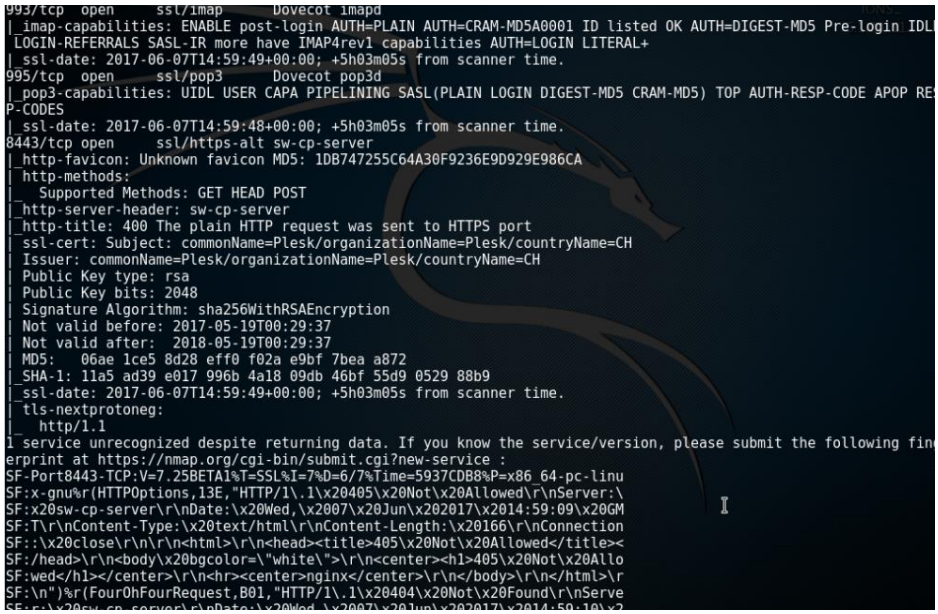
Fuente: Autoria Propia

Figura 16. Resultado de ejecutar nmap en la terminal de Kali Linux



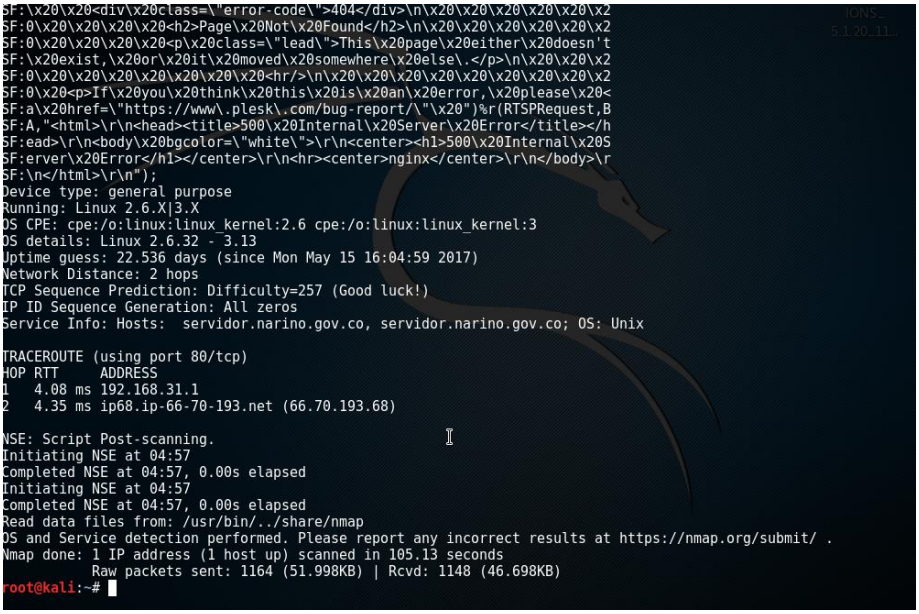
Fuente: Autoria Propia

Figura 17. Resultado de ejecutar nmap en la terminal de Kali



Fuente: Autoria Propia

Figura 18. Resultado de ejecutar nmap en la terminal de Kali Linux



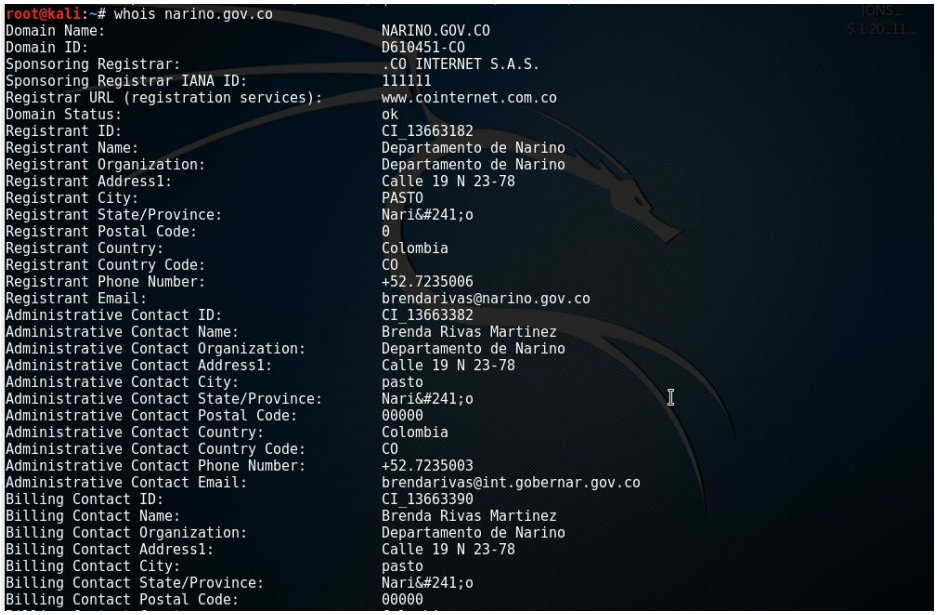
Fuente: Autoria Propia

En la terminal de Kali Linux ejecutamos el siguiente comando whois el cual trata de recolectar la mayor parte de información posible acera del dominio

whois narino.gov.co

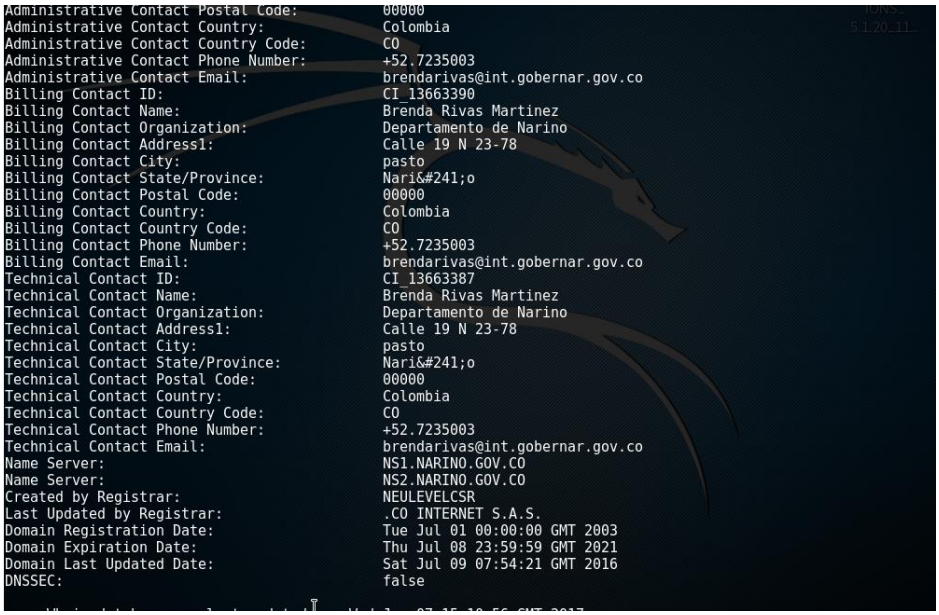
Nos da como resultado la información sobre el Dominio muestran información, como la ubicación de la empresa, número de teléfono, correo electrónico, nombre de la persona de contacto “Brenda Rivas Martínez” contacto técnico y dns del registrante del dominio, en este caso .co Internet S.A.S

Figura 19. Resultado de ejecutar whois en la terminal de Kali Linux



Fuente: Autoria Propia

Figura 20. Resultado de ejecutar whois en la terminal de Kali Linux



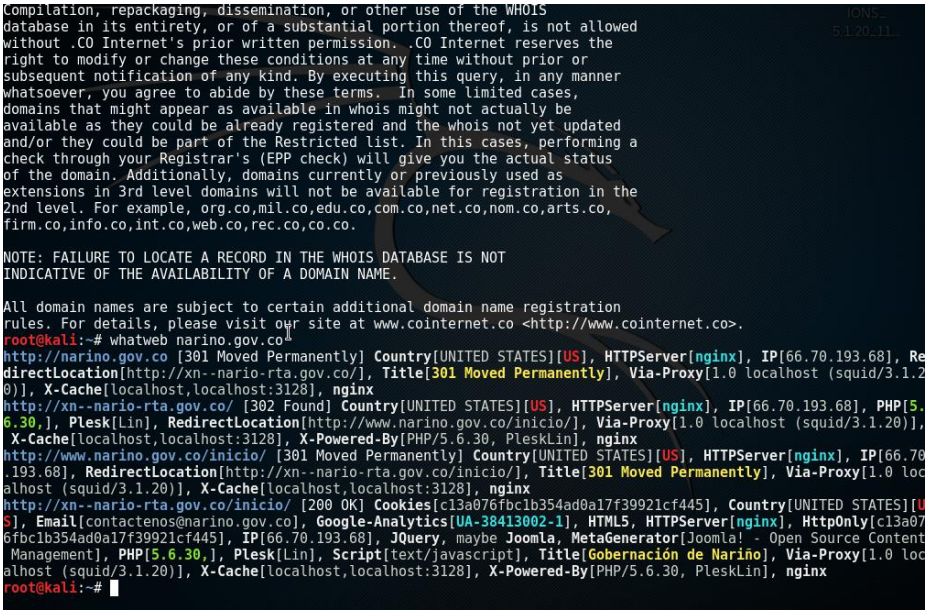
Fuente: Autoria Propia

En la terminal de Kali Linux ejecutamos el siguiente comando whatweb el cual nos mostrara la información del sitio web

Whatweb narino.gov.co

Nos da como resultado el escaneo del sitio web de la Gobernación de Nariño

Figura 21. Resultado de ejecutar whatweb en la terminal de Kali Linux



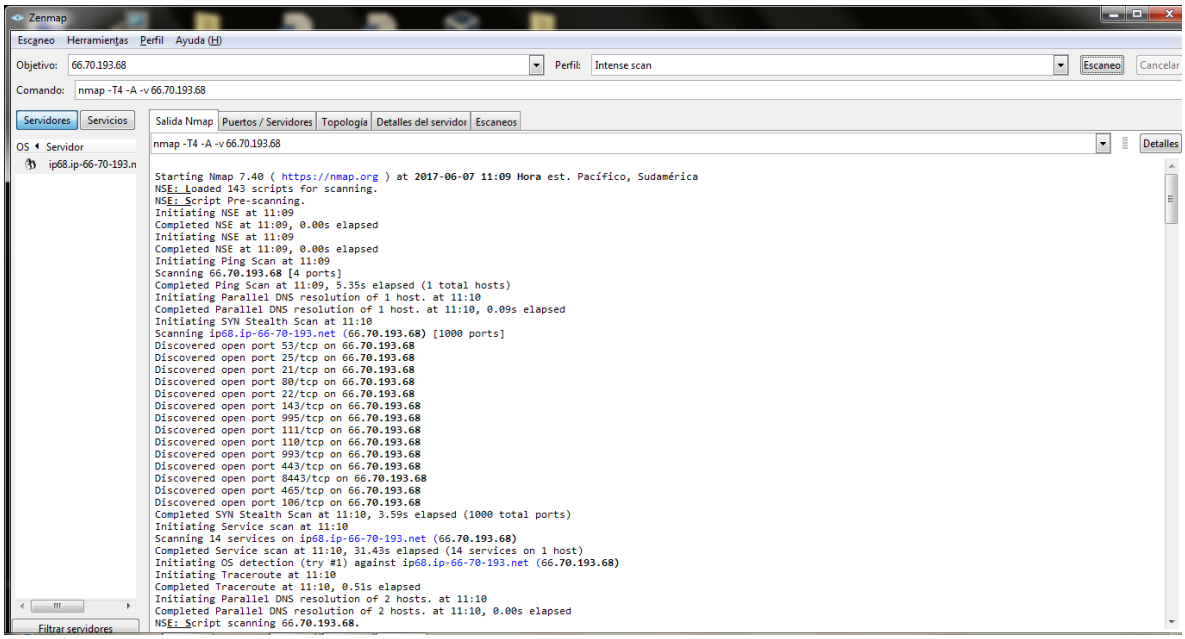
Fuente: Autoria Propia

Ahora realizaremos las pruebas con la herramienta Zenmap, en la interfaz gráfica ejecutaremos el siguiente comando nmap –T4 –A –v (IP)

nmap –T4 –A –v 66.70.193.68

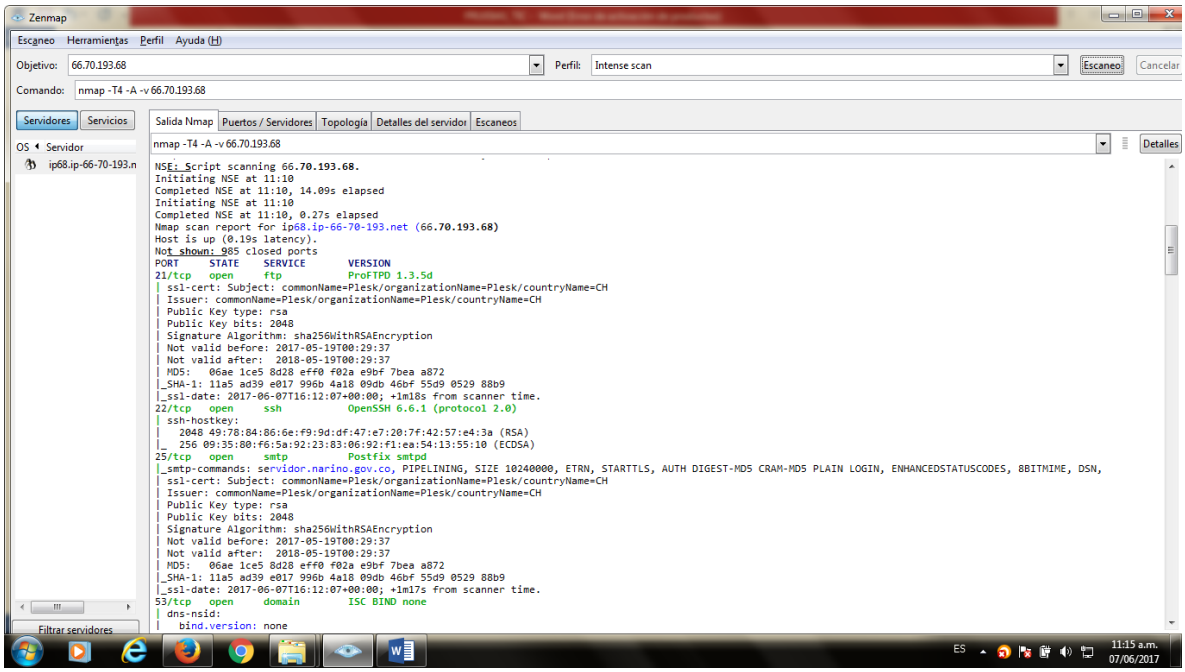
El cual nos da como resultado lo siguiente se evidencia los puertos abiertos pero en entorno gráfico junto con el nombre de cada servicio. Esto permite determinar los puertos que se encuentran abiertos, en este caso el puerto 21, 22, 25, 53, 80,106, 110,111,143, 443, 465, 993, 995, 8443, 4190, 7080, 7081, 8880, al igual permite identificar qué servicios se encuentran activos por cada puerto.

Figura 22. Resultado de análisis de puertos realizado con Zenmap.



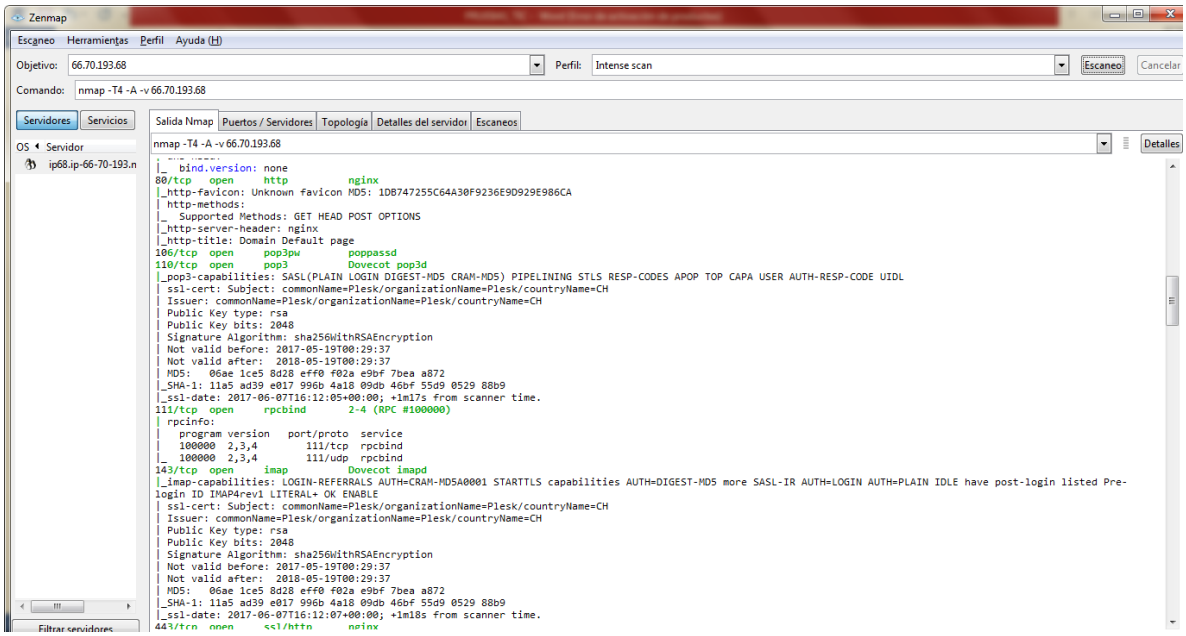
Fuente: Autoria Propia

Figura 23. Resultado de análisis de puertos realizado con Zenmap.



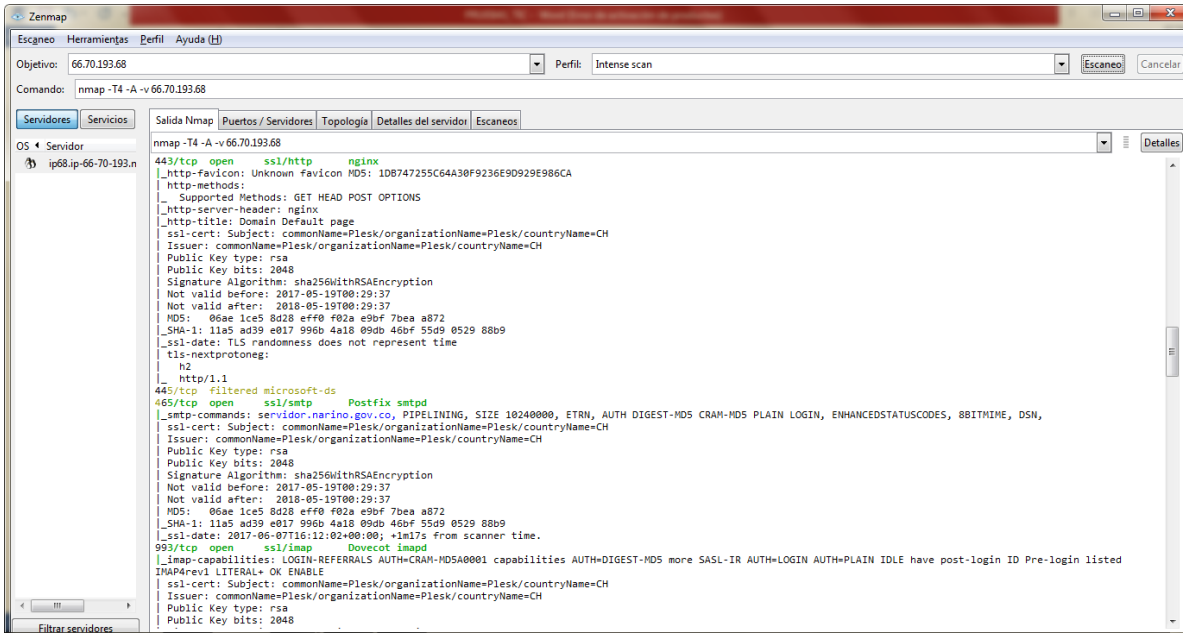
Fuente: Autoria Propia

Figura 24. Resultado de análisis de puertos realizado con Zenmap.



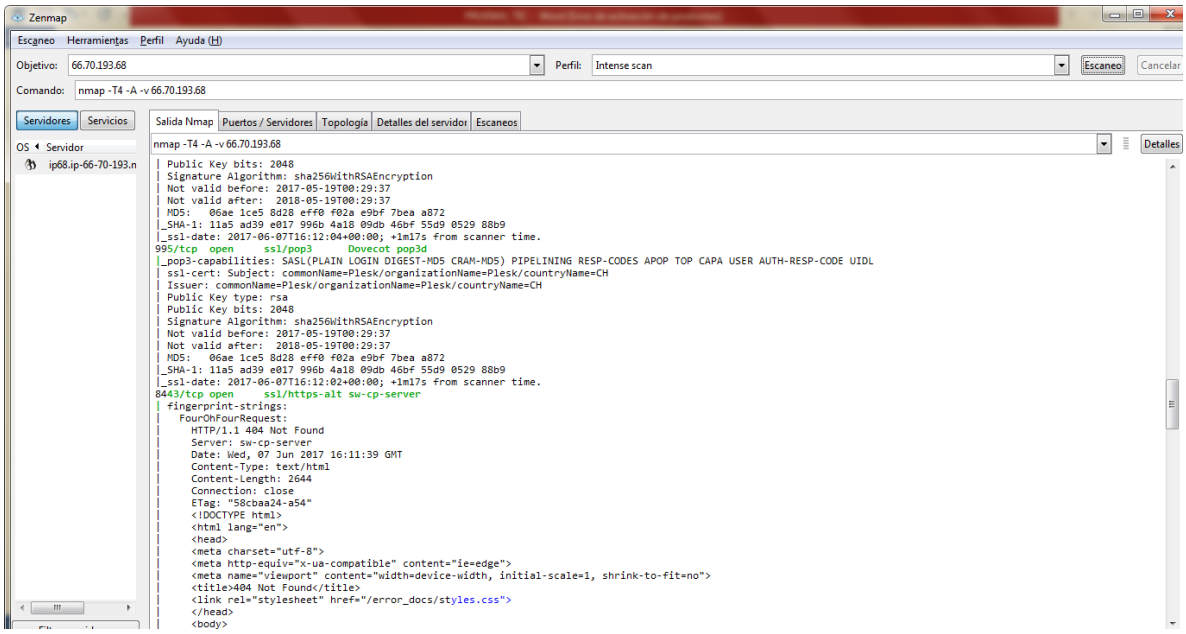
Fuente: Autoria Propia

Figura 25. Resultado de análisis de puertos realizado con Zenmap.



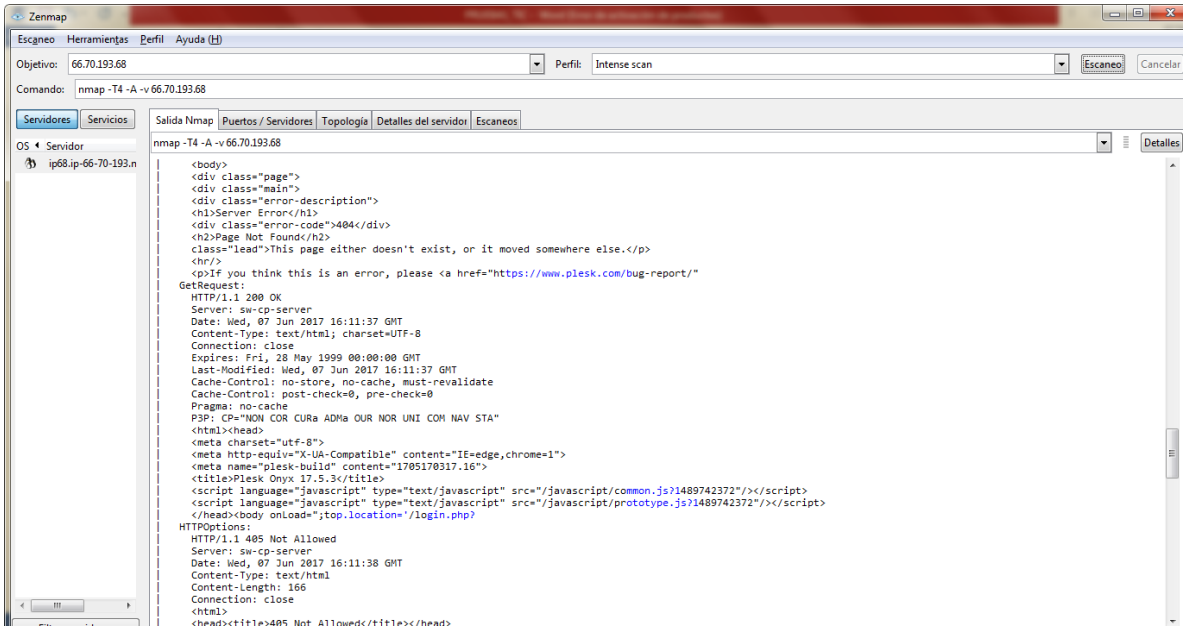
Fuente: Autoria Propia

Figura 26. Resultado de análisis de puertos realizado con Zenmap.



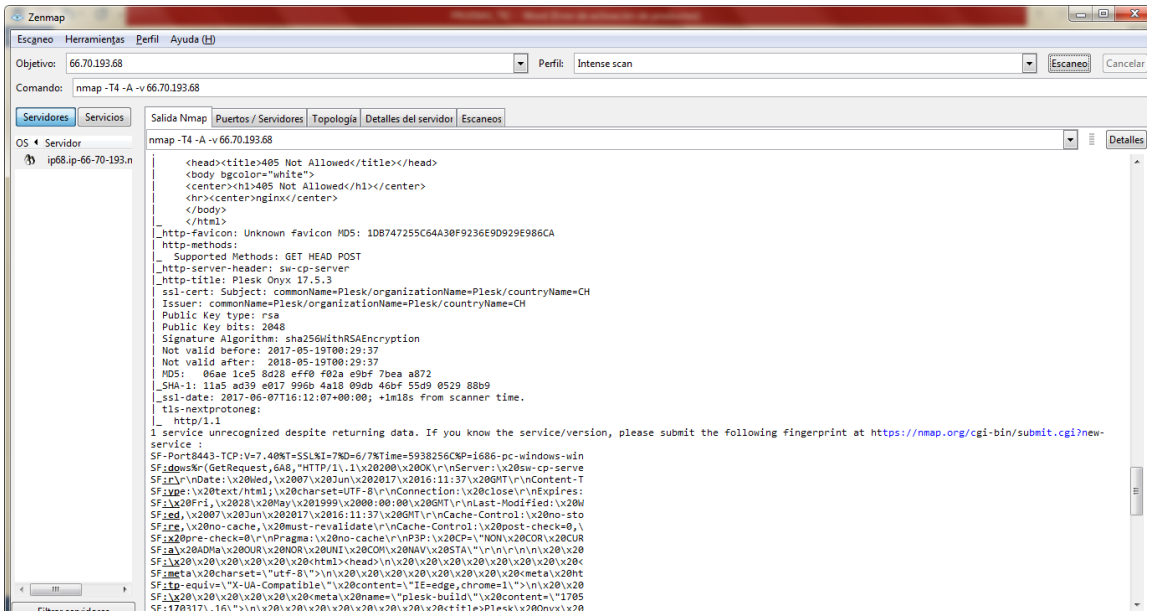
Fuente: Autoria Propia

Figura 27. Resultado de análisis de puertos realizado con Zenmap.



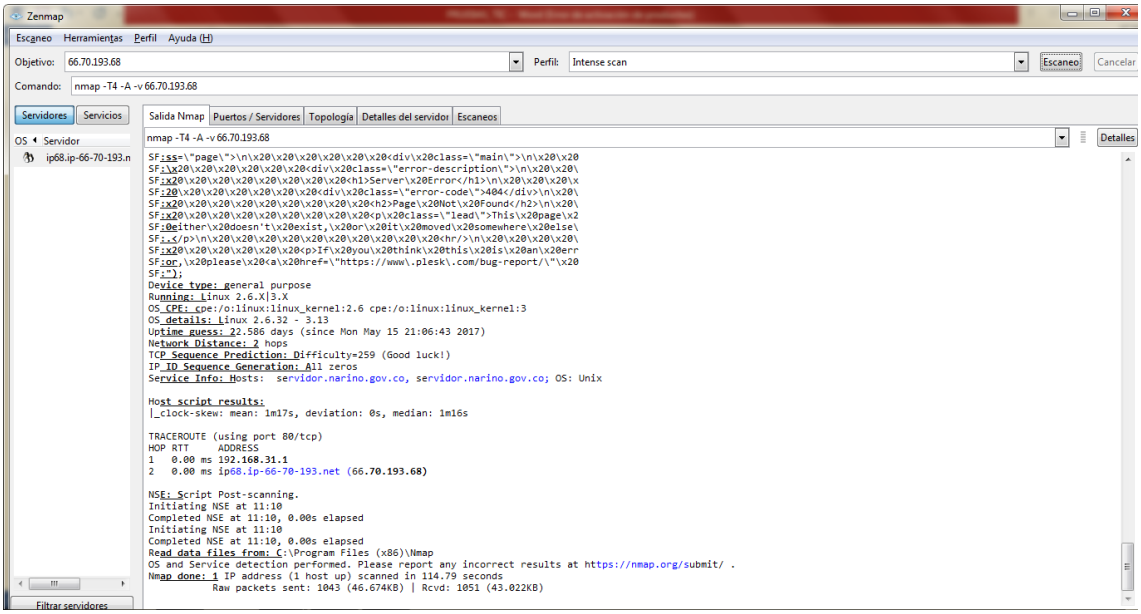
Fuente: Autoria Propia

Figura 28. Resultado de análisis de puertos realizado con Zenmap.



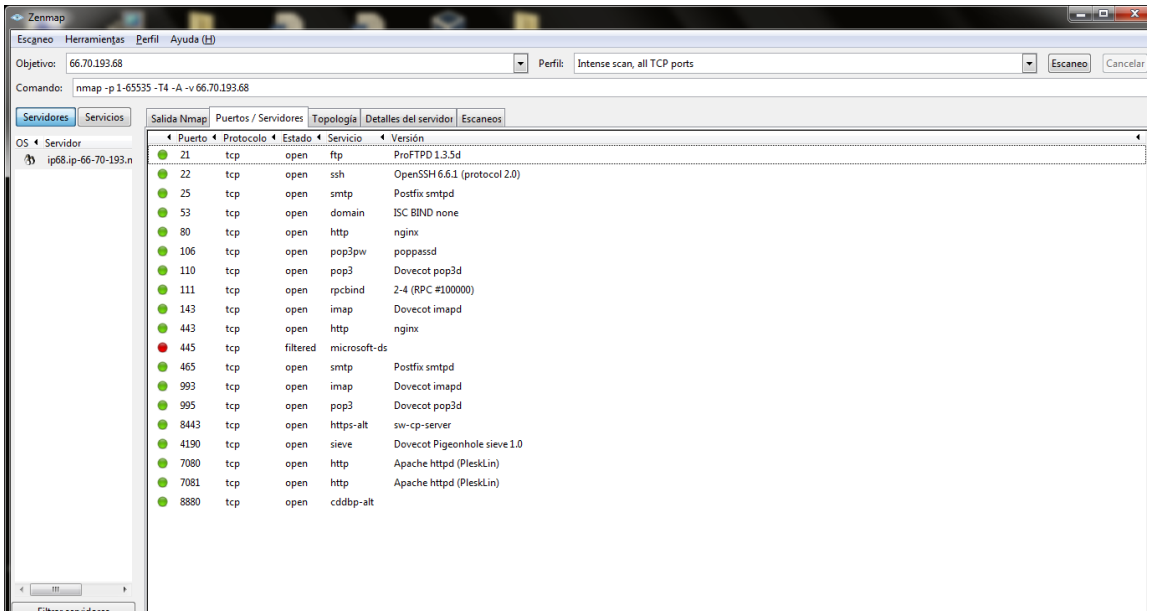
Fuente: Autoria Propia

Figura 29. Resultado de análisis de puertos realizado con Zenmap.



Fuente: Autoria Propia

Figura 30. Resultado de análisis de puertos realizado con Zenmap.



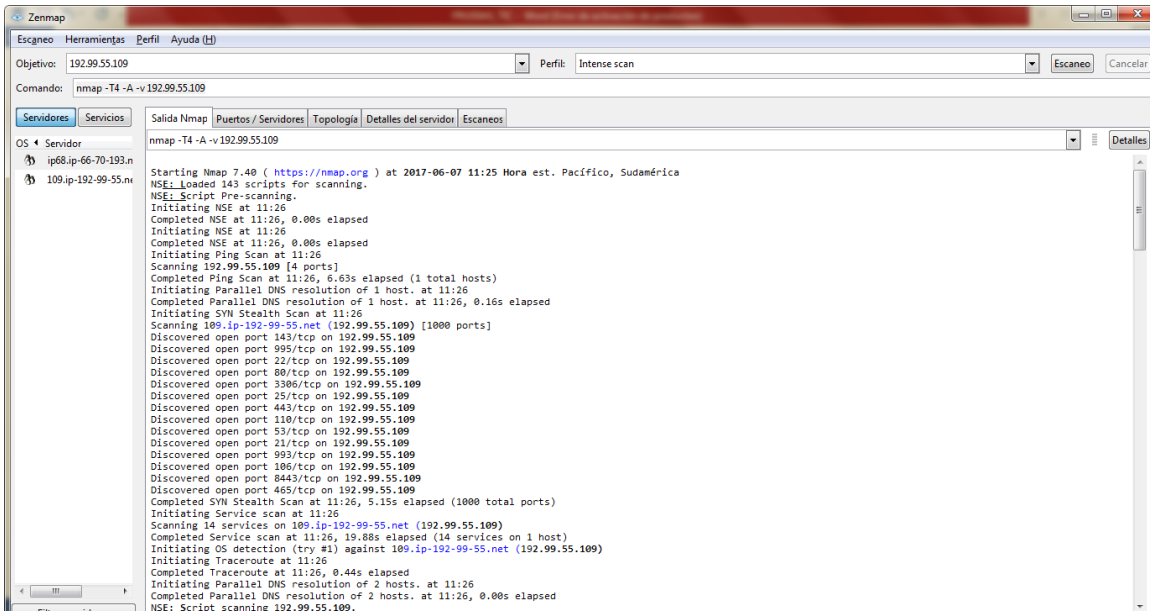
Fuente: Autoria Propia

Ahora ejecutaremos el mismo comando pero con diferente dirección IP en la herramienta Zenmap

nmap –T4 –A –v 192.99.55.109

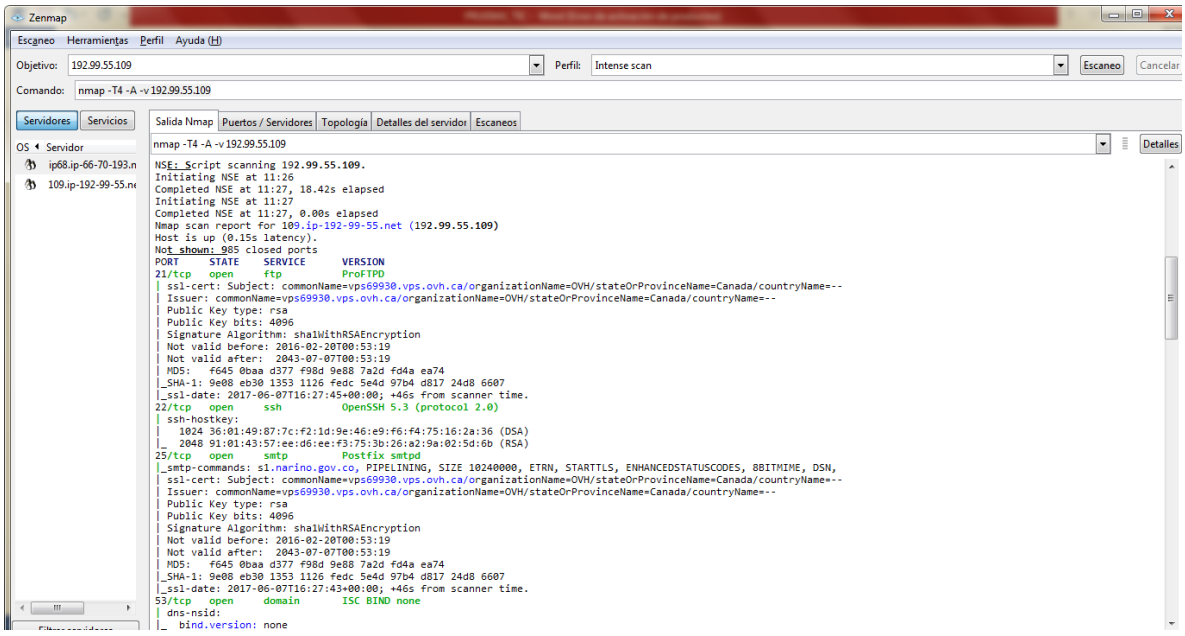
El cual nos da como resultado lo siguiente se evidencia los puertos abiertos pero en entorno gráfico junto con el nombre de cada servicio, al igual permite identificar qué servicios se encuentran activos por cada puerto, arroja el sistema operativo de los servidores y los servicios instalados en el mismo

Figura 31. Resultado de análisis de puertos realizado con Zenmap.



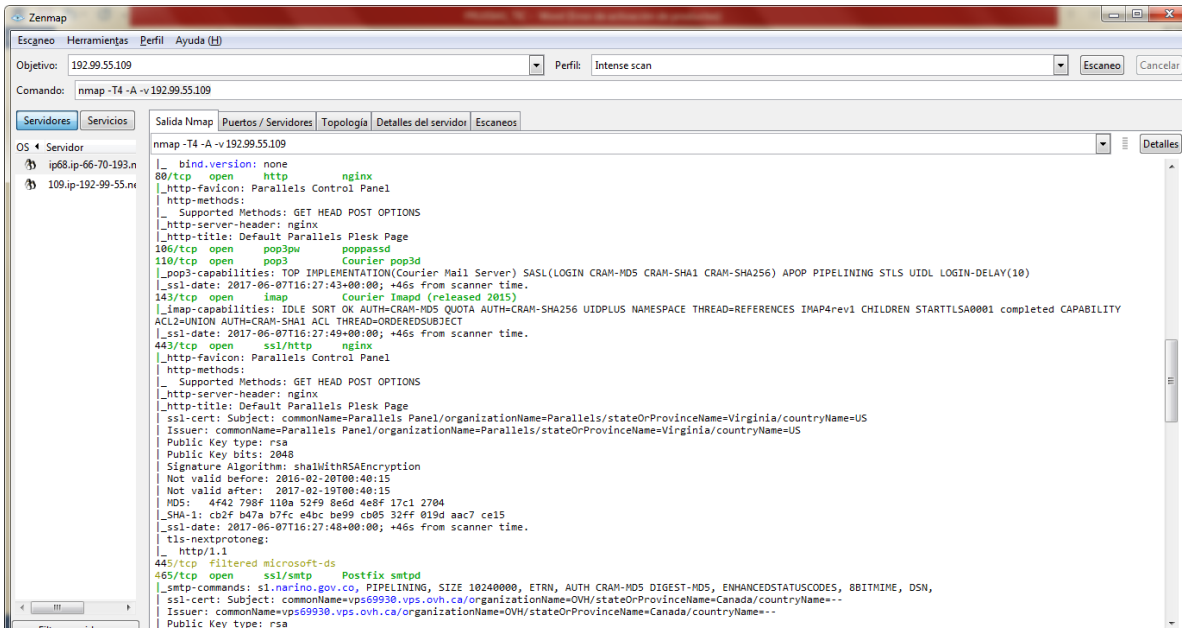
Fuente: Autoria Propia

Figura 32. Resultado de análisis de puertos realizado con Zenmap.



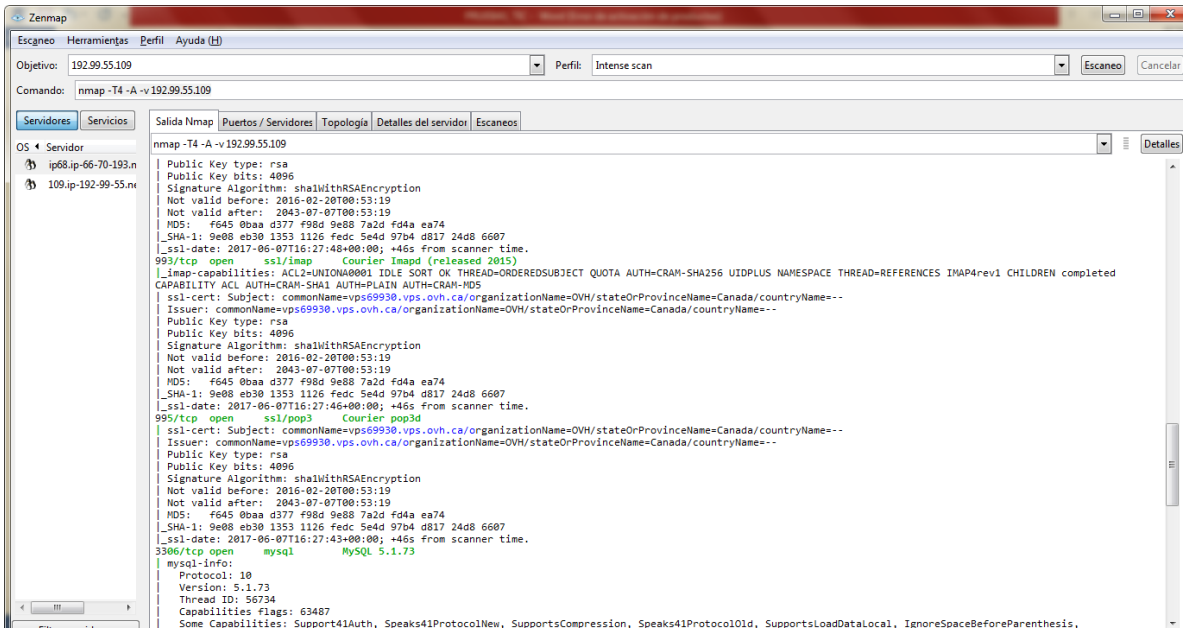
Fuente: Autoria Propia

Figura 33. Resultado de análisis de puertos realizado con Zenmap.



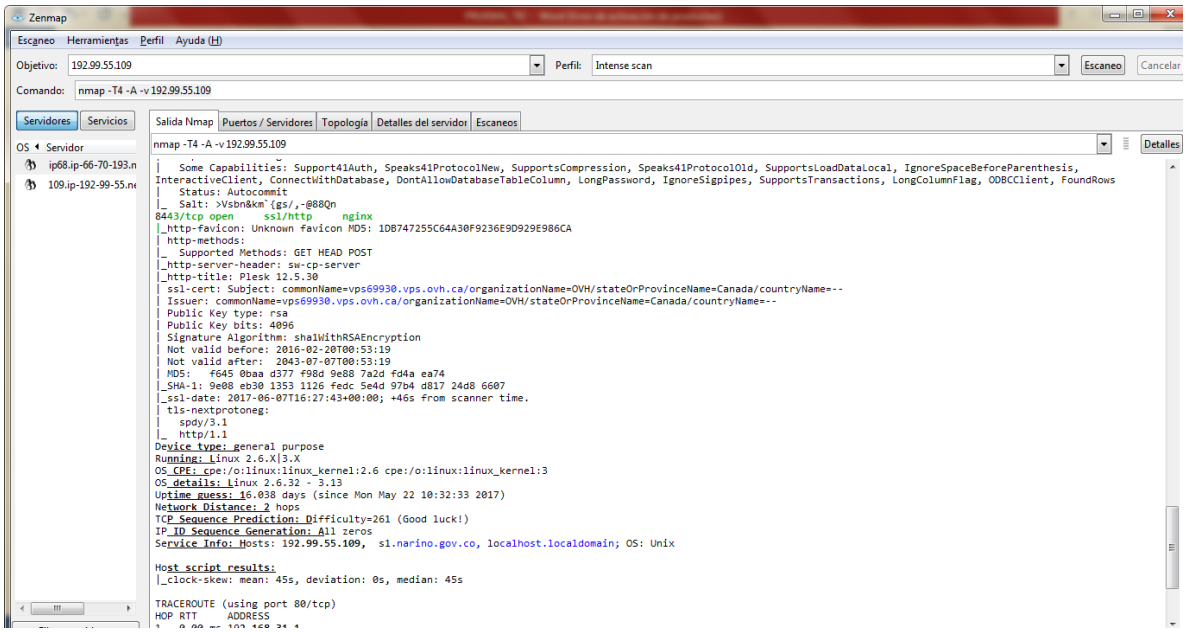
Fuente: Autoria Propia

Figura 34. Resultado de análisis de puertos realizado con Zenmap.



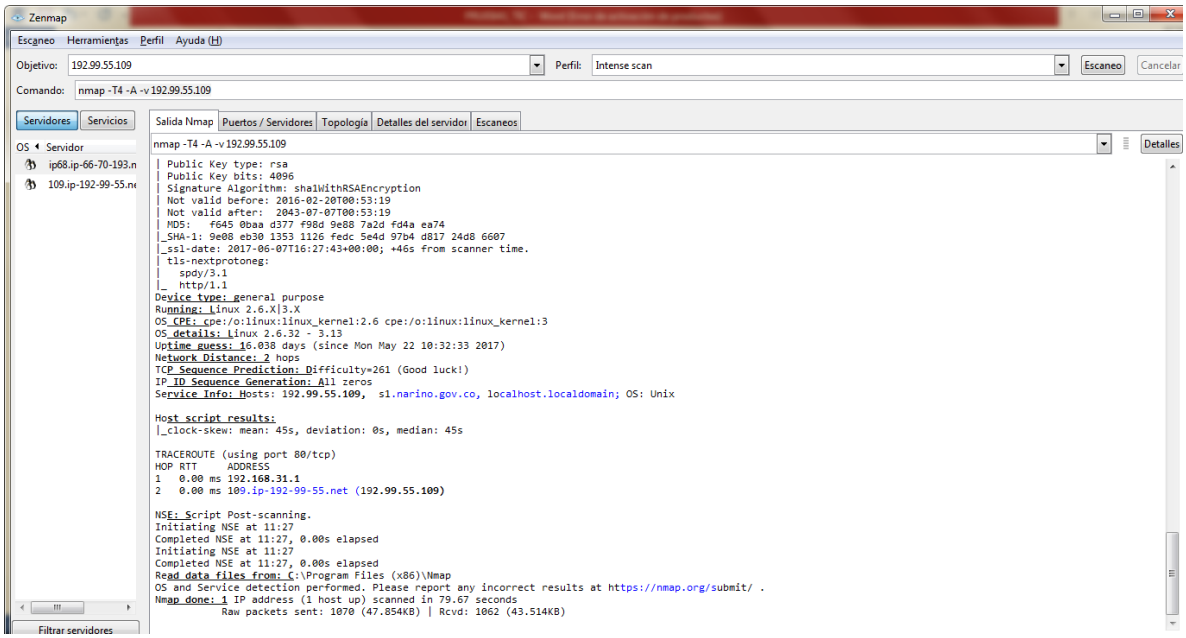
Fuente: Autoria Propia

Figura 35. Resultado de análisis de puertos realizado con Zenmap.



Fuente: Autoria Propia

Figura 36. Resultado de análisis de puertos realizado con Zenmap.



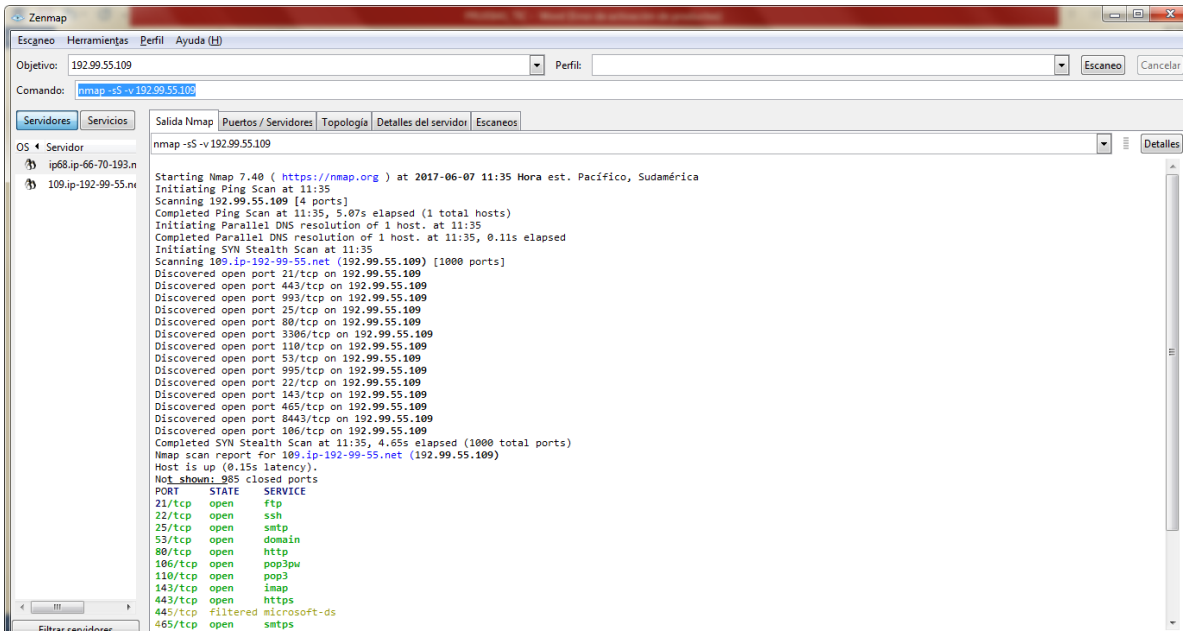
Fuente: Autoria Propia

En la herramienta Zenmap, en la interfaz gráfica ejecutaremos el siguiente comando nmap -sS -v (IP)

nmap -sS -v 192.99.55.109

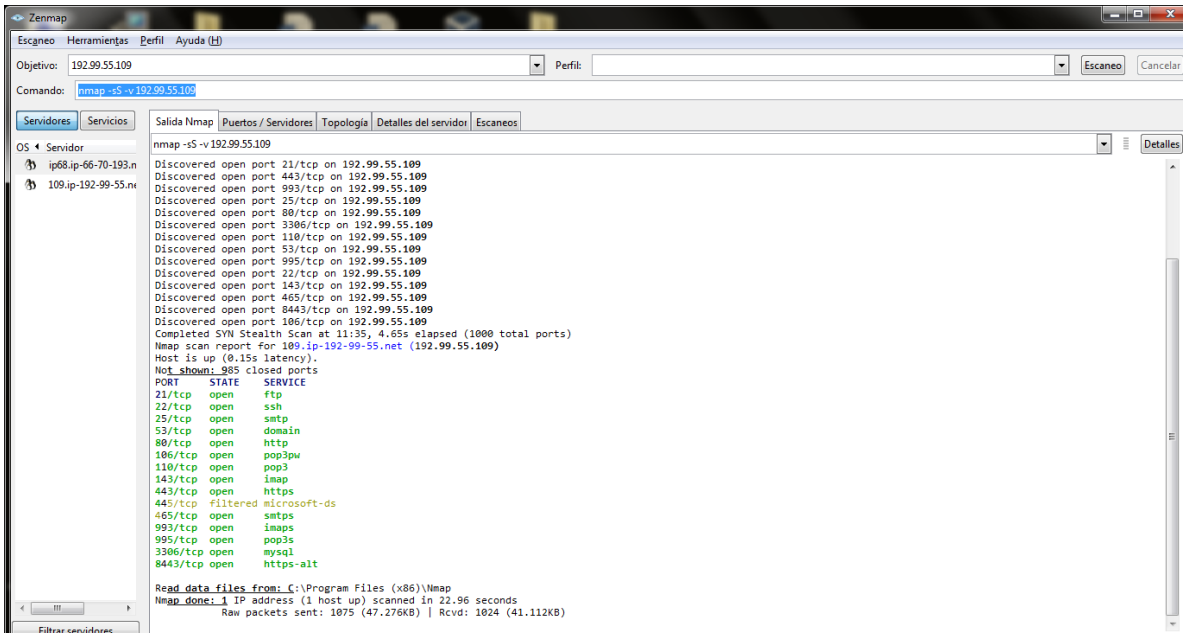
Como resultado nos indica que puertos están abiertos su estado y su servicio

Figura 37. Resultado de análisis de puertos realizado con Zenmap.



Fuente: Autoria Propia

Figura 38. Resultado de análisis de puertos realizado con Zenmap.



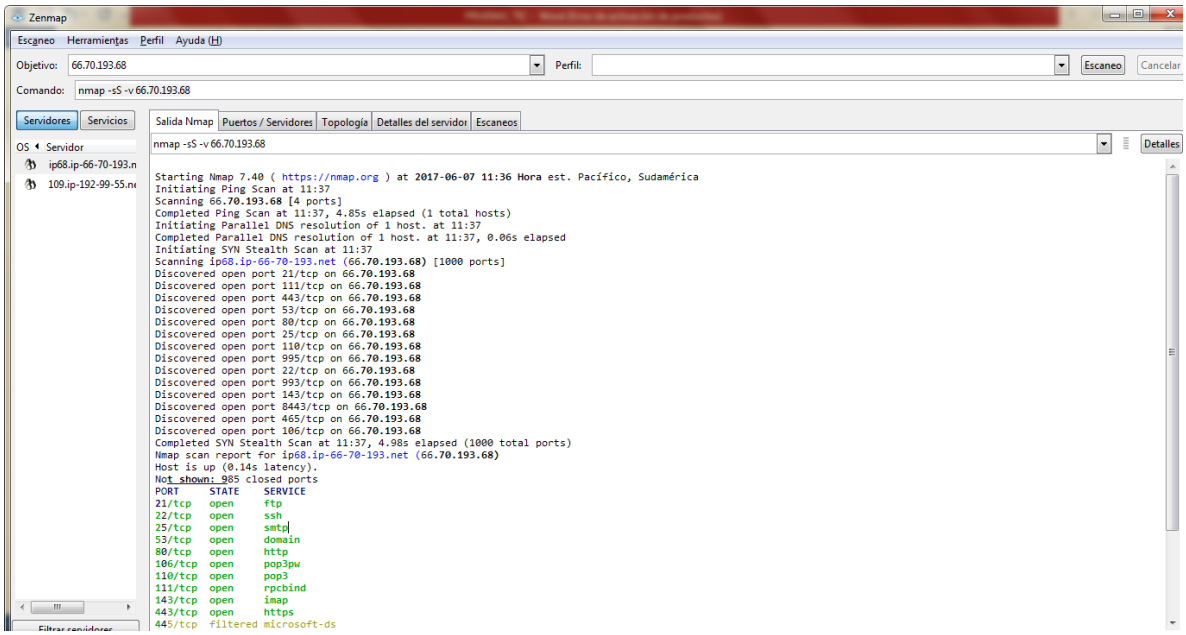
Fuente: Autoria Propia

Ahora ejecutaremos el mismo comando pero con diferente dirección IP en la herramienta Zenmap

nmap -sS -v 66.70.193.68

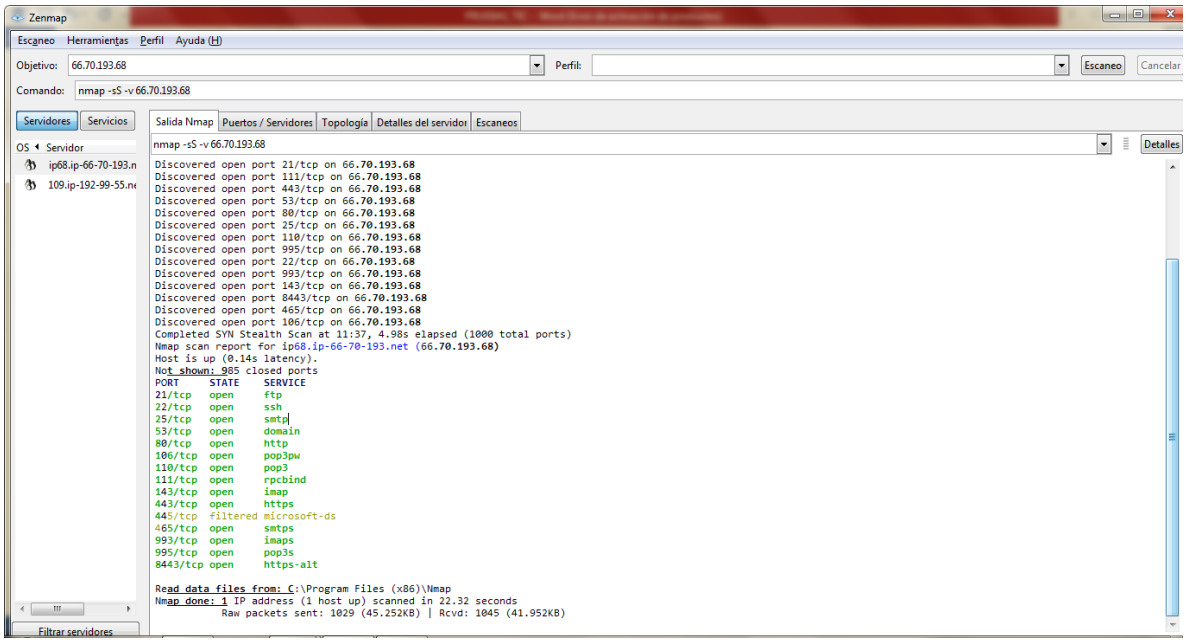
Como resultado nos indica que puertos están abiertos su estado y su servicio

Figura 39. Resultado de análisis de puertos realizado con Zenmap.



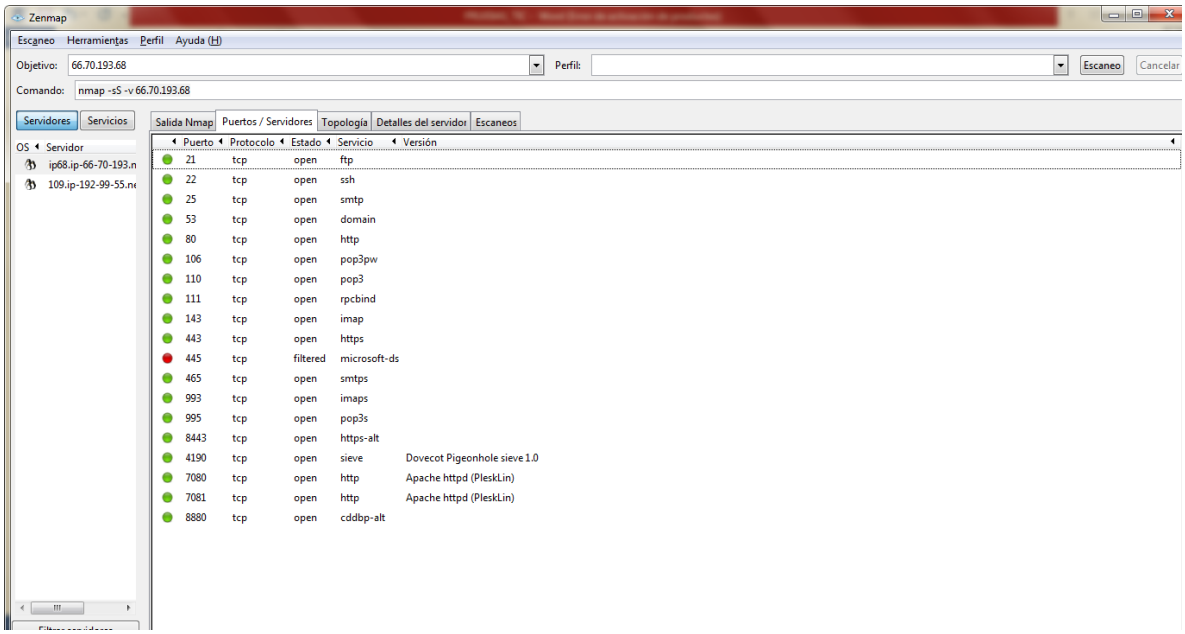
Fuente: Autoria Propia

Figura 40. Resultado de análisis de puertos realizado con Zenmap.



Fuente: Autoria Propia

Resultado de análisis de puertos realizado con Zenmap.
Figura 41. Resultado de análisis de puertos realizado con Zenmap.



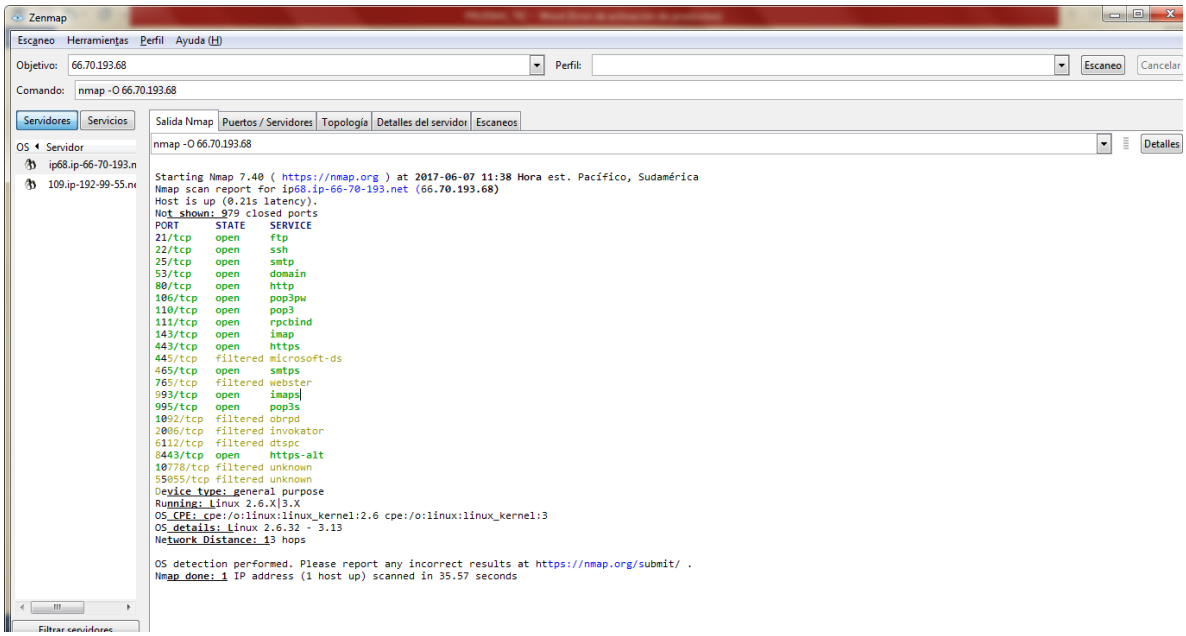
Fuente: Autoria Propia

En la herramienta Zenmap, en la interfaz gráfica ejecutaremos el siguiente comando nmap -O (IP)

nmap -O 66.70.193.68

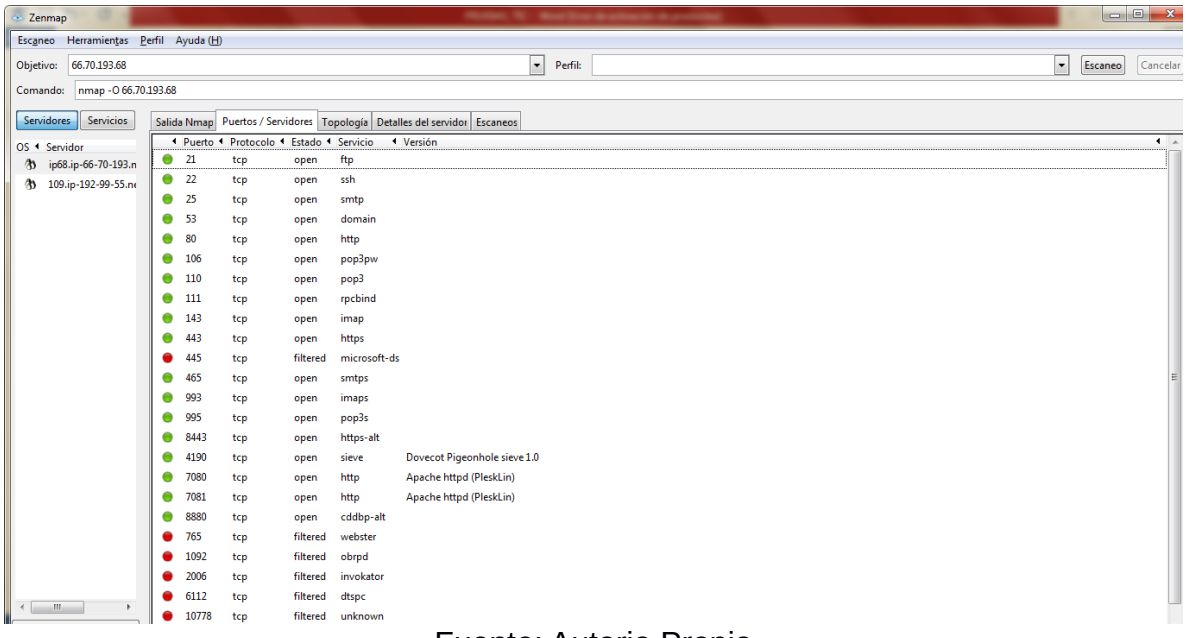
Nos da como resultado el sistema operativo que se está utilizando en el objetivo, en este caso el Sistema Operativo Utilizado es Linux 2.6, también se observa que algunos puertos se encuentran cerrados

Figura 42. Resultado de análisis de puertos realizado con Zenmap.



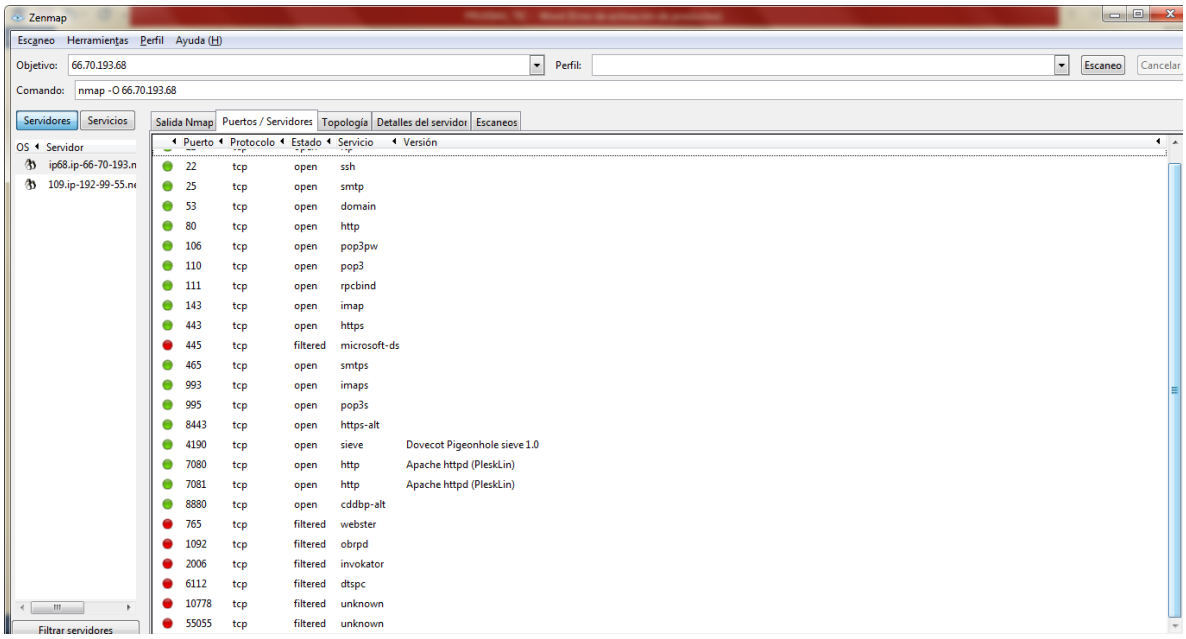
Fuente: Autoria Propia

Figura 43. Resultado de análisis de puertos realizado con Zenmap.



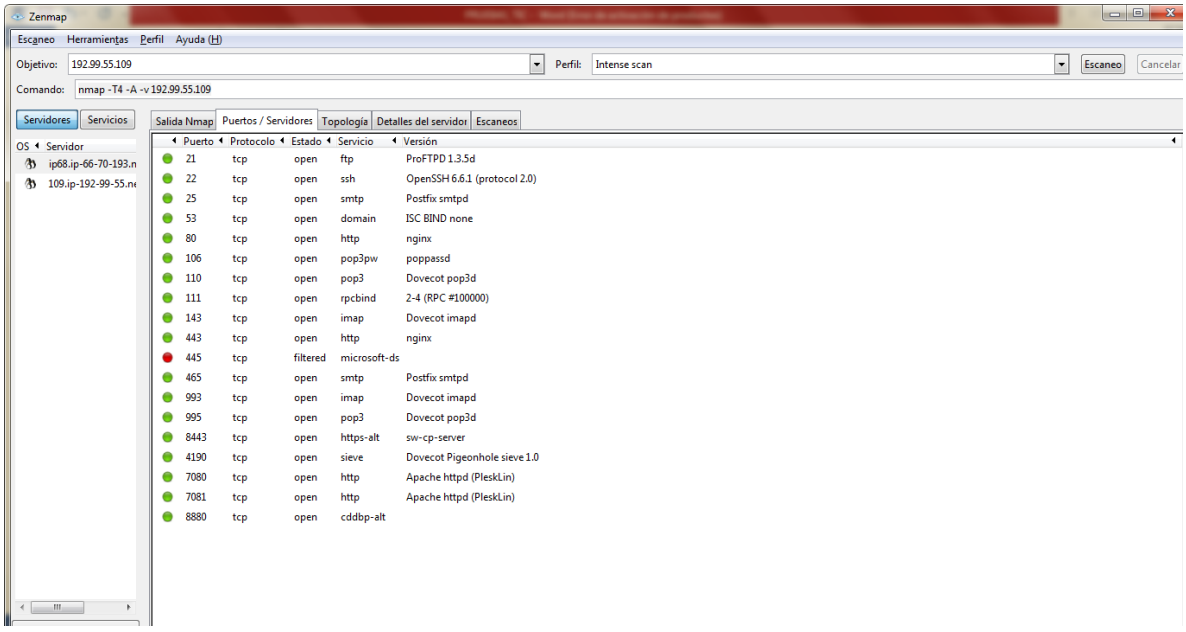
Fuente: Autoria Propia

Figura 44. Resultado de análisis de puertos realizado con Zenmap.



Fuente: Autoria Propia

Figura 45. Resultado de análisis de puertos realizado con Zenmap.

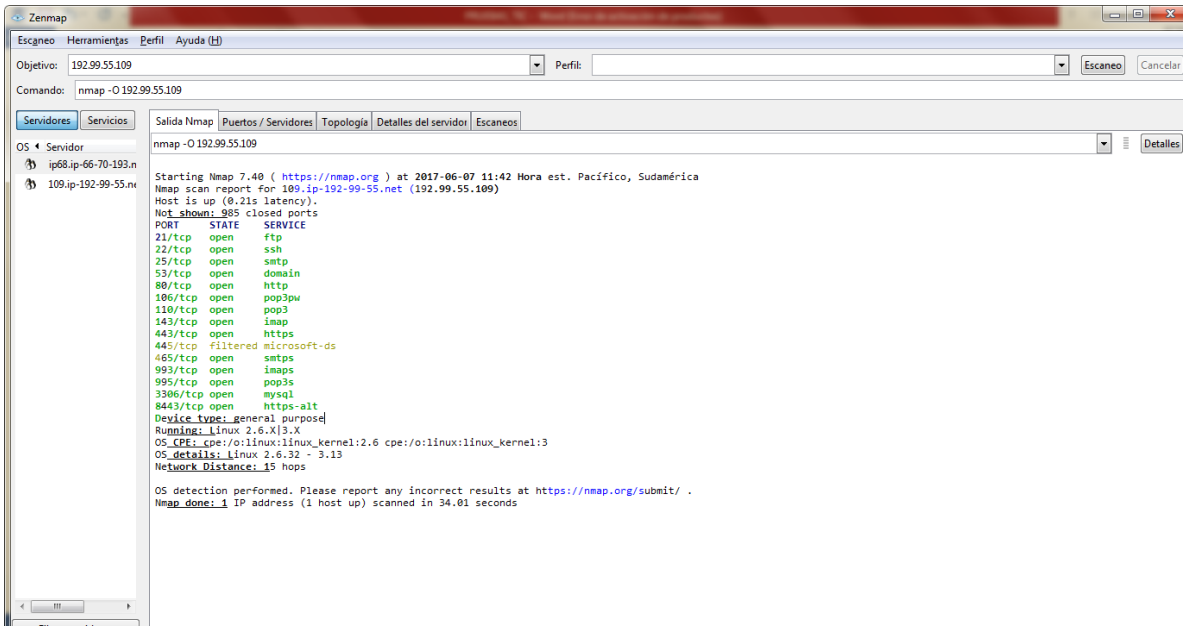


Fuente: Autoria Propia

Ahora ejecutaremos el mismo comando pero con diferente dirección IP en la herramienta Zenmap

nmap -O 192.99.55.109
Nos da como resultado el sistema operativo que se está utilizando en el objetivo, en este caso el Sistema Operativo Utilizado es Linux 2.6

Figura 46. Resultado de análisis de puertos realizado con Zenmap.



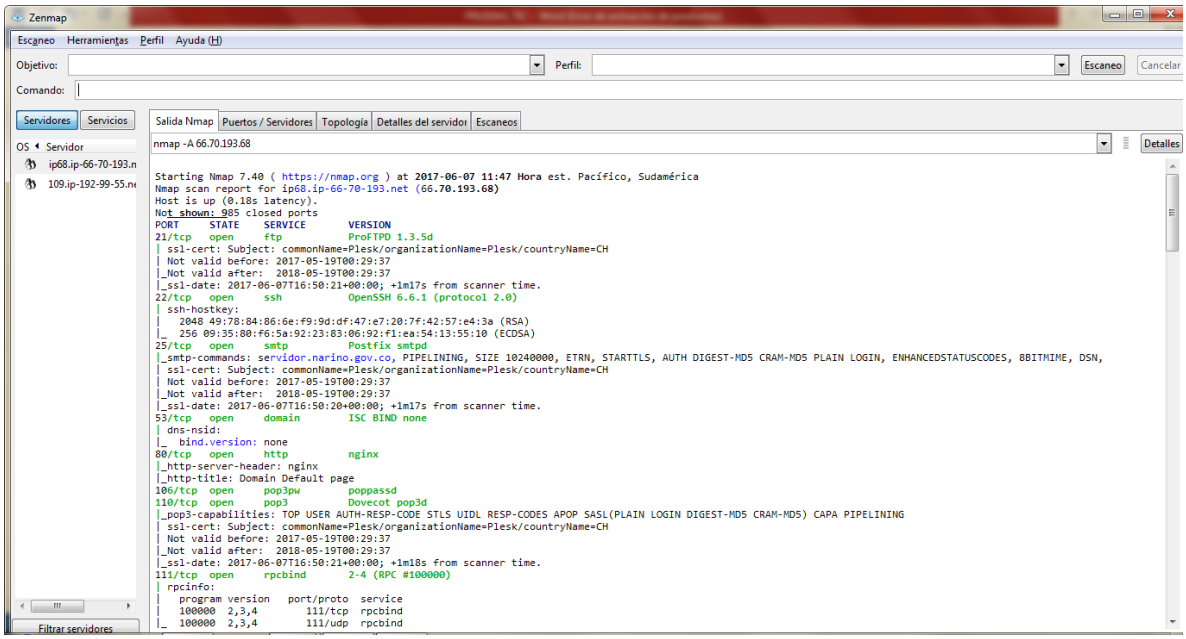
Fuente: Autoria Propia

En la herramienta Zenmap, en la interfaz gráfica ejecutaremos el siguiente comando Nmap –A (IP)

Nmap –A 66.70.193.68

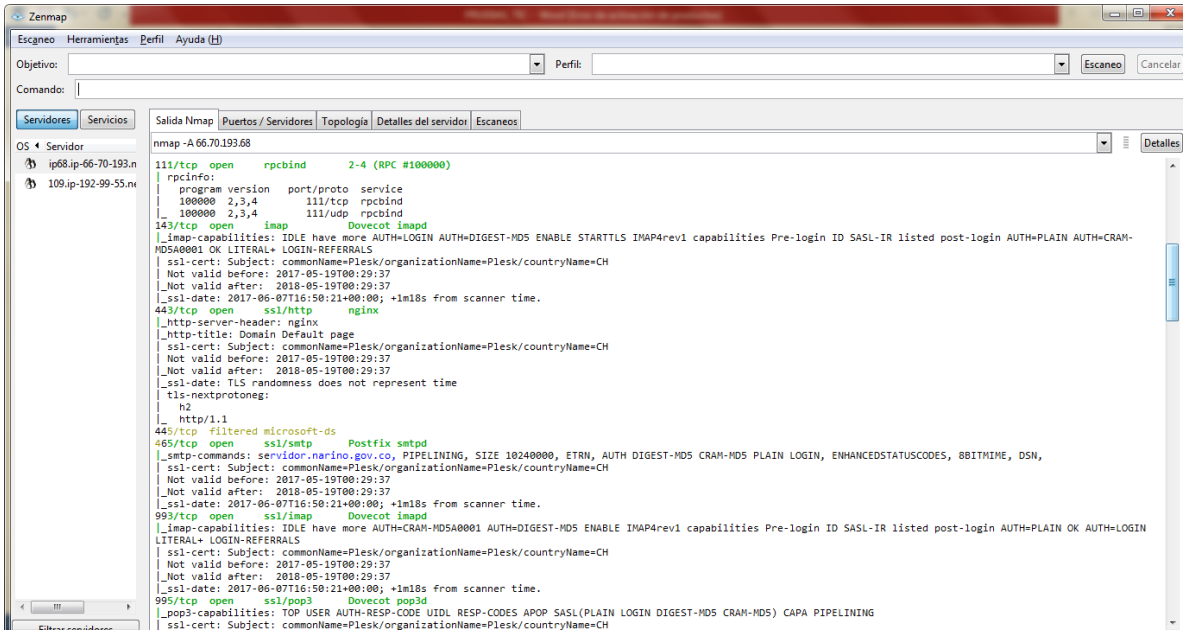
Nos da como resultado el sistema operativo y la versión que se está ejecutando en el host remoto.

Figura 47. Resultado de análisis de puertos realizado con Zenmap.



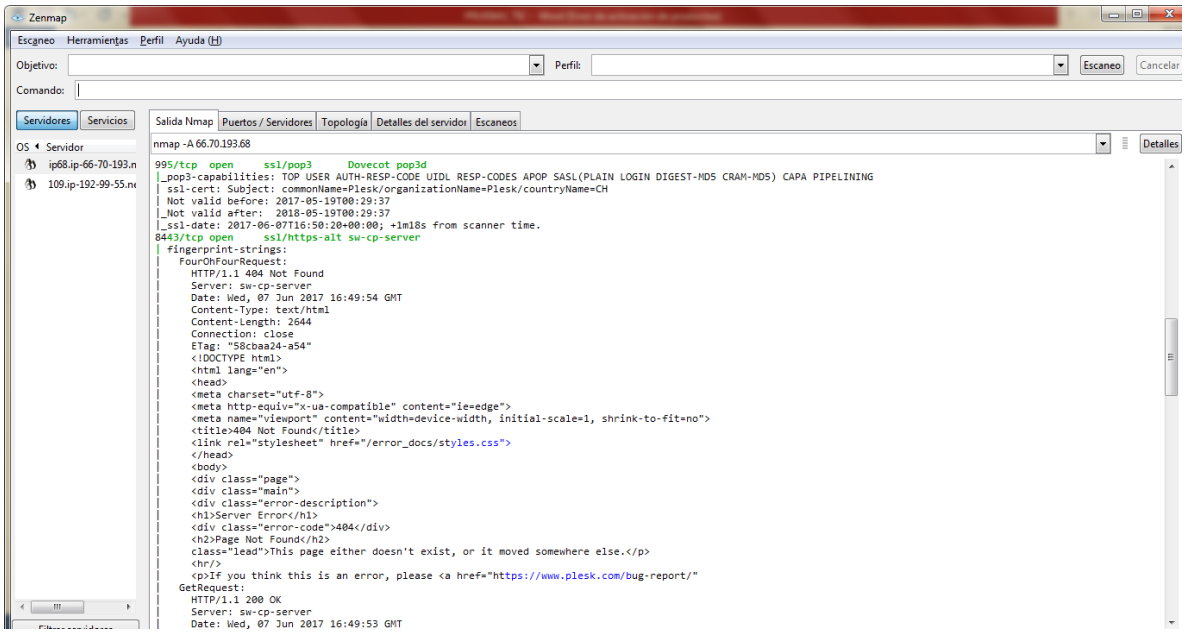
Fuente: Autoria Propia

Figura 48. Resultado de análisis de puertos realizado con Zenmap.



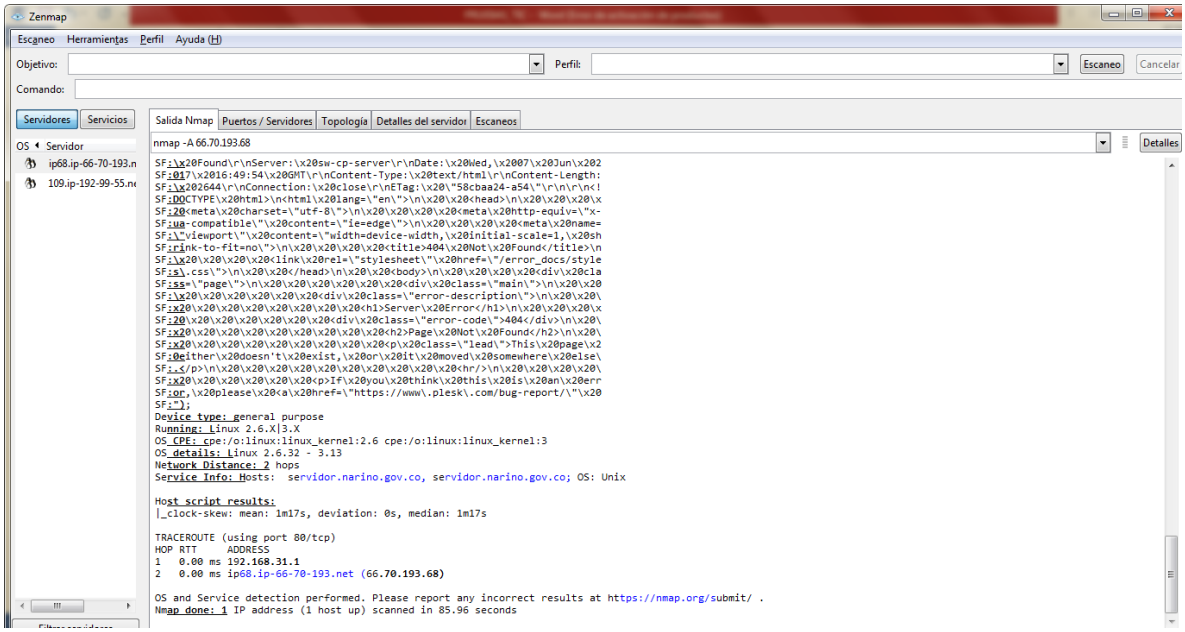
Fuente: Autoria Propia

Figura 49. Resultado de análisis de puertos realizado con Zenmap.



Fuente: Autoria Propia

Figura 50. Resultado de análisis de puertos realizado con Zenmap.

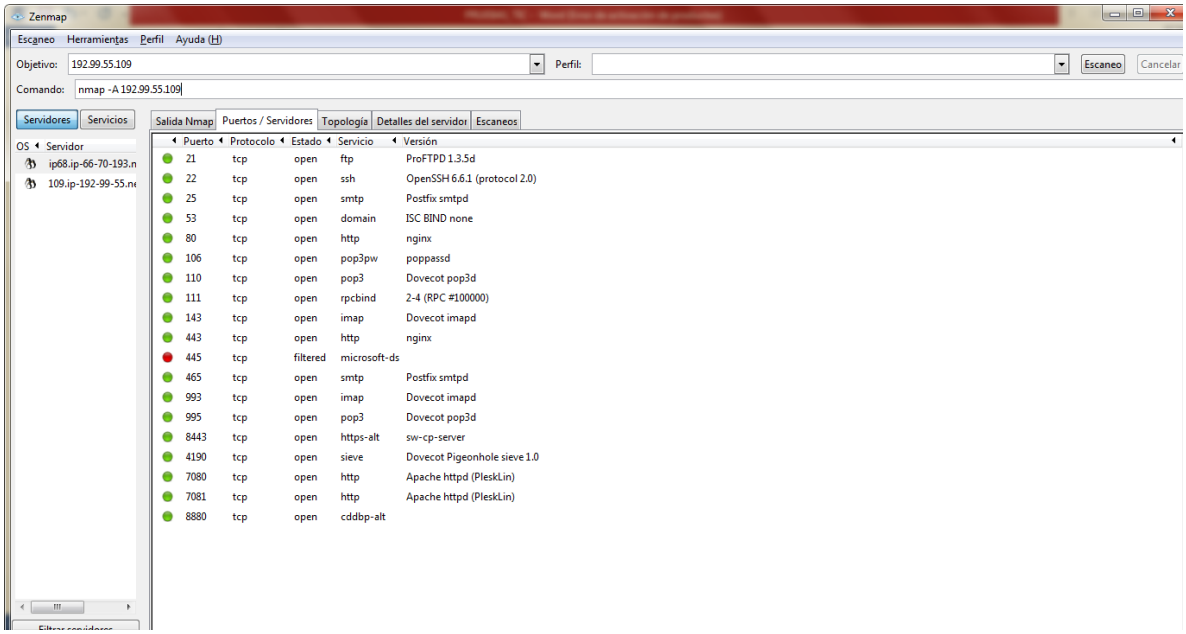


Fuente: Autoria Propia

Ahora ejecutaremos el mismo comando pero con diferente dirección IP en la herramienta Zenmap

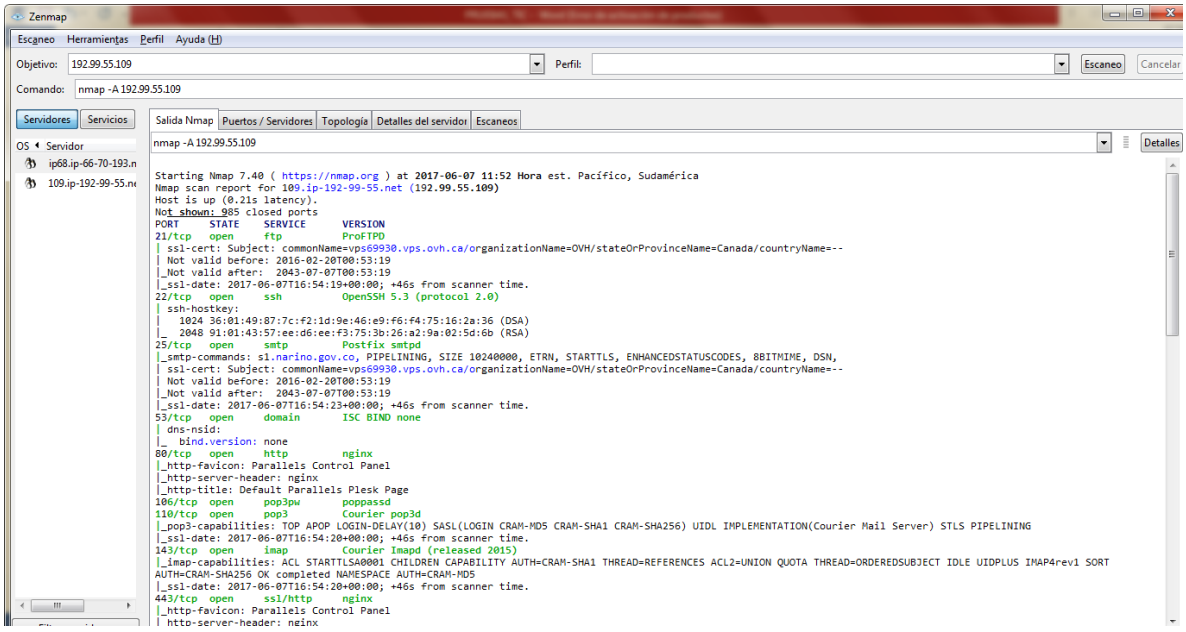
nmap -A 192.99.55.109
Nos da como resultado el sistema operativo y la versión que se está ejecutando en el host remoto.

Figura 51. Resultado de análisis de puertos realizado con Zenmap.



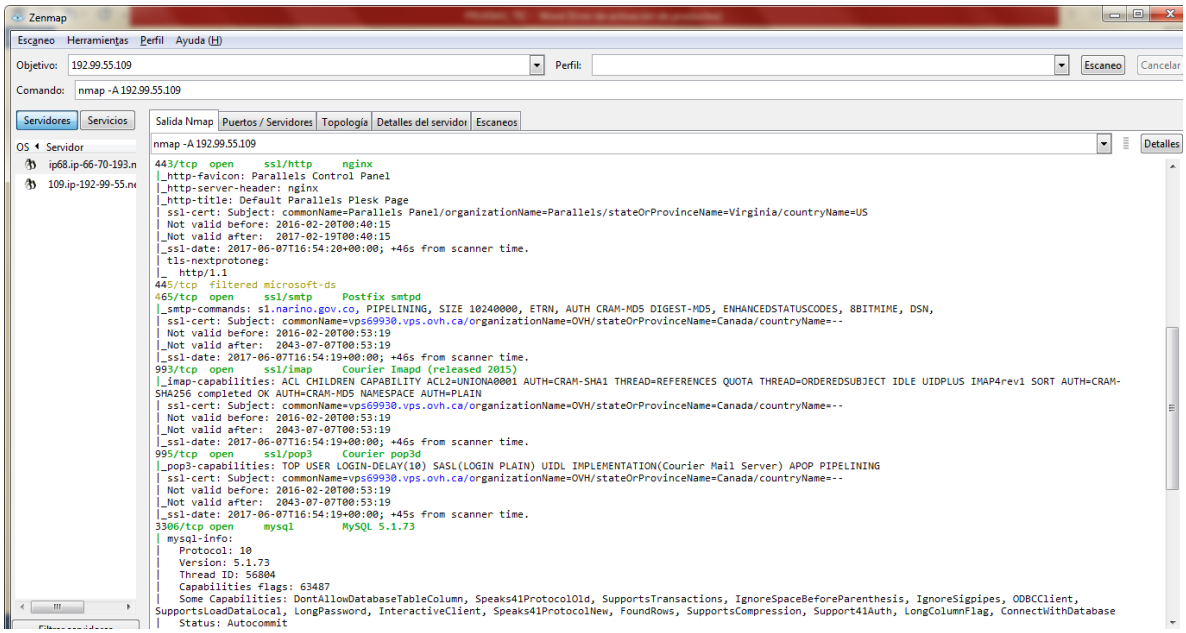
Fuente: Autoria Propia

Figura 52. Resultado de análisis de puertos realizado con Zenmap.



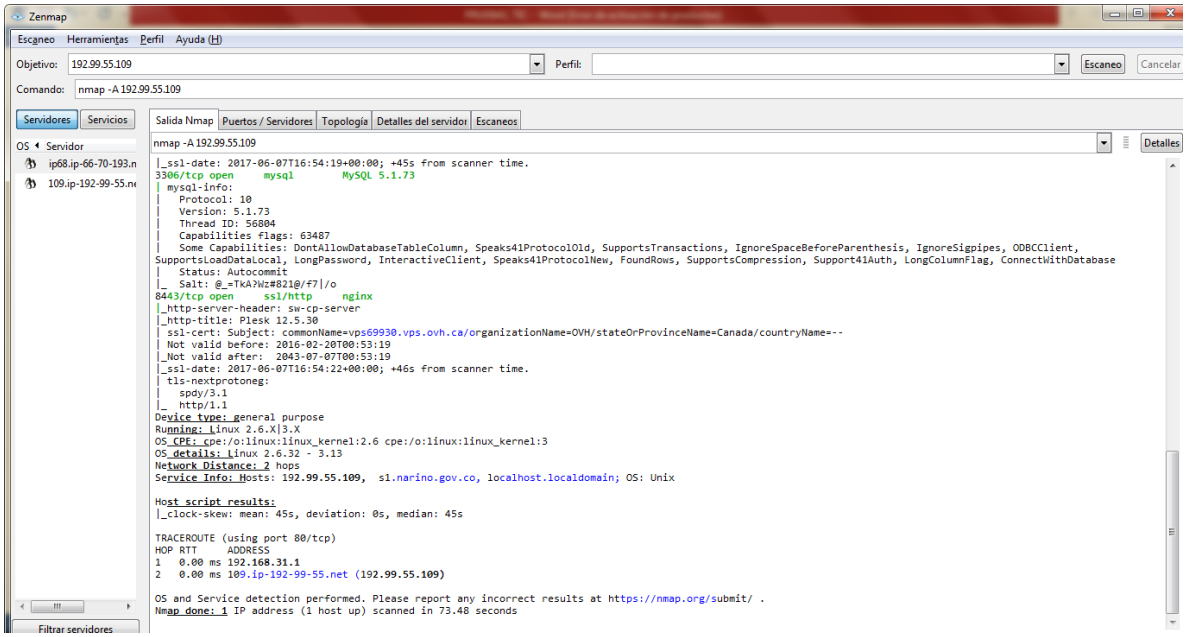
Fuente: Autoria Propia

Figura 53. Resultado de análisis de puertos realizado con Zenmap.



Fuente: Autoria Propia

Figura 54. Resultado de análisis de puertos realizado con Zenmap.



Fuente: Autoria Propia

Ahora realizaremos las pruebas con la herramienta Vega, en la interfaz gráfica

El portal web www.nariño.gov.co es el portal institucional donde se encuentra información relacionada a la entidad y sirve como plataforma de re direccionamiento hacia los otros portales y aplicaciones web que utiliza la institución. Este portal puede apreciarse en la siguiente imagen.

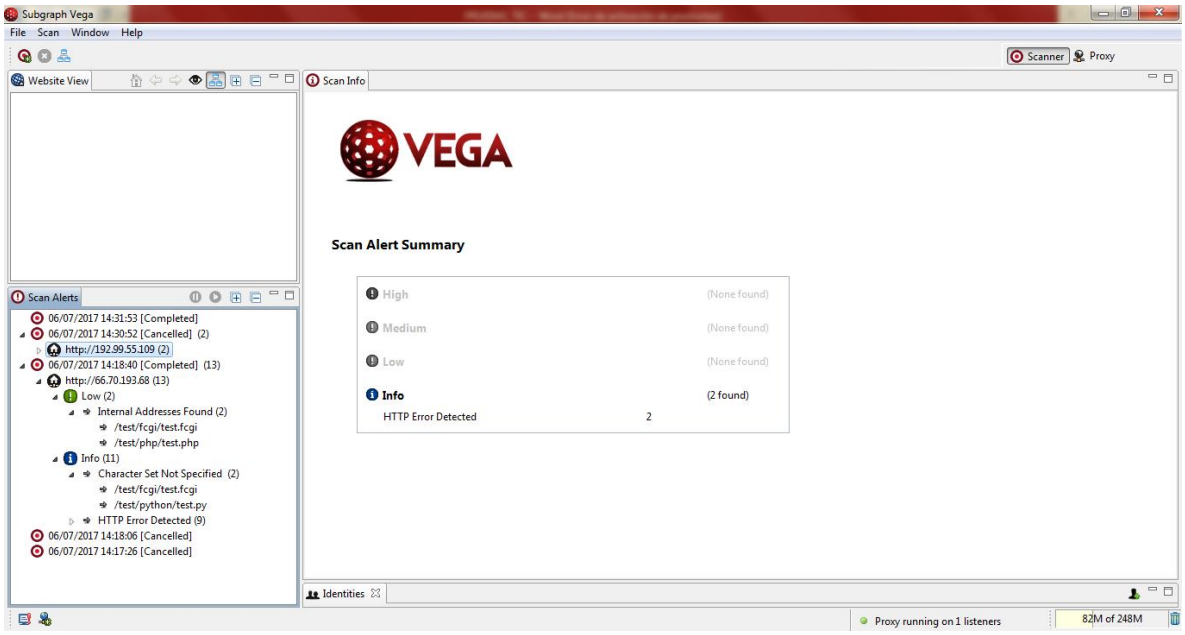
Figura 55.

Fuente: www.nariño.gov.co

Este portal fue sometido a las pruebas con la herramienta Subgraph Vega, a continuación las siguientes pruebas, con las direcciones IP encontradas ejecutamos la IP en la herramienta vega ejecutaremos la dirección **IP 192.99.55.109**

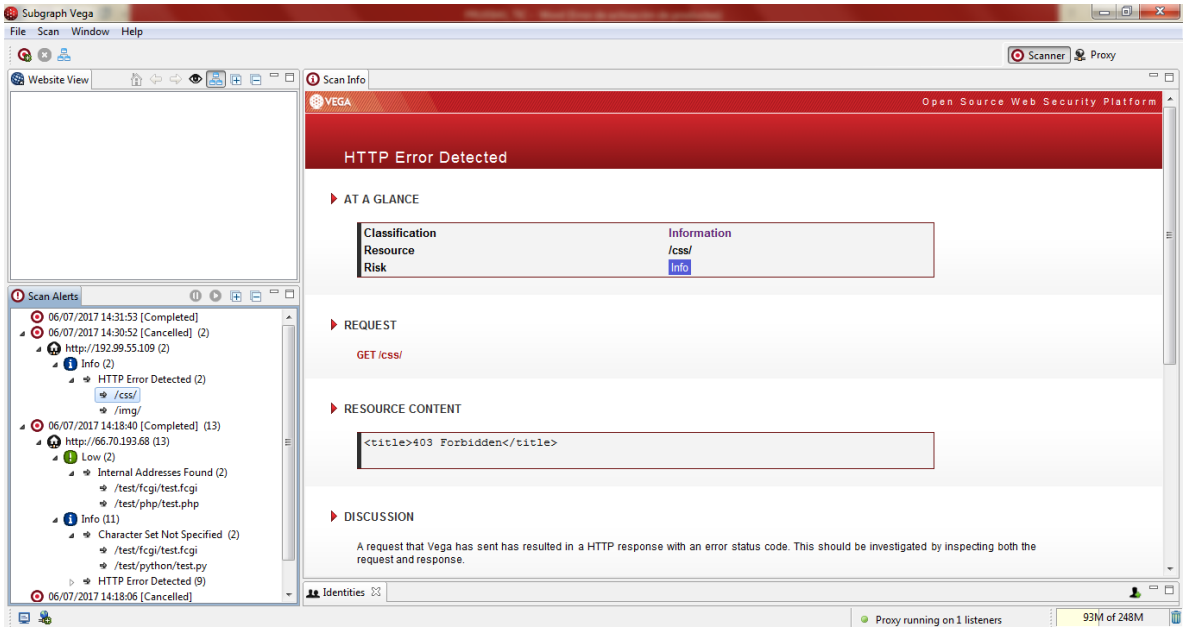
Nos da como resultado que no encontró errores altos ni medios, solo dos errores de información que no son tan graves los cuales son css y una img

Figura 56. Resultado de análisis con VEGA.



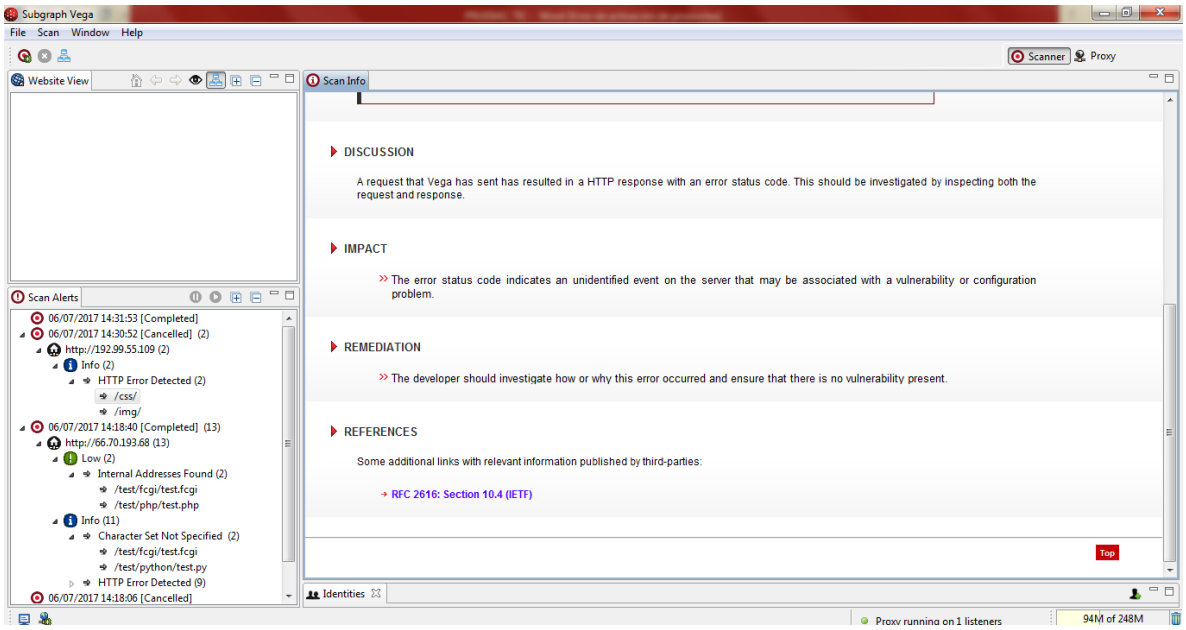
Fuente: Autoria Propia

Figura 57. Resultado de análisis con VEGA.



Fuente: Autoria Propia

Figura 58. Resultado de análisis con VEGA.



Fuente: Autoria Propia

DISCUSIÓN

Una solicitud que Vega ha enviado ha resultado en una respuesta HTTP con un código de estado de error. Esto debe ser investigado inspeccionando tanto la solicitud como la respuesta.

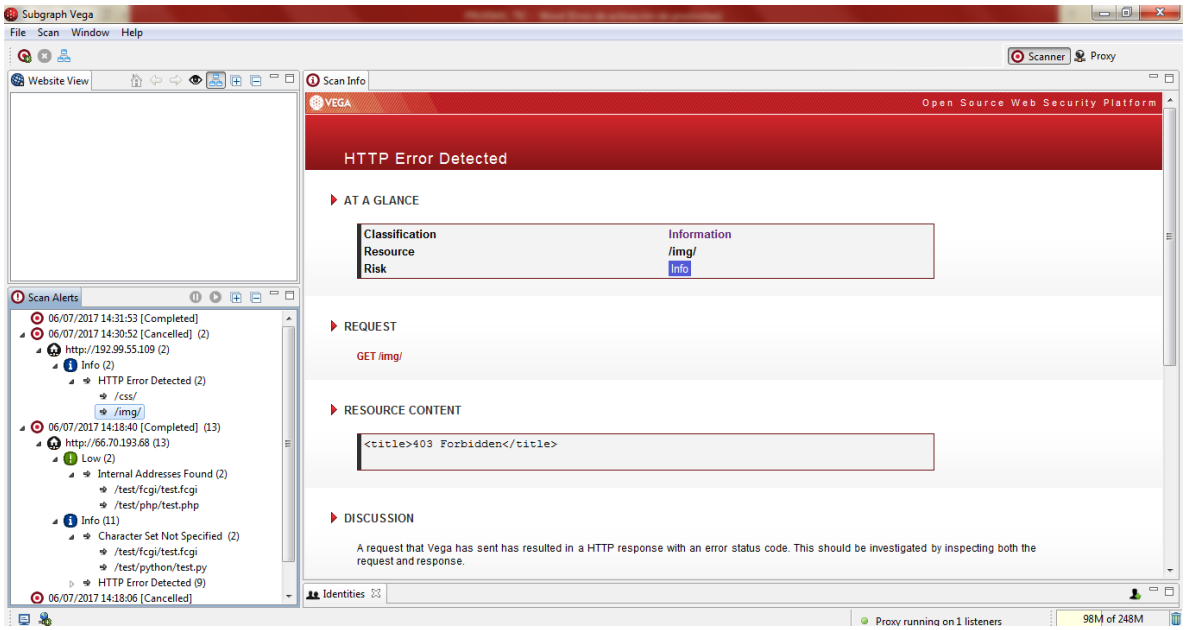
IMPACTO

El código de estado de error indica un evento no identificado en el servidor que puede estar asociado con un problema de vulnerabilidad o configuración.

REMEDIACION

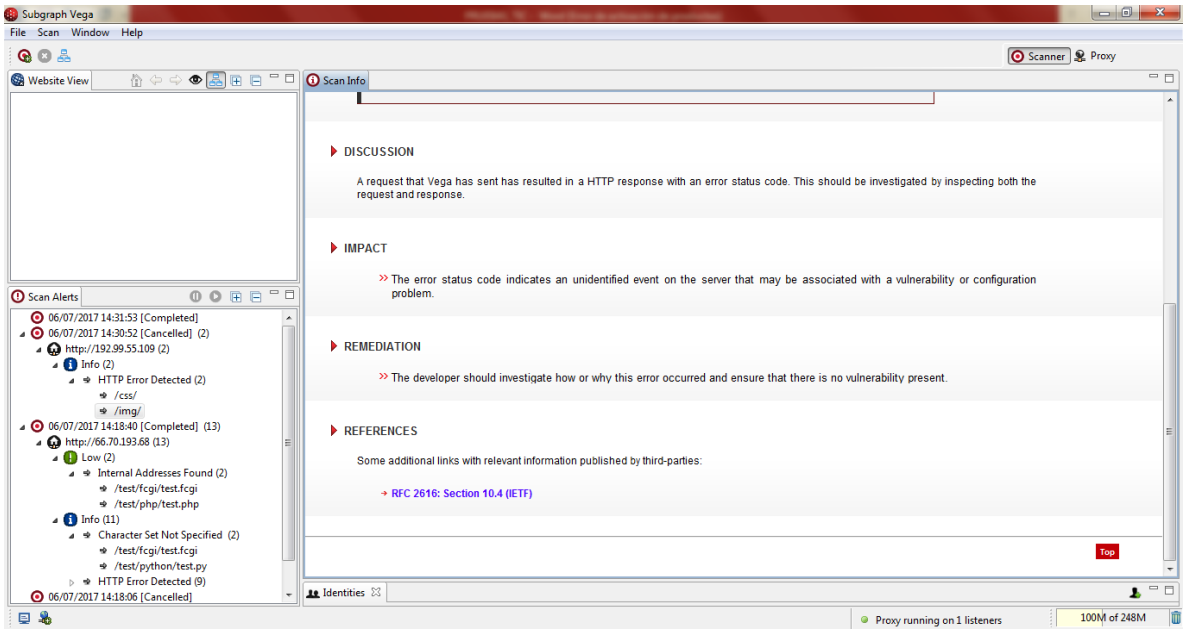
El desarrollador debe investigar cómo o por qué ocurrió este error y asegurarse de que no hay ninguna vulnerabilidad presente.

Figura 59. Resultado de análisis con VEGA.



Fuente: Autoria Propia

Figura 60. Resultado de análisis con VEGA.



Fuente: Autoria Propia

DISCUSIÓN

Una solicitud que Vega ha enviado ha resultado en una respuesta HTTP con un código de estado de error. Esto debe ser investigado inspeccionando tanto la solicitud como la respuesta.

IMPACTO

El código de estado de error indica un evento no identificado en el servidor que puede estar asociado con un problema de vulnerabilidad o configuración.

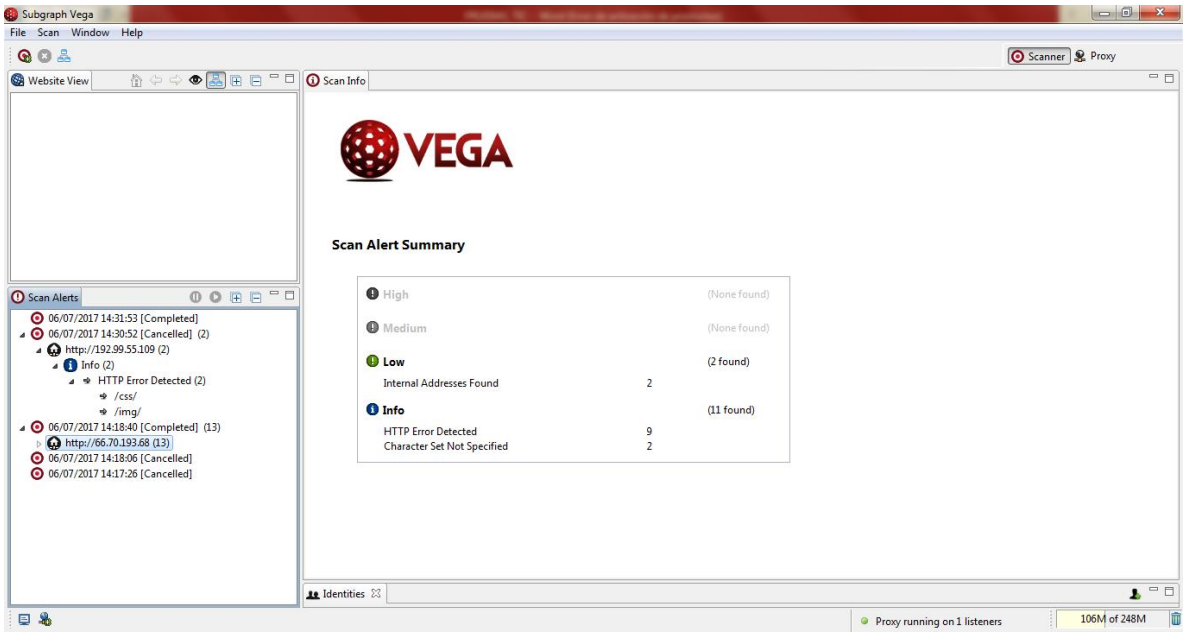
REMEDIACION

El desarrollador debe investigar cómo o por qué ocurrió este error y asegurarse de que no hay ninguna vulnerabilidad presente.

En la herramienta Vega ejecutaremos la siguiente dirección IP
IP 66.70.193.68

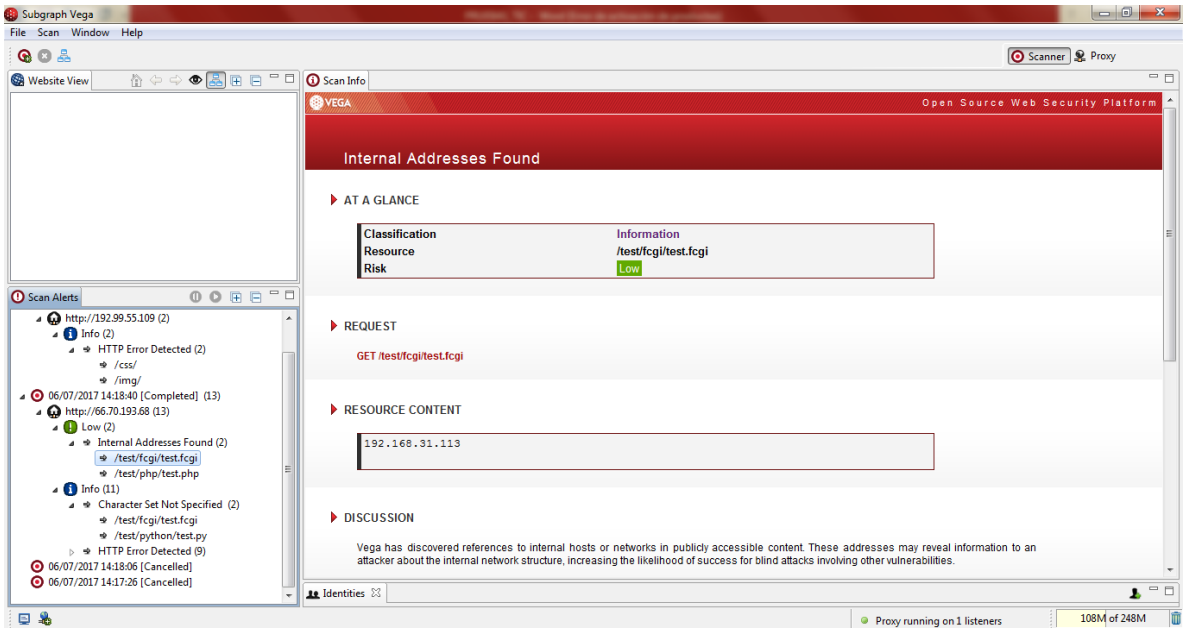
Nos da como resultado que no encontró errores altos ni medios, solo dos errores bajos y uno de información al igual que el anterior no es tan grave

Figura 61. Resultado de análisis con VEGA.



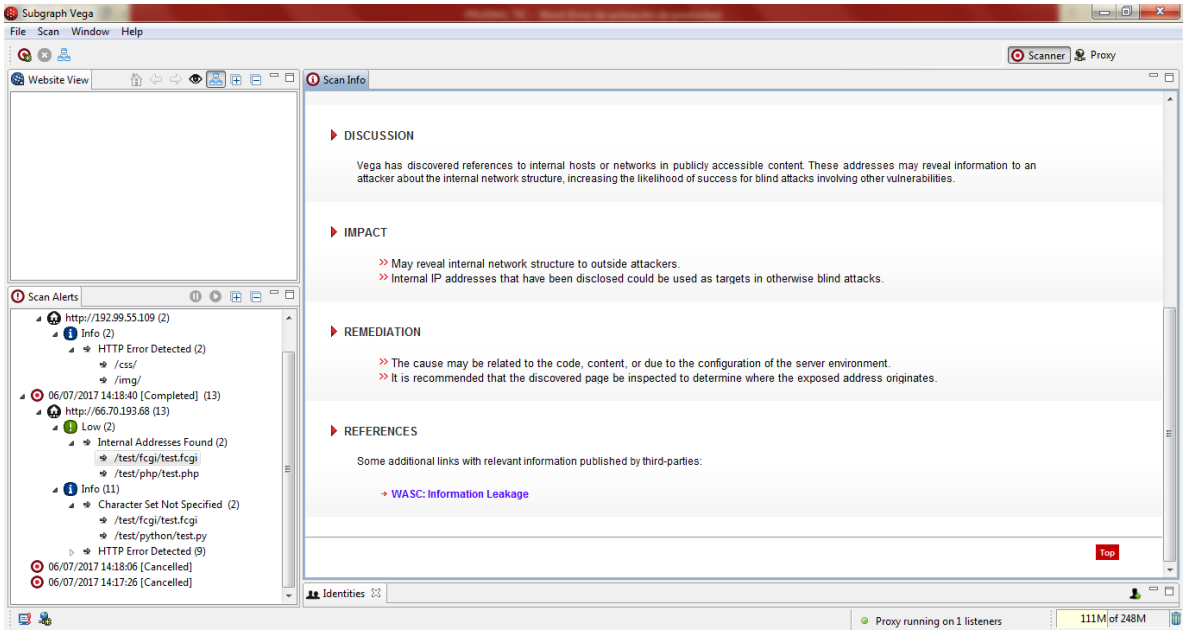
Fuente: Autoria Propia

Figura 62. Resultado de análisis con VEGA.



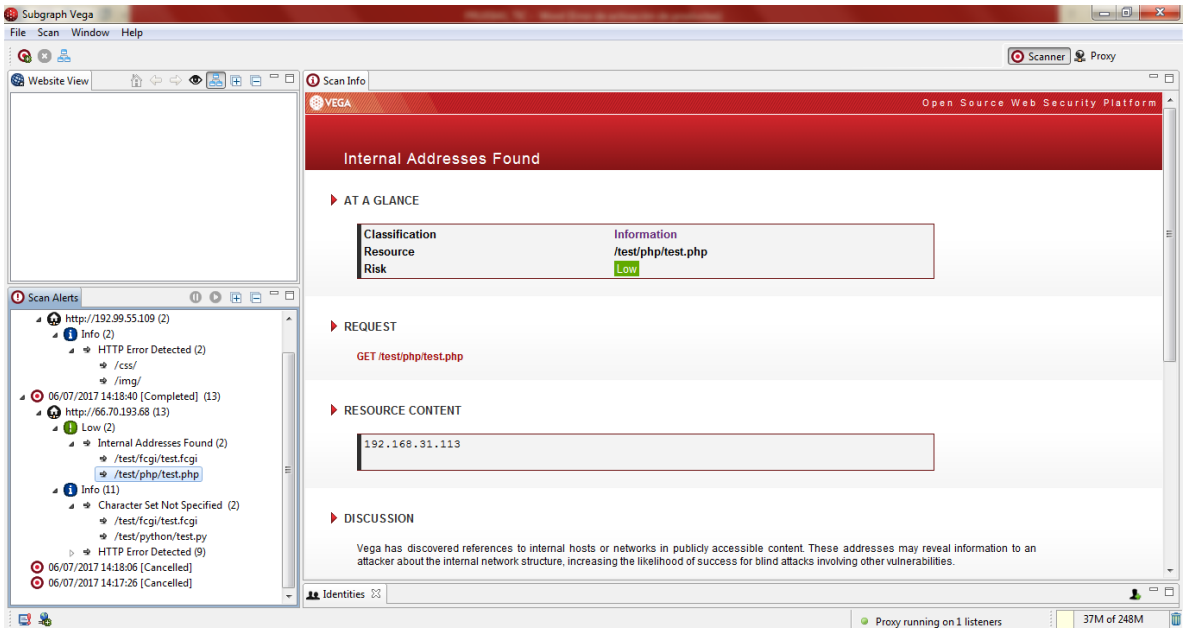
Fuente: Autoria Propia

Figura 63. Resultado de análisis con VEGA.



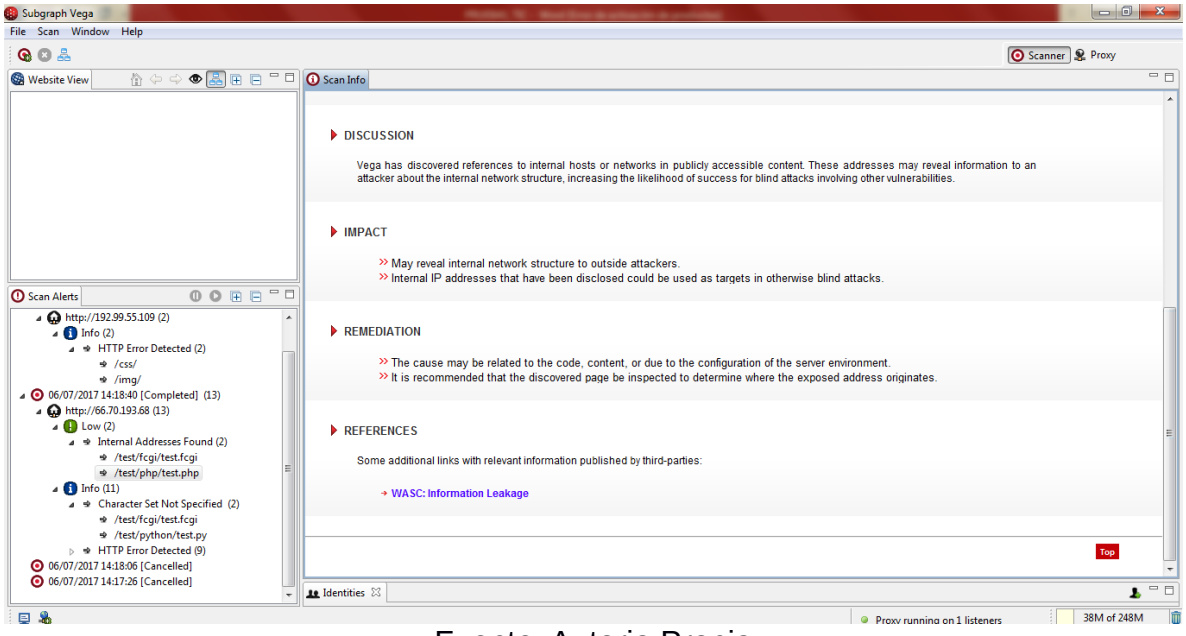
Fuente: Autoria Propia

Figura 64. Resultado de análisis con VEGA.



Fuente: Autoria Propia

Figura 65. Resultado de análisis con VEGA.



Fuente: Autoria Propia

9. RESULTADOS ESPERADOS O PRODUCTO A ENTREGAR

Se realizará el informe final, el cual es un documento técnico que contendrá todos los procesos evaluados con la descripción del comportamiento que estos tienen dentro de la Gobernación con los hallazgos encontrados con sus respectivas recomendaciones que permitan mitigarlos al máximo.

Este informe se presentará y se entregará al coordinador a la secretaria Tic.

- Rediseño de las políticas de seguridad informática de la gobernación de Nariño(Ver Anexo G)

- Informe Ejecutivo acerca de Reunion de información acerca de la Gobernacion de Nariño y sus respectivos dominios (DNS) (Ver Anexo H)

10. RECURSOS

10.1 RECURSOS HUMANOS

Para el desarrollo de este proyecto los ingenieros de la Gobernación de Nariño Jorge Daniel Álvarez García y Ana Julia Cárdenas Bravo. Las estudiantes de Ingenieria de Sistemas de la Universidad de Nariño Argenis Geraldin Fajardo Guerrero y Angela María Timaran Jimenez .

10.2 RECURSOS TECNOLÓGICOS

Tabla 15. Presupuesto Proyecto

PRESUPUESTO			
Cant.	**Descripción**	**Gobernación**	**Proyecto**
1	Computadores.	3000000	
1	Impresora.	2000000	
1	Escáner	2000000	
2	Medios de Almacenamiento DIgitales		20000
1	Resma de papel carta		8000
Talento Humano			
2	Estudiantes Ingenieria de Sistemas	0	
6	Jorge Daniel Alvarez Garcia		12000000
		7000000	12028000
TOTAL 19028000			

10.3 RECURSOS FINANCIEROS

En el desarrollo del proyecto, los gastos que conlleva este serán asumidos por los integrantes del proyecto.

10.4 RECURSO OPERATIVO

En el proyecto a desarrollar no se realizara la etapa de implementación debido a que las políticas de seguridad informática solo quedaran planteadas, pero serán evaluadas por el comité TIC, que será el encargado de su implementación.

11.RECOMENDACIONES

- Mediante el procedimiento planteado se puede verificar la información expuesta en un servidor como es el caso de nariño.gov.co, el cual contiene varios puertos expuestos, determinar qué tipo de servicios se encuentran publicados y a partir de ello determinar si son o no vulnerables.

- En la herramienta Kali Linux se encontró que Sistema Operativo utiliza la organización, esta es una opción muy apreciada por un posible atacante, ya que le permitirá iniciar una búsqueda de herramientas de explotación específicas, según el sistema operativo que se encuentre tras los equipos explorados.

- Mediante la herramienta Zenmap se realizó el mapeo de red, a partir de las direcciones IP obtenidas, los resultados obtenidos fueron conocer en detalle los puertos, el estado y sus servicios que están abiertos.

- El análisis de vulnerabilidades con Vega, no arrojo ninguna vulnerabilidad crítica en los servicios que se están ejecutando en el servidor, ni tampoco alguna configuración errónea que permitiera lograr una intrusión, se pudo observar que en general es un sitio web muy estable.

- En cuanto a las otras vulnerabilidades debido a su contenido informativo, no presenta riesgo a nivel de información importante o de llegar perpetrar alguna intrusión.

- Se conoció la documentación de procesos y procedimientos de seguridad informática con el fin de determinar las políticas existentes en la Gobernación y así realizar un nuevo diseño de las mismas.
- Se aplicó la Metodología Magerit versión 3.0 la cual permite garantizar la seguridad de los activos de la entidad, con el fin de contrarrestar las amenazas, vulnerabilidades y riesgos a los que está expuesta la Gobernación de Nariño.
- Se determinó las vulnerabilidades, amenazas y riesgos de seguridad existentes en la Secretaría de TIC, donde se puede concluir que la información está expuesta en cuanto a confidencialidad, integridad, Autenticidad, Disponibilidad y Trazabilidad.
- Se identificó los riesgos a los que está expuesta la Gobernación y se determinó unos controles de seguridad adaptados a cada una de las necesidades que requiera la misma, todo esto con el fin de garantizar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja la Gobernación de Nariño, utilizando la Norma Internacional ISO 27001/2013.
- Se realizó una serie de pruebas sobre los sistemas de información para determinar las vulnerabilidades a las que están expuestos.
- Se realizaron encuestas y entrevistas y se determinó que el personal interno de la Gobernación conoce algunas de las políticas de seguridad para la protección de los activos informáticos, mas sin embargo no las aplica a cabalidad para mitigar el riesgo al que estos están expuestos.
- Se aplicó el Diseño del SGSI con el fin de realizar una planeación anticipada de diferentes eventos, para que todo esté bajo control, lo que significa que utilizando esta estrategia la Secretaría de TIC de la

Gobernación de Nariño minimice cualquier falla que se presente tanto es su infraestructura o en su información.

- Se realizó el Diseño de Políticas y Procedimientos de Seguridad Informática y de Información utilizando la norma ISO 27001/2013 y Magerit versión 3.0, para obtener una serie de diagnósticos que permite ver el estado de madurez en que se encuentra la Secretaría de TIC frente a la gestión de la seguridad informática.
- Se concluyó que el Diseño de Políticas y Procedimientos de Seguridad Informática y de Información mediante el SGSI en la Secretaría de TIC de la Gobernación de Nariño, puede ayudar al mejoramiento de actualización de diferentes procesos que esta lleva, a corto y mediano plazo, logrando fortalecer la continuidad de la Entidad, y mitigando los riesgos a los que puede estar expuesta alguna información.

12.RECOMENDACIONES

- Capacitar al personal en cuanto a las políticas de seguridad Informática y de la Información permitiendo con ello minimizar las márgenes de riesgo de los activos de la Gobernación de Nariño.
- Realizar campañas de concientización entre los funcionarios de la Gobernación desde los guardias de seguridad hasta los administrativos, con la finalidad de que ellos comprendan:
- Categorizar información confidencial, secreta, sensible o clasificada, y porque dicha información no está catalogada de esta forma.

- Conozcan las implicaciones legales que puedan tener si comparten, copian o divulgan dicha información, en la que se pueden presentar consecuencias desde una amonestación, el despido o incluso la cárcel.
- Hacer revisiones de las contrataciones para verificar que dichos contratos tengan cláusulas de confidencialidad de la información y protección de los datos.
- Se recomienda que haya una revisión periódica de las amenazas y riesgos ya que la tecnología está cambiando constantemente y deben ser controlados para evitar futuros problemas.
- Ausencia de manual de funciones para cada puesto de trabajo dentro del área y también la usencia de puestos creados ya que la mayoria son contratistas , se recomienda definir una arquitectura empresarial como la IT4+
- Establecer guardia de seguridad, durante horarios no habilitados para el ingreso a la Secretaría de TIC, Innovación y Gobierno Abierto de la Gobernación de Nariño
- Instalar alarmas y cámaras como sugerencia de seguridad y o habilitar las existente.
- Establecer un plan de contingencia escrito, en donde se establezcan los procedimientos manuales e informáticos para restablecer la operatoria normal de la organización y establecer los responsables de cada sistema.
- Efectuar pruebas simuladas en forma periódica a efectos de monitorear el desempeño de los funcionarios responsables ante eventuales desastres.

13.BIBLIOGRAFÍA

ALONSO, David. Evaluación de seguridad a sistemas de información en cuanto a ataques maliciosos con base a normatividad, tendencias, impacto y técnicas vigentes para ambientes empresariales a nivel nacional. Trabajo de grado Ingeniería en Informática. Cundinamarca.: Universidad de la Sabana. 2014.

BALDECCHI, Rodrigo. Implementación efectiva de un SGSI ISO 27001 [En línea]. Montevideo: Sonda, 4 de Septiembre de 2014. Disponible en: https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf.

CAO, Javier. Sistemas de Gestión Seguridad de la Información [En línea]. España: Blog spot, Junio de 2014. Disponible en: http://sgsi-iso27001.blogspot.com.

Guía de Implantación de un Sistema De Gestión de Seguridad de la Información Une–ISO/IEC 27001:2007 con la herramienta GLOBAL SGSI [En línea]. Disponible en: http://www.criptored.upm.es/descarga/GUIA_AUDISEC_GLOBALSGSI.pdf

ISO27000. El portal de ISO 27001 en español [En línea]. Octubre de 2005. Disponible en Internet: http://www.iso27000.es/.

PATIÑO, Luis. Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, PROPOLSINECOR. Tesis de Especialización en Seguridad Informática. San Juan de Pasto.: Universidad Nacional Abierta y a Distancia UNAD. 2014. 130p.

CONTRERAS. Lidia. Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la dirección de sistemas de

la Gobernación de Boyacá. Tesis de Especialización en Seguridad Informática. Tunja.: Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas e Ingeniería. 2017. 300p.

SARRIA, Mercedes. Diseño de un modelo de un Sistema de Gestión de Seguridad de la Información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001:2013. Tesis de Especialización en Seguridad Informática. Florencias.: Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2015. 175p.

BUENO. Shirley. Diseñar de un sistema de gestión de seguridad de la información mediante la norma ISO 27001 en el Instituto Colombiano de Bienestar Familiar Centro Zonal Virgen y Turístico de la Regional Bolívar. Tesis de Especialización en Seguridad Informática. Cartagena.: Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2015. 155p.

HENAO, Jaime. Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001 para la empresa USOMET LTDA. En la ciudad de Ibagué. Tesis de Especialización en Seguridad Informática. Bogotá D.C.: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2016. 130p.

PULIDO, Ana Milena y MANTILLA, Jenith. Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina tic de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático. Tesis de Especialización en Seguridad Informática. Fusagasugá.: Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2016. 11p.

SOLARTE, FRANCISCO N J, GUSTIN LOPEZ ENITH ENILSE HERNÁNDEZ REVELO RICARDO JAVIER. Manual de Procedimientos para llevar a la práctica la auditoría informática. Colombia: Editorial CESMAG, 2012.

FALTAN conclusiones y recomendaciones

FALTAN ANEXOS

¿Existe algún informe que contenga el Rediseño de las políticas de seguridad informática de la gobernación de Nariño? el Manejo de las Normas ISO 27001 y 27002 con respecto y la Adquisición de conocimiento acerca de la importancia de Gobierno en Línea tanto para la Gobernación como para sus usuarios.?

No se realiza ningún tipo de citaciones bibliográficas

Adecuar el documento según la norma NORMA TÉCNICA COLOMBIANA - NTC 1486

No veo como anexo la Carta de solicitud de aprobación por parte de la gobernación que autorice la realización del proyecto.

ANEXO A POLITICAS DE SEGURIDAD ANTERIORES

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 1.3-2014

Política de Seguridad y Privacidad de la Informació
Gobernación de Nariño.

Elaborador por: New Technologie- San Juan de Pasto – Celular: 3014326374

Conceptos Básicos

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimien de las siguientes características de la información:

• Confidencialidad: Los activos de información solo pueden ser accedidos y custodiados usuarios que cuente con permisos para ello.

• Integridad: El contenido de los activos de información debe permanecer inalterado y complet Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

• Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo p usuarios que cuenten con los permisos adecuados.

Comité para la Seguridad de la Información.

La Gobernación de Nariño, proyecta la organización de la Seguridad de la información, por m de la creación de una comisión técnica denominada Comité de Seguridad de la Información cu composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Secretario de Gobierno o Líder GEL
- Secretaria General del Departamento.
- Subsecretaria Talento Humano
- Jefe Oficina de Control Interno de la Gestión
- Jefe Archivo General
- Oficina de Gestión Tecnológica.

Los integrantes del comité deberán revisar y actualizar anualmente la Política de Seguridad de Información, presentando los proyectos o propuestas al Gobernador del Departamento para s aprobación mediante acto administrativo correspondiente.

L@s Secretari@s, Directores de departamento o Jefes de Dependencias u Oficinas, deben identificar y valorar los activos de información que pertencen a las respectivas áreas, y debe seguir los lineamientos de gestión enmarcados en esta política y en los estándares, m guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprob y adoptados por el Gobernador del Departamento.

Política de Seguridad de la Información

La política de seguridad es un documento de alto nivel que denota el compromiso del Goberna del Departamento con la seguridad de la información. Esta política contribuye a minimizar lo riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento d funciones misionales de la entidad apoyadas en el uso adecuado de TICs.

ALCANCE

Esta política es de aplicación en el conjunto de Secretarias, Departamentos, subsecretarias , o y dependencias que componen la Gobernación de Nariño, a sus recursos, a la totalidad de lo procesos internos o externos vinculados a la Administración Pública a través de contra

convenios con terceros y a todo el personal de Gobernación, independiente de su t vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores q ejecute.

OBJETIVOS

a) Preservar, proteger y administrar de forma eficiente la información de la Gobernación de Nariño junto con las medios utilizados para la manipulación o procesamiento, frente a amenaz internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento los características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

b) Mantener la Política de Seguridad de la Información actualizada, vigente, operativa controlada, enmarcada en el tratamiento de los riesgos de la información de la Gobernación d Nariño, para asegurar la sostenibilidad de la misma y el nivel de eficacia.

Responsabilidades asignadas

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de Gobernación de Nariño, independiente del tipo de vinculación, el área o dependencia a la cual encuentre adscrito y el nivel del cargo o funciones que desempeñe.

El Gobernador del Departamento de Nariño aprueba esta Política y es responsable de la aprobac y adopción de las actualizaciones.

El Comité de Seguridad de la Información de la entidad es responsable de revisar proyec proponer a la administración departamental en cabeza del Gobernador, para su aprobación, el documento de la Política de Seguridad de la Información, las funciones generales en mate de seguridad de la información y la estructuración, recomendación, seguimiento y me continua del Sistema de Gestión de Seguridad de Información de la Gobernación de Nariño. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad la información al interior de la Administración Departamental.

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar la acciones del Comité de Seguridad de la Información y de impulsar la socialización, implementación, seguimiento y control de la política.

Los propietarios de activos de la información, son responsables de la clasificación, mantenimie actualización y valoración de la misma; así como de documentar y mantener actualiz clasificación efectuada, definiendo el perfil de los usuarios, y el nivel de permisos de acceso a la información de acuerdo a sus cargos, funciones y competencias. Tienen la responsabilid mantener de forma íntegral, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Quien ejerza el cargo de Subsecretari@ de Talento Humano, deberá notificar a todo el persona que se vincule con la Gobernación de Nariño, el detalle de las obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos procedimientos, prácticas , guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación y socializ de la presente Política y de los cambios o actualizaciones que en ella se produzcan a todo

personal, a través de la suscripción de los acuerdos de Confidencialidad y de labore capacitación continua en materia de seguridad según los lineamientos establecidos por Comité de Seguridad de la Información de la Entidad.

Los profesionales universitarios y equipo de trabajo de la Oficina de Gestión Tecnológic coordinación con la Secretaría General del Departamento deben seguir los lineamientos de presente política y cumplir los requerimientos que en materia de seguridad informát establezcan para la operación, administración, comunicación y mantenimiento de los siste de información e infraestructura tecnológica de la Entidad.

El Archivo General del Departamento en colaboración con la oficina de Gestión tecnológ determinaran el inventario de activos de información y recursos tecnológicos de los cuales propietarios o custodios, el cual será revisado y avalado por el Almacén General del Departam en responsabilidad de los respectivos líderes.

Quien ejerza el cargo de Director@ del Departamento Administrativo de Contratación verifica que los contratos, convenios u otra documentación de la entidad con servidores públicos y con terceros incluya los lineamientos de la Política de Seguridad de la Información de la Entidad.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son respons de conocer y cumplir la Política de Seguridad de la Información vigente.

La Oficina de Control Interno de la Gestión, es responsable de realizar seguimiento y c periódico sobre información contenida en documentos, sistemas de información y/o actividade vinculadas con la gestión de activos de información. Es responsabilidad de esta área informar el cumplimiento de los lineamientos y medidas de seguridad de la información establecidas po esta Política, y normas adicionales vigentes.

Identificación, clasificación y valoración de activos de información.

Cada área o dependencia de la Entidad, bajo supervisión del Comité de Seguridad de Información, y con base en el inventario de activos de la información, entregado por la empres NEW TECHNOLOGIE debe mantener un inventario de los activos de información con la que cuenta, ya sea procesada y producida. La forma y medios en donde se incorpore la clasificació valoración, ubicación y acceso de la información, las especifica el Comité de Seguridad Información, correspondiendo a la Oficina de gestión tecnológica brindar herramientas permitan la administración eficiente del inventario por cada área o dependencia, garantizando disponibilidad, integridad y confidencialidad de los datos.

Seguridad de la información en el Talento Humano

Todas y todos los servidores públicos de la Gobernación de Nariño, independiente del tipo de vinculación laboral o contractual, la dependencia o área a la cual se encuentre adscrito y el de funciones, tareas o actividades que desempeñe debe contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La oficina de Gestión Tecnológica debe mantener un directorio completo y actualizado de los perfiles creados.

El Comité de Seguridad de la Información determina cuales son los atributos que deben definirs para los diferentes perfles.

El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difund el manual de "Responsabilidades Personales para la Seguridad de la Información en la Gobernación de Nariño".

La responsabilidad de custodia de cualquier documento o archivo mantenido, usado o produ por el personal que se retira, o cambia de cargo, recae en el jefe de departamento, secretaría dependencia o supervisor del contrato; en todo caso el proceso de cambio en la cad custodia de la información debe hacer parte integral del procedimiento de terminación de l relación contractual o de cambio de cargo.

Asuntos Operacionales y de Manejo

Para que las Políticas y estándares de seguridad sean efectivos, la Gobernación de Nariño debe utilizar métodos de trabajo, prácticas de negocios y procedimientos en el contexto de cumplir co las estrategias de la organización. Por lo tanto hay algunos asuntos como el control de cambios documentación de sistemas, procedimientos y estructura organizacional, que aunque no e relacionados directamente con la seguridad de la información, deben ser establecidos o implementados para proveer una protección adecuada de los activos de la información d Entidad.

Responsabilidades del personal de la Gobernación

Todas y todos los servidores públicos de la Gobernación de Nariño, independiente del tip vinculación laboral o contractual, departamento, secretaría o dependencia, a la cual se encuentr adscrito y las tareas o labores que desempeñe debe suscribir un acuerdo que contenga los térm y condiciones que regulan el uso de recursos de TI y las reglas y perfles que autorizan el uso de información institucional.

Los procedimientos para obtener los respectivos perfles y las características de cada uno de e deben ser mantenidos y actualizados por cada departamento, secretaría o dependencia, acuerdo a los lineamientos establecidos por la oficina de Gestión Tecnológica de la Entidad, e cuanto a los dispositivos de hardware y los elementos de software.

La Subsecretaria de Talento humano, en coordinación con la Oficina de gestión tecnológi encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de información que proyecte la socialización y concientización individual y colectiva en tema seguridad de la información en todo el personal.

La Oficina de gestión tecnológica deberá publicar en medios impresos y virtuales como intran correo electrónico, entre otros, información relacionada con temas de seguridad de la informac tales como responsabilidad en la administración de documentos, archivos, buenas prácti amenazas de seguridad, entre otros.

Responsabilidades de Usuarios Externos

Los usuarios externos y personal de organizaciones o empresas externas, debe autorizados por una persona designada en la Gobernación de Nariño quien será responsable control y vigilancia en el uso adecuado de los accesos a la información y propender por la b utilización de recursos tecnológicos si le son facilitados . Los procedimientos para el reg control de dichos usuarios debe ser diseñado, implementado y mantenido por la Oficina de ges en Tics, en coordinación con la sección de atención a la ciudadanía.

Los dueños de los activos de la información se encargaran en orientar a los usuarios autorizados para que hagan adecuado uso de la información y componentes tecnológicos facilitados.

Todos los usuarios externos sin excepción deben aceptar por escrito los términos y condiciones uso de la información y recursos TICs institucionales. Las cuentas de usuarios externos deben s de perfiles específicos y tener caducidad no superior a dos (2) meses, renovables de acuerdo a naturaleza del usuario.

Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web, a modo de informaci institucional o interacción y transacción como ciudadanos, igualmente el servicio de internet al puedan acceder debe estar protegido con contraseña pública, pero se debe contar con restricc de sitios web no autorizados y limites en la capacidad de ancho de banda. Si los usuarios invita no surtieron el proceso de registro, no se permite el acceso a cualquier otro tipo de recursos d información, aplicación y/o herramientas TICs.

Seguridad Física y del entorno

Se debe tener acceso controlado y restringido al datacenter y cuartos de comunicacio principales. La Oficina de gestión en TICs elaborarán y mantendrán las normas, controles y regi de acceso a dichas áreas.

Seguridad en los equipos:

Los servidores que contengan información y servicios institucionales deben ser mantenid un ambiente seguro y protegido por lo menos con:

- Controles de acceso y seguridad física.
- Detección de incendio y sistemas de extinción de conflagraciones.
- Controles de humedad y temperatura.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en servidores aprobad por la Oficina de Gestión en TICs. No se permite el alojamiento de información institucional en

servidores externos sin respectiva aprobación escrita del comité de seguridad de la información la Entidad.

Los equipos importantes de comunicaciones deben ser alimentados por sistemas de pote eléctrica regulados y estar protegidos por UPS.

La oficina de Gestión de TICs, debe asegurar que la infraestructura a red de datos de área local e cubierta por mantenimiento y soporte adecuados tanto para hardware como para software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de institución el cual debe estar capacitado acerca del contenido de esta política y de responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acue a las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad e Información.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas par la creación y el manejo de copias de seguridad.

Administración de las comunicaciones y operaciones

Reporte y revisión de incidentes de seguridad

El personal vinculado a la Gobernación de Nariño, debe reportar con diligencia, efici responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia a la Oficina de Gestión en TICs. Cuando la ocasión lo amerite y existan casos especiales dichos repor podrán realizarse directamente por la persona que encuentre el incidente o novedad. La oficina gestión en TICs , debe garantizar las herramientas informáticas para que se realicen tales report

El Comité de Seguridad de la Información debe diseñar, mantener y difundir las normas, proces y guías para el reporte y revisión de incidentes de seguridad.

En conformidad con la ley, la Gobernación de Nariño podrá interceptar o realizar seguim a las comunicaciones por diferentes mecanismos previa autorización del Comité de seguridad la información, y en todo caso notificando previamente a los afectados por esta decisión.

La Oficina de Gestión de TICs mantendrá procedimientos escritos para la operación de sisten de información cuya no disponibilidad suponga un impacto alto en el desarrollo normal actividades o afecte la continuidad del negocio. Se debe realizar seguimiento a los procedimient establecidos para asegurar la confiabilidad del servicio que prestan.

Protección contra software malicioso y hacking.

Se debe proteger todos los sistemas de información teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguric de la Información elaborará y mantendrá un conjunto de políticas, normas, estándar procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de softw malicioso y técnicas de hacking.

Como control básico, todas las estaciones de trabajo de la Gobernación de Nariño, edificio central y sedes externas deben estar protegidas por software antivirus con arquitectura cliente servidor, con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de la estaciones no están autorizados a deshabilitar este control.

Es deber de la Oficina de Gestión en TICs, hacer seguimiento al tráfico de la red de área local, cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

El área encargada deben mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas de información, aplicativos y software en general.

Copias de Seguridad

Toda información que se encuentre contenida en el inventario de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en lugares seguros.

Los registros de copias de seguridad deberán almacenarse en una base de datos creada para este fin. El comité debe definir el procedimiento de copia de seguridad, administración y custodia de los backups. La Oficina de Gestión en TICs debe proveer las herramientas para que las dependencias puedan consultar la bitácora de la información y registros de copias de seguridad. La Oficina de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Las actividades de copias de seguridad de información crítica debe ser ejecutada y mantenida de acuerdo a cronogramas definidos y publicados por el área encargada.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir La responsabilidad de realizar las copias y mantener actualizadas las mismas, recae directamente sobre cada dueño de activo de la información en la Entidad. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia. Se debe facilitar los medios para realizar dichas actividades, sin que esto genere responsabilidad a la oficina de Gestión de Tics.

Administración de redes de área local.

La configuración de terminales de red, enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la oficina de Gestión de Tics en la Entidad.

Todo equipo tecnológico debe ser revisado, registrado y aprobado por la oficina de Gestión en Tics, antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar la conexión como un incidente de seguridad para ser analizado e investigado.

Intercambio de Información con Entidades Externas.

Las peticiones de información por parte de entes externos deben ser aprobadas por la oficina de Control Interno de la Gestión, y redireccionados a los responsables del manejo y custodia

Las peticiones de información por parte de entes externos debe ser realizada por un medio valid que permita el registro de la solicitud, donde debe identificarse, el remitente, el asunto y la fech T

oda la información institucional debe ser manejada de acuerdo a la legislación colombia normatividad vigente.

Internet y Correo Electrónico Y Sistemas de información automatizados

Las normas de uso de Intranet, Internet, antivirus, sistemas operativos, sistemas de información automatizados, paquetes ofimáticos y de los servicios de correo electrónico serán elaborada mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este co debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información y las comunicaciones.

Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas operativos previam instalados en la Gobernación de Nariño, deben ser aprobadas por la Oficina de Gestión en TICs de acuerdo a los procedimientos elaborados para tal fin .

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. La Oficina de Gestión en TICs debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde a la Oficina de Gestión en TICs, mantener una base de datos actualizada contenga un inventario del software autorizado para su uso e instalación en los sis informáticos institucionales.

Control de Acceso

Categorías de Acceso

El acceso a los recursos de tecnologías de información institucionales deben estar restrin según los perfiles de usuario definidos por el Comité de Seguridad de la Información.

Control de Claves y Nombres de Usuario

El acceso a información restringida debe estar controlado. Se recomienda el uso de sis automatizados de autenticación que manejen credenciales o firmas electrónicas.

Corresponde a la Oficina de Gestión en TICs elaborar, mantener y publicar los documentos de servicios de red que ofrece la institución a sus funcionarios, ciudadanía y terc Adicionalmente debe elaborar, mantener y publicar procedimientos de administración de cuer de usuario para el uso de servicios de red.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclus personal encargado de tales aplicativos o sistemas de información.

La Gobernación de Nariño debe propender por mantener al mínimo la cantidad de cuentas de usuario que los funcionarios y terceros deben poseer para acceder a los servicios de red.

El control de acceso a los dispositivos intermedios de red es responsabilidad de la Oficina de Gestión en TICs. Dichas contraseñas deben ser codificadas o encriptadas y almacenadas de for segura.

Las claves de administrador de los diferentes sistemas deben ser conservadas por la coordin de la Oficina de Gestión de TICs y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

Adicionalmente la oficina de gestión en Tics debe elaborar, mantener y actualizar el procedimie y las guías para la correcta definición, uso y complejidad de claves de usuario.

Una vez se termine la relación contractual o laboral del personal con la Gobernación de Nariño, oficina de gestión en TICs, debe expedir un certificado de suspensión y/o cancelación de las cu creadas al respectivo usuario, en todos y cada uno de los sistemas de información en los cuale estuviera activo (intranet, correo electrónico, sistemas de información automatizados, entre ot durante un tiempo prudencial por la posible renovación de la relación contractual o laboral, un vez transcurrido el tiempo se dará de baja las cuentas si no hay renovación.

Computación Móvil

La Gobernación de Nariño, en cabeza de la Oficina de gestión en TICs debe reconocer el alto de exposición que presenta la información y los datos almacenados en dispositivos por (computadores portátiles, notebooks, PDA, celulares, etc). Con base a lo anterior, correspon la Subsecretaria de Talento Humano en conjunto con la Oficina de gestión en TICs elabo mantener e implementar planes de capacitación que propendan por la formación y mantenimi de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deb ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seg en redes inalámbricas que debe elaborar el Comité de Seguridad de la Información..

Auditoria y Seguimiento

Todo uso que se haga de los recursos de tecnologías de la información en la Gobernación d Nariño deben ser seguidos y auditados de acuerdo con los lineamientos establecidos por la Ofi de Gestión en TICs

Acceso Remoto

El acceso remoto a servicios de red ofrecidos por la Gobernación de Nariño debe estar sujeto
medidas de control definidas por el comité de seguridad de la información las cuales deben
incluir acuerdos escritos de seguridad de la información.

Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Software

Para apoyar los procesos misionales y estratégicos la Gobernación de Nariño debe hacer
intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software
utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal vincula
a la Gobernación de Nariño.

La Oficina de gestión en TICs debe, elaborar, mantener y difundir el " La Metodología de Desarro
de Sistemas Software en la Gobernación de Nariño" que incluya lineamientos, procesos,
buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de sof
internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de
Identificación y Valoración de Riesgos del proyecto. La Gobernación de Nariño no debe empren
procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos
altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento
estándares de calidad en el proceso de desarrollo y la integración con la plataformma tecnológic
existente en la entidad.

Administración de Continuidad del Negocio

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administraci
de Riesgos de la Gobernación de Nariño

Cumplimiento

Todo uso y seguimiento adecuado en el uso de los recursos de Tecnologías de la Informació
las comunicaciones en la Entidad, debe estar de acuerdo a las normas y estatutos internos así
a la legislación nacional y normatividad vigente, incluyendo la resolución 266 de 30 de Septiemb
de 2013 , por medio de la cual se regula el soporte tecnológico, compra de hardware y adquisici
y/o desarrollo de software en la Gobernación de Nariño.

REFERENCIAS

- Ley 527-1999 Ley de comercio electrónico.
- NTC- ISO-IEC -27001:2013. Sistema de Gestión de la Seguridad de la Información.
- Política para la Seguridad de la Información de la Universidad Distrital Francisco José de Caldas
- Manual de Procesos y Procedimientos de la Entidad -2008.

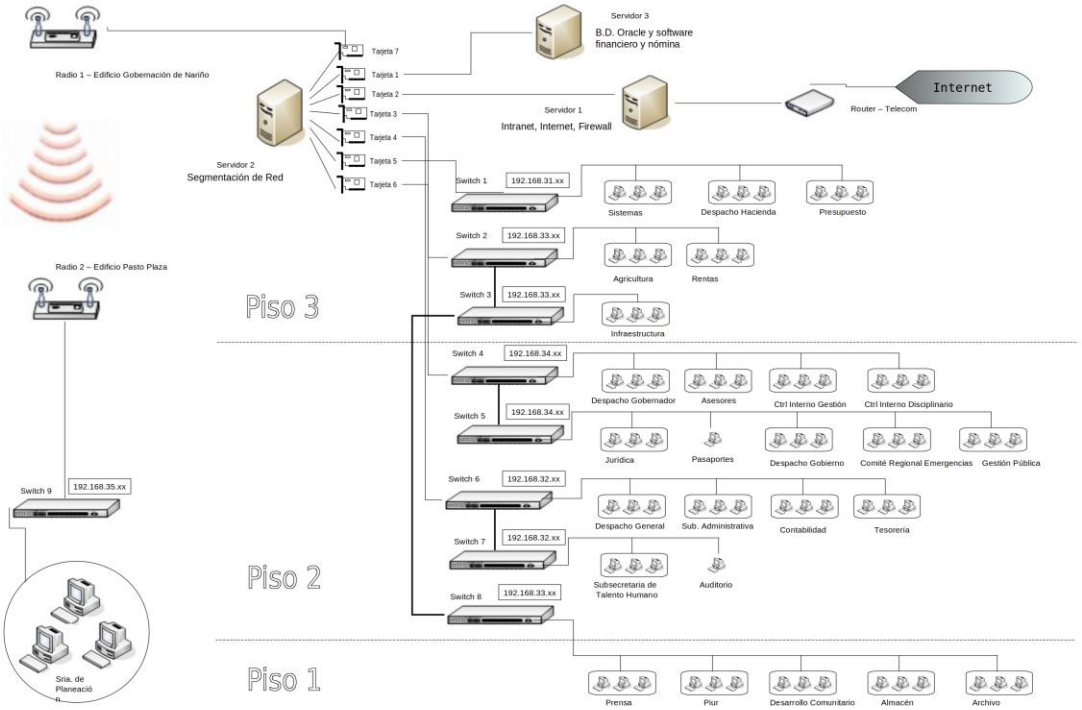
ANEXO B ACTIVOS DE INFORMACION 2015

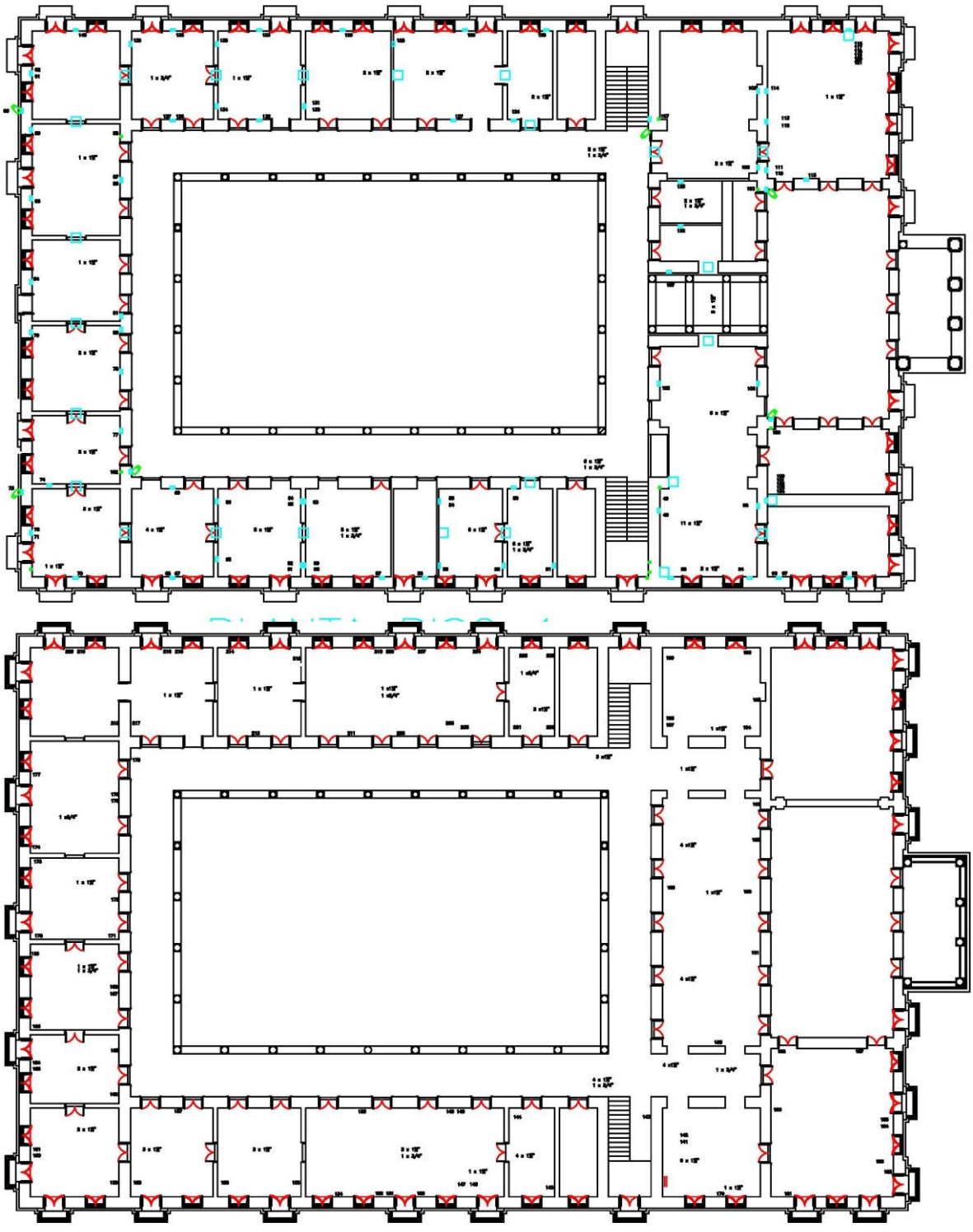
Ver documento anexo ANEXO B-Activos de Informacion 2015

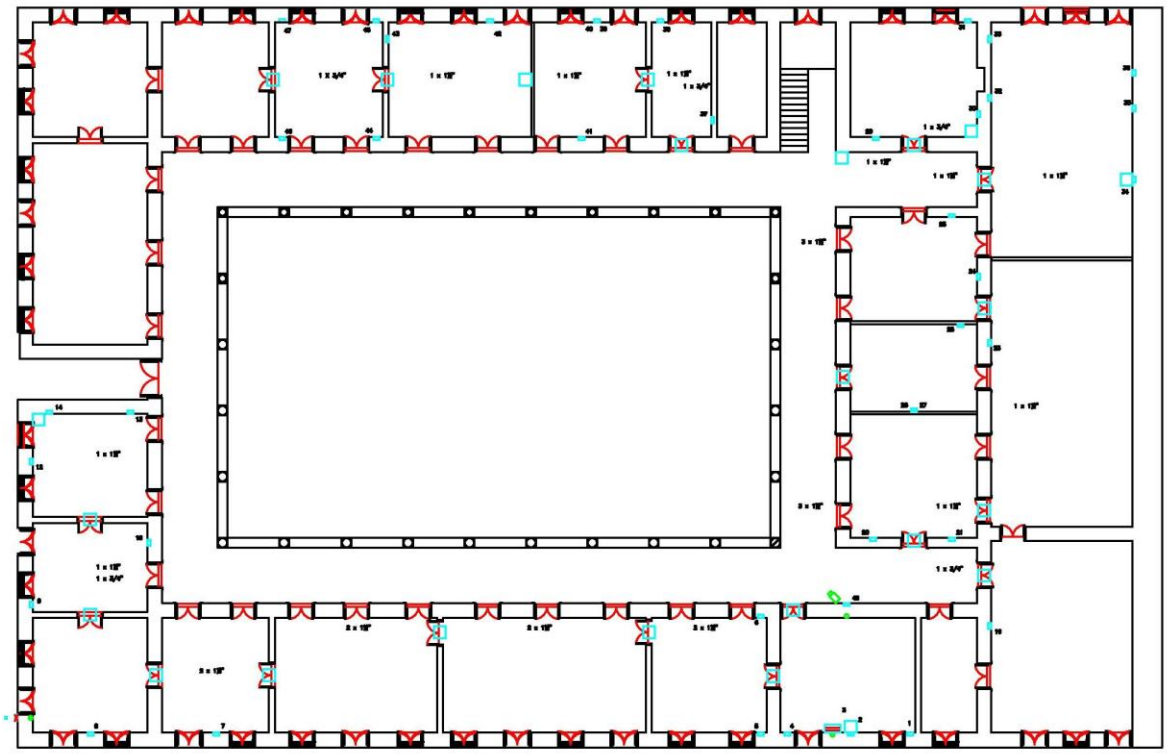
ANEXO C PROCESOS SECRETARIA TIC

Ver documento anexo ANEXO C-Procesos Secretaria TIC

ANEXO D PLANOS DE RED







ANEXO E CARTA DE INTENCION UNAD

Libertad y Orden

Gobernación de Nariño

Secretaría TIC Innovación y Gobierno Abierto

San Juan de Pasto, 11 de agosto de 2017

SECTIC-411

SEÑORES

Grupo de Investigación GMETIS

Universidad Nacional Abierta y a Distancia

Pasto - Nariño

REF. Carta de Intención

Cordial Saludo,

En el marco actual de iniciativas de la Gobernación de Nariño se encuentra la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), este sistema es de un gran importancia para nosotros y nos gustaría invitarlos a participar en el diseño e implementación del SGSI integrando el proyecto presentado por el ingeniero auditor Francisco Solarte denominado "Medición del nivel de Seguridad y Madurez de la Seguridad Informática en los Portales Web de la Gobernación de Nariño de Acuerdo a Norma ISO 27001 y la guía de pruebas OWASP", proyecto que sin duda alguna ayudará a la implementación de la seguridad en nuestro portal web y en el SGSI de la institución, Sabemos de buenas fuentes que dicho docente y su Universidad son conocedores expertos de esta temática, por lo tanto reiteramos la invitación y nuestro interés en el proyecto planteado por el Ingeniero Solarte, el cual tendrá toda la colaboración y apoyo de nuestra parte para que se obtenga los resultados deseados.

Agradecemos mucho su atención y quedamos atentos a cualquier inquietud, y a una respuesta afirmativa de su parte.

Atentamente,

CARLOS ANDRES CORDOBA CELY

Secretario Tic Innovación y Gobierno Abierto

Gobernación de Nariño

Proyecto Daniel Alvarez

danielalvarez@narino.gov.co

ANEXO F RESULTADOS ENTREVISTAS PREVIAS

RESULTADOS ENTREVISTAS PREVIAS

Evaluar el funcionamiento de los sistemas de información del Proceso de Gestión TIC de la Gobernación de Nariño

¿Las condiciones generales de trabajo de los sistemas computacionales del Proceso de Gestión TIC son cómodas para el usuario del sistema? (Incluye equipos, infraestructura, dotaciones etc.)

SI	NO
4	4

¿Tiene protección contra la humedad en el ambiente dentro del Proceso de Gestión TIC? (Incluye ventilación, calefacción etc.)

SI	NO
6	2

¿Toman medidas para prevenir que los sistemas computacionales y las instalaciones eléctricas, telefónicas dentro del Proceso de Gestión TIC tengan contacto con el agua?

SI	NO
6	2

¿Tienen suficientes suministros de energía dentro del Proceso de Gestión TIC? (En cuanto al número de equipos eléctricos utilizados, tienen conexión individual o compartida)

SI	NO
7	1

¿Del Proceso de Gestión TIC el rendimiento y uso del sistema computacional es adecuado? (Los equipos están en sus óptimas condiciones para su uso)

SI	NO
6	2

¿La configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos del Proceso de Gestión TIC se encuentran de una forma adecuada (organizada) y protegen la información? (En cuanto a ubicación, buen funcionamiento y seguridad dentro de la independencia)

SI	NO
7	1

Evaluación de Políticas de Seguridad dentro del Proceso de Gestión TIC de la Gobernación de Nariño

¿Existen medidas, controles, procedimientos, normas y estándares de seguridad dentro del Proceso de Gestión TIC?

SI	NO
6	2

¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal? (Tareas asignadas dentro del Proceso de Gestión TIC)

SI	NO
7	1

¿Existe procedimientos de realización de copias de seguridad y de recuperación de datos dentro del proceso de Gestión TIC?

SI	NO
6	2

¿Existen procedimientos en cuanto a la asignación y distribución de contraseñas para proteger la información dentro del Proceso de Gestión TIC?

SI	NO
6	2

¿Existe un período de vida de las contraseñas dentro del Proceso de Gestión TIC?

SI	NO
1	7

Cuestionario Sobre Gestión de Activos Informáticos dentro del Proceso de Gestión TIC de la Gobernación de Nariño

¿Existe un control sobre el acceso físico a las copias de seguridad dentro del Proceso de Gestión TIC?

SI	NO
6	2

¿Existe un inventario de los recursos informáticos existentes dentro del Proceso de Gestión TIC?

SI	NO
7	1

¿Las copias de seguridad, o cualquier otro soporte, se almacena fuera del Proceso de Gestión TIC?

SI	NO
7	1

¿Existen procedimientos de etiquetado e identificación de los soportes informáticos dentro del Proceso de Gestión TIC?

SI	NO
4	4

¿Existen procedimientos para la realización de copias de seguridad dentro del Proceso de Gestión TIC?

SI	NO
7	1

¿Existe algún programa que permita gestionar y almacenar claves secretas dentro del Proceso de Gestión TIC?

SI	NO
0	8

¿Las contraseñas de los trabajadores del Proceso de Gestión TIC están almacenadas en algún fichero de claves?

SI	NO
0	8

Cuestionario Sobre Seguridad Relacionada con el Personal dentro del Proceso de Gestión TIC de la Gobernación de Nariño

¿Ha sufrido accidentalmente pérdida de información en su puesto de trabajo dentro del Proceso de Gestión TIC?

SI	NO
2	6

En caso de pérdida de información ¿Ha logrado recuperar total o parcialmente la información? (Responda solo en caso de que su anterior respuesta fue SI)

SI	NO
3	1

¿Alguna persona ha divulgado información personal o privada dentro del Proceso de Gestión TIC?

SI	NO
0	8

¿Existe un procedimiento o manual que ayude a manejo de la información privada o restringida dentro del Proceso de Gestión TIC?

SI	NO
3	5

¿Separa la información dependiendo de su importancia dentro del Proceso de Gestión TIC?

SI	NO
3	5

¿Alguna vez se le ha perdido algún dispositivo de almacenamiento, con información del Proceso de Gestión TIC?

SI	NO
2	6

¿Se ha olvidado de cerrar su sesión de su equipo de trabajo dentro del Proceso de Gestión TIC?

SI	NO
2	6

Cuando está ausente en su puesto de trabajo dentro del Proceso de Gestión TIC ¿Su ordenador se queda prendido?

SI	NO
5	3

¿Ha instalado cualquier tipo de programa en su puesto de trabajo dentro del Proceso de Gestión TIC? (Programa diferente al que se usa con frecuencia en las labores diarias de su puesto de trabajo)

SI	NO
1	7

¿Dentro del Proceso de Gestión TIC en su puesto de trabajo ha intentado ingresar a documentos o archivos y se le ha denegado el acceso?

SI	NO
2	6

¿Dentro del Proceso de Gestión TIC, ha grabado información en su puesto de trabajo desde algún dispositivo de almacenamiento diferente al de su uso diario?

SI	NO
3	5

¿Dentro del Proceso de Gestión TIC, al terminar sus labores diarias apaga su computadora?

SI	NO
5	3

¿Dentro del Proceso de Gestión TIC, en caso de ausencia en su puesto de trabajo y este prendido su computador? ¿Cierra usted su sesión?

SI	NO
5	3

¿Dentro del Proceso de Gestión TIC, cuando se instala un programa nuevo? ¿Existe su debida capacitación para su correcto uso?

SI	NO
4	4

Dentro del Proceso de Gestión TIC, por cualquier motivo, ¿Su puesto de trabajo ha sido reemplazado temporalmente por personal interno?

SI	NO
1	7

¿Dentro del Proceso de Gestión TIC, ha sufrido alguna pérdida de información?

SI	NO
2	6

¿Dentro del Proceso de Gestión TIC, ha realizado alguna vez un cambio de clave en su computadora?

SI	NO
6	2

¿Dentro del Proceso de Gestión TIC, ha logrado alguna vez, por su cuenta, arreglar algún error en su computador?

SI	NO
7	1

¿Dentro del Proceso de Gestión TIC, existe un área restringida en alguna carpeta de su computadora? (En cuanto a la información y su nivel de seguridad)

SI	NO
1	7

¿Dentro del Proceso de Gestión TIC, realiza respaldos de su información diariamente en dispositivos de almacenamiento?

SI	NO
2	6

¿Dentro del Proceso de Gestión TIC, se ha desconectado su computadora por apagones?

SI	NO
5	3

¿Dentro del Proceso de Gestión TIC, se ha perdido información importante o su adelanto de trabajo por causa de apagones?

SI	NO
1	7

¿Dentro del Proceso de Gestión TIC, ha llevado archivos digitales para terminar en su casa por falta de tiempo?

SI	NO
3	5

¿Dentro del Proceso de Gestión TIC, tiene su ordenador información personal como fotos, videos, música, etc.?

SI	NO
3	5

¿Cómo trabajador activo Dentro del Proceso de Gestión TIC usted separa por categorías los documentos públicos, privados, confidenciales, etc.?

SI	NO
5	3

¿Dentro del Proceso de Gestión TIC, usted comparte su computador con otro compañero de trabajo?

SI	NO
2	6

¿Dentro del Proceso de Gestión TIC, en su puesto de trabajo alguna vez se ha activado advertencias de antivirus?

SI	NO
3	5

Dentro del Proceso de Gestión TIC, ¿Tienen definido sus funciones y obligaciones?

SI	NO
8	0

A parte de usted ¿Alguna otra persona conoce su contraseña de acceso a su computador?

SI	NO
3	5

¿Dentro del Proceso de Gestión TIC, usted guarda información privada en distintas carpetas? (por medida de seguridad)

SI	NO
3	5

¿Dentro del Proceso de Gestión TIC, usted ha intentado ingresar a una página web y se ha bloqueado el acceso?

SI	NO
7	1

¿Dentro del Proceso de Gestión TIC, usted ha tenido alguna capacitación del manejo de nuevo software, con el objetivo de informar y mejorar su trabajo diario?

SI	NO
2	6

¿Ha llevado archivos o documentos informáticos fuera del Proceso de Gestión TIC en Memoria, CD, etc.?

SI	NO
4	4

Dentro del Proceso de Gestión TIC, su cuenta de usuario ¿Tiene la misma clave que la de su correo electrónico?

SI	NO
0	8

¿Dentro del Proceso de Gestión TIC, ha rotado alguna vez una memoria para pasar información?

SI	NO
4	4

¿Dentro del Proceso de Gestión TIC, usted tiene manuales de todas las aplicaciones en su computador o en físico?

SI	NO
1	7

¿Dentro del Proceso de Gestión TIC, su contraseña tiene como caracteres nombres de hijos, esposo, padres, mascotas, etc.?

SI	NO
0	8

¿Dentro del Proceso de Gestión TIC, se ha instalado alguna aplicación para el mejor manejo de la información?

SI	NO
2	6

ANEXO G Rediseño de Politicas ISO 27000 2013

Ver Documento Anexo ANEXO G-Rediseño de Politicas ISO 27000 2013

ANEXO H INFORME EJECUTIVO

INFORME EJECUTIVO: RECOLECCIÓN DE LA INFORMACIÓN O INFORMATION GATHERING DE GOBERNACIÓN DE NARIÑO.

REALIZADO POR:
JORGE DANIEL ALVAREZ GARCIA

UNAD
ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SAN JUAN DE PASTO
2019

INTRODUCCION

El presente informe ejecutivo pretende Investigar y analizar los diferentes medios web y redes sociales que componen a la Gobernación de Nariño para determinar su vulnerabilidad frente a un posible ataque, haciendo énfasis en uno de los sitios mas visitados que es la intranet.narino.gov.co que es el punto de informativo base para los funcionarios de la gobernación, se hace una recolección de información inicial permitiendo estimar algunas posibles vulnerabilidades.

RECOLECCION INICIAL

Etapa 1: Para el desarrollo de la primera etapa se realizó una búsqueda de información con el fin de reconocer la infraestructura física y tecnológica, utilizamos los medios de internet, redes sociales que nos permitan extraer lo más relevante de la sede de la Gobernación de Nariño.

PETIC 2.0 (Plan Estratégico De Tecnología Informática y Comunicación)

A través de la consulta previa al PETIC se obtienen las siguientes páginas web vinculadas directamente con la plataforma de la gobernación de Nariño:

- ✓ **GANACONTROL:** Donde se maneja todo lo relacionado con presupuesto y contratación abierta con la cual se cubre la necesidad de veeduría ciudadana; cuenta con una base de datos MySQL, servidor Apache y lenguaje de programación Php versión 5.5. (PETIC, 2018, p. 62)
- ✓ **GANA web:** Corresponde a la dependencia de Gobierno abierto de Nariño considerada como el pilar de la organización la cual tiene como fin brindar información útil a la ciudadanía con relación a política pública y otras dependencias que más adelante se nombraran. Cuenta con una base de datos MySQ, servidor Apache y lenguaje de programación Php versión 5.5. (PETIC, 2018, p. 32)

- ✓ **GanaEdu:** Es un sistema de evaluación de calidad educativa dentro del departamento, dicha plataforma aún está en desarrollo; cuenta con una base de datos MySQL 5.5.50, lenguaje de programación PHP versión 5.5.50 y servidor Apache 2.4.1.0. (PETIC, 2018, p. 39)
- ✓ **GANA Municipales:** Corresponde a la plataforma que contiene el presupuesto participativo del gobierno abierto para los municipios del departamento de Nariño, los cuales se organizan de acuerdo a su localización. (Ex provincia de Obando, cordillera, Sanquianga, pacifico sur, Rio Mayo, Pie de monte costero). (PETIC, 2018, p. 42)
- ✓ **Gana Datos:** Es un portal que permite realizar veedurías y gestión de gobierno ya que en esta plataforma se encuentran publicados los datos de las distintas dependencias de la Gobernación de Nariño. De igual forma es útil para llevar a cabo investigaciones o construir aplicaciones y servicios. Entre las dependencias se encuentran: Udenar, turismo, tránsito, TIC, salud, riesgos, paz, justicia, infraestructura, hacienda, gobierno abierto y género e inclusión. Cuenta con una base de datos MySQL 5.5.50; lenguaje PHP versión 5.6.30 y servidor Apache 2.4.1.0. (PETIC, 2018, p. 78)
- ✓ **Gana Pienso:** Plataforma que permite la participación de la ciudadanía en línea a través del debate como mecanismo de participación ciudadana, así mismo, la comunidad puede aportar propuestas con fines de mejoramiento del departamento. Cabe aclarar que dentro de esta plataforma se encuentra Nariño Joven Debate, espacio especial para la opinión de los jóvenes y sus sugerencias. Maneja una base de datos Postgesql 9.4.8, lenguaje de programación y versión Ruby 2.3.2-p 217 / Rails 4.2.9 y servidor Phusion Passenger 5.1.8. (PETIC, 2018, p. 75)

REDES SOCIALES

Se realizó una búsqueda semi detallada de la información suministrada por la Gobernación de Nariño en las diferentes redes sociales con el fin de analizar la vulnerabilidad de la información dicha entidad cuenta con varias redes sociales donde la

podemos encontrar cierta información que podemos visualizarla en dichas redes no es tan relevante para extraer y que nos permita un estudio a profundidad de lo que la gobernación le expone a la ciudadanía en cuanto a su información

FACEBOOK

A continuación se encuentra el perfil que maneja esta red social https://www.facebook.com/GobNarino/, se reportan 21.209 me gusta, la siguen 21.258 personas, su actualización se realiza en intervalos de 7 a 8 horas, maneja una periodicidad media ya que su función es netamente informativa.

La Gobernación de Nariño cuenta con varios perfiles de sus dependencias tanto en páginas web como en perfiles privados, dentro de las páginas pertenecientes al dominio de la entidad se evidencia que no está en continua actualización sobre las distintas actividades que se realizan, pero ofrece información sobre el correo de la plataforma y un link que direcciona a la página principal de la gobernación, también se encuentra información sobre su ubicación, número de teléfono, fotos y reacciones del personal que trabaja en la gobernación de Nariño.

TWITTER

El siguiente enlace conlleva al perfil que maneja la Gobernación en la red social https://twitter.com/gobnarino. Dado que es la red social más utilizada por la entidad, se mantiene la actualización constante de información lo que la convierte en la red social más importante. Cuenta con 23.483 seguidores, es actualizada cada 3 horas aproximadamente, maneja una periodicidad alta ya que es la red que está en continua actualización, adicional a lo anterior, se contabilizan 13.300 me gusta y 51.939.

.La gobernación de Nariño y su personal cuenta con varios perfiles de donde es posible extraer información sobre el personal que realiza y reporta las actividades realizadas por parte de las distintas dependencias que la conforman, en esta red social se puede extraer información del personal que hace parte de la gobernación de Nariño ya que mantiene actualización permanente de las acciones relacionadas a la actividad de la entidad.

INSTAGRAM

El siguiente enlace re direcciona hacia el perfil que maneja la Gobernación dentro de la

red social mencionada: https://www.instagram.com/gobernaciondenarino/?hl=es-la. En ella se encuentran 2.031 seguidores y 1.250 publicaciones, maneja una periodicidad baja ya que el perfil no se encuentra en constante actualización.

En cuanto a esta red social, la Gobernación de Nariño cuenta con un perfil informativo dentro de Instagram donde comparte fotografías de los principales eventos llevados a cabo tanto en la ciudad como en cada uno de los municipios que conforman el departamento, de esta manera se destaca la cultura, deporte, turismo entre otras actividades al tiempo que permite recolectar información de la ciudadanía de acuerdo a las reacciones y visitas a las historias, de esta manera se lleva un registro de usuarios a través de direcciones IP de las distintas cuentas que interactúan con el perfil.

Etapa 2: Reconocimiento de las herramientas y su funcionamiento para su posterior aplicación a las páginas web pertenecientes a la Gobernación de Nariño.

Para el desarrollo de esta etapa se realizó varias consultas en internet tales como información básica de las herramientas a desarrollar, así también se hizo uso de ayudas audiovisuales tales como tutoriales que faciliten la comprensión de cada una de las herramientas ofrecidas por Kali Linux, sus comandos y forma de aplicación a cada una de las páginas web pertenecientes a la Gobernación de Nariño con el fin de realizar el escaneo de las mismas.

Etapa 3: Recolección de información y filtración de páginas web pertenecientes a la Gobernación de Nariño.

Para el desarrollo de la tercera etapa la recolección de información a través de diferentes herramientas que se nombraran a continuación así como también se realizó el escaneo respectivo a las páginas seleccionadas.

Recolección de información (Information gathering)

Se realizó el escaneo de puertos del dominio narino.gov.co donde se identificó las páginas más importantes de la Gobernación de Nariño y su respectiva dirección IP de la siguiente manera:

Tabla 1 . Servidores de la Gobernacion de Nariño(Parcial)

Página web	Dirección IP
datos.narino.gov.co	198.100.153.250
intranet.narino.gov.co	167.114.170.153
mail.narino.gov.co	66.70.193.68
servicio.narino.gov.co	142.4.200.202
ganacontrol.narino.gov.co	167.147.114.163

Pentesting

Se realizó la búsqueda de los dominios, sitios web, direcciones IP, plataformas, enumeración de puertos, servicios y protocolos mediante el uso de herramientas suministradas por Kali Linux (Khepri, W., 2018) las cuales facilitaron el escaneo de todas las versiones instaladas en cada una de las páginas web pertenecientes a la Gobernación de Nariño. En este orden de ideas, se utilizaron las siguientes herramientas:

Maltego: Es una herramienta de recopilación de inteligencia en internet la cual permite la recolección de información para descubrir datos determinados datos sobre determinados objetivos de empresas, personas y organizaciones permitiendo visualizar fácilmente los datos en un gráfico para su posterior análisis.

Whois: Es una base de datos mundial en internet que permite observar los resultados de una consulta, su utilidad es consultar bases de datos donde se encuentran almacenados los usuarios con algún recurso en internet a través del nombre de dominio o las direcciones IP.

WhatWeb: Es una herramienta de Fingerprint que permite encontrar diferentes sitios web existentes dentro de una página web o dominio.

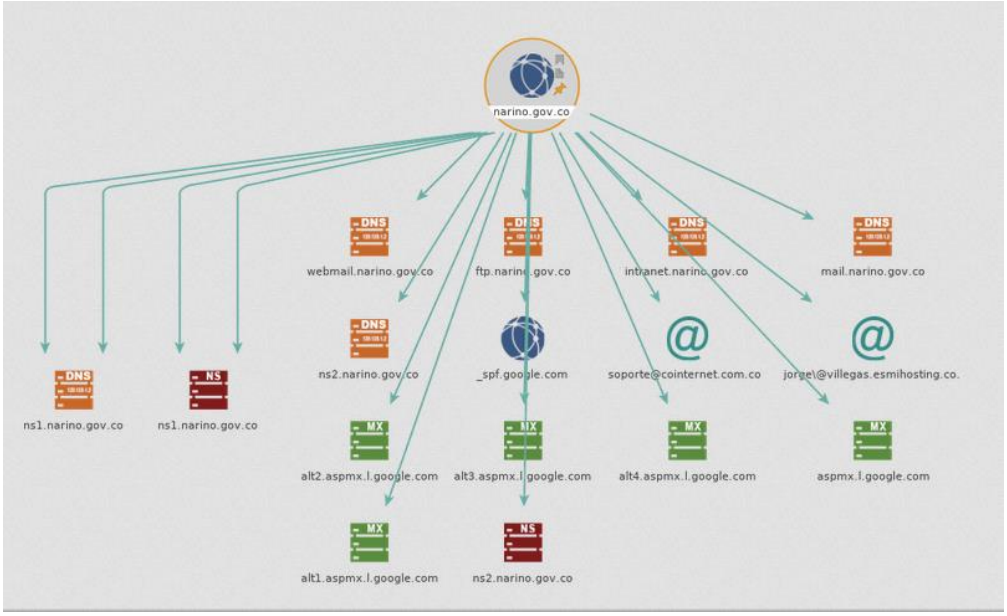
Tracerroute: Es una herramienta de diagnóstico de red, su funcionalidad se basa en mostrar la ruta completa de las redes de una determinada conexión.

Nmap: Herramienta utilizada para la detección de redes y auditorías de seguridad a través de un potente escáner de puertos y servicios dentro de una red.

MetaSploit: Herramienta utilizada para encontrar la vulnerabilidad informática de una página web.

A continuación se presenta una gráfica de las páginas, archivos y emails que están alojados dentro del dominio de narino.gov.co la cual fue desarrollada con Maltego.

Imagen 1. Dominio narino.gov.co



Fuente:autoria propia

- En el gráfico suministrado por la herramienta maltego se visualizan las distintas páginas que contiene el dominio de la gobernación de Nariño
- Se observa también los servidores de correos institucionales que maneja la Gobernación de Nariño destacando que estos tienen contrato con google

Como segundo paso, se realizó el escaneo de los dns de la página narino.gov.co con la herramienta de recolección suministrada por Kali Linux

Imagen 2 dns narino.gov.co

fuente:autoria propia

- ✓ MX el servidor de correo que se encarga del procesamiento de correo electrónico es google
- ✓ TXT con google ayuda a garantizar la seguridad de los correos

Cuando se realiza un escaneo común con la herramienta **Whois**, es frecuente no conseguir el resultado esperado debido a que los servidores tienden a ocultar información lo que dificulta la transferencia de zona y nos muestra una información que no es tan relevante, es por esta razón que se hace uso de la herramienta **fierce** la cual facilita llegar a un resultado óptimo en el proceso de recolección de información sobre los dominios y subdominios que componen dicho servidor. Una vez llevado a cabo lo anterior se obtiene:

Imagen 3. Fierce- dns

```
        ns2.narino.gov.co

Trying zone transfer first...
        Testing ns1.narino.gov.co
                Request timed out or transfer not allowed.
        Testing ns2.narino.gov.co
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
198.100.153.250 datos.narino.gov.co
66.70.193.68    narino.gov.co
66.70.193.68    ftp.narino.gov.co
167.114.170.153 int.narino.gov.co
167.114.170.153 intranet.narino.gov.co
66.70.193.68    ipv4.narino.gov.co
190.14.247.71   lab.narino.gov.co
66.70.193.68    mail.narino.gov.co
```

fuente:autoria propia

El tercer paso consistió en el escaneo a la página narino.go.co con la herramienta **whatweb** la cual brinda información detallada sobre versiones de base de datos, emails, plataformas y nombres de los autores de la página en mención obteniendo como resultado la imagen 4.

Imagen 4. Whatweb

```
root@KaliLinux:~# whatweb narino.gov.co
http://narino.gov.co [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[ngin
x], IP[66.70.193.68], Plesk[Lin], RedirectLocation[http://xn--nario-rta.gov.co/], Title[
301 Moved Permanently], X-Powered-By[PleskLin], nginx
http://xn--nario-rta.gov.co/ [302 Found] Country[UNITED STATES][US], HTTPServer[nginx],
IP[66.70.193.68], PHP[7.0.33,], Plesk[Lin], RedirectLocation[http://www.narino.gov.co/in
icio/], X-Powered-By[PHP/7.0.33, PleskLin], nginx
http://www.narino.gov.co/inicio/ [301 Moved Permanently] Country[UNITED STATES][US], HTT
PServer[nginx], IP[66.70.193.68], Plesk[Lin], RedirectLocation[http://xn--nario-rta.gov.
co/inicio/], Title[301 Moved Permanently], X-Powered-By[PleskLin], nginx
http://xn--nario-rta.gov.co/inicio/ [200 OK] Cookies[c13a076fbc1b354ad0a17f39921cf445],
Country[UNITED STATES][US], Email[contactenos@narino.gov.co,joobga@gmail.com,notificacio
nes@narino.gov.co], Frame, Google-Analytics[UA-38413002-1], HTML5, HTTPServer[nginx], Ht
tpOnly[c13a076fbc1b354ad0a17f39921cf445], IP[66.70.193.68], JQuery, maybe Joomla, Meta-A
uthor[Jonnathan Bucheli Galindo | joobga@gmail.com], MetaGenerator[Joomla! - Open Source
 Content Management], PHP[7.0.33,], Plesk[Lin], Script[application/json,text/javascript]
, Title[Gobernación de Nariño], probably WordPress, X-Powered-By[PHP/7.0.33, PleskLin],
YouTube, nginx
```

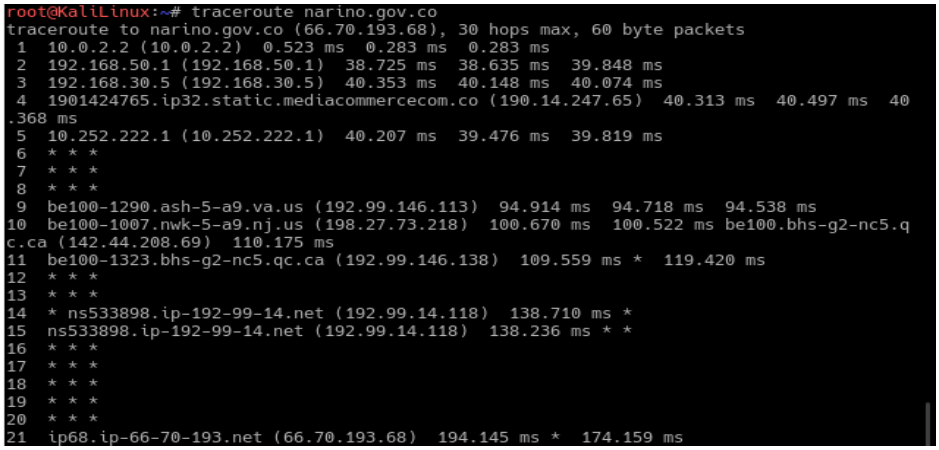
fuente:autoria propia

- Con esta herramienta se obtuvo como resultados el tipo de servidor web que maneja la página que en este caso es **Nginx**
- La versión de PHP 7.0.33

- ❖ Se encontró distintos correos electrónicos tanto de la entidad como de las personas que crearon la página web (joobga@gmail.com, contactenos@narino.gov.co, notificaciones@narino.gov.co)
- ❖ Maneja la plataforma WordPress y Joomla

Como último paso se realizó el reconocimiento de diagnóstico de red y las rutas de conexión de la página, esto se llevó a cabo con la ayuda de la herramienta **traceroute** obteniendo como resultado no indica cómo es la comunicación entre las redes y sus distintos procesos imagen 5.

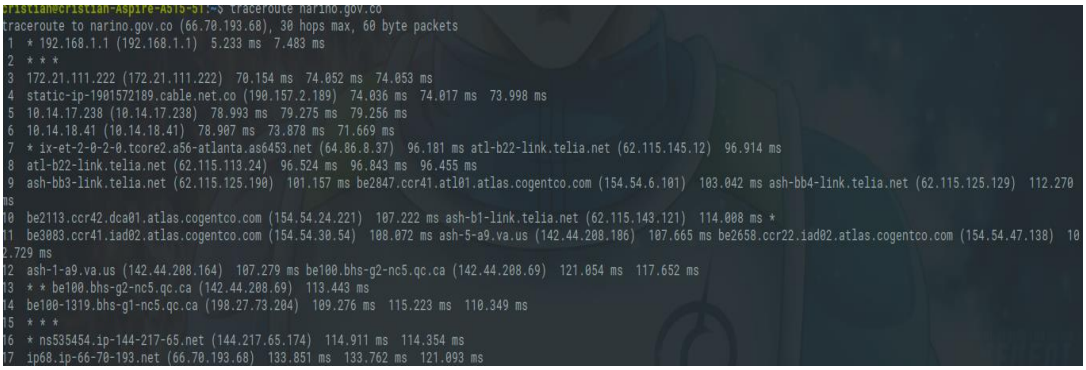
Imagen 5. Traceroute (se utilizó esta herramienta en dos ocasiones)



fuente:autoria propia

- Desde la red de la gobernación de Nariño no se brinda la información que usan los servicios de mediacomerce.co para la conexión tecnológica y en segunda instancia se realizó otro escaneo desde otra red tal y como se muestra en la imagen 6.

Imagen 6. Escaneo de red



fuente:autoria propia

Con ayuda de la herramienta online suministrada por https://dnsdumpster.com se permitió extraer la mayoría de dominios pertenecientes a la gobernación de Nariño, a continuación se muestra algunos de los dominios y el servidor en el cual están alojadas las distintas páginas que existentes dentro de la entidad

Servidores de las páginas que contiene la gobernación de Nariño

Las siguientes páginas se alojan en el mismo servidor apache utilizando la misma IP (198.100.153.250)

Tabla 2. Sistema Operativo de servidores gobernacion

participa.narino.gov.co	Apache/2.4.10 (Debian) es un servidor muy conocido que ofrece distintos módulos. Su funcionalidad de es muy alta
ganapienso.narino.gov.co	
datos.narino.gov.co	
ganadatos.narino.gov.co	

participa.narino.gov.co	**198.100.153.250**
ganapienso.narino.gov.co	**198.100.153.250**

Tabla 3. direcciones de gobernaciond de Nariño Alojadas en el mismo servidor con distinta dirección IP

datos.narino.gov.co	**198.100.153.250**
ganadatos.narino.gov.co	**198.100.153.250**
aplicaciones.narino.gov.co	**190.14.247.68**
sgc.narino.gov.co	**190.14.247.76**
impuestovehicular.narino.gov.co	**35.185.33.40**

- **intranet.narino.gov.co** 167.114.170.153 usa servidor xgnix

Las siguientes páginas tienen la misma dirección IP 167.114.170.163 alojadas en el mismo servidor Xgnix

Tabla 4. Servidor Web Ngnix de algunas plataformas de la gobernacion

	Ngnix es un servidor web de Open Source, es ligera y muy flexible, es fácil de instalar, trabaja con diferentes tecnologías de desarrollo y lenguajes
gana.narino.gov.co	
tic.narino.gov.co	
ganacontrol.narino.gov.co	
redadn.narino.gov.co	

herramientas.narino.gov.co	
ganamunicipales.narino.gov.co	
buscohechos.narino.gov.co	

Tabla 5 . Dominios con diferentes IP

subdetra.narino.gov.co	**66.70.159.190**
stiga.narino.gov.co	**142.4.200.202**
ganapae.narino.gov.co	**142.4.200.202**
servicio.narino.gov.co	**142.4.200.202**

Tabla 6. Direcciones alojadas en el servidor Xgnix con la misma dirección IP

ns1.narino.gov.co	**66.70.193.68**
ns2.narino.gov.co	**66.70.193.68**
pinacoteca.narino.gov.co	**66.70.193.68**
ns1.pinacoteca.narino.gov.co	**66.70.193.68**
ns2.pinacoteca.narino.gov.co	**66.70.193.68**

mail.pinacoteca.narino.gov.co	**66.70.193.68**
mail.narino.gov.co	**66.70.193.68**
gestiondelriesgo.narino.gov.co	**66.70.193.68**
ns1.gestiondelriesgo.narino.gov.co	**66.70.193.68**
ns2.gestiondelriesgo.narino.gov.co	**66.70.193.68**
mail.gestiondelriesgo.narino.gov.co	**66.70.193.68**
turismo.narino.gov.co	**66.70.193.68**
ns1.turismo.narino.gov.co	**66.70.193.68**
ns2.turismo.narino.gov.co	**66.70.193.68**
mail.turismo.narino.gov.co	**66.70.193.68**
servidor.narino.gov.co	**66.70.193.68**
ns1.servidor.narino.gov.co	**66.70.193.68**
ns2.servidor.narino.gov.co	**66.70.193.68**
mail.servidor.narino.gov.co	**66.70.193.68**
webmail.servidor.narino.gov.co	**66.70.193.68**
guaguas.narino.gov.co	**66.70.193.68**
ns1.guaguas.narino.gov.co	**66.70.193.68**
ns2.guaguas.narino.gov.co	**66.70.193.68**

mail.guaguas.narino.gov.co	**66.70.193.68**
playlist.narino.gov.co	**66.70.193.68**
ns1.playlist.narino.gov.co	**66.70.193.68**
ns2.playlist.narino.gov.co	**66.70.193.68**
mail.playlist.narino.gov.co	**66.70.193.68**
NS2.narino.gov.co.	**66.70.193.68**
NS1.narino.gov.co.	**66.70.193.68**

RECOLECCION DE INFORMACION DE INTRANET.NARINO.GOV.CO

Este procedimiento de hizo empleando algunas herramientas disponibles en Kali Linux tales como nmap, dnstracer, dmitry, whatweb, dnsrecon, nikto, joomscan, de igual manera se usó FOCA, es un programa para Windows que sirve para el encontrar metadatos, también se aprovechó sitios web online para obtener información del dominio: https://threatintelligenceplatform.com, http://dr.xoozoo.com, https://www.robtex.com, https://www.shodan.io/ y https://censys.io/
Durante la recolección de información del sistema con las herramientas anteriormente mencionadas, efectuada a la intranet de la gobernación de Nariño (intranet.nariño.gov.co) se hicieron los siguientes hallazgos.

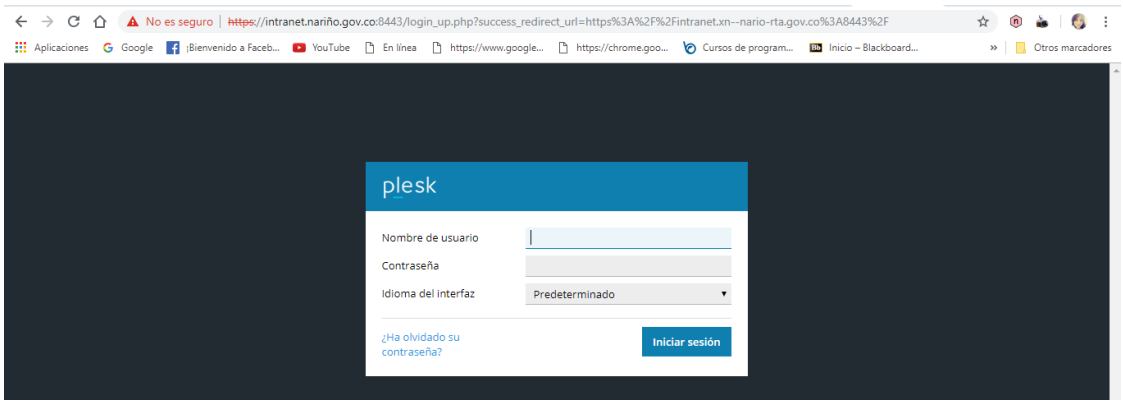
Cuadro 1. Informacion de Dominio intranet.narino.gov.co

INFORMACIÓN DEL DOMINIO	
Nombre del Dominio	***Dirección IP***
intranet.nariño.gov.co	**167.114.170.153**
Registro del Dominio	
Datos	**Descripción**
Registrado por **CO Internet SAS**	Entidad Colombiana encargada de administrar y otorgar los dominios ccTLD (dominios de nivel superior de código de país) que los son dominios que identifican al país o región a la que pertenece el dominio, ejemplo .co (Colombia).
Fecha de Registro	21 de mayo de 2014
Fecha de Expiración	20 de mayo de 2023
Fecha de Actualización	26 de mayo de 2018

Propietario	Gobernación de Nariño
País	Colombia
FORMATO IDN (Nombre de Dominio Internacionalizado) DEL DOMINIO	
Formato que acepta caracteres especiales que no forman parte del código básico ASCII, ejemplo la ñ) y este formato se representa en código Punycode.	
Dominio	**Descripción**
intranet.nariño.gov.co	Es el dominio que el usuario ingresa en el navegador, éste internamente se redirige a **intranet.xn--nario-rta.gov.co**
intranet.xn--nario-rta.gov.co	Dominio principal **registrado** está formato **IDN,** representado en código Punycode.
intranet.narino.gov.co	**Dominio alternativo registrado,** cuando el usuario escribe el dominio con **n**, llegará de la misma manera al sitio web en cuestión porque dicho dominio se ha configurado como alias.

Cuadro 2. Informacion de Servidor

INFORMACIÓN DEL SERVIDOR	
Ubicación	
Datos	**Descripción**
Se tiene contratado un servicio de alojamiento a **OVH.**	Proveedor de servicios de alojamiento web y telecomunicaciones Francés pero con sede en CANADÁ.
País	Canadá
Región	Quebec
Ciudad	Montreal
Información De La Subred	
Es el rango de direcciones IP que el proveedor dispone para sus clientes es. Este rango es asignado por ARIN (Registro Americano de Números de Internet), organización de Estados Unidos que administra y controla las direcciones IP de Canadá, Estados Unidos, islas del Caribe y el Atlántico Norte, debido a que los espacios de direcciones en Internet son limitados y las direcciones IP deben ser únicas.	
Nombre de red	OVH-DEDI-167.114.17
Rango	167.114.170.0 - 167.114.170.255
País	US
NOMBRE SERVIDOR	**IP**
ns1.narino.gov.co	66.70.193.68 (**Servidor de nombres primario)**
ns2.narino.gov.co	66.70.193.68
Administrador del Servidor con Plesk	



Administrador	Versión	Descripción
Plesk	**Onyx 17.5.3**	Panel de control que permite administrar el servidor. Entre las actividades que se pueden realizar son: configurar el sitio web, configurar cuentas de correo electrónico y entradas de DNS, a través de una interfaz basada en la web

Cuadro 3. Dominios Asociados a intranet.narino.gov.co

DOMINIOS CONECTADOS AL SITIO WEB DE LA INTRANET DE NARIÑO	
Dominios a los que se pueden acceder por medio del sitio web de la intranet	
Dominio	**IP**
narino.gov.co xn--nario-rta.gov.co	66.70.193.68 66.70.193.68
aplicaciones.narino.gov.co aplicaciones.xn--nario-rta.gov.co	190.14.247.68 190.14.247.68
googlemail.l.google.com	216.58.217.197
accounts.google.com	72.217.14.77
docs.google.com	172.217.14.110
ganacontrol.xn--nario-rta.gov.co	167.114.147.163
www.multilegis.com	168.197.70.105
intranet.narino.gov.co	167.114.170.153
sgc.narino.gov.co	190.14.247.76
bpid.xn--nario-rta.gov.co	190.14.247.78
bpidconsulta.xn--nario-rta.gov.co	190.14.247.72
lab.narino.gov.co	190.14.247.71
www.idsn.gov.co	190.69.156.11
www.sednarino.gov.co	168.90.15.229
turismo.narino.gov.co	66.70.193.68
www.colombiacompra.gov.co	129.213.79.208
www.dnp.gov.co	190.145.152.181
www.portalterritorial.gov.co	190.145.152.224
maps.l.google.com	172.217.11.174
SISTEMA DE APLICACIONES	

Se encontró la página de acceso a un sistema de aplicaciones el cual maneja un conjunto de aplicaciones que se emplean en el desarrollo de las tareas o actividades y el manejo de la información de la gobernación de Nariño

Información Del Dominio	
Dominio	**IP**
aplicaciones.nariño.gov.co	190.14.247.68
Formato IDN del Dominio y Dominio Alternativo	
Dominio	**Descripción**
aplicaciones.nariño.gov.co	Dominio que el usuario ingresa en el navegador pero que internamente se redirige a aplicaciones.xn--nario-rta.gov.co
aplicaciones.xn--nario-rta.gov.co	Dominio principal en formato IDN, representado en código Punycode.
aplicaciones.narino.gov.co	Dominio alternativo (alias)
Información de la Subred	
Nombre	Departamento de Nariño
Rango de IP	190.14.247.64 - 190.14.247.79
País	CO

Cuadro 4. Informacion de CMS usado por Intranet.narino.gov.co

CMS (sistema de gestión de contenido) Y LENGUAJES DE PROGRAMACIÓN		
Componentes	**Versión**	**Descripción**
joomla	2.5.17	Sistema de administración de contenido sirve para la creación y administración de sitios web
JavaScript (Lenguaje de Programación)		Son lenguajes de Programación, para hacer el sitio web dinámico es decir que se actualiza cada vez que los usuarios
PHP (Hypertext Preprocessor)	5.4.45	

		ingresan nuevo contenido, además permite el manejo de archivos de multimedia
HTML5 (Lenguaje de marcado de hipertexto)		Para estructurar el contenido web

Página De Administrador De Joomla
http://intranet.xn--nario-rta.gov.co/administrator/

Cuadro 6. Informacion de Servidores de correo electronico

SERVIDORES DE CORREO ELECTRÓNICO	
Los correos electrónicos se manejan con Gmail, por ende se muestran los servidores de correo de Google	
Nombre del Servidor	**IP**
alt1.aspmx.l.google.com	209.85.234.26
aspmx.l.google.com	74.125.142.27
alt3.aspmx.l.google.com	173.194.208.27
alt4.aspmx.l.google.com	74.125.141.27
alt2.aspmx.l.google.com	64.233.177.26

Cuadro 7. Informacion de puertos y servicios de intranet.narino.gov.co

PUERTOS Y SERVICIOS					
Puerto	**Servicio**	**Estado**	**Servidor**	**Versión**	**Descripción**
80	http	Abierto	**nginx**	**1.16.0**	Servidor web
993	IMAPS	Abierto			**IMAPS** (IMAP (Internet Message Access Protocol o protocolo de acceso a mensajes de Internet

					Seguro**))**
465	SMTPS	Abierto	**Postfix**		SMTPS (Simple Mail Transfer Protocol o protocolo simple de transferencia de correo Seguro) este protocolo permite que los emails viajen a través de internet. **Postfix** (Servidor de correo electrónico que sirve para el enrutamiento y envío de correo electrónico es seguro)
995	POP3S	Abierto			**POP3S** (Post Office Protocol o Protocolo de Oficina Postal Seguro). Este protocolo permite a un cliente conectarse a un servidor remoto para descargar los correos en el ordenador personal, una vez descargados los mensajes estos se eliminan del servidor.
443	HTTPS				**HTTPS** (Protocolo de transferencia de hipertexto seguro), es usado para la transferencia segura de páginas web.
21	FTP	Abierto	**ProFTPD**	**1.3.5d**	**FTP** (File Transfer Protocol o Protocolo de Transferencia de Archivos), permite a los usuario desde su ordenador subir o bajar archivos de un servidor
22	SSH	Abierto	**OpenSSH**	**5.3**	OpenSSH (herramientas para establecer conexiones seguras a través de Internet)
25	SMTP	Abierto	**Postfix**		**SMTP** (Protocolo simple de transferencia de correo), protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos
143	IMAP	Abierto	**Courier**		**IMAP** (Protocolo de acceso a mensajes de Internet), permite obtener acceso a su correo electrónico donde quiera que esté y desde cualquier dispositivo. Courier: Servidor de correo

					empresarial.
110	POP3	Abierto	**Courier**		(Post Office Protocol o Protocolo de Oficina Postal) Permite descargar los correos desde el servidor directamente en el ordenador del usuario
8443	https	Abieto	**sw-cp-server**		**https** (Protocolo Seguro de Transferencia de Hipertexto). **sw-cp-server** este proporciona servicio de acceso a la interfaz de Plesk
135	msrpc	Filtrado			**msrpc** (Permite el acceso y gestión del sistema de manera remota)
139	netbios-ssn	Filtrado			**netbios-ssn** (permite el intercambio de archivos y aplicaciones de uso compartido de impresoras)
445	Microsoft-ds	filtrado			**Microsoft-ds** (Permite para compartir archivos)

Cuadro 8. Certificados SSL de intranet.narino.gov.co

CERTIFICADOS SSL(Secure Socket Layer)/TLS(Transport Layer Security)	
Sirven para cifrar la información que viaja entre el cliente (navegador web) y el servidor (servidor web) por ejemplo las contraseñas de los usuarios.	
Puerto	**Descripción**
80	El certificado SSL ha caducado el 2018-05-28 21:16:28
443	TLS v1.2 **Suit de Cifrado**: Conjunto de instrucciones para garantizar la seguridad de la comunicación: **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)** **Tipo de Cifrado: AES** (Advanced Encryption Standard) **Tamaño de Cifrado** 256 bits.
21	SSL v 3 **Algoritmo de Firma**: Algoritmo matemático que permite verificar si una firma digital es auténtica: **sha256WithRSAEncryption** **Firma Digital:** Firma electrónica avanzada y segura, permite cumplir con los requisitos legales y normativos, es una manera de autentificar la identidad de una persona o empresa y sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico.
22	Tipo de Clave: **RSA** (Rivest, Shamir y Adleman) Algoritmo de cifrado asimétrico, o de clave pública trabaja con dos claves, una pública y una privada y sirve para cifrar y descifrar información, por ello también provee servicios de autenticidad y de integridad.
25 443	**SSL v1** **Algoritmo de firma:** sha256WithRSAEncryption **Periodo de validez:** 28 de mayo 21:16:28 2017 - 28 de mayo 21:16:28 2018 **Tipo de Clave:** RSA

	Tamaño de Cifrado: 2048 bits
110 143	**TLSv1.0** **Suite de Cifrado:** TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013) **Tipo de Cifrado: AES** (Advanced Encryption Standard) **Tamaño de Cifrado:** 128bits
465 993 995	**SSL v1** **Algoritmo de firma:** sha256WithRSAEncryption **Periodo de validéz:** 28 de mayo 21:16:28 2017 - 28 de mayo 21:16:28 2018 **Tipo de Clave:** RSA **Tamaño de Cifrado:** 2048 bits TLSv1.2 **Suite de cifrado:** TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
8443	**SSL v3** **Algoritmo de firma:** sha256WithRSAEncryption **Periodo de validéz:** 18 de marzo 14:26:45 2019- 16 de junio 14:26:45 2019 **Tipo de Clave:** RSA **Tamaño de Cifrado:** 2048 bits

Cuadro 9. Metadatos de intranet.narino.gov.co

METADATOS	
Tipos de Documentos que se manejan através de la intranet	.doc:13, .docx:19, .PDF:100, .pptx:4, .xls:17, .xlsx:33
Usuarios que crearon los archivos	/-/ GP /-/, Gobernacion, Luis Carlos, Equipos 2-21, DANIEL FERNANDO, ANA JULIA, Brendita, Juan M. Beltrán V. - jmbeltranv@yahoo.com, DessarrolloWEB EQUIPO-PC, GOBENLINEA, Daniel Mongua, Samsung, USER, DanielCer?n, Hewlett-Packard, Alicia_Torres, Administrador, ASUS, Usuario_2, Contratacion JHON EDWARD, Sylvia Peñaranda Méndez, P8102, Juridico CIG CID, Fabian Andres, edwinmauriciobolañosnarvaez, JonnathanBucheli Control Interno, Sophie Hernandez, Sistemas, Microsoft Corporation, DanielCerón, Lilian Rodriguez, Impuestos, PatyMartínez, JoomlaGoberNar, Jmalagon, LCjj.
Folders	http://ns.adobe.com/xap/1.0/, http://www.w3.org/1999/02/ http://aplicaciones.narino.gov.co/
Impresoras	HP LaserJet P3015 TH HP LaserJet Professional P1102 \\192.168.32.91\KONICA MINOLTA HP LaserJet P3015 Tesoreria HP LaserJet P3015 General

	Microsoft Office Document Imag HP OfficeJet Pro x476dw KONICA MINOLTA 215 HP P1102w Gral 0 H HP LaserJet P3015 Sistemas \\192.168.31.28\HP LaserJet 24 PDFCreator \\192.168.31.28\HP LaserJet P3 EPSON TX125 Series ' D - RICOH Aficio MP 301 RICOH Aficio MP 301 PCL 6 MP 3 HPLaserJ P3015 Secretaria Gene HP Color LaserJet CM4540 MFP P HPLaserJet P3015 Talento Humao HP LaserJet P3015 Talento Huma NPIBD46E3 (HP LaserJet MFP M42 RICOH Aficio MP 301 PCL 6 icio \\192.168.31.44\HP LaserJet P3 \\172.17.7.245\HP LaserJet M10 \\P7507\RICOH Aficio MP 301 PC \\192.168.32.124\KONICA MINOLT HP Deskjet 1010 series LASERTIC
Software	Microsoft Office 2007 Microsoft Office Microsoft Office XP EPSON Scan Microsoft Office for Mac GPL Ghostscript 8.61 PDFCreator 0.9.5 Windows XP HP Scan HP Scan Extended Application Bullzip PDF Printer / www.bullzip.com / Freeware Edition Canon Adobe PDF Library 10.0.1 Adobe InDesign CS6 (Windows) wxPdfCOM wxPdfDocument 0.8.0 Adobe PDF Library 10.01 Adobe Illustrator CS6 (Windows) Document Imaging Eastman Kodak Company DPE Build 5656 DPE Build 5095 PDF Printer / www.bullzip.com / FG / Freeware Edition (max 10 users) Bullzip PDF Printer (11.1.0.2600) Microsoft Office 95

	Mac OS X 10.12.5 Quartz PDFContext
Emails	institucional@narino.gov.co, ledyc18@yahoo.es, gustavomontenegro@narino.gov.co, estebansarasty@narino.gov.co magdadelgado@narino.gov.co, ginavega@narino.gov.co, vlahebo@gmail.com, turismo@narino.gov.co, ritarodriguez@narino.gov.co angelacadena@narino.gov.co, julianalvear@narino.gov.co, cesarparedes@narino.gov.co, richardfuelantala@narino.gov.co zaidamunoz@narino.gov.co, juancarlosbravo@narino.gov.co angiemelo@narino.gov.co, elderburbano@narino.gov.co yhon202@hotmail.com, cristhianaguilar@narino.gov.co luiscarlosdelgado@narino.gov.co, vivis_lasso@hotmail.com mercedesalazar@narino.gov.co , silviamaguana@narino.gov.co victorefrain.munoz@gmail.com, general@narino.gov.co, dorismejia@narino.gov.co, brendarivas@narino.gov.co
S O	Windows XP, Windows 7
Clientes de la Red	PC_Alicia_Torres PC_ASUS PC_Brendita PC_Control Interno PC_DANIEL PC_Daniel Mongua PC_DanielCer?n PC_DanielCerón PC_DessarrolloWEB PC_edwinmauriciobolañosnarvaez PC_EQUIPO-PC PC_FERNANDO PC_GOBENLINEA PC_Gobernacion PC_Hewlett-Packard Company PC_Impuestos PC_JHON EDWARD PC_jmalagon PC_JoomlaGoberNar PC_Juridico CIG PC_LCjj PC_Obras Publicas PC_P8102 PC_Sistemas PC_Sophie Hernandez PC_Sub Sec Presupuesto PC_USER PC_Usuario

CONCLUSIONES

- La intranet no deberia estar expuesta publicamente en internet sino solo para red interna de la Gobernacion de Nariño, o pedir un sistema de logueo inicial antes de entrar
- La ubicación del servidor muestra que está en Canadá, esto quiere decir que se tiene contratado un servicio de hosting. Lo que va a complicar hacer el hacking ético puesto que el mismo proveedor del servicio se encarga de la seguridad del servidor.
- Los puertos 445, 135, 139,593 aparecen filtrados, no se puede determinar si el puerto se encuentra abierto o cerrado, lo que permite deducir que está siendo bloqueado por un firewall, o por las reglas de un enrutador, o tal vez por una aplicación de cortafuegos instalada en el propio equipo.
- microsft-ds es un servicio para compartir archivos que se ejecuta en el puerto 445 que está muy ligado a Windows por lo que se concluye que hay un **Microsoft** Windows Server ejecutándose esto puede permitir obtener acceso remoto al contenido de los directorios o unidades de disco duro
- Por el puerto 139 está corriendo el servicio netbios-ssn que es un **Servicio de sesión NETBIOS** para establecer una comunicación orientada a la conexión. Estas conexiones TCP forman "sesiones de NetBIOS" para admitir actividades de intercambio de archivos y aplicaciones de uso compartido de impresoras, generalmente para Windows; esto permitiría tratar de ingresar al servidor de archivos a través de este puerto y hacer un ataque de Denegacion de Servicio (DoS).
- El tipo de archivos que más se manejan son archivos PDF.
- Al obtener información de los usuarios y sus correos electrónicos se puede aplicar ingeniería social, que es el acto de persuadir a las víctimas para que compartan información confidencial.
- Hay gran número de puertos abiertos, esto quiere decir que tanto los usuarios legítimos como los atacantes se conectan al sistema por medio de estos puertos. Cuantos más puertos se encuentren abiertos más formas hay para que alguien se conecte. Por lo tanto, es importante mantener abiertos sólo los puertos imprescindibles para que el sistema funcione

correctamente y el resto de los puertos deben ser cerrados o en su defecto poner un firewall.

- Conociendo la IP de la intranet de la gobernación de Nariño, ésta puede ser víctima de un ataque DoS (Denial of service) es decir un ataque de denegación de servicios, donde el atacante envía varias peticiones o solicitudes al servidor haciendo que éste se sature y no pueda responder, de manera que cuando los usuarios legítimos quieran acceder a los servicios y recursos de la intranet se les negará el acceso y como consecuencia no podrán realizar normalmente sus actividades.

- Como el dominio de la intranet está en formato IDN (Nombre de Dominio Internacionalizado), el sitio podría ser suplantado por alguien que aprovechando la internacionalización de los dominios, algunas letras de algunos alfabetos son muy parecidas y eso puede ser usado para crear un dominio falso, al cual los usuarios pueden ingresar pensando que están en la página web legítima cuando en realidad se está visitando una página falsa, de esta manera de podría obtener información confidencial de la entidad.

- La intranet al no tener un certificado SSL (Secure Socket Layer), capa de conexión segura), un atacante podría robar información confidencial por ejemplo las contraseñas de los usuarios.

- Al encontrar los dominios enlazados a la intranet, el atacante podría fijar nuevos objetivos de ataque, para dañar más información.

- La versión de joomla que se tiene instalado está desactualizada esto puede dar oportunidad a que el atacante realice ejecución remota de comandos alterando el código fuente del sitio web, esta vulnerabilidad es crítica y afecta a todas las versiones de 1.5 a 3.4.

- Al manejar las cuentas de correo con Gmail hay más privacidad y seguridad de los datos ya que la seguridad de Google siempre será mayor que cualquier servidor de correo que se tenga contratado.

- La suite de cifrado que emplea el servicio IMAPS se considera débil puesto que la versión de TLS v1.0 es obsoleta.

- La mayoría de los servidores que usan Proftp siguen siendo vulnerables a los ataques, ya que están utilizando versiones obsoletas. Si está utilizando Proftpd versión 1.3.5 o anterior, su servidor es vulnerable y es solo cuestión de tiempo antes de que alguien aproveche esa vulnerabilidad.

- La versión de OpenSSH v5.3 está dentro del rango de las versiones que tienen la vulnerabilidad de ejecución remota de código, ésta vulnerabilidad afecta a las versiones OpenSSL 5.0 a 7.3, los atacantes pueden aprovechar esta vulnerabilidad para ejecutar comandos de forma remota y provocar fugas de datos.

BIBLIOGRAFIA

Keprhi, W. (2018). Las 25 mejores herramientas de Kali Linux. [En línea]. Obtenido de https://bit.ly/2HDNu6Y. [Recuperado el 14 mar. 2019]

PETIC (2018). Plan Estratégico De Tecnología Informático y Comunicación. Secretaría TIC innovación y Gobierno Abierto. Gobernación de Nariño. Págs. 32-78

DNSDumpster [En línea] Obtenido en https://dnsdumpster.com