DISEÑO DEL PLAN DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN MISIONAL DE LA PROCURADURÍA GENERAL DE LA NACIÓN

IVAN ANDRÉS ALFARO VIANA
EDWIN VARGAS LEÓN

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ DC.
2016

DISEÑO DEL PLAN DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN MISIONAL DE LA PROCURADURÍA GENERAL DE LA NACIÓN

IVAN ANDRÉS ALFARO VIANA
EDWIN VARGAS LEÓN

Trabajo de Grado Diseño del Plan de Seguridad Informática para optar al titulo de Especialista en Seguridad Informática

Tutor
JUAN CARLOS ALARCÓN SUESCÚN
Ingeniero De Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMATICA
BOGOTÁ DC.
2016

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____
Firma presidente del Jurado

_____
Firma Jurado

_____
Firma Jurado

Bogotá. 1 de marzo del 2016

DEDICATORIA

Dedicamos este proyecto de posgrado a Dios, quien ha estado al lado de cada uno de nosotros, porque nos dio la fortaleza y la fe necesaria para culminar este gran objetivo, pese a las dificultades, iluminando cada paso de nuestras vidas, y por darnos la salud, la esperanza de terminar este trabajo.

A nuestras familias, quienes nos apoyaron y han estado en todo momento con cada uno de nosotros, para la superación personal; y a todas las personas que han creído en nosotros.

AGRADECIMIENTOS

Los integrantes de este proyecto rinden un especial tributo de agradecimiento a todas y cada una de las personas que contribuyeron con la realización del presente trabajo de posgrado.

En primer lugar dar gracias a Dios, el dador de todas las cosas y quien permite que todo ocurra, al llegar a este momento de culminación de un logro más en la vida.

Una mención de gratitud a las autoridades y cada uno de los integrantes de la Facultad de Ingeniería de Sistemas de la Especialización de Seguridad Informática ya que gracias a los aportes de cada uno de ellos, día tras día fuimos enriqueciendo nuestros conocimientos y formación profesional en este grandioso camino de la seguridad informática.

Agradecemos a los docentes de la especialización por la dedicación, sus conocimientos, las orientaciones y su paciencia, que fueron fundamentales para nosotros. La seriedad y el rigor académico sin los cuales no podría tener la formación tan completa que hemos tenido como investigadores.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCIÓN

La información, los procesos, sistemas y redes que brindan apoyo a las organizaciones constituyen un recurso importante para el logro de sus objetivos. Desarrollar un plan de seguridad informática permitiría generar las medidas de seguridad para proteger los sistemas de información de daños contra la confidencialidad, la integridad y la disponibilidad.

El presente trabajo tiene como finalidad comprender la importancia de contar con un plan de seguridad informática en los sistemas de información institucionales, más exactamente en el sistema de información misional –SIM– de la Procuraduría General de la Nación, para lo cual es necesario realizar un recorrido por distintas nociones de esta disciplina, con el fin de acercarnos un poco a su naturaleza. Para ello nos permitimos citar algunas definiciones relacionadas con la seguridad informática; "La seguridad informática consiste en asegurar en que los recursos del sistema de información de una organización se utilizan de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización".[1]

Posteriormente, argumentaremos la importancia de tener un plan de seguridad informática y se realizará un diagnóstico del estado actual de la entidad respecto de la seguridad informática, para adentrarse en el análisis de riesgos existentes al interior del sistema de información misional, el cual permitirá conocer sus vulnerabilidades, vacíos en el manual de procedimientos, políticas de la seguridad informática de la entidad y estos a su vez son soportados con directrices internas y normativas de ley, de igual manera se identificarán los recursos para la gestión de continuidad del negocio.

Finalmente con la obtención de esta información se brinda un diseño con elementos que permitieron obtener un plan de seguridad informática seguro para el sistema de información misional SIM.

[1] SEGURIDAD INFORMATICA SMR. Definición Seguridad informática. [en línea], [consultado en marzo 2016]. Disponible en: https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

1. JUSTIFICACIÓN

El sistema de información misional -SIM- de la Procuraduría General de la Nación es la herramienta tecnológica que apoya integralmente las funciones misionales de intervención, disciplinaria y preventiva. “Es un software moderno, integral y robusto que cumple las necesidades de información misional de la PGN en las diferentes dependencias de todo el territorio nacional.”[2]

Por la naturaleza de la información que manejan las entidades gubernamentales es importante contar con un plan de seguridad que se encargue de proteger su confidencialidad, integridad y disponibilidad. Los sistemas y procesos que manejan esta información se han vuelto indispensables en todas las entidades y constituyen una parte esencial de las infraestructuras y un factor crítico para alcanzar su misión.

En relación a lo anterior, el diseño de un plan de seguridad informática para el sistema de información misional de la Procuraduría General de la Nación permitiría brindar una protección completa al sistema y una mejora a las políticas, gestión del riesgo, personas y procesos.

Con este proyecto se busca plasmar unas estrategias para proteger el sistema de información misional mediante el uso de metodologías conocidas que permiten evaluar la seguridad en activos de información.

Adicionalmente este trabajo podrá beneficiar a la Procuraduría General de la Nación, ya que es un insumo para que posteriormente se pueda implementar el plan de seguridad informática para el sistema misional.

[2] PROCURADURIA GENERAL DE LA NACION. REPUBLICA DE COLOMBIA. Sistema de información Misional. Definición de manual del usuario aplicativo SIM. Primera edición. Bogotá D.C 2015.: [citado en marzo de 2015] p 26.

2. PROBLEMA

¿De qué forma se puede proteger la información institucional que se maneja en el sistema de información misional –SIM- de la Procuraduría General de la Nación?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un plan de seguridad informática para el sistema de información misional de la Procuraduría General de la Nación mediante la aplicación de buenas prácticas de seguridad, que permita desarrollar políticas y estándares claros para la preservación de confidencialidad, integridad y disponibilidad.

3.2 OBJETIVO ESPECÍFICOS

- Analizar el estado actual de seguridad informática para el sistema misional de la Procuraduría General de la Nación.

- Verificar la metodología utilizada para el análisis de riesgo usada en el sistema de información misional.

- Identificar los riesgos asociados al sistema de información misional.

- Determinar las posibles políticas de seguridad informática del sistema de información misional SIM.

- Plantear las medidas y procedimientos adecuados para dar cumplimiento a las políticas de seguridad informática del sistema de información misional.

4. MARCO TEÓRICO

4.1 MARCO INSTITUCIONAL

La Procuraduría General de la Nación (PGN), es la Entidad que representa a los ciudadanos ante el estado, cuenta con cerca de 4.00 servidores y "tiene autonomía administrativa, financiera y presupuestal en los términos definidos por el Estatuto Orgánico del Presupuesto Nacional"[3].

La obligación de la PGN es "velar por el correcto ejercicio de las funciones encomendadas en la Constitución Política de Colombia y la Ley, a servidores públicos y lo hace a través de tres funciones misionales principales"[4]: Preventiva de Intervención y disciplinaria.

La función preventiva se considera la principal responsabilidad de la PGN y está empeñada en la prevención antes que imponer sanciones mediante la vigilancia del actuar de los servidores públicos y la advertencia de los hechos que puedan ser violatorios de las normatividad vigente, "sin que ello implique coadministración o intromisión de la gestión de las entidades estatales"[5]

La función de intervención, en su calidad de sujeto procesal la Procuraduría General de la Nación, interviene ante las jurisdicciones contenciosas administrativas, constitucionales y ante las diferentes instancias de las jurisdicciones penal, penal militar, civil, ambiental y agraria, de familia, laboral, ante el Consejo Superior de la Judicatura y las autoridades administrativas y de policía. Su facultad de intervención no es facultativa sino imperativa y se desarrolla de forma selectiva cuando el Procurador General de la Nación lo considere necesario y cobra trascendencia siempre que se desarrolle en defensa de los derechos y las garantías fundamentales.[6]

Por último, la función disciplinaria en la que la PGN "es la encargada de iniciar, adelantar y fallar las investigaciones que por faltas disciplinarias se adelanten contra los servidores públicos y contra los particulares que ejercen funciones

[3] PROCURADURÍA GENERAL DE LA NACIÓN. REPÚBLICA DE COLOMBIA. Objetivos y funciones. [en línea], [consultado en marzo de 2015]. Disponible en: http://www.procuraduria.gov.co/portal/Objetivos-y-funciones.page
[4] Ibíd.
[5] Ibíd.
[6] Ibíd.

públicas o manejan dineros del estado, de conformidad con lo establecido en el Código Único Disciplinario o Ley 734 de 2002"[7]

4.2 FORTALECIMIENTO TECNOLÓGICO DE LA PROCURADURÍA GENERAL DE LA NACIÓN

En el año 2001, la PGN con apoyo del Banco Interamericano de Desarrollo - BID, elaboró un diagnóstico para identificar las debilidades que limitaban su capacidad de funcionamiento. Este diagnóstico señaló una serie de deficiencias de tipo organizacional y funcional, destacando el rezago tecnológico como una de las principales debilidades. Con el fin de resolver la problemática identificada, la Entidad formuló el programa de apoyo al fortalecimiento Institucional, el cual fue aprobado en documento Conpes 3211 de enero 9 de 2003, que autorizó a la Nación para contratar con el BID un crédito para financiarlo. Este programa se agrupó conceptualmente en bloques temáticos así: actividades jurídicas, gestión institucional, infraestructura tecnológica y adecuaciones físicas.[8]

La infraestructura tecnología se considera un apoyo transversal para los demás componentes del programa, ya que la tecnología es un medio no un fin.

La PGN estructuró el componente de tecnología bajo las siguientes premisas:

- Iniciar la modernización tecnológica con la consecución de la infraestructura básica de hardware, software, redes y comunicaciones, necesaria para implementar posteriormente sobre ésta, los sistemas de información y servicios informáticos requeridos por los funcionarios para el cumplimiento de sus funciones y para agilizar la gestión de la Entidad. Adicionalmente, en forma paralela a la consecución de la infraestructura básica, conceptualizar y diseñar los servicios informáticos que se implementarían sobre ésta.

- Desarrollar los sistemas de información requeridos por la Entidad, con base en una evaluación previa de las necesidades de información en cada una de las áreas misionales de la Procuraduría General de la Nación y en la optimización de los procedimientos, para que tales sistemas respondan al deber ser y no a la mera automatización de procedimientos actuales.

---

[7] Ibíd.

[8] PROCURADURÍA GENERAL DE LA NACION. REPÚBLICA DE COLOMBIA. Sistema de información Misional. Guía de capacitación. [pdf. en línea], [citado en marzo de 2015] p.8. Disponible en: http://www.procuraduria.gov.co/infosim/media/file/capacitacion/guia/Guia_de_capacitacion.pdf

- Implementar mecanismos y normas de seguridad informática.

- Brindar la capacitación requerida por los funcionarios tanto a nivel de usuario final como a nivel técnico, para poder asumir el cambio tecnológico que se implementaría.[9]

Los grandes frentes en los cuales se trabajó en la modernización de la PGN se muestran en la figura 1.

Figura 1. Frentes de modernización tecnológica

Fuente: PROCURADURÍA GENERAL DE LA NACION. REPÚBLICA DE COLOMBIA. Sistema de información Misional. Guía de capacitación. [pdf. en línea], [citado en marzo de 2015] p.9. Disponible en: http://www.procuraduria.gov.co/infosim/media/file/capacitacion/guia/Guia_de_capacitacion.pdf

"El principal propósito de todo lo que se ha implementado a nivel tecnológico ha estado orientado a entregarle a la Entidad un sistema de información que sea efectivo y que soporte de manera conveniente su operación"[10]

[9] Ibíd., p. 8-9.
[10] Ibíd., p 9.

4.3 CARACTERIZACIÓN DEL SISTEMA DE INFORMACIÓN MISIONAL SIM

4.3.1 Definición. "El Sistema de Información Misional (SIM), permite integrar las funciones misionales de intervención, disciplinaria y preventiva de la Procuraduría General de la Nación, puesto corresponde a un sistema moderno, integrado, actualizado y robusto que cubre las necesidades de información de la PGN en los ámbitos central, regional y territorial". [11]

4.3.2 Contexto Institucional. La Procuraduría General de la Nación en cumplimiento del mandato constitucional establecido en el artículo 277, debe vigilar el cumplimiento de la Constitución, las leyes, las decisiones judiciales y los actos administrativos, proteger los derechos humanos y asegurar su efectividad, defender los intereses de la sociedad, defender los intereses colectivos, en especial el ambiente, velar por el ejercicio diligente y eficiente de las funciones administrativas, ejercer vigilancia superior de la conducta oficial de quienes desempeñen funciones públicas, inclusive las de elección popular, ejercer preferentemente el poder disciplinario, adelantar las investigaciones correspondientes, e imponer las respectivas sanciones conforme a la ley e intervenir en los procesos y ante las autoridades judiciales o administrativas, cuando sea necesario en defensa del orden jurídico, del patrimonio público, o de los derechos y garantías fundamentales, funciones a partir de las cuales sus misiones son de naturaleza preventiva, de intervención y disciplinaria. [12]

Para apoyar el ejercicio de estas funciones misionales, la Procuraduría General de la Nación, con el respaldo del Banco Interamericano de Desarrollo –BID -, creó el Programa de Apoyo al Fortalecimiento de la entidad, entre otros fines, en busca de la modernización tecnológica de la Procuraduría General de la Nación, a través de la formulación de un plan estratégico de tecnología de la información, que requirió la ejecución de un proyecto de diseño, desarrollo e implantación de un Sistema de Información Misional, para: i) soportar las funciones misionales de la Entidad; ii) cubrir las necesidades de la Entidad en los ámbitos central, regional y local; iii) integrar los sistemas de información misional de la Entidad, y iv) permitir ser adaptado a cambios en la normatividad.

[11] PROCURADURÍA GENERAL DE LA NACIÓN. REPÚBLICA DE COLOMBIA. Sistema de información Misional. Bogotá DC, 2015. [en línea] [citado en marzo de 2015]. Disponible en: http://www.procuraduria.gov.co/infosim/Que-es-El-SIM_.page

[12] COLOMBIA. PROCURADURIA GENERAL DE LA NACION. Sistema de información Misional. Bogotá DC, 2015, Disponible en: Grupo SIM, Carpeta Contrato N° 179-169 de 2013 - Perfeccionamiento del Sistema de Información Misional de la Procuraduría.

El proyecto se enmarcó dentro de los bloques de actividades jurídico-misionales e infraestructura tecnológica, definidos gracias a la consultoría efectuada por la Universidad de los Andes, quién "propuso el modelo de procesos de negocio optimizado que debe apoyar el sistema de información. La firma Synapsis Ltda. Teniendo como punto de partida dicha propuesta, estructuró los procesos que corresponden a las funciones misionales de la PGN, los cuales fueron validados y aprobados por las directivas y un grupo representativo de funcionarios de la Entidad, constituyéndose en la base para la construcción del SIM". [13]

Para lograr el objetivo general del proyecto, se adquirió una solución integral que incluyó el diseño, desarrollo e implantación de la herramienta denominada Sistema de Información Misional – SIM -, al igual que el acompañamiento y soporte a la Entidad durante un año y el suministro y soporte del software de base necesario para el funcionamiento del sistema, es por esto que luego de realizar varias pruebas de carácter técnico-funcional sobre el ambiente de pruebas del sistema, se dio inicio a la puesta en marcha del aplicativo en producción el cual se fue implementando de manera gradual durante las vigencias 2008 y 2009, junto con la ejecución del plan de migración de datos de los diferentes sistemas de información que desde ese momento quedarían integrados en el SIM. De igual manera se desarrolló el plan de capacitación a nivel central y territorial, cubriendo la totalidad de dependencias y funcionarios misionales de la entidad, conforme al mapa estratégico PGN 2009-2012, enmarcado con el lema "Aprendizaje, tecnología y crecimiento", descrito en la circular Nº 028 del 12 de marzo 2010, emitida por el despacho del Procurador General de la Nación.

A mediados de 2010 se realizó una convocatoria interna dentro de las dependencias de nivel territorial para capacitar y designar a un funcionario por cada dependencia, denominado "Líder territorial", quienes facilitaran la comunicación entre el grupo de administración del SIM con las procuradurías Regionales, Provinciales, Distritales y Judiciales, de igual manera capacitaran a los nuevos funcionarios y prestaran acompañamiento sobre el uso del sistema en todo el territorio nacional.

Desde su puesta en marcha y durante los primeros 5 años de vida de sistema, periódicamente los responsables del registro presentan solicitudes de mejora, ajustes o nuevas funcionalidades por cambios normativos o de procedimientos que implican el desarrollo de nuevas funcionalidades de software y, a la vez, evidencian la urgente necesidad de realizarle a la herramienta un mantenimiento perfectivo de afinamiento, de tal manera que a finales de 2013, con recursos del

[13] PROCURADURÍA GENERAL DE LA NACIÓN. REPÚBLICA DE COLOMBIA. Modelo de Procesos de Negocio que Apoya el SIM [En línea], [citado en abril de 2015] Disponible en: http://www.procuraduria.gov.co/infosim/Modelo-SIM.page

Banco Interamericano de Desarrollo, BID, se establece el contrato N° 179-169 de 2013 de consultoría entre la Procuraduría General de la Nación y la Sociedad *Business* Technology S.A. para el perfeccionamiento del sistema de información misional de la PGN – Fase I .

La ejecución del contrato N° 179-169 de 2013, tuvo un tiempo estimado de 10 meses, por lo que a mediados de Octubre de 2014 se implementaron en el sistema, los ajustes, mejoras y nuevas funcionalidades desarrolladas al aplicativo, las cuales impactaron las actividades comunes a las misiones preventiva, de intervención y disciplinaria, mejorando su desempeño y preparando el sistema para el diseño, desarrollo e implementación del Nuevo Modelo de Gestión Preventivo recientemente adoptado por el señor Procurador General de la Nación.

Por lo anterior y bajo esta premisa, en la actualidad se está desarrollando la fase II para el perfeccionamiento del sistema de información misional de la PGN, bajo la ejecución del contrato N° 179-088 de 2014, nuevamente con la Sociedad *Business Technology* S.A., donde se desarrolla los módulos para el modelo preventivo, procesos judiciales de restitución de tierras y el módulo de relatoría, que es trasversal a las tres áreas misionales de la entidad.

4.3.3 Contexto Normativo. El Sistema de Información Misional está enmarcado bajo una serie de normatividades propias de la función y objetivos de la Procuraduría General de la Nación a través de alguna de sus misiones, preventiva, intervención o disciplinaria, de igual manera el sistema debe responder a cualquier cambio normativo que involucre la participación de la entidad.

Es por eso que el SIM, en su diseño, se especificó a partir de las funciones constitucionales asignadas a la entidad en el artículo 277 de la constitución política de Colombia, en ese orden, se tuvo en cuenta la normatividad orgánica vigente al momento de realizarse el desarrollo técnico:

(i) Decreto Ley 262 de 2000, "*Por el cual se modifican la estructura y la organización de la Procuraduría General de la Nación y del Instituto de Estudios del Ministerio Público; el régimen de competencias interno de la Procuraduría General; se dictan normas para su funcionamiento (…)*".
(ii) Ley 200 de 1995 anterior Código Disciplinario Único
(iii) Ley 734 de 2002, "*Por la cual se expide el Código Disciplinario Único*".
(iv) Códigos Penal y de Procedimiento Penal
(v) Códigos Civil y de Procedimiento Civil
(vi) Código Sustantivo del Trabajo y Procesal del Trabajo

(vii) Código de Infancia y Adolescencia
(viii) Código Contencioso Administrativo
(ix) Régimen Especial de las Fuerzas Militares
(x) Régimen Especial de la Policía Nacional
(xi) Resoluciones internas de la PGN sobre el trámite para el ejercicio del poder disciplinario preferente y de los asuntos preventivos

Las normas anteriormente citadas, contiene la forma como la Procuraduría General de la Nación ejerce sus funciones de intervención, preventiva y disciplinaria, normatividades que a la fecha ha tenido cambios legislativos o cuyos procedimientos internamente han variado y, por ende, fue indispensable incluir dentro de la fase I y fase II del perfeccionamiento del sistema de información misional, la modificación de algunos flujos alternativos de trabajo y la creación de nuevas funcionalidades y módulos que contemplen las disposiciones vigentes, que se relacionan a continuación:

(i) Ley 1437 de 2011, "*Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo*"
(ii) Ley 1448 de 2011 de Víctimas y Restitución de Tierras
(iii) Ley 1474 de 2011, *"por la cual se expide el nuevo Estatuto Anticorrupción".*
(iv) Ley 905 de Justicia Transicional
(v) Ley 1564 de 2002, "*Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones*".
(vi) Resoluciones internas 490 de 2008 y 016 de 2010 por las cuales se reglamenta el ejercicio de la función preventiva de la PGN
(vii) Resolución 344 de 2009 por medio de la cual se delega a la dirección nacional de investigaciones especiales la facultad de comisionar a servidores de otras dependencias de la Procuraduría General de la Nación.
(viii) Resolución 132 de 2014 donde se reglamenta el nuevo Modelo de Gestión Preventiva de la entidad.

El marco normativo del SIM, muestra claramente que el sistema de información misional de la PGN, desde su planteamiento ha estado enmarcado con la normatividad y legislación colombiana. Es por ello que el sistema evolucionará día tras día, de acuerdo a la dinámica propia de la legislación colombiana.

4.3.4 Contexto Técnico. El Sistema de Información Misional SIM, es una aplicación Web basada en la plataforma J2EE, donde la información que maneja es almacenada principalmente en una base de datos relacional, y la lógica del negocio es llevada a cabo por el motor de procesos de negocio BPEL. Todo el diseño del sistema está basado en estándares, en la aplicación de patrones y frameworks que permiten asegurar calidad a nivel de la arquitectura ensamblada y de las funcionalidades que la utilizan.

4.3.4.1 Arquitectura Física. El SIM cuenta con una arquitectura soportada directamente por tres servidores físicos, e indirectamente interactúa con otros servidores. A continuación se describen algunos de ellos:

- **Servidor "Oracle Database".** Contiene el motor de base de datos del sistema SIM, contiene la infraestructura del servidor de aplicaciones.

- **Servidor "Oracle Application Server".** Sobre el cual se despliega la aplicación J2EE. Además, se encuentra el motor de procesos de negocio Oracle BPEL donde se encuentran desplegados los procesos del SIM.

- **Servidor "Oracle Reports".** Soporta los reportes para el SIM. De esta forma se independiza el procesamiento o generación de los reportes de servidor principal del SIM.

- **Servidor "Gestión Documental".** Contiene el framework de gestión documental que permitirá realizar las funcionalidades relacionados con estos aspectos, así como la aplicación SIREL que encapsula la relatoría en el SIM.

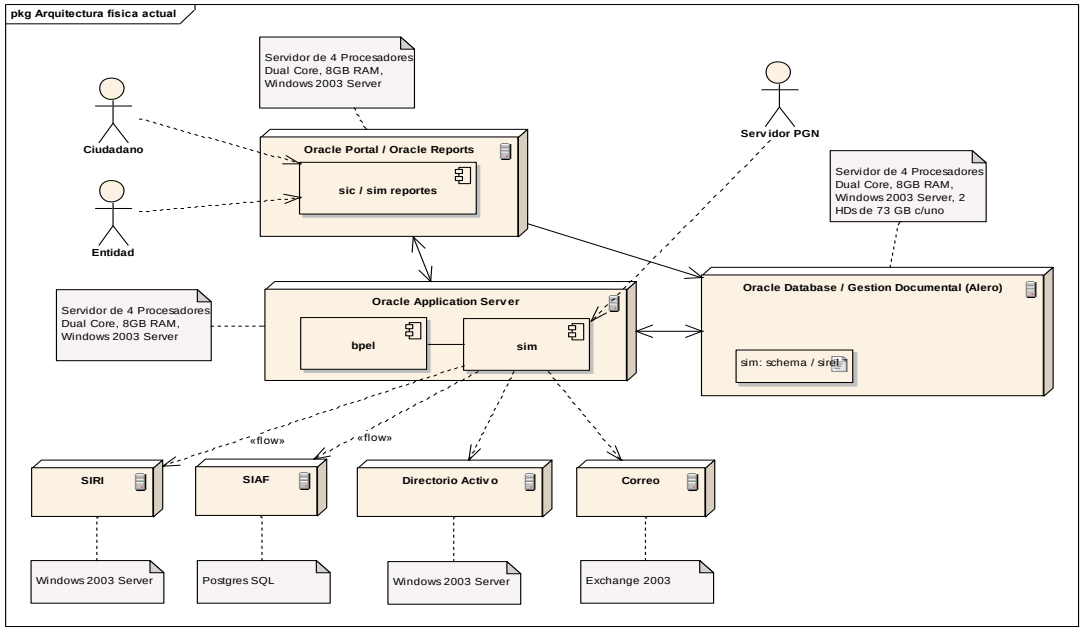
- **Servidor "SIRI".** Esta máquina corresponde al sistema de sanciones de la PGN, el cual tendrá interacción desde y hacia el SIM, utilizando WEB SERVICES en doble sentido

- **Servidor "SIAF".** Esta máquina provee los servicios relacionados con radicaciones y correspondencia de la PGN. La integración a este sistema se realiza a través de JDBC y WEB SERVICES.

- **Servidor "Directorio Activo".** Esta máquina ofrece los servicios de LDAP. Sobre este servidor el SIM consume en modo lectura los datos relacionados con login y password de los usuarios.

La figura 2. Arquitectura Física del SIM, muestra la estructura de alto nivel del SIM de la PGN.

Figura 2. Arquitectura Física del SIM



Fuente: autores

4.3.4.2 Arquitectura Lógica. En su lógica el SIM se encuentra estructurado en cuatro capas, web, bpel, servicios y datos, que se describen a continuación:

- **Web.** encapsula los servicios de presentación en módulos funcionales

- **Bpel.** donde se despliegan los procesos de negocio, conformados por las actividades que representan los pasos necesarios para ejecutar los procesos misionales y complementarios.

- **Servicios.** Estos servicios pueden ser llamados desde un cliente externo (por ejemplo capa web), ser publicados para consumo externo (por ejemplo los de integración como servicios Web), o ser orquestados dentro del motor de procesos de BPEL.

- **Datos.** La capa de datos y/o persistencia de la aplicación.

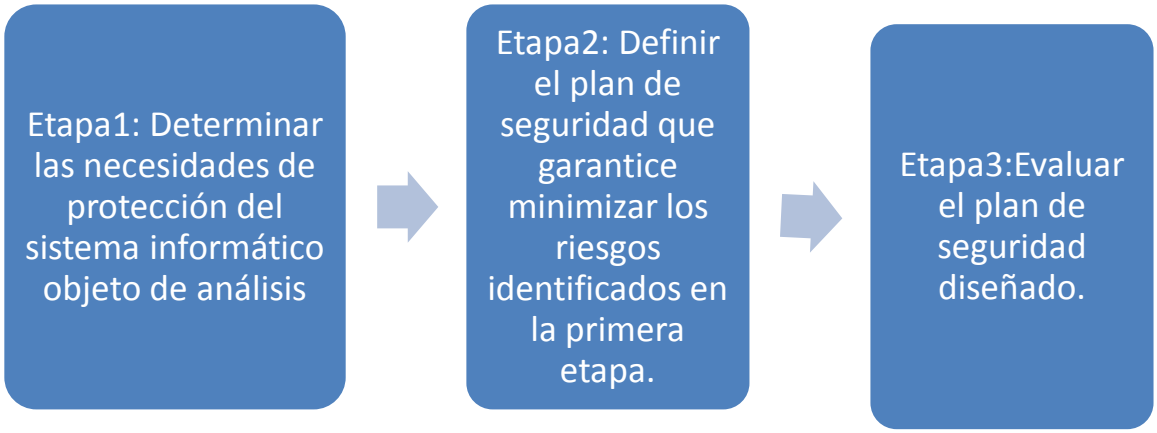
4.4 PLAN DE SEGURIDAD INFORMÁTICA

De acuerdo con el documento METODOLOGIA PARA LA ELABORACION DEL PLAN DE SEGURIDAD INFORMATICA[14] "Un plan de Seguridad Informática es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados".

El plan de seguridad informática es el documento básico en donde se establecen los principios organizativos y funcionales de la actividad de seguridad informática para las entidades y aglomera todas la políticas de seguridad y las responsabilidades de los participantes en el proceso informático, y las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.[15]

Durante el proceso de diseño de un plan de Seguridad Informática que se plantea en el documento se distinguen tres etapas que se ilustran en la figura 3.

Figura 3. Etapas de diseño de un plan de seguridad informática



Fuente: autores

[14] METODOLOGÍA PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA. [en línea], [consultado en marzo 2016]. Disponible en: http://dokumen.tips/documents/metodologia-para-la-elaboracion-del-plan-de-seguridad-informaticapdf.html p.3

[15] Ibíd.

En la figura 3, se relacionan las tres etapas claves para el diseño de un plan de seguridad informática, que se enumeran a continuación:

- **Etapa 1: Determinar las necesidades de protección del sistema informático objeto de análisis.** En esta etapa es donde se realiza la caracterización del sistema informático objeto que requiere ser protegido, su clasificación y valoración según su importancia, se determinan las necesidades de seguridad mediante la identificación de amenazas y estimación de los riesgos y evaluando el estado actual de la seguridad.

- **Etapa 2: Definir el plan de seguridad que garantice minimizar los riesgos identificados en la primera etapa.** Cuando ya se ha determinado que activo debe ser protegido y estimado los riesgos, es necesario definir políticas de seguridad que deben regir el funcionamiento del sistema de información y las medidas y procedimientos que hay que implementar para garantizar el cumplimiento de estas políticas.

- **Etapa 3: Evaluar el plan de seguridad diseñado**. Durante el proceso de evaluación es necesario establecer si se ha logrado una correspondencia adecuada entre las políticas de seguridad definidas y las medidas y procedimientos que garantizan su implementación.

5. METODOLOGÍA

En esta sección del proyecto se pretende describir la metodología utilizada para conocer el estado actual de seguridad del sistema misional de la Procuraduría General de la Nación y tener un punto de partida para desarrollar el plan de seguridad informática. Con esta metodología se pretende realizar la familiarización del sistema misional mediante una lista de chequeo, de igual forma, se pretende identificar, medir, controlar los diferentes eventos, vulnerabilidades y/o amenazas, a los que puede verse enfrentado sistema misional, al momento generar, capturar, procesar, transportar, almacenar y la disposición final de la información propia.

En la metodología se tienen en cuenta 3 aspectos: el desarrollo de un diagnóstico de seguridad mediante la aplicación de una lista de chequeo, un análisis de riesgos aplicando la norma ISO/IEC 27005:2009 y *Magerit* v3 y, un escaneo de vulnerabilidades.

La metodología es el resultado de la combinación de diferentes propuestas para la identificación de vulnerabilidades y amenazas. A continuación se explican las diferentes metodologías utilizadas para el desarrollo de este proyecto.

5.1 DIAGNÓSTICO

La metodología del diagnóstico, tiene por objeto realizar una evaluación del estado actual de seguridad informática del sistema misional de la Procuraduría General de la Nación. Esto permite identificar aquellas áreas en las cuales se debe mejorar.

Como marco de referencia esta metodología se alinea al anexo A de la norma Técnica Colombiana NTC ISO/IEC 27001:2013 – Sistemas de gestión de seguridad de la información-Especificaciones. Igualmente se incluyó un dominio para la evaluación de los riesgos de seguridad, para lo cual se diagnosticaron los siguientes dominios:

1. Evaluación de los riesgos de seguridad.
2. Políticas de seguridad de la información
3. Seguridad en los recursos humanos
4. Gestión de activos
5. Control de accesos
6. Criptografía

7. Seguridad física
8. Seguridad de las operaciones.
9. Seguridad de las comunicaciones
10. Adquisición, desarrollo y mantenimiento de sistemas
11. Gestión de incidentes de seguridad de la información
12. Cumplimientos.

Para cada dominio se desarrollaron una serie de preguntas cerradas enfatizadas al sistema misional de la Procuraduría General de la Nación, con el fin de evaluar el estado de cumplimento de cada una de las áreas y tener una base de lo que se debe mejorar en temas de seguridad y lo que permitirá identificar amenazas y vulnerabilidades necesarias para el análisis de riesgos. Para el diagnostico se desarrollan las siguientes actividades:

- Solicitar permiso a la Procuraduría para realizar una entrevista a los administradores del sistema misional de la Procuraduría (funcionales, no funcionales)

- Listas de chequeo e informe de resultados.

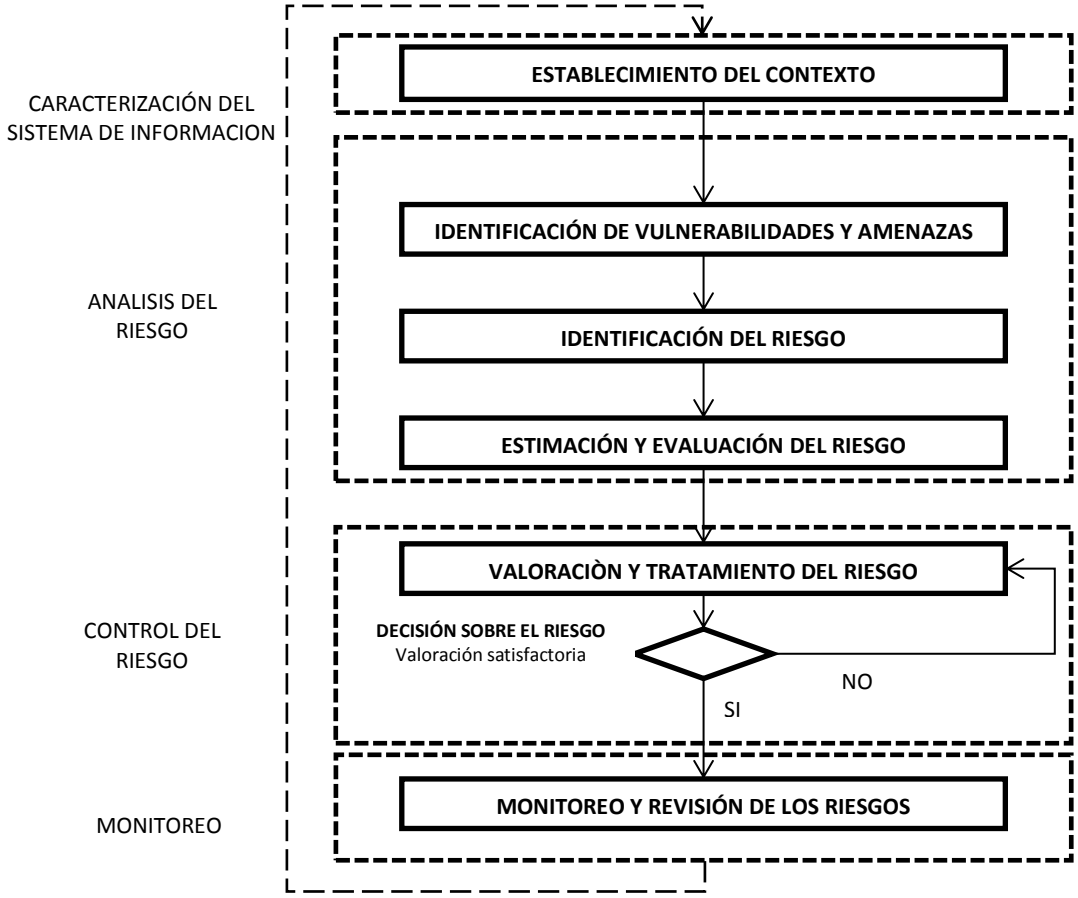
5.2 ESCANEO DE VULNERABILIDADES

En la ejecución del escaneo de vulnerabilidades, se utilizó la herramienta *opensource Nesus*, para identificar las posibles vulnerabilidades que afectan al sistema de información misional SIM. Se eligió esta herramienta, debido a que tiene mayores ventajas con respecto a las otras.
Nessus posee mayor cantidad de plugins por lo tanto permite detectar mayor cantidad de vulnerabilidades, de igual forma, permite mayor flexibilidad en su uso.

5.3 METODOLOGIA PARA EL ANALISIS DE RIESGOS

La figura 4 Visión general del proceso de análisis de riesgos se muestra el diagrama con el proceso de Análisis de Riesgos de Seguridad de la Información el cual consta de las siguientes etapas: Caracterización del sistema de información, Análisis del Riesgo, Control del Riesgo y Monitoreo.

Figura 4. Visión general del proceso de análisis de riesgos.



Fuente: autores

5.3.1 Marco contextual. Como marco de referencia en la construcción de la metodología, se usó la Gestión del Riesgo en Seguridad de la información contenida en la norma técnica ISO/IEC 27005 - TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN.

También se tuvo en cuenta la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT – versión 3.

El Análisis de riesgos es el proceso cuantitativo o cualitativo que permite evaluar los riesgos. Así bien, se debe tener en cuenta que al presentarse riesgos se están comprometiendo los pilares de la Seguridad de la información: la confidencialidad, la integridad y la disponibilidad de la información, para lo cual dentro del presente

análisis se tomaron como base varios insumos; la lista de chequeo la cual se encuentra estructurada y definida bajo la norma ISO 27001: 2013 y que fue aplicada a la parte técnica que maneja la oficina de sistema y a la parte misional y de soporte a usuarios que maneja el grupo de administración y apoyo, adicionalmente se tomó el resultado de los riesgos identificados en la matriz de análisis de riesgos dentro de la cual se incluyen los resultados del proceso global de análisis y evaluación de riesgos de Seguridad de la Información.

Para la identificación, análisis, valoración y tratamiento de los riesgos, se define un el mapa de riesgos (Riesgos Inherentes – Riesgos Residuales), en el cual se ubican los riesgos identificados y su nivel de probabilidad e impacto (Anexo F).

5.3.2 Definición de criterios básicos. Para la gestión del riesgo se definen los siguientes criterios tales como: Criterios de impacto, Criterios de probabilidad y criterios de aceptación del riesgo.

5.3.2.1 Criterios de Impacto*.* En los criterios de impacto (Entendiéndose por impacto las consecuencias o efectos que pueden ocasionar la materialización del riesgo) se especificaron en términos de daño para la organización causados por un evento de seguridad, se consideraron los siguientes aspectos:

- Operaciones deterioradas
- Daños a la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Cuadro 1. Impactos por materialización de amenaza

Categoría	Valor	Operacional	Reputacional	Legal
Catastrófico	5	Afecta la operación total de la PGN	Se afecta gravemente la imagen del PGN hay pérdida de credibilidad y opinión pública negativa. Hay divulgación en medios de comunicación.	Incumplimiento de la normatividad legal vigente establecida en Colombia (Constitución, leyes, decretos).
Severo	4	Afecta a todas las actividades del SIM.	Se afecta la imagen de la PGN por pérdida de credibilidad y opinión pública negativa.	Incumplimiento de la normatividad exigida por los entes de control.

Cuadro 1. (Continuación)

Categoría	Valor	Operacional	Reputacional	Legal
Moderado	3	Afecta la operación de algunas actividades del SIM.	Puede generarse una opinión pública negativa sobre la prestación del servicio.	Incumplimiento de las Políticas internas de Seguridad de la Información, organizacionales
Leve	2	Genera reprocesos en las actividades pero no afecta significativamente el SIM	La afectación de la Imagen del SIM es Leve y resolver este tema implica recursos y puede durar buen tiempo.	Incumplimiento a los procedimientos y prácticas definidas para la operación adecuada.
Insignificante	1	No se afecta la operación del SIM	La afectación de la Imagen del SIM es insignificante y fácil de resolver.	No genera afectación legal.

Fuente: autores

5.3.2.2 Criterios de Probabilidad. En los criterios de probabilidad (entendiéndose la probabilidad como la medida para estimar la posibilidad de que ocurra un riesgo) se especificaron en términos de materialización de ocurrencia de una amenaza, con una calificación que va de uno (1) a cinco (5) siendo uno (1) la probabilidad más baja de materialización y cinco (5) la probabilidad más alta de materialización de la amenazas.

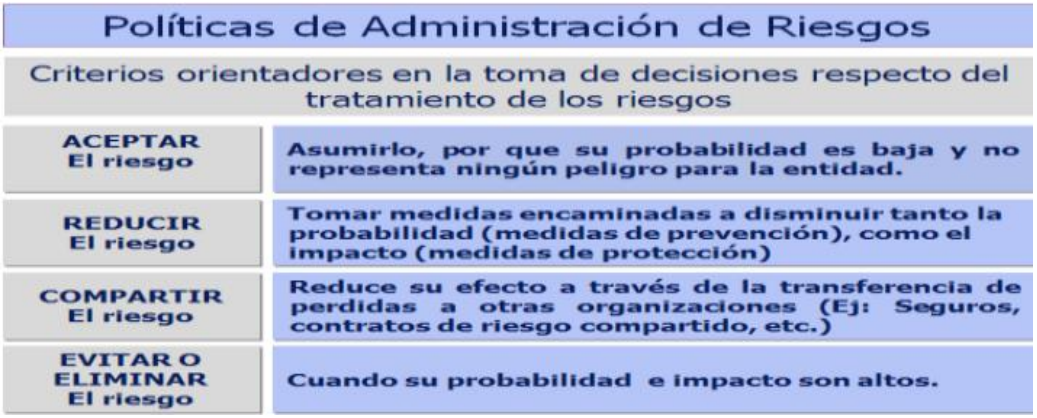
Cuadro 2. Probabilidad de ocurrencia de una amenaza

Categoría	Valor	Descripción
Inminente	5	La materialización de la amenaza ocurre diariamente.
Frecuente	4	La materialización de la amenaza ocurre una vez al mes.
Ocasional	3	La materialización de la amenaza ocurre una vez al año.
Remoto	2	La materialización de la amenaza ocurre en periodo de 2 a 5 años.
Improbable	1	Nunca se ha materializado la amenaza pero no se descarta su ocurrencia.

Fuente: autores

5.3.2.3 Criterios de Aceptación del Riesgo. La entidad ha definido políticas de Administración de Riesgos por parte de la Alta Dirección, permite establecer los lineamientos los criterios orientadores en la toma de decisiones respecto del tratamiento de los riesgos, "con el fin de identificar las opciones para tratar y manejar los riesgos y tomar decisiones basadas en la valoración de los mismos."[16] La figura 5. Políticas de administración del riesgo, muestra los criterios para la evaluación de riesgo en la PGN.

Figura 5. Políticas de administración del riesgo



Fuente: PROCURADURIA GENERAL DE LA NACION. Mapa de Riesgos Institucional y de Riesgos de Corrupción. [pdf en línea], [consultado en marzo de 2015]. Disponible en http://www.procuraduria.gov.co/portal/media/file/MAPA.pdf p5.

Estos criterios se desarrollaron con base en el actual mapa de riesgos Institucional, de acuerdo con lo estipulado en el Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano - MECI 2014.

Teniendo en cuenta la política de administración del riesgo de la entidad, se realizó una homologación para definir la aceptación del riesgo del sistema de información misional SIM, el cual se presenta a continuación:

- Para todo riesgo inherente que se tipifique en los niveles "EXTREMO" y "ALTO", se deberá gestionar su tratamiento y mitigarlo a través de la implementación de controles.

[16] PROCURADURIA GENERAL DE LA NACION. REPUBLICA DE COLOMBIA. Mapa de Riesgos Institucional y de Riesgos de Corrupción. [pdf en línea], [consultado en marzo de 2015]. Disponible en http://www.procuraduria.gov.co/portal/media/file/MAPA.pdf p5.

- Los riesgos inherentes en los niveles "MEDIO" y "BAJO" son aceptados por el grupo SIM. Sin embargo como buena práctica de seguridad se aplicarán controles y se evaluará su estado.

- Para todo riesgo residual que se tipifique en los niveles "EXTREMO" y "ALTO", se deberá gestionar su tratamiento a través del diseño de planes de seguridad.

5.3.3 Caracterización del Sistema De Información. Se define como la primera etapa del proceso de análisis de riesgos en la cual se busca conocer más a fondo el flujo de actividades del sistema de información misional mediante la identificación de entradas, salidas, responsables y activos de información necesarios para la ejecución de las tareas diarias.

A continuación se definen algunos conceptos básicos que son necesarios para llevar a cabo la identificación de los activos de información:

- **Software [SW].** Son todos aquellos programas, aplicativos, desarrollos, a través de los cuales se han automatizado ciertas tareas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. En esta clasificación no se incluye el código fuente, porque será incluido en la tipología o caracterización de datos o información.

- **Hardware [HW].** Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo depositarios temporales o permanentes de los datos, soporte de la ejecución de aplicaciones informáticas o responsables del procesado o transmisión de los datos.

- **Redes [COM].** Incluye instalaciones dedicadas como servicios de comunicaciones contratados a terceros, centrándose en ellos como medios de transporte que llevan datos de un sitio a otro.

- **Ubicación [L].** Lugares donde se hospedan el sistema de información y comunicaciones.

- **Personal [P].** Personas relacionadas con el sistema de información.

- **Información [D].** Documentación física y lógica (archivos, bases de datos, mallas) procesada en cada una de las actividades del subproceso.

- **Terceras Partes [ST].** Socios de negocio y proveedores con los cuales se tiene tercerizada alguna actividad del sistema de información.

La Clasificación de activos de información lista los activos de información para el sistema de información misional los cuales fueron identificados y discriminados por tipo de activo de acuerdo a la metodología utilizada:

Tabla 1. Clasificación de activos de información

Tipo de Activo	Activos identificados
Software - [SW]	Base de datos Oracle, Aplicación, S.O Servidores, Sistema Operativo de Servidores
Hardware - [HW]	Servidores, PCs de los usuarios
Servicios Internos- [SI]	Directorio Activo, Gestión documental, Web Service SIM-SIRI, Web Service SIM-SIAF
Servicios Subcontratados - [SE]	Contrato de mantenimiento y desarrollo
Datos / Información - [D]	Información Interna de los Procesos Misionales.
Personal - [P]	usuarios SIM, Servidores PGN
Instalaciones Física - [L]	Instalaciones de la procuraduría, Data Center

Fuente: autores

5.3.4 Análisis del Riesgo. Esta etapa consiste en evaluar los riesgos identificados, con el fin de determinar la probabilidad y el impacto de los mismos. Para ello, el dueño del proceso identifica las amenazas, vulnerabilidades y riesgos de cada uno de los activos de información, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de la información.

Los puntos importantes a considerar son:

- Identificar de manera clara cuales son los riesgos que pueden afectar al sistema de información misional.

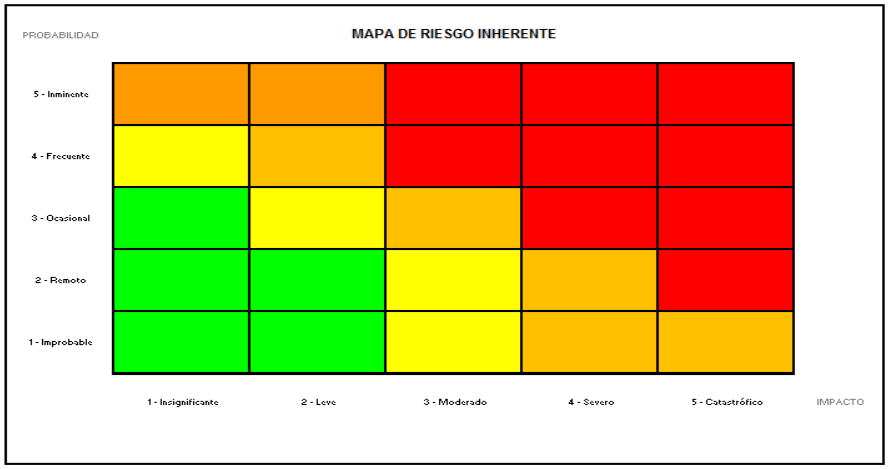
- Cuáles son las amenazas y vulnerabilidades.

- Cuál es el impacto que se generaría al materializarse una o más amenazas identificadas

- La probabilidad de que dicho riesgo se materialice.

A continuación se generará el mapa de riesgos inherentes, en el cual se ubican los riesgos identificados y su nivel de probabilidad e impacto. Vale la pena recordar que en esta etapa no se han definido los controles respectivos para mitigar los riesgos. La figura 6, muestra el modelo de mapa de riesgos que se usará en el proceso.

Figura 6. Modelo de mapa de riesgo



Fuente: autores

5.3.4.1 Identificación de Amenazas. Las amenazas tienen el potencial de causar daños a los activos identificados y en últimas a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Para este proyecto se identificaron las amenazas más relevantes del sistema, caracterizándolos por el tipo de activo. Se utilizó como referencia el catálogo de amenazas de Magerit v3, y fueron segregadas en los siguientes grupos:

- Ataques [A]
- Errores humanos [E]
- De origen industrial [I]
- De origen natural [N]

NOTA: No todas las amenazas del catálogo fueron aplicables para el sistema de información misional.

5.3.4.2 Identificación de Vulnerabilidades. La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Para este proyecto se especificaron vulnerabilidades de acuerdo al catálogo de la norma ISO 27005, ajustándolas al negocio.

El objetivo es identificar las vulnerabilidades del activo que puedan ser explotadas por las amenazas del catálogo propuesto.

5.3.4.3 Identificación del Riesgo. Apoyándose en las amenazas y vulnerabilidades identificadas se debe determinar el riesgo de seguridad de la información para el sistema de información misional SIM, en el cual se identifican las fallas de seguridad que se verían afectadas por el incumplimiento de los objetivos si las amenazas se materializaran (Confidencialidad, Integridad, Disponibilidad, Autenticidad de los Usuarios, Autenticidad del origen de los Datos, Trazabilidad del Servicio y Trazabilidad de los Datos), sobre dicho grupo de activos, estas se utilizan para valorar las consecuencias de la materialización de una amenaza y la medida del perjuicio para la entidad si el activo se ve afectado por determinado falla de seguridad.

Para la identificación de los riesgos se toma como guía el incumplimiento de los objetivos de control de la norma ISO27001:2013, adicionalmente los riesgos que el dueño del proceso como conocedor del mismo considere.

5.3.4.4 Estimación del Riesgo. Para realizar la estimación del riesgo, la metodología utilizada contempla los siguientes ítems:

- Inicialmente se debe dar una calificación a la probabilidad de materialización de la amenaza, en una escala de uno (1) a cinco (5) tal y como se planteó en los criterios de probabilidad.

- Se califica cada uno de los impactos (reputacional, legal y operativo), a continuación, se realiza un promedio entre los mismos para determinar el valor único de impacto generado por la materialización de una amenaza utilizando la siguiente fórmula:

$$Itotal = (Operacional + Reputacional + Legal)/3$$

- Se calcula el nivel del riesgo inherente concatenando la probabilidad de ocurrencia de la amenaza y el total del impacto, luego es ubicado el riesgo inherente en el mapa de calor.

Una vez identificado el riesgo inherente[17], se deben ejecutar los controles requeridos en los criterios de aceptación del riesgo definidos para el sistema de información misional SIM.

5.3.4.5 Evaluación del Riesgo. Una vez identificado el riesgo inherente se debe realizar una comparación con criterios de evaluación de los riesgos. Los criterios determinan el riesgo en la seguridad de una organización, sin embargo, este proyecto se basa en el sistema de información misional en donde se tuvo en cuenta los siguientes aspectos:

- El sistema de información misional tienen un valor estratégico para la Procuraduría General de la Nación, por lo tanto cualquier riesgo identificado con nivel Alto o Extremo se le debe dar mayor prioridad en el tratamiento.

- Criticidad de los activos de información involucrados con el sistema de información misional, que no se valoraron cualitativamente, ya que en la etapa de identificación de activos se seleccionaron los que generan una dependencia mayor sobre el sistema de información misional.

5.3.5 Control del Riesgo. Consiste en determinar los controles existentes de los riesgos y causas identificadas, con el fin de determinar qué tan efectivos son en la reducción de la probabilidad y/o el impacto de los riesgos inherentes.

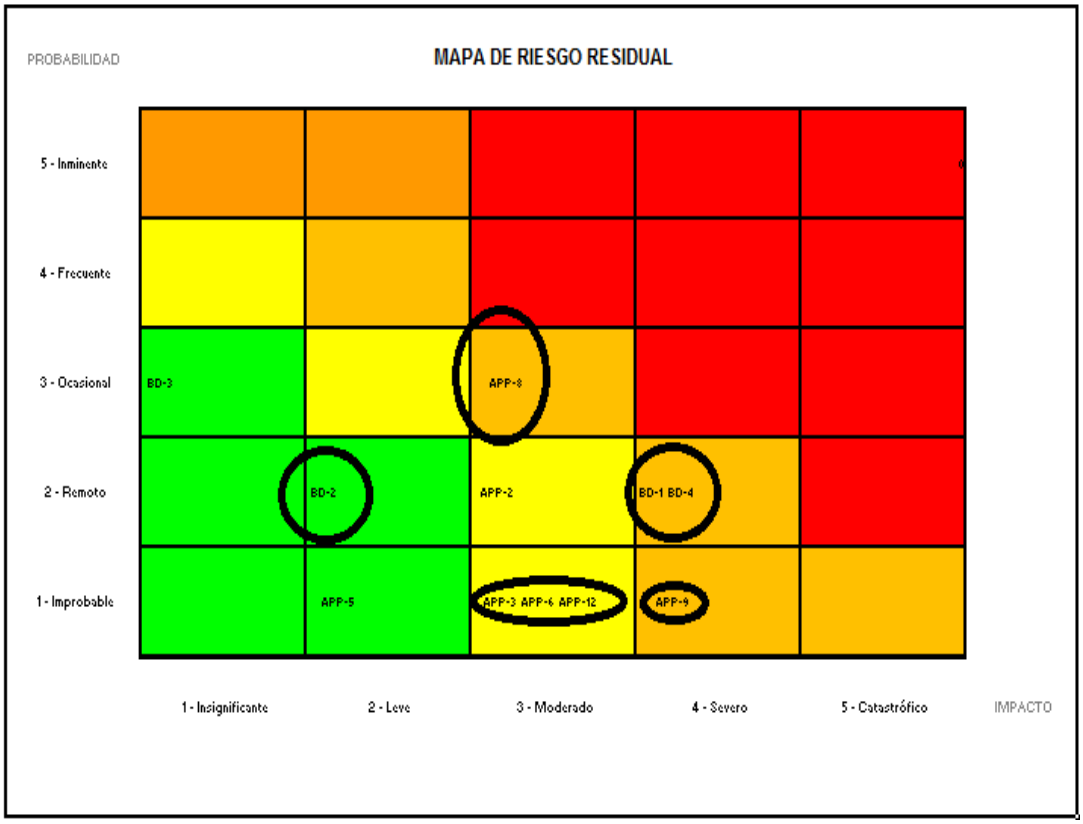
Adicionalmente, en esta etapa se identifican los controles que actualmente se tienen para mitigar los riesgos, con el fin de evaluar su efectividad en la implementación de los controles y la reducción del impacto en caso que el riesgo se materialice.

El resultado final de esta etapa es la generación del mapa de riesgos residual el cual se obtiene de la medición de la efectividad de los controles existentes, que

[17] **Riesgo inherente**: Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Este riesgo surge de la exposición que se tenga a la actividad en particular y de la probabilidad que un choque negativo afecte la rentabilidad y el capital de la compañía. [en línea], [consultado en abril 2015]. Disponible en: http://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual

buscan minimizar el grado de severidad y el nivel de riesgo de los riesgos inherentes. La figura 7 Mapa de riesgo residual muestra el modelo de mapa a utilizar.

Figura 7. Mapa de riesgo residual



Fuente: autores

5.3.5.1 Valoración del Riesgo. Basándose en la etapa de estimación del riesgo, en donde se identifica el riesgo inherente, a partir del "Anexo F. Matriz de Análisis de Riesgos SIM", donde se ingresar la calificación numérica del impacto, probabilidad y la descripción de los riesgos, así como los controles para cada una de las vulnerabilidades identificadas. La valoración del riesgo se refleja en la severidad, que es el resultado de cruzar el impacto y la probabilidad, mide la intensidad en que un riesgo está presente lo que permite asignarle un valor y un nivel de riesgo de acuerdo a los colores correspondientes:

Rojo = Extremo. Naranja = Alto. Amarillo = Moderado o Medio. Verde = Bajo.

El cuadro 3 muestra los criterios para Valoración del riesgo con controles.

Cuadro 3. Criterios para Valoración del riesgo con controles

Nivel de exposición o de severidad del riesgo	
Riesgo	**Descripción**
Extremo	Se requiere acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la alta dirección. INACEPTABLE
Alto	Se requiere atención de la alta dirección. Planes de tratamiento requeridos, implementados y reportados a los jefes delegados, Oficina, Divisiones, etc. IMPORTANTE
Moderado	Aceptable, debe ser administrado con procedimientos normales de control. TOLERABLE
Bajo	Menores efectos que pueden ser fácilmente remediados. Se administra con procedimientos rutinarios. No se requiere de ninguna acción. ACEPTABLE.

Fuente: PROCURADURIA GENERAL DE LA NACION. REPUBLICA DE COLOMBIA. Mapa de Riesgos Institucional y de Riesgos de Corrupción. [pdf en línea], [consultado en marzo de 2015]. Disponible en http://www.procuraduria.gov.co/portal/media/file/MAPA.pdf p9.

5.3.4.2 Tratamiento del Riesgo. En esta etapa se analizan los riesgos inherentes identificados y se toman decisiones sobre su tratamiento. Para lo cual se aplican los controles que actualmente tiene la entidad para dar cumplimiento al objetivo de control y por consiguiente mitigar los riesgos, claro está, que algunas actividades pueden ser sencillas, mientras que otras alcanzarán el suficiente nivel de complejidad y costo como para que su ejecución se convierta en un proyecto para la entidad.

Para realizar una adecuada ejecución de los controles, se determinó asignar una valoración (criterios) que permiten calificar la efectividad de los mismos, para lo cual se ha definido un conjunto de criterios que se presentan en el cuadro 4 Criterios para evaluación de controles:

Cuadro 4. Criterios para evaluación de controles

Características del control	Descripción
Tipo de control	Especifica el tipo de control que será implementado (Preventivo, Detectivo - Correctivo, Correctivo).
Frecuencia	Periodicidad con que se utiliza el control.
Ejecución	Forma de implementar el control.
Complejidad	Grado de dificultad para ejecutar el control.
Documentación	Especifica el grado de identificación del control.

Cuadro 4. (Continuación)

Características del control	Descripción
Evidencia	Registros del uso del control.
Desviación	Evidencia si el control ha sido glosado o puesto en observación por un ente auditor.
Recursos para ejecutar el control	Cantidad de recursos que cuenta el área / subproceso para ejecutar el control.

Fuente: autores

A cada uno de los anteriores criterios se les asignó una valoración comprendida entre 1 y 3, y a cada uno de los controles implementados se les asigna una valoración de acuerdo con los criterios.

Una vez escogido el valor de cada uno de los criterios, se promedia el valor de los criterios para cada control, entregando como resultado el valor total de los criterios y a partir de este se calcula la probabilidad e impacto residual, teniendo en cuenta que los controles Preventivos y Detectivos, permiten mitigar la probabilidad de ocurrencia de los riesgos, mientras que los controles Correctivos solamente mitigan el impacto que pueden generar dichos riesgos, para lo cual se utilizaron los siguientes patrones:

- Si el control es preventivo o detectivo, tome la calificación de probabilidad de materialización de la amenaza y divídala por el valor total de los criterios, como resultado se muestra la probabilidad residual, mientras que el valor del impacto continua igual.

- Si el control es correctivo, toma la calificación total del impacto y divídala por el valor total de los criterios, como resultado se muestra el impacto residual, mientras que el valor de la probabilidad continúa igual.

El resultado final de esta etapa es el valor del riesgo residual, este se da concatenando el valor de la probabilidad residual y el valor del impacto residual, para finalmente ubicarlo el riesgo residual en el mapa de calor, luego para los que se tipifique en los niveles "EXTREMO" y "ALTO", se deberá gestionar su tratamiento a través del diseño de planes de seguridad.

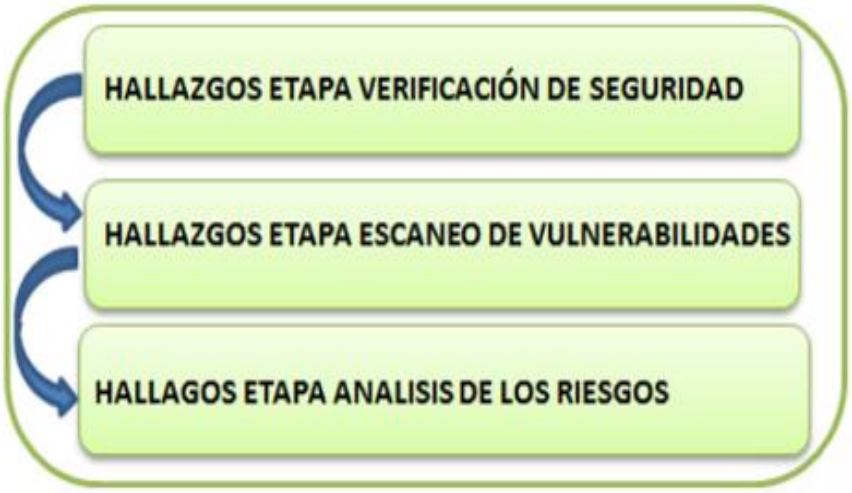
5.4.5 Etapa de Monitoreo. Corresponde a la última fase del proceso de análisis de riesgos, la cual consiste en hacer seguimiento, al cumplimiento de los planes de acción definidos para los riesgos identificados con severidad extrema y alta.
Si el valor del riesgo residual es despreciable, los controles implementados son los adecuados, esto no quiere decir que se debe descuidar el riesgo, simplemente hay gestión efectiva del sistema de seguridad de la información.

Es importante entender que un valor residual es sólo un valor, el riesgo residual es un indicador, su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer para mitigar este riesgo, lo cual se involucra en el plan de tratamiento de riesgos acompañado de un monitoreo constante evaluando continuamente los controles y su efectividad.

6. HALLAZGOS

Para el cumplimiento del objetivo del proyecto se obtuvieron varios hallazgos, como consecuencia del plan desarrollado en la metodología planteada. Estos hallazgos fueron obtenidos en diferentes momentos durante la ejecución del proyecto, sirviendo posteriormente como insumo para la elaboración del diseño del plan de seguridad informática del sistema de información misional SIM. En la figura 9 Etapas de hallazgos de la evaluación de seguridad del SIM PGN se muestran las diferentes actividades de la evaluación del sistema.

Figura 8. Hallazgos obtenidos dentro al Proyecto



Fuente: autores

6.1 HALLAZGOS ETAPA VERIFICACIÓN DE SEGURIDAD

Dada la importancia de los sistemas de información dentro de las organizaciones y los avances en la tecnología, estos, aparecen asociados a nuevos riesgos que es necesario evitar, mitigar o minimizar al máximo. Así bien, se debe tener en cuenta que al presentarse riesgos se están comprometiendo los pilares de la Seguridad de la Información; la confidencialidad, la integridad y la disponibilidad de los datos, frente a las amenazas de la infraestructura física, de la tecnológica que pueden llegar a ocasionar impactos legales y reputacionales para la entidad.

El Sistema de Información Misional SIM, apoya integralmente las funciones misionales de intervención, disciplinaria y preventiva de la PGN. El sistema cuenta

con una parte técnica que maneja la oficina de sistemas de la entidad y la parte funcional y de soporte a usuarios, que es manejada por el grupo de administración y apoyo, el Grupo SIM.

Las jefaturas de la oficina de sistemas y el grupo SIM, autorizan realizar la verificación del estado de la seguridad a través de una lista de chequeo (Anexo. D), la cual se encuentra estructurada y definida bajo la norma ISO 27001 del 2013, agrupando la calificación en 12 dominios:

1. Evaluación y Tratamiento del Riesgo
2. Política de Seguridad de la Información
3. Seguridad de los Recursos Humanos
4. Gestión de Activos
5. Criptografía
6. Control de Acceso
7. Seguridad Física y del Entorno
8. Seguridad de Operaciones
9. Seguridad de las Comunicaciones
10. Adquisición, desarrollo y Mantenimiento de Sistemas
11. Relaciones con los Proveedores
12. Gestión de incidentes de la seguridad informática
13. Cumplimiento

6.1.1 Objetivos Verificación de Seguridad

- Ejecutar un checklist a los administradores técnicos y funcionales del SIM para lograr obtener una visión generar del estado actual de la seguridad del sistema de información misional SIM, desarrollada a través Objetivos Específicos

- Aplicar cada uno de los dominios de la norma ISO 27001 de 2013 para el sistema de información misional.

- Analizar el estado actual en que se encuentra la seguridad informática del sistema de información misional.

6.1.2 Conclusiones Verificación de Seguridad. Con la información obtenida con la realización de la lista de chequeo, se pudo obtener una visión general del estado de seguridad del sistema de información misional SIM (Anexo. A), la cual servirá como parte del insumo necesario para el diseño del plan de seguridad información del SIM.

Dentro de la información obtenida se pudo llegar a concluir algunas cosas puntuales:

- La entidad cuenta con un documento de políticas de seguridad de la información, pero este no ha sido dado a conocer por completo a los administradores funcionales de los diferentes sistemas de información, ni a los demás funcionarios de la entidad. Adicionalmente el documento no cuenta con una aprobación formar por parte de la dirección, lo que impide su ejecución y cumplimiento.

- Se debe definir un conjunto de políticas para la seguridad de la información propias para el sistema de información misional que posteriormente puede ser extendido a los demás sistemas de información de la entidad. Dicho documento debe ser aprobado por la entidad, publicado y comunicado a los empleados y a las partes externas pertinentes

- Se deben definir procedimientos para el manejo de información sensible, teniendo en cuenta la confidencialidad, integridad, disponibilidad y el no repudio.

- No existe un procedimiento establecido para eliminación o cambio los derechos de acceso al sistema después de que se le notifica de un retiro o cambio de funciones de los funcionarios.

- La matriz de roles y perfiles que se maneja para dar acceso a las diferentes funcionalidades del sistema se debe redefinir, puesto que al parecer se están dando privilegios a usuarios que no corresponden. Adicionalmente se debe incluir dentro de la matriz las funcionalidades de consultas y reportes que genera la aplicación.

- Los resultados consolidados de cumplimiento por dominio de seguridad se muestran en la tabla 2.

Tabla 2. Resultados de la evaluación por dominio

Dominios	Estado de cumplimiento
Evaluación y trata miento del riesgo	25%
Políticas de la seguridad de la información	83%
Seguridad de los recursos humanos	70%
Gestión de activos	32%
Control de acceso	67%
Criptografía	67%
Seguridad física y del entorno	100%
Seguridad de las operaciones	69%
Seguridad de las comunicaciones	100%
Adquisición, desarrollo y mantenimiento de sistemas	73%
Relaciones con los proveedores	86%
Gestión de incidentes de seguridad de la información	75%
Cumplimiento	33%

Fuente: autores

6.2 HALLAZGOS ETAPA ESCANEO DE VULNERABILIDADES

Las vulnerabilidades de seguridad informática han existido desde siempre, en los años 90 la gran mayoría de intrusos ingresan a los sistemas informáticos utilizando técnicas de *scanning*, ataques de fuerza bruta, probando usuarios, diferentes *passwords*, ingeniería social y a través de la explotación de vulnerabilidades. Hoy en día el internet y al avance de la tecnología, permiten y brinda una gran cantidad de información sobre como ingresar a los sistemas, servicios virtuales en la nube y plataformas móviles.

El presente informe, pretende mostrar el resultado del análisis de vulnerabilidades realizadas sobre el Sistemas de información Misional SIM (Anexo. B), ofreciendo una visión global sobre las posibles vulnerabilidades del sistema. De igual manera

se pretende concientizar a la entidad y a los dueños de los activos involucrados sobre de la importancia de las actualizaciones en los sistemas para minimizar los riesgos generados por las vulnerabilidades, adicionalmente determinar los posibles vectores de ataque dentro de la red interna de la entidad que pongan en riesgo la disponibilidad, integridad y disponibilidad de la información.

El análisis comprende las siguientes fases: Entendimiento de la infraestructura, pruebas, Medidas Preventivas, Realización de pruebas de vulnerabilidades, Análisis de resultados; no se intentara explotar la vulnerabilidad.

Para la ejecución del análisis de vulnerabilidad se utilizó la herramienta NESSUS, esta se compone de una estructura de cliente-servidor y sirve para detectar a través de la red vulnerabilidades en un sistema remoto, ya sea un cliente o un servidor (Anexo. E). Existen versiones para GNU/Linux, Mac OS X, *Solaris*, *FreeBSD* y para Windows, en nuestro caso el análisis fue lanzado para la versión Windows desde dos máquinas diferentes, una maquina se encontraba en la red interna de la entidad y otra máquina se encontraba fuera de ella, permitiendo obtener un posible ataque interno o externo al sistema de información.

6.2.1 Objetivos Escaneo de Vulnerabilidades

- Realizar la ejecución del análisis de vulnerabilidad al servidor donde se encuentra hospedado el sistema de información misional SIM de la Procuraduría General de la Nación, para ello utilizando la herramienta de escaneo opensourse NESSUS.

- Identificar las posibles vulnerabilidades que afecten al sistema de información misional SIM.

- Analizar y clasificar las vulnerabilidades identificadas según su promedio de criticidad respecto de la afectación en el SIM.

6.2.2 Conclusiones Escaneo de Vulnerabilidades. Luego de realizar el escaneo de vulnerabilidades, se obtuvo información importante que brinda el conocimiento al cual está expuesto el sistema de información misional en un posible ataque por explotación de alguna de las vulnerabilidades identificadas.

Teniendo en cuenta el análisis se debe adelantar una evaluación detallada y profunda de los componentes de infraestructura para solucionar las vulnerabilidades identificadas, comenzando por aquellos de mayor vulnerabilidad para determinar las áreas específicas en que se requiere asistencia. La Tabla 3, muestra los resultados obtenidos con la herramienta NESSUS.

Tabla 3. Resultado de análisis de vulnerabilidades SIM PGN

Severidad	**Cantidad**
Criticas	1
Altas	2
Medias	11
Bajas	5
Informativas	37
Total	**56**

Fuente: autores

6.4 HALLAZGOS ETAPA ANALISIS DE RIESGOS

El acelerado crecimiento de la tecnología de la información y la importancia que los sistemas de información han tomado en las organizaciones, han llevado a estas, a depender de dichos sistemas, provocando que la atención día tras día crezca en torno a los mismos. Los sistemas de información de TI se crean, diseñan y desarrollan a partir de las necesidades de negocio de las instituciones, de sus estrategias misionales y en el caso del sector público se diseñan también desde su normatividad interna y la legislación del estado. Por este motivo la consecución de los objetivos de la entidad depende y van de la mano de sus sistemas de información, por esto se hace necesario garantizar el correcto funcionamiento y la seguridad de los sistemas de información en las instituciones.

Dada la importancia de los sistemas de información, la entidad a través de los administradores técnicos y funcionales designados mediante resolución 114 del 10 de mayo de 2006 autorizan realizar el análisis de riesgos del sistema institucional de información misional SIM; sistema que apoya integralmente las funciones misionales de intervención, disciplinaria y preventiva de la entidad.

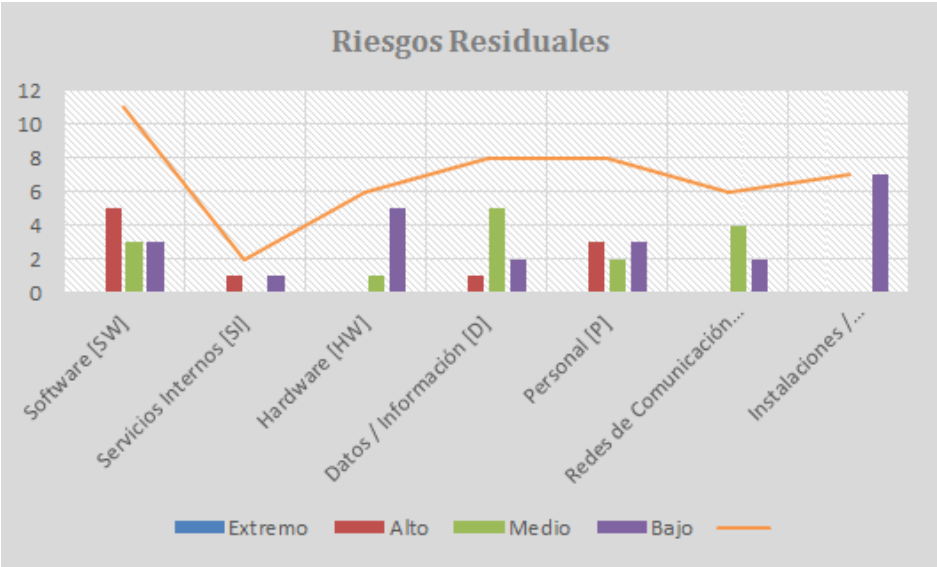
En presente informe, muestra el resultado del análisis y gestión de riesgos aplicados al sistema de información misional SIM (Anexo. C). Para ello se toma como referencia la metodología que se alinea a la gestión del riesgo en seguridad de la información contenida en el documento de la norma técnica ISO-IEC 27005 - tecnología de la información y la metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT – versión 3. De igual manera se tuvieron en cuenta los lineamientos de la estrategia GEL del Ministerios de las TIC.

Para realizar el análisis se tuvieron en cuenta las siguientes fases:

- Caracterización del sistema de información
- Medición del riesgo
- Control del riesgo.

En cada una de estas fases se identificaron una serie de características y criterios permitiendo hallar posibles fallas de seguridad que se verían afectadas por el incumplimiento de los objetivos y de esta manera comprometiendo a la Confidencialidad, Integridad y Disponibilidad de la información del SIM y de la entidad. La figura 10, Identificación de riesgo Residual SIM PGN muestra los resultados de las actividades de análisis de riesgos.

Figura 9. Identificación de riesgo Residual SIM PGN



Fuente: autores

6.4.1 Objetivos Análisis de Riesgos. Ejecutar el análisis y gestión del riesgo, aplicado al sistema de información misional SIM, siguiendo la metodología desarrollada permitiendo obtener una serie de pautas el diseño del plan de seguridad informático del SIM.

- Identificar las amenazas, vulnerabilidades y riesgos para cada uno de los activos a evaluar.

- Analizar los riesgos inherentes identificados y la efectividad de los controles aplicados sobre cada uno de ellos.

- Clasificar los riesgos residuales para el desarrollo del plan de seguridad informático del SIM.

6.4.2 Conclusiones Análisis de Riesgos. Con la información obtenida con la realización del análisis y gestión de riesgos, se logró obtener una visión general de cada uno de los activos de información del sistema de información misional SIM, adicionalmente se alcanzó identificar los riesgos que afectan al SIM, así como sus controles y la efectividad de los mismos, el cual servirá como parte del insumo necesario para el diseño del plan de seguridad información del SIM.

Dentro de la información obtenida se pudo llegar a concluir aspectos puntuales:

- Aunque los contratos de mantenimiento y desarrollo son los controles que presentan mayor efectividad, al no mantener una adecuada y constante contratación de dichos servicios, estos pueden llevar a incrementar el número de riesgos identificados para cada activo en los que se ve involucrado.

- Se debe actualizar el sistema operativo del servidor de aplicaciones y base de datos, puesto que en este momento aún están soportados con Windows server 2013; sistema operativo que caduco en el primer semestre del año 2015, quedando sin soporte, sin actualizaciones y expuesto a vulnerabilidades.

- Se deben definir procedimientos para el manejo de información sensible, teniendo en cuenta la confidencialidad, integridad y el no repudio.

- Se pudo evidenciar que la mayor irregularidad en los recursos dispuestos para los controles están focalizados en los activos de hardware y redes de comunicación con un 100% de disponibilidad, razón por la cual para estos

dominios no se gestiona su tratamiento, pero de igual manera deben continuar su monitoreo.

- Los recursos para la ejecución de los controles tienen una irregularidad alta, ya que solo en el 8,33 % de los casos se presenta insuficiencia de recursos.

- Aun cuando el 50% de los controles se encuentra debidamente documentados, este porcentaje sigue siendo bajo ya que el deber ser, es que dicha documentación debe estar documentada al 100 %, para tener por lo menos la evidencia del control en medio físico.

- En la actualidad la entidad se encuentra en renovación de personal (concurso de méritos), este impacta directamente al sistema de información misional, ampliando la posibilidad de ocurrencia de riesgos que se encuentran "controlados". Uno de ellos es "Posible afectación de la disponibilidad e integridad de la información por errores de usuario"; en este caso se debe tener un plan de contingencia junto con la administración para ampliar las campañas de capacitación al momento del ingreso masivo de personal nuevo a la entidad. Posible riesgo EXTREMO.

- La seguridad perimetral es uno de pilares de la entidad, esto se ve reflejado en la efectividad de sus controles. Tal vez su falencia se encuentra en la ausencia de un plan de continuidad del negocio, que hasta el momento se encuentra en los planes de la entidad, pero dada la robustez de la misma se debe contar con un presupuesto muy alto para logar este cometido.

En cuanto a este tema la entidad se tuvo al margen, prefiriendo no entregar información al respecto y solicitando no presentar propuesta ni comentarios del tema.

7. PLANES DE SEGURIDAD INFORMATICA

Un Plan de seguridad es un conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.[18] Teniendo en cuenta esta premisa, ya se cuenta con el conjunto de decisiones necesarias para realizar los planes de seguridad del sistema de información SIM, de igual manera sirviendo como insumo para cualquier otro sistema de información de la Entidad.

Luego de la identificación de riesgos, amenazas y vulnerabilidades se pudo determinar un conjunto de actividades que son importantes que sean realizadas en la Procuraduría, las cuales permitirán alinear las medidas de seguridad existentes con las exigidas y la reducción de los riesgos identificados.

Las actividades se agrupan en un plan de implementación, el cual contiene el riesgo tratado identificado, el objetivo, el tiempo estimado de ejecución, responsable de la implementación y las etapas a ser cubiertas en cada actividad identificada.

De acuerdo con los criterios de aceptación de riesgos definidos en la metodología, los riesgos residuales a los cuales se les realiza un plan de seguridad informática son los siguientes:

Cuadro 5. Riesgos residuales identificados

#	Riesgos identificados	Cod.	Categoría residual
1	Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios	BD-1	ALTO
2	Posible suplantación de usuarios por falta de protección de contraseñas	BD-4	ALTO
3	Posible afectación de la confidencialidad e integridad de la información por suplantación de usuario	APP-8	ALTO
4	Posible afectación de la disponibilidad de los servicios por errores de mantenimiento y actualización	S-2	ALTO
5	Posible uso no previsto por parte de los usuarios por ausencia de políticas para el uso de los recursos	P-3	ALTO
6	Posible afectación en equipos o archivos por uso incorrecto	P-4	ALTO

[18]https://seguridadinformaticaufps.wikispaces.com/Politicas,+Planes+y+Procedimientos+de+Seguridad

	de hardware y software		

Cuadro 5. (Continuación)

#	Riesgos identificados	Cod.	Categoría residual
7	Posible afectación a la confidencialidad, integridad o disponibilidad de los sistemas por extorsión o presión mediante amenazas.	P-6	ALTO
8	Posible afectación en la disponibilidad e integridad del sistema por la manipulación de la configuración.	APP-9	ALTO
9	Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de las mismas en el sistema de información.	APP-3	ALTO
10	Posible afectación de la confidencialidad de la información.	D-5	ALTO

Fuente: autores

Los planes a realizar para tratar estos riesgos son:

- Gestión de vulnerabilidades técnicas
- Gestión de respuesta a incidentes de seguridad informática.
- Concientización sobre seguridad de la información
- Establecer una política de control de acceso, basada en requisitos de negocio.
- Establecer política de adquisición, desarrollo y mantenimiento de los sistemas de información.
- Control de cambios sobre los sistemas
- Política del uso aceptable de los activos
- Clasificación de la información.

7.1 ELABORACION DE LOS PLANES

Para cada actividad se ha elaborado una breve descripción y las tareas a ser desarrolladas.

7.1.1 Gestión de vulnerabilidades técnicas. A continuación se relaciona en el Cuadro 6 el plan para la gestión de vulnerabilidades técnicas.

Cuadro 6. Plan para gestión de vulnerabilidades técnicas

Nombre del plan:	**Gestión de vulnerabilidades técnicas**
Objetivo:	Prevenir el aprovechamiento de las vulnerabilidades técnicas
Riesgo Tratado:	Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de las mismas en el sistema de información.
Ejecutor/Responsable:	Seguridad de la información y administradores del sistema misional
Actividades:	1. Definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica. Los roles a ser empleados pueden ser los siguientes: - Responsable de hacer análisis de vulnerabilidades sobre los activos identificados - Responsable de la remediación de vulnerabilidades técnicas del sistema de información Misional. - Responsables de hacer seguimiento a la remediación y cualquier responsabilidad de coordinación requerida. 2. Definición del recurso que se usará para identificar las vulnerabilidades técnicas pertinentes. La identificación se realiza a través de escaneos periódicos de vulnerabilidades. Estos escaneos pueden ser realizados por herramientas automatizadas como Nessus o QualysGuard. 3. Definición de una línea de tiempo para reaccionar frente a las notificaciones de vulnerabilidades técnicas identificadas. 4. Toma de acciones con respecto a las vulnerabilidades identificadas. Una vez detectada una vulnerabilidad técnica potencial, la Procuraduría debe identificar los riesgos asociados a esa vulnerabilidad y las acciones a tomar. Por ejemplo: realizar

Cuadro 6. (Continuación)

Actividades:	una aplicación de parches sobre el sistema o aplicar otros controles. De acuerdo con la gravedad y urgencia con la que se necesite tratar la vulnerabilidad, es necesario realizar la acción teniendo en cuenta los controles de control de cambios o siguiendo procedimientos de respuesta a incidentes de seguridad de la información, que son relacionados en este proyecto. Procedimientos de respuesta a incidentes de seguridad de la información, que son relacionados en este proyecto. Se recomienda que los parches se prueben y evalúen antes de la instalación, para asegurarse que son eficaces y que no producen efectos secundarios sobre el sistema. Si no hay parches disponibles se recomienda considerar los siguientes controles: a) Bajar o detener servicios relacionados con la vulnerabilidad. b) Adicionar controles de acceso, por ejemplo: un Firewall. c) Incrementar el monitoreo para detectar ataques reales 5. Definición del procedimiento para la gestión de vulnerabilidades técnicas teniendo en cuenta las siguientes actividades: a) Identificación de vulnerabilidades técnicas. b) Priorización. c) Tratamiento del riesgo. d) Verificación de la efectividad de la remediación. 6. Definición de un procedimiento para la realización del seguimiento y evaluación regulares del proceso de gestión de vulnerabilidades, con el fin de asegurar la eficacia y eficiencia. Nota: Como recomendación el proceso de gestión de vulnerabilidades debe ir alineado con las actividades de gestión de incidentes y así tener una base para actuar en caso de que ocurra un incidente debido a una vulnerabilidad detectada.

Fuente: autores

7.1.2. Gestión de respuesta a incidentes de seguridad informática. A continuación se relaciona en el Cuadro 7 el plan para la gestión de respuesta a incidentes de seguridad.

Cuadro 7. Plan de gestión de respuesta a incidentes de seguridad informática

Nombre del plan:	**Gestión de respuesta a incidentes de seguridad informática**
Objetivo:	Actuar de forma eficaz ante la presencia de incidentes de seguridad informática.
Riesgo Tratado:	1. Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de las mismas en el sistema de información. 2. Posible afectación en la disponibilidad e integridad del sistema por la manipulación de la configuración.
Ejecutor/Responsables:	Seguridad de la información, administradores del sistema y jefatura oficina de sistemas.
Actividades:	1. Definición de responsabilidades y procedimientos. Inicialmente se deben definir los responsables para llevar a cabo la gestión de incidentes y que este se pueda comunicar de forma adecuada dentro de la Procuraduría. Se deben tener en cuenta los siguientes procedimientos: - Procedimiento para planificación y preparación de respuesta a incidentes. - Procedimientos para seguimiento, detección, análisis y reporte de eventos de seguridad. - Procedimientos para el registro de los diferentes incidentes - Procedimientos para el manejo de evidencia forense. - Procedimientos para la valoración y toma de decisiones sobre eventos de seguridad y valoración de vulnerabilidades. - Procedimientos para respuesta a incidentes que incluya la recuperación controlada de un incidente y la comunicación con las partes interesadas dentro de la Procuraduría. Estos procedimientos deben asegurar que el personal que maneje los temas relacionados con incidentes sea competentes, de igual forma, se debe establecer un punto de contacto para la detección y reporte de incidentes de seguridad y mantener los contactos apropiados con autoridades, grupos de interés o foros. a) Llevar a cabo análisis forense de seguridad.

	b) Escalar el caso cuando se requiera c) Asegurarse de que todo quede registrado adecuadamente d) Llevar a cabo análisis forense de seguridad. e) Asegurarse de que todo quede registrado adecuadamente f) Comunicar la existencia del incidente a personal interno o externo.

Cuadro 7. (Continuación)

	g) Comunicar la existencia del incidente a personal interno o externo. h) Tratar las debilidades de seguridad que se encontraron que causan o contribuyen a un incidente. i) Una vez el incidente se haya tratado, cerrarlo formalmente y realizar un registro. 6. Registrar las lecciones aprendidas de los incidentes de seguridad. Se debe usar todo el conocimiento aprendido sobre un incidente para poder reducir la posibilidad o impacto de incidentes futuros.

Fuentes: Autores

7.1.3. Concientización sobre seguridad de la información. A continuación se relaciona en el Cuadro 8 el plan para concientización de seguridad de la información.

Cuadro 8. Plan de concientización de seguridad de la información

Nombre del plan:	**Concientización de seguridad de la información**
Objetivo:	Generar cultura de la seguridad de la información entidad.
Riesgo Tratado:	Posible afectación de la confidencialidad e integridad de la información por suplantación de usuario.
Ejecutor/Responsables:	Seguridad de la información, administradores del sistema y jefatura oficina de sistemas.
	1. Generar una campaña de sensibilización al interior de la entidad. Antes de iniciar la campaña de sensibilización se recomienda, crear al interior de la entidad el grupo de seguridad a la información. Etapa de Expectativa: a) Captar la atención de los funcionarios con el fin de lograr

	su receptividad, haciendo uso de los medios con los que actualmente cuenta la entidad a través de; Boletines. Etapa de Ejecución: a) Talleres de sensibilización en las diferentes sedes de la entidad, a través de actividades personalizadas y de iteración, en grupos no mayores a 20 funcionarios.

Cuadro 8. (Continuación)

Actividades:	b) Formación básica, de hasta 3 horas, en componentes técnicos como: divulgación de políticas, delitos informáticos, seguridad de la información, aspectos laborales y legales, ingeniería social. Dicha formación debe cubrir el máximo posible de funcionarios de la entidad y podría ser mayor al 80 % del total de funcionarios. Quienes no pueden asistir a la formación, se le debe entregar la documentación digital y material didáctico utilizado en la campaña. c) Evaluación teórica por medio digital, de los asistentes a la formación básica. Etapa de Divulgación Continua : a) Diseñara y entregar una cartilla digital, cuyos temas sean alusivos a la seguridad de la información y debe estar publicada en la intranet de la entidad para consulta de los funcionarios. b) Para los funcionarios nuevos en la entidad, al momento de realizar la inducción de ingreso que realiza el instituto de estudios del ministerio público (IEMP), se debe incluir un ítem donde trate la importancia de las buenas prácticas de la seguridad de la información, así mismo se debe entregar: material en medio digital y la ubicación de la cartilla en la intranet. c) Actualizar y divulgar constantemente la cartilla y los medios generados en la etapa de expectativa. **Nota:** La campaña puede ser realizada directamente por el grupo de seguridad de la información de la entidad o en su defecto se puede ver la posibilidad de contratar una firma para que adicionalmente a la campaña, se entregue el análisis

Fuente: autores

7.1.4. Establecer una política de control de acceso, basada en requisitos de negocio. A continuación se relaciona en el Cuadro 9 el plan para establecer una política de control de acceso, basada en requisitos de negocio.

Cuadro 9. Plan para establecer una política de control de accesos

Nombre del Plan	**Establecer una política de control de acceso, basada en requisitos de negocio.**
Objetivo:	Controlar la asignación de los derechos de acceso de los usuarios a los recursos de la Entidad.
Riesgo Tratado:	• Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios. • Posible suplantación de usuarios por falta de protección de contraseñas.

Cuadro 9. (Continuación)

Ejecutor/Responsables:	Seguridad de la información, administradores del sistema y jefatura oficina de sistemas.
Actividades:	1. Definir una política sobre control de acceso de usuario Registro de Usuarios: a) Identificación única de usuario (ID), verificación de permisos del usuario para uso de los sistemas, servicios de información y propósitos del negocio. b) Declaración formal y escrita de los derechos de acceso con firma del usuario del entendido de las condiciones y sanciones a que haya lugar en caso de acceso no autorizado. c) Asegurar que los proveedores del servicio no otorguen acceso hasta que el usuario esté autorizado. d) Registro de personas autorizadas para usar el servicio y retiro o bloqueo en caso de cambio de función, de trabajo o retiro de la Entidad. e) Verificar, retirar o bloquear cuentas redundantes de usuario y garantizar que dichas cuentas no se otorguen a otros usuarios. Asignación de Privilegios: a) Sólo se deben otorgan los permisos necesarios para la ejecución de las funciones, presta solicitud del jefe de la dependencia dueña de la información quien es el responsable de autorizar formalmente los privilegios (permisos) o niveles de acceso correspondientes a las cuentas de los usuarios autorizados. b) Manejar una matriz de roles y perfiles por cada sistema de información, aplicación y/o recursos de red. c) Revisión de las autorizaciones para acceso privilegiados a intervalos más frecuentes d) Revisión periódica de cambios en cuentas privilegiadas. e) Revisiones periódicas de los *logs* de auditoria. Manejo de contraseñas de usuarios: Adicionalmente a lo ya establecido por la entidad, lo cual corresponden a cambios de contraseñas periódicamente; longitud y composición de la contraseña; validación con el directorio activo; al ingresar por primera vez se debe cambiar la contraseña con os parámetros establecidos, adicionalmente a todo esto se debe tener en cuenta lo

	siguiente: a) Es responsabilidad de los administradores técnicos, el cambio de contraseñas predefinidas por proveedores o de fábrica inmediatamente después de la instalación de los sistemas o del software. b) No permitir en el sistema iniciar más de una sesión con el mismo usuario.

Cuadro 9. (Continuación)

	c) Como buena práctica se debe promulgar con los funcionarios, boquear el equipo y/o cerrar sesión al momento de retirarse de su puesto de trabajo. d) Los aplicativos, sistemas de información y equipos de cómputo deben tener configurado la desconexión automática de sesión por inactividad cuando transcurran el tiempo determinado establecido. Desactivar los usuarios de los funcionarios al momento de retirarse de la entidad.

Fuente: autores

7.1.5 Establecer política de adquisición, desarrollo y mantenimiento de los sistemas de información. A continuación se relaciona en el Cuadro 10 el plan para establecer política de adquisición, desarrollo y mantenimiento de los sistemas de información.

Cuadro 10. Plan para establecer una política de adquisición, desarrollo y mantenimiento de los sistemas de información

Nombre del plan	**Establecer política de adquisición, desarrollo y mantenimiento de los sistemas de información.**
Objetivo:	Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información.
Riesgo Tratado:	Posible afectación de la disponibilidad de los servicios por errores de mantenimiento y actualización
Ejecutor/Responsable:	Seguridad de la información, administradores del sistema, oficina de sistemas, oficina Jurídica, oficina administrativa y secretaria general.
Actividades:	1. Definir política análisis y requisitos de seguridad de la información. Se debe delimitar los requerimientos funcionales, no funcionales, requerimientos técnicos y los requerimientos de seguridad y control. Esto se debe efectuar teniendo en cuenta la participación de los propietarios de los activos de Información, el grupo de seguridad y terceras partes en caso de ser necesario.

	Análisis y especificación de requerimientos : a) Identificación de los controles que se deben tener en cuenta en los nuevos requerimientos a los sistemas de información. b) Validar los requisitos del sistema para la seguridad de la información y los procesos para su implementarla.

Cuadro 10. (Continuación)

	2. Definir política procesamiento correcto de las aplicaciones. Se debe definir controles de validación de los datos de entrada, del procesamiento interno y de los datos de salida para evitar errores y uso inadecuado de las aplicaciones. Validación Datos de Entrada: a) Se debe validar los diferentes tipos de datos, datos obligatorios, longitud del campo, rangos de razonabilidad, conjuntos de valores válidos, despliegue protegido de valores y reglas del negocio que afecten o sean trasversales a los datos. b) Validar la mayor cantidad de campos de una transacción, validar contra tablas, utilizar datos de transacciones previamente generadas, razonabilidad de fechas, incluir datos de tipo referencial del documento fuente. c) Validación de llaves únicas, llaves foráneas, creación o eliminación de padres e hijos y los *joins* entre las tablas. d) Segregación de funciones y responsabilidades para el personal que participa en el proceso de entrada de datos. e) Generación de pistas de auditoría de las transacciones de creación, modificación y eliminación. f) Revisión periódica del contenido de los campos para confirmar su validez e integridad. Validación Procesamiento Interno: a) Se debe validar que los procesos contenidos en el software de la aplicación sean acordes a los procedimientos que soportan el negocio. b) Validación automática de la ejecución lógica del procesamiento. c) Uso de procedimientos automatizados de los datos recibidos y procesados desde cada una de las fuentes de ingreso. d) Generación de pistas de auditoría de las transacciones de creación, modificación y eliminación. e) Generación automática de reportes de inconsistencias presentadas durante el procesamiento. f) Procedimientos para reportar y reprocesar transacciones que se detectaron fallidas en la ejecución de los procesos. Validación Datos de Salida:

	a) Contrastar la información de salida con los requerimientos y procedimientos establecidos para la aplicación. b) Clasificar la información para identificar los destinatarios de la misma y poder aplicar los controles respectivos a la información privada y confidencial teniendo en cuenta la normatividad vigente. c) Facilidades para generar en forma automática los reportes del sistema. Los reportes manuales deben ser excepcionales

Cuadro 10. (Continuación)

	3. Definir política de seguridad de los archivos del sistema. Control de Software: a) La actualización del software, las aplicaciones y las librerías de los programas sólo debería ser realizadas por administradores técnicos de cada sistema con la debida autorización de la jefatura de oficina de sistemas. b) El software de las aplicaciones y del sistema operativo sólo se deberían implementar luego de la aprobación técnica y funcional. c) Los despliegues de nuevas versiones o liberaciones de software, deben estar documentados y debidamente versionados. d) El almacenamiento de las versiones antiguas de software y la documentación se debe almacenar. aprobación e) Se debe tener en cuenta una estrategia de restauración al estado anterior antes de implementar nuevas versiones o cambios. f) Los sistemas que tengan integraciones con otros sistemas, requieren de la aprobación de cada uno de los líderes técnicos y funcionales de dichos sistemas para su correspondiente despliegue a cualquiera de los ambientes dispuesto ello. Protección de los Datos de Prueba: Los datos de prueba deben ser cuidadosamente seleccionados, protegidos y controlados, por tal motivo la Entidad evitará el uso de base de datos operativas que contenga información personal o catalogada como sensible en el entorno de pruebas, en caso de ser necesarios hacer uso de este tipo de información, se debe retirar o modificar antes de su uso, sin olvidar la cercanidad a los datos operativos. a) Definición de perfiles de usuarios de pruebas. b) La utilización de datos de prueba debe ser autorizada por las jefaturas técnicas y funcionales del sistema involucrado.

	c) Los programas fuente deben estar protegidos en el ambiente de desarrollo de forma que solo el administrador técnico asignado tenga acceso. **Nota:** Toda solicitud de restauración de datos para pruebas (orden de proceso), tendrá un solicitante que en todos los casos debe ser un funcionario de la Entidad. El solicitante debe establecer la vigencia de los datos y será el responsable del borrado de los mismos tan pronto expira la vigencia. Si se requiere aplazar la vigencia de los datos de prueba.

Cuadro 10. (Continuación)

	d) deberá tramitar una nueva orden de proceso con todos los requisitos establecidos. e) El control de las vigencias de los datos de prueba se hará a través de la herramienta que posea la entidad, para lo cual se creará una categoría denominada "Datos de Prueba" que poseerá como mínimo los siguientes datos: ▪ Nombre de la aplicación ▪ Nombre del archivo o librería ▪ Fecha a la que corresponden los datos ▪ Vigencia de los datos ▪ Nombre del responsable de los datos f) Los ambientes de desarrollo y producción se deben mantener independientes y no se permite la transferencia de datos o código fuente del ambiente de desarrollo al de producción. Por otra parte, ningún usuario de desarrollo puede tener cuentas activas en el ambiente de producción. g) Los datos almacenados en el ambiente de prueba, son propiedad del mismo usuario que realiza las pruebas, y por tanto no existen medidas de control distintas que el cumplimiento natural de la confidencialidad que le compete a todos los funcionarios de la Entidad. Dentro de éste ambiente, los Desarrolladores tendrán acceso a los datos únicamente en modo de consulta. Los ambientes de prueba y producción se deben mantener independientes y no se permite la transferencia de datos del ambiente de pruebas al de producción. Por otra parte, los usuarios definidos en este ambiente no deben utilizar la misma contraseña utilizada en el ambiente de producción.

Fuentes: autores

7.1.6 Control de cambios sobre los sistemas. A continuación se relaciona en el Cuadro 11 el plan para controlar los cambios sobre los sistemas.

Cuadro 11. Plan de control de cambios sobre los sistemas

Nombre del plan:	**Control de cambios sobre los sistemas**
Riesgo Tratado:	1. Posible afectación en la disponibilidad e integridad del sistema por la manipulación de la configuración. 2. Posible afectación de la disponibilidad de los servicios por errores de mantenimiento y actualización
Objetivo:	Controlar la asignación de los derechos de acceso de los usuarios a los recursos de la Entidad.
Ejecutor/Responsables:	Seguridad de la información, administradores del sistema y jefatura oficina de sistemas.

Cuadro 11. (Continuación)

Actividades	1. Realizar un procedimiento formal de control de cambios. La introducción de nuevos cambios importantes se debe documentar y hacer cumplir para asegurar la integridad del sistema. En este procedimiento se debe incluir una valoración de riesgos, el análisis de los impactos de los cambios y la especificación de los controles de seguridad. Se debe tener en cuenta los siguiente en el procedimiento: a) Identificación y clasificación de los componentes expuestos a los cambios b) Identificación y clasificación de los posibles cambios a realizar por componentes c) Generar rastros de auditoria ya sean operativos o tecnológicos (logs de los sistemas operativos o de información, bases de datos, sistemas de comunicaciones, herramientas de administración, sistemas transaccionales, sistemas digitales y de voz, y los demás sistemas que requieren ser monitoreados) d) Efectuar un análisis de riesgos del potencial impacto de cada uno de los tipos de cambios determinados, que involucre el impacto en la seguridad de los sistemas y operación de la Procuraduría. e) Planificación y pruebas de los cambios f) Procedimiento formal de aprobación para los cambios propuestos g) Comunicación de los detalles del cambio a todas las personas interesadas implicadas. Implementar un procedimiento de emergencia, incluyendo los procedimientos y las responsabilidades de cancelación y retorno ante un cambio fallido o eventos imprevistos. Los cambios se deben ejecutar cuando existe una razón válida para la Procuraduría ya que pueden generar algún tipo de

	impacto sobre la operación normal de la aplicación del sistema de información.

Fuente: autores

7.1.7 Establecer política de uso aceptable de los activos. A continuación se relaciona en el Cuadro 12 el plan para establecer política de uso aceptable de los activos.

Cuadro 12. Plan para establecer una política de uso aceptable de los activos

Nombre del plan:	**Establecer política de uso aceptable de los activos**
Objetivo:	Establecer los activos existentes con su respectiva clasificación, propietarios y responsabilidades asignadas a los mismos.
Riesgo Tratado:	Posible afectación en equipos o archivos por uso incorrecto de hardware y software
Ejecutor/Responsable:	Seguridad de la información, administradores del sistema y jefatura oficina de sistemas.
Actividades:	1. Definir una política sobre el inventario de los activos: Para esta política se hace necesario realizar y/o actualizar de forma periódica la Matriz de riesgos y el inventario cuantificado de activos informáticos (hardware, software, información), los cuales deben estar clasificados y etiquetados en términos de su valor, requisitos legales, sensibilidad e importancia de los mismos dentro de la Entidad. Inventario de Activos: a) Se debe incluir dentro del inventario toda la información necesaria donde se pueda identificar el tipo de activo, el formato, ubicación, información sobre licencias, el valor para el negocio y su clasificación de seguridad. b) Se debe tener inventario sobre el software, aplicativo y sistema de información que posee la entidad, para ello se hace necesario incluir las características generales y técnicas del software, el contrato al que pertenecen, los datos de la administración técnica y de seguridad. c) Se debe tener inventario de software de producción para servidores y PC´s, para ello se hace necesario incluir sistemas operativos, programas utilitarios, controladores de dispositivos, compiladores, ensambladores, interfaz gráfica, software de oficina y su licenciamiento. d) Inventario de activos físicos para este harán parte los equipos de cómputo, equipos de comunicaciones, medios removibles. La información de debe contener las características y especificaciones técnicas. e) Inventario de personal, este al ser un activo de información, debe existir un registro del personal

	presente en la Entidad, el cual según el decreto 262 de 2000 debe ser administrado por la Secretaría General. Se recomienda que por lo menos 2 veces en el año el Grupo de Seguridad realice una revisión detallada de los inventarios de los activos de información de la Entidad, con el objetivo de verificar que se encuentren actualizados, para asegurar la disponibilidad, confidencialidad e integridad de la información allí relacionada. 2. Propietarios de los activos: Por parte de la administración se deben asignar responsabilidades a aquellos funcionarios o terceros para el

Cuadro 12. (Continuación)

	control de la producción, el desarrollo, el mantenimiento, el uso, servicios de procesamiento y la seguridad de los activos de información garantizando la responsabilidad frente a las restricciones de acceso y controles aplicables. 3. Uso aceptable de los activos: Todos los usuarios de activos informáticos deben cumplir con las políticas con las que actualmente se cuentan al interior de la entidad y las descritas en los planes aquí descritos. 4. Devolución de activos: Todos los funcionarios de la entidad y terceras partes, deben hacer entrega de los activos de información al momento de su traslado a otra dependencia, licencia por comisión o su retiro de la entidad. a) Aquellos funcionarios que manejen información misional de expedientes debe hacer entrega de la misma de manera física y electrónicamente a través del sistema de información misional SIM, dicha entrega debe estar avalada por el jefe inmediato en el formato dispuesto para ello. b) Realizar entrega de los activos físicos, para ser descargado de los vienes a su cargo, esta labor le corresponde a la dependencia almacén e inventarios. c) Se debe hacer entrega de la documentación que soporta el mantenimiento y actualización de equipos de

	cómputo, aplicativos, bases de datos, servidores, sistemas de información entre otros. En caso de tratarse de la finalización de la relación contractual de una tercera parte, ésta debe entregar al Supervisor/Interventor del contrato los elementos asignados, mediante Acta, quien se encargará de obtener el documento de paz y salvo respectivos e informará de dicha finalización a los jefes de las dependencias propietarias de los servicios informáticos que utilizaba el contratista con copia a la Oficina de Sistemas.

Fuente: autores

7.1.8 Establecer política de clasificación de la información. A continuación se relaciona en el Cuadro 13 el plan para establecer política de clasificación de la información.

Cuadro 13. Plan para establecer una política de clasificación de la información

Nombre del plan	**Establecer política de clasificación de la información**
Objetivo:	Proteger la información de la entidad directamente de acuerdo a su nivel de sensibilidad e importancia
Riesgo Tratado:	Posible afectación de la confidencialidad de la información.
Ejecutor/Responsable:	Seguridad de la información, administradores del sistema y jefatura oficina de sistemas.
Actividades:	1. Clasificación de la información: La Entidad debe clasificar la información con el fin de identificar su nivel de valor y criticidad, dicha clasificación debe ir ajustada a la normatividad colombiana vigente y a los parámetros y procedimientos de la Entidad. Esta política de clasificación de la información aplica para toda la información en posesión o bajo el control de la PGN e información recibida por terceros, la cual puede clasificarse en alguna de las siguientes tres (3) categorías de seguridad: pública, privada y reservada de acuerdo con las características que se describen a continuación: **Publica**: "Como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. Por vía de ejemplo, pueden contarse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución,

	y las providencias judiciales debidamente ejecutoriadas; igualmente serán públicos, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno"[19]. (…) Esta información normalmente es transitoria, por esta razón puede ser almacenada en diferentes medios utilizados por la Entidad, pero su copia debe ser controlada. **Privada:** (…) "será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

Cuadro 13. (Continuación)

Actividades	La información semi-privada, será aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales"[20]. (…) Dentro de la entidad esta información se debe mantener almacenada en los medios designados para ello y únicamente tendrán acceso los funcionarios autorizados. **Reservada**: (…) "Que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, Intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensible o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.

[19] CORTE CONSTITUCIONAL. REPUBLICA DE COLOMBIA. Sentencia T-216/04 [en línea], [consultado en marzo de 2015]. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2004/t-216-04.htm

[20] Ibíd.

	El acceso a esta información debe ser estrictamente restringido, basándose en el concepto de "necesidad de saber". La divulgación de esta información, requiere la aprobación de su respectivo dueño y en el caso de terceros, el acuerdo de confidencialidad debe ser debidamente firmado entre la Entidad y el tercero".[21] (…) Para trasportar esta información se debe hacer utilizando medios seguros, encriptados y siempre se debe recibir el acuse de recibo. Su almacenamiento se debe mantener en un medio cifrado y protegido con controles de acceso o bajo llave. Solo deberá tener acceso a ella el dueño de la información o los funcionarios autorizados. 2. Etiquetado y manejo de la información: a) Para la información reservada los responsables deben velar por la adecuada protección de la misma, con el fin de evitar la divulgación no autorizada a otras personas. b) Para la protección adecuada, se recomienda no dejar desatendida la información en ningún momento de tiempo.

8. CONCLUSIONES Y RECOMENDACIONES

- El plan de seguridad informática fue planteado para desarrollarse sobre el sistema de información misional de la Procuraduría, sin embargo, se puede adaptar para otros sistemas de información que se busquen proteger.

- Se debe destacar la importancia de utilizar metodologías organizadas que permitan identificar el estado real de la seguridad para los activos. En el caso del sistema misional de la Procuraduría gracias a las metodologías empleadas se logró identificar debilidades y riesgos que sirvieron como punto de partida para el planteamiento de los planes que permitirán una mejora en la seguridad.

- Es importante entender por qué se necesita proteger la información. En la Procuraduría se maneja información para cumplir con funciones preventivas, de intervención y disciplinaria, por lo tanto, es clave saber cuál es la información sensible y confidencial, donde se encuentra para que se puedan definir los controles necesarios para protegerla.

- Un factor para la implementación de controles es el recurso financiero. Es posible que la Procuraduría requiera de alguna inversión adicional, pero esto

[21] Ibíd.

depende del enfoque adoptado para el desarrollo de los planes. Por lo general, las empresas requieren inversión en seguridad para cumplir con regulación vigente o para proteger la información y aunque no siempre el uso de la inversión garantiza el éxito, es recomendable tener un presupuesto asignado para cumplir con estos fines.

- Se puede asegurar que el establecimiento de un plan de seguridad informática sirve como un primer acercamiento para el conocimiento al interior de la Procuraduría en temas de seguridad de la información y seguridad informática. Para llegar a definir el plan se requirió de diferentes actividades como medir el estado de seguridad y análisis de riesgos. Estas son actividades que se desprenden de estándares o modelos más robustos de seguridad como ISO 27001, COBIT o hasta el modelo propuesto por Gobierno en línea, por lo tanto se puede recomendar a la Procuraduría la implementación de uno de estos modelos y así tener un plan más robusto y organizado de seguridad.

- Para que un plan de seguridad sea efectivo se deben interrelacionar varios factores que son: La tecnología, las personas, las políticas, los procedimientos, el recurso financiero y las regulaciones. Esta interrelación nos indica que un solo factor no es clave para cumplir con la seguridad, cada factor es dependiente de otro y tienen igual importancia para el cumplimiento de una estrategia de seguridad.

- Para el plan planteado sobre la gestión de incidentes de seguridad, se recomienda que la Procuraduría utilice los siguientes eventos posibles:

- Perdida de servicio, equipos o instalaciones
- Fallos o sobrecargas del sistema
- Incumplimiento de políticas o directrices
- Incumplimiento de los acuerdos de seguridad física
- Cambios del sistema no controlados
- Fallos del software o del hardware
- Violaciones de acceso
- Eventos que afecten a la identificación y autenticación de los usuarios
- Eventos que afecten a los derechos de acceso a los datos
- Eventos que afecten a los procedimientos de copias de seguridad y recuperación
- Incidencias que afecten a la gestión de soportes.

- Actualmente la procuraduría cuenta con un mapa de riesgos de institucional y de riesgos de corrupción, pero no se relacionan los riesgos asociados a la seguridad informática. Se recomienda que la Procuraduría implemente una metodología para tratar los riesgos enfocados en seguridad de la información y

seguridad informática o integrarlos con el mapa de riesgos existente. Lo anterior, permitirá tener una visión más amplia de los riesgos identificados sobre los procesos misionales.

BIBLIOGRAFIA

SEGURIDAD INFORMATICA SMR. Definición Seguridad informática. [en línea], [consultado en marzo 2016]. Disponible en: https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Sistemas de gestión de la seguridad de la información. Primera actualización. Bogotá D.C.: ICONTEC, 2013. NTC ISO/IEC 27001.

MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. [en línea], [consultado en Marzo de 2015.]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#Vlo6huKLOW4

PROCURADURIA GENERAL DE LA NACION. REPUBLICA DE COLOMBIA. Sistema de información Misional. Definición de manual del usuario aplicativo SIM. Primera edición. Bogotá D.C 2015.: [citado en marzo de 2015] p 26.

PROCURADURIA GENERAL DE LA NACION. REPUBLICA DE COLOMBIA. Sistema de información Misional. Bogotá DC, 2015, Disponible en: Grupo SIM, Carpeta Contrato N° 179-169 de 2013 - Perfeccionamiento del Sistema de Información Misional de la Procuraduría.

CORTE CONSTITUCIONAL. REPUBLICA DE COLOMBIA. Sentencia T-216/04 [en línea], [consultado en marzo de 2015]. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2004/t-216-04.htm

_____. Objetivos y funciones. Información institucional. Bogotá DC, 2015. Disponible en: http://www.procuraduria.gov.co/

_____. Sistema de información Misional. Guía de capacitación. Bogotá DC, 2015. Disponible en: http://www.procuraduria.gov.co/infosim/media/file/capacitacion/guia/Guia_de_capacitacion.pdf

ANEXOS

Anexo A. Verificación del Estado de Seguridad

A.1 Resumen

Dada la importancia de los sistemas de información dentro de las organizaciones y los avances en la tecnología, estos, aparecen asociados a nuevos riesgos que es necesario evitar, mitigar o minimizar al máximo. Así bien, se debe tener en cuenta que al presentarse riesgos se están comprometiendo los pilares de la Seguridad Informática; la confidencialidad, la integridad y la disponibilidad de los datos, frente a las amenazas de la infraestructura física, de la tecnológica que pueden llegar a ocasionar impactos legales y reputacionales para la entidad.

El Sistema de Información Misional SIM, apoya integralmente las funciones misionales de intervención, disciplinaria y preventiva de la PGN y que entro en producción en todo el país en marzo de 2009. El sistema cuenta con una parte técnica que maneja la oficina de sistemas de la entidad y la parte funcional y de soporte a usuarios, que es manejada por el grupo de administración y apoyo, el Grupo SIM.

Las jefaturas de la oficina de sistemas y el grupo SIM, autorizan realizar la verificación del estado de la seguridad a través de una lista de chequeo la cual se encuentra estructurada y definida bajo la norma ISO 270001 del 2010, agrupando la calificación en 13 dominios:

- Evaluación y Tratamiento del Riesgo
- Política de Seguridad de la Información
- Seguridad de los Recursos Humanos
- Gestión de Activos
- Control de Acceso
- Criptografía
- Seguridad Física y del Entorno
- Seguridad de Operaciones
- Seguridad de las Comunicaciones
- Adquisición, desarrollo y Mantenimiento de Sistemas
- Relaciones con los Proveedores
- Gestión de incidentes de la seguridad informática
- Cumplimiento

A.2 Objetivos

Ejecutar un checklist a los administradores técnicos y funcionales del SIM para lograr obtener una visión generar del estado actual de la seguridad del sistema de información misional SIM, que sirvan como insumo para el diseño del plan de seguridad informática del mismo.

- Aplicar cada uno de los dominios de la norma ISO 27001 de 2013 para el sistema de información misional.

- Analizar el estado actual en que se encuentra la seguridad informática del sistema de información misional.

- Clasificar cada uno de los dominios según el porcentaje de cumplimiento, para cada uno de ellos.

A.3. Resultados por dominio

El primero de los dominios tiene que ver con la **Evaluación y Tratamiento del Riesgo**, donde con un 25 % de cumplimiento es el que corresponde al de menor rendimiento, todo porque actualmente en la entidad ni al interior de grupo sim se tiene una metodología de análisis de riesgos que permita identificar, analizar y tratar los riesgos asociados con el SIM.

En cuanto a las evaluaciones de riesgos para abordar los cambios en los requisitos de seguridad, hace un poco más de dos años que no se realiza el levantamiento ni análisis de riesgos, cuya documentación plasmada en el mapa de riesgos es de carácter general, se mencionan algunas debilidades, pero no la forma como se deben mitigar, por consiguiente se requiere construir un mapa de riesgos específico para el sistema de información misional.

El dominio **Política de Seguridad de la Información**, indica un porcentaje del 83% respecto de las políticas de seguridad de la información, su divulgación, comunicación y aprobación de la dirección. Adicionalmente se puedo identificar que existe en la actualidad un documento de políticas de seguridad de la información, diseñadas, documentadas y encabeza de la oficina de sistemas, pero dicho documento aún no cuenta con una aprobación formar por parte de la dirección.

Dentro del este documento existe un punto específico para los sistemas de información de la entidad, es un punto muy general a la administración funcional de los mismos; a la fecha el sistema de información misional SIM, no cuenta con un documento interno formal con políticas de seguridad de la información.

La **Seguridad de los Recursos Humanos**, si bien la entidad cuenta con la certificación ISO en el proceso de selección de personal, gracias a este proceso no existe riesgo evidente en la fase antes de asumir el empleo, donde se identificaron algunos posibles riesgos corresponde a la fase durante el ejercicio del empleo regulares en políticas y procedimientos organizacionales, puesto que no existe una formación adecuada en concientización y actualización políticas y procedimientos, puesto que a pesar que existe un programa de capacitación funcional sobre el sistema, este se encuentra incompleto ya que se debe enfocar en la seguridad de la información, no existe un procedimiento claro y el personal es insuficiente para cumplir con la demanda de capacitación.

El dominio de **Gestión de Activos** pretende lograr mantener la protección adecuada de los activos de la entidad, permite identificar los dueños para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados. En el documento de políticas y procedimientos de la entidad existe un punto que enmarca la política de medios removibles como respaldo de almacenamiento, pero no se tienen procedimientos para la autorización, instalación y administración controlada de quemadores de CD/DVD, unidades removibles (disquetes) y memorias USB (flash drives) que puedan utilizarse para copiar información del Sistema de Información Misional. Tarea que se hace compleja por el modelo de negocio que se maneja en el SIM, ya que se hace necesario la utilización de medios removibles para el trasporte de información confidencial del sistema. Adicionalmente no existe un procedimiento establecido para cifrar la información digital en tránsito.

El domino de **Criptografía**, muestra un cumplimiento del 50%, respecto de los controles criptográficos, puesto que a pesar que existen certificados digitales para varios servicios del sistema, en algunos otros como el certificado de derechos humanos, se presenta deficiencia en este tema.
Es responsabilidad de la Oficina de Sistemas definir los algoritmos de cifrado más apropiados para ser utilizados en los sistemas de información críticos, con base en un análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad, no repudio así como las tecnologías de cifrado disponibles y los costos relacionados.

Seguridad Física y del Entorno, es el primero de los dos dominios, según el checklist tienen el 100% de cumplimiento, ya que la entidad cuenta con perímetros de seguridad física claramente definidos (paredes, puertas, control de acceso, recepciones en los pisos, circuito cerrado de televisión, entre otros controles) para proteger las áreas que contienen los activos de información. Todas las salidas de emergencia en el perímetro de seguridad cuentan con alarmas sonoras, señales de evacuación y cierre automático de las puertas. De igual manera la entidad cuenta una política de seguridad establecida para este dominio que desarrollarán controles a las áreas restringidas, registro de usuarios, registro de visitantes y las medidas de protección física de los equipos.
Las áreas de Tecnología de Información (TI) con acceso restringido, están protegidas con controles de acceso biométricos que sólo se permite el ingreso a personal autorizado.

El dominio correspondiente a la **Seguridad de las Operaciones**, en cuanto a los procedimientos, operaciones y responsabilidades; cada recurso tecnológico a cargo, deben monitorizar continuamente a través de software especializado, sus servidores, sistemas de almacenamiento, redes, sistemas de información y de respaldo, con el fin de establecer adecuados niveles de capacidad y desempeño en el presente y a futuro. Para proteger la información confidencial contra acceso no autorizado en los sistemas de producción, pruebas y desarrollo; se tienen perfiles de acceso dependiendo de los privilegios a la información.

Con respecto a las copias de respaldo, aun que se realizan con frecuencia semanal y aun que se cuenta actualmente con un contrato de almacenamiento de copias de respaldo con un proveedor externo, no se tiene un procedimiento establecido para realizar pruebas sobre los sistemas de respaldo que permitan verificar que la información se puede recupera.

Finalmente existe una bitácora donde se lleva un registro de los incidentes que se presenten con el sistema, no se evidencia que el log de auditoria refleje en reportes, violaciones o actividades de seguridad que permitan resolver incidentes que involucren actividades no autorizadas, adicionalmente no existe un procedimiento establecido para revisar las bitácoras de logs.

Seguridad de las Comunicaciones, es el segundo de los dos dominios, que según el checklist tienen el 100% de cumplimiento, ya que la entidad cuenta con n controles de conectividad LAN y WAN, tienen ANS en caso de caídas de canales de comunicaciones, la red se encuentra segmentada, de tal forma que se pueda identificar servicios y se cuenta con políticas y procedimientos para la transferencias de información relacionadas con el sistema de información misional.

La **Adquisición, Desarrollo y Mantenimiento de Sistemas;** en este dominio se definen las políticas y procedimientos para mantener la seguridad en los sistemas de información que incluyen sistemas operativos, infraestructura, aplicaciones del negocio, servicios y aplicaciones desarrolladas para usuarios antes del desarrollo e implementación. Todos los requisitos de seguridad se deben identificar en la fase de requisitos de un proyecto y se deben justificar, acordar y documentar como parte de todo el caso del negocio. Esta tarea corresponde a responsabilidades compartidas de varias dependencias de la entidad, entre ellas el grupo SIM y la oficina de sistemas; en la actualidad la Entidad se ha preocupado por mantener al día el sistema y bajo dos (2) contratos de perfeccionamiento se han mejorado la funcionalidad y operatividad del SIM, haciéndolo más amigable y más rápido. En cuanto a la administración de controles de cambios del sistema, esta se encuentra bien documentada, se han establecido procedimientos de control de cambios y mantenimientos de la aplicación. Todas las solicitudes de requerimiento son evaluadas según su impacto y nivel de importancia; teniendo en este dominio un cumplimiento del 68% quedando faltando un 32% correspondiente a los datos de prueba que no existe un procedimiento que asegure el borrado de información de producción usados en ambientes de prueba y desarrollo, adicionalmente no existen controles para usar información confidencial sin enmascarar fuera del ambiente de producción.

El dominio de **Relaciones con los Proveedores** tiene un alto nivel de cumplimiento correspondiente al 86% y donde se requiere asegurar la protección

de los activos de la organización que sean accesibles a los proveedores, para lo cual los funcionarios, contratistas, proveedores y terceros que tengan acceso a los activos de información están obligados a cumplir las políticas de seguridad de la información y comprometidos a reportar a la oficina de sistemas cualquier incidente de seguridad del que tengan conocimiento. Con el propósito de garantizar la confidencialidad e integridad de la información institucional, la entidad suscribe acuerdos de confidencialidad de la información con funcionarios y terceros (proveedores y contratistas).

De esta forma, todos los funcionarios de la entidad y terceras partes quienes realicen labores para la Entidad que involucren el manejo de información a través de medios lógicos o físicos, deben conocer, entender, firmar y aceptar el correspondiente compromiso de confidencialidad e integridad de la información institucional. Actualmente existe una falencia con respecto a la información confidencial que se intercambia del SIM o con los subcontratistas ya que no se encuentra cifrada.

El dominio de **Gestión de incidentes de Seguridad de la Información**, aunque para el sistema de información misional existe una mesa de ayuda exclusiva, donde se recepciona toda clase de solicitudes y estas a la vez son a tendidas directamente por el grupo sim, cuando corresponden a temas meramente funcionales, administrativos y de capacitación. Cuando los temas corresponden a la parte técnica del sistema, como errores del sistema, modificación de información por errores de ingreso de los usuarios y cambios de la plataforma o alguno de sus componentes, estas solicitudes son requeridas por medio de un formato a la oficina de sistemas, quienes manejan la parte técnica, configuración y seguridad del sistema. De igual manera ocurre con los incidentes de seguridad, aunque existe una bitácora donde se lleva un registro de los incidentes que se presenten con el sistema, no se evidencia que el log de auditoria refleje en reportes, violaciones o actividades de seguridad que permitan resolver incidentes que involucren actividades no autorizadas. Adicionalmente no se cuenta con un procedimiento establecido para la revisión de estos logs; la revisión de dichos logs se realiza de manera correctiva, es decir cada vez que se presenta un inconveniente es que se revisan los logs.

En el grupo sim existe una lista de contactos de la parte técnica y funcional del Sistema de Información misional con nombres, números de teléfono para permitir un rápido escalamiento de incidentes, pero no siempre existe disponibilidad de personal para el escalamiento de los incidentes.

Dominio de **Cumplimiento** con el 33% de cumplimiento es uno de los dominios más bajo según los resultados obtenidos; en cuanto al cumplimiento de requisitos legales y contractuales, gracias al modelo de negocio del Sistema de Información Misional, este se encuentra enmarcado bajo una serie de normatividades propias de la función y objetivos de la Procuraduría General de la Nación a través de alguna de sus misiones preventiva, de intervención o disciplinaria. De igual manera el sistema debe responder a cualquier cambio normativo que involucre la participación de la entidad. Es por eso que el SIM, en su diseño, se especificó a partir de las funciones constitucionales asignadas a la entidad en el artículo 277 de la constitución política de Colombia, en ese orden, se tuvo en cuenta la normatividad orgánica vigente al momento de realizarse su desarrollo.

El mayor inconveniente de este dominio se evidencia en cuanto a las revisiones de seguridad de la información, puesto que no se realizan auditorias periódicas al sistema de información para verificar el cumplimiento de las políticas de seguridad de la información, no existe un procedimiento que permita el alcance de cumplimiento del SIM, adicionalmente el documento de políticas de seguridad de la información, diseñadas, documentadas y encabeza de la oficina de sistemas, no ha sido dado a conocer de manera formal a los administradores funcionales del

sistema de información, al parecer porque aún no cuenta con una aprobación formar por parte de la dirección.

A.4 Conclusiones

Con la información obtenida con la realización de la lista de chequeo, se pudo obtener una visión general del estado de seguridad del sistema de información misional SIM, la cual servirá como parte del insumo necesario para el diseño del plan de seguridad información del SIM. Dentro de la información obtenida se pudo llegar a concluir algunas cosas puntuales:

- La entidad cuenta con un documento de políticas de seguridad de la información, pero este no ha sido dado a conocer por completo a los administradores funcionales de los diferentes sistemas de información, ni a los demás funcionarios de la entidad. Adicionalmente el documento no cuenta con una aprobación formar por parte de la dirección, lo que impide su ejecución y cumplimiento.

- Se debe definir un conjunto de políticas para la seguridad de la información propias para el sistema de información misional que posteriormente puede ser extendido a los demás sistemas de información de la entidad. Dicho documento debe ser aprobado por la entidad, publicado y comunicado a los empleados y a las partes externas pertinentes.

- Se deben definir procedimientos para el manejo de información sensible, teniendo en cuenta la confidencialidad, integridad y el no repudio.

- No existe un procedimiento establecido para que se elimine o cambie los derechos de acceso al sistema después de que se le notifica de un retiro o cambio de funciones de los funcionarios.

- La matriz de roles y perfiles que se maneja para dar acceso a las diferentes funcionalidades del sistema se debe redefinir, puesto al parecer se están dando privilegios a usuarios que no corresponden. Adicionalmente se debe incluir dentro de la matriz las funcionalidades de consultas y reportes que genera la aplicación.

Anexo B. Informe de vulnerabilidades SIM

B.1 Resumen

Las vulnerabilidades de seguridad informática han existido desde siempre, en los años 90 la gran mayoría de intrusos ingresan a los sistemas informáticos utilizando técnicas de scanning, ataques de fuerza bruta, probando usuarios, diferentes passwords, ingeniería social y a través de la explotación de vulnerabilidades. Hoy en día el internet y al avance de la tecnología, permiten y brinda una gran cantidad de información sobre como ingresar a los sistemas, servicios virtuales en la nube y plataformas móviles.

El presente informe, pretende mostrar el resultado del análisis de vulnerabilidades realizadas sobre el Sistemas de información Misional SIM, ofreciendo una visión global sobre las posibles vulnerabilidades del sistema. De igual manera se pretende concientizar a la entidad y a los dueños de los activos involucrados sobre de la importancia de las actualizaciones en los sistemas para minimizar los riesgos generados por las vulnerabilidades, adicionalmente determinar los posibles vectores de ataque dentro de la red interna de la entidad que pongan en riesgo la disponibilidad, integridad y disponibilidad de la información

El análisis comprende las siguientes fases: Entendimiento dela infraestructura, pruebas, Medidas Preventivas, Realización de pruebas de vulnerabilidades, Análisis de resultados; no se intentara explotar la vulnerabilidad.

Para la ejecución del análisis de vulnerabilidad se utilizó la herramienta NESSUS, este se compone de una estructura de cliente-servidor y sirve para detectar a través de la red vulnerabilidades en un sistema remoto, ya sea un cliente o un servidor. Existen versiones para GNU/Linux, Mac OS X, Solaris, FreeBSD y para

Windows, en nuestro caso el análisis fue lanzado para la versión Windows desde dos máquinas diferentes, una maquina se encontraba en la red interna de la entidad y otra máquina se encontraba fuera de ella, permitiendo obtener un posible ataque interno o externo al sistema de información.

B.2 Objetivos

- Realizar la ejecución del análisis de vulnerabilidad al servidor donde se encuentra hospedado el sistema de información misional SIM de la Procuraduría General de la Nación, para ello utilizando la herramienta de escaneo opensourse NESSUS.

- Identificar las posibles vulnerabilidades que afecten al sistema de información misional SIM.

- Analizar y clasificar las vulnerabilidades identificadas según su promedio de criticidad respecto de la afectación en el SIM.

B.3 Análisis de Vulnerabilidades

A continuación se muestra el resultado luego de realizar el escaneo de vulnerabilidades sobre el servidor donde se aloja el sistema de información misional SIM, en dicho análisis se identificaron un total de 56 vulnerabilidades, clasificadas según su criticidad de impacto sobre el sistema; Criticas, Altas, Madias, Bajas e Informativas.

B.4 Clasificación de Vulnerabilidades

- **CVE-2013-2344.** Una vulnerabilidad clasificada como crítica, puesto que el control remoto HP Data Protector instalación se ve afectada por múltiples vulnerabilidades que podrían permitir a un atacante remoto obtener privilegios elevados, desencadenando una vulnerabilidad de denegación de servicio, o en

el peor de los casos ejecutar código arbitrario. Se ven afectadas las versiones HP Storage Data Protector v6.2X para Windows 2003/2008, que actualmente corresponde al sistema operativo del servidor y esto puede llegar a ocasionar inconvenientes con la disponibilidad e integridad de la información.

Para dar una solución a esta vulnerabilidad se debe parchar la versión afectada, para lo cual HP dispuso la actualización correspondiente directamente en su sitio web.

- **Nessus Plugin ID: 34460.** De acuerdo la versión, el servidor web remoto es obsoleto. La falta de apoyo implica que no hay nuevos parches de seguridad para el producto se dará a conocer por el proveedor. Como resultado, puede contener vulnerabilidades de seguridad.

Para dar una solución a esta vulnerabilidad se hace necesario quitar el servicio si ya no es necesario. De lo contrario se recomienda actualizar a una nueva versión, si es posible, o cambiar a otro servidor.

- **Nessus Plugin ID: 71215.** Esta vulnerabilidad corresponde a una aplicación que se encuentra alojada en el servidor web (Jenkins), un programa de gestión de trabajos para el sistema. Al permitir acceso no autenticado a la aplicación, cualquier persona puede ser capaz de configurar Jenkins y emplearlo para realizar cambiar es la configuración del sistema.

En la configuración predeterminada, Jenkins no realiza ninguna comprobación de seguridad. Esto significa que cualquier persona que acceda al sitio web puede configurar Jenkins y modificar configuraciones. Aunque esta configuración es aceptable durante la evaluación inicial del software, Jenkins debe ser configurado para autenticar usuarios y hacer cumplir el control de acceso en la mayoría de otras situaciones, especialmente cuando se expone a la Internet.

- **CVE-2005-1794.** Microsoft Terminal Server utilizando el protocolo de escritorio remoto (RDP) 5.2 almacena una clave privada RSA en mstlsapi.dll y lo utiliza para firmar un certificado, que permite a atacantes remotos falsificar claves públicas de los servidores legítimos y llevar a cabo ataques man-in-the-middle.
Para dar solución a esta vulnerabilidad, se debe forzar el uso de SSL como una capa de transporte y por este servicio las reglas or/and. De igual manera se puede seleccionar las conexiones para permitir sólo conectarse a escritorio remoto

desde equipos que se ajusten del nivel de red con autenticación, incluso de doble factor.

- **Nessus Plugin ID: 71215.** Esta vulnerabilidad toma el servicio remoto, encripta el tráfico mediante un protocolo que presenta algunas debilidades. El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Un atacante puede explotar estas fallas para llevar a cabo man-in-the-middle ataques, o para descifrar las comunicaciones entre el servicio y los clientes afectados.

- **CVE-2002-1117.** El host remoto que está ejecutando Microsoft Windows. Es posible acceder a él mediante una sesión NULL (es decir, sin ningún usuario o contraseña). Dependiendo de la configuración, puede ser posible para un atacante sin autenticarse. Esto tiene repercusión sobre la confidencialidad e integridad.
- **Nessus Plugin ID: 57608.** La firma no es necesaria en el servidor SMB remoto. Esto puede permitir man-in-the-middle ataques contra el servidor SMB y puede tener repercusión sobre la confidencialidad, integridad y disponibilidad.

Para dar solución, elimine vulnerabilidad del protocolo SMB por medio de instalar las actualizaciones correspondientes Microsoft de seguridad. De igual manera asegure que el servicio del Servidor de administración esté corriendo bajo una otra cuenta – FUERA del grupo de Administradores de dominio.

- **CVE-2010-0386.** La configuración predeterminada de Sun Java System Application Server 7 y 7 2004Q2 permite el método HTTP TRACE, que hace que sea más fácil para los atacantes remotos robar cookies y credenciales de autenticación a través de un sitio cruz trazado (XST) ataque, un tema relacionado con CVE-2004 -2763 y CVE-2005.

- **CVE-2007-5944.** El servidor web remoto es vulnerable a un ataque de cross-site scripting. Esta vulnerabilidad le permite a los atacantes remotos inyectar secuencias de comandos web o HTML a través de la cabecera HTTP esperar.

- **CVE-2012-0053.** El servidor web que se ejecuta en el host remoto se ve afectada por una Información sobre la vulnerabilidad de la divulgación. Permite a atacantes remotos obtener los valores de HttpOnly las cookies a través de vectores relacionados con un (1) o largo (2) cabecea mal formado junto con secuencias de comandos web diseñado.

La versión del servidor que ejecuta Apache HTTP en el host remoto es afectado por una vulnerabilidad de divulgación de información. Enviar una solicitud de con cabeceras HTTP el tiempo suficiente para superar el límite del servidor hace que el servidor web para responder con un HTTP 400.

B. 5 Conclusiones

Luego de realizar el escaneo de vulnerabilidades, se obtuvo información importante que brinda el conocimiento al cual está expuesto el sistema de información misional en un posible ataque por explotación de alguna de las vulnerabilidades identificadas.

Teniendo en cuenta el análisis se debe adelantar una evaluación detallada y profunda de los componentes de infraestructura para solucionar las vulnerabilidades identificadas, comenzando por aquellos de mayor vulnerabilidad para determinar las áreas específicas en que se requiere asistencia.

Anexo C. Informe Análisis de Riesgos

C.1 Resumen

El acelerado crecimiento de la tecnología de la información y la importancia que los sistemas de información han tomado en las organizaciones, han llevado a estas, a depender de dichos sistemas, provocando que la atención día tras día crezca en torno a los mismos. Los sistemas de información de TI se crean, diseñan y desarrollan a partir de las necesidades de negocio de las instituciones, de sus estrategias misionales y en el caso del sector público se diseñan también desde su normatividad interna y la legislación del estado. Por este motivo la consecución de los objetivos de la entidad depende y van de la mano de sus sistemas de información, por esto se hace necesario garantizar el correcto funcionamiento y la seguridad de los sistemas de información en las instituciones.

Dada la importancia de los sistemas de información, la entidad a través de los administradores técnicos y funcionales designados mediante resolución 114 del 10 de mayo de 2006 autorizan realizar el análisis de riesgos del sistema institucional de información misional SIM; sistema que apoya integralmente las funciones misionales de intervención, disciplinaria y preventiva de la entidad.

En presente informe, muestra el resultado del análisis y gestión de riesgos aplicados al sistema de información misional SIM. Para ello se toma como referencia la metodología que se alinea a la gestión del riesgo en seguridad de la información contenida en el documento de la norma técnica colombiana NTC-ISO-IEC 27005 - tecnología de la información y la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT – versión 3. De igual manera se tuvieron en cuenta los lineamientos de la estrategia GEL del Ministerios de las TIC.

Para realizar el análisis se tuvieron en cuenta las siguientes fases:

- Caracterización del sistema de información
- Medición del riesgo
- Control del riesgo

En cada una de estas fases se identificaron una serie de características y criterios permitiendo hallar posibles fallas de seguridad que se verían afectadas por el incumplimiento de los objetivos y de esta manera comprometiendo a la Confidencialidad, Integridad y Disponibilidad de la información del SIM y de la entidad.

C. 2 Objetivos

Ejecutar el análisis y gestión del riesgo, aplicado al sistema de información misional SIM, siguiendo la metodología desarrollada permitiendo obtener una serie de pautas el diseño del plan de seguridad informático del SIM.

- Identificar las amenazas, vulnerabilidades y riesgos para cada uno de los activos a evaluar.

- Analizar los riesgos inherentes identificados y la efectividad de los controles aplicados sobre cada uno de ellos.

- Clasificar los riesgos residuales para el desarrollo del plan de seguridad informático del SIM.

C.3 Caracterización del Sistema de Información

Para esta primera fase se definieron siete (7) activos de información necesarios para la ejecución de las tareas diarias del sistema, permitiendo con ello identificar para cada uno los riesgos del sistema.

C.4 Medición del Riesgo

Esta fase se evaluar los riesgos identificados, sobre los cuales se determinan la probabilidad y el impacto de los mismos. Para ello, el dueño del proceso identifica

las amenazas, vulnerabilidades y riesgos de cada uno de los activos de información, con el fin de generar el plan de implementación de los controles que aseguren un ambiente informático seguro.

Dentro de los activos se identificaron un total de 48 riesgos, dada la calificación de probabilidad e impacto se clasificaron de acuerdo a su severidad.

- Teniendo en cuenta la política de administración del sistema de información misional SIM, a continuación se relacionan los 23 riesgos inherentes que se identificaron en esta etapa y que por su calificación presentan la mayor severidad quedando tipificados en los niveles "EXTREMO" y "ALTO".

- Con el 22.91 % el activo "Software" es el de mayor número de riesgos identificados, de igual manera es el que presenta el mayor número de riesgos extremos con un total de 3, al igual que el activo "Datos/ Información".

- Luego de la calificación de los riesgos inherentes el riesgo con mayor nivel de severidad "EXTREMO" correspondiente a "posible afectación de la integridad y disponibilidad de la información por abuso de privilegios", del activo software.

- Para cada riesgo identificado se determinó una amenaza, siendo las de tipo "Datos" y "Personas" las de mayor presencia con el 16,66 % para cada una de ellas y en conjunto llegan al 33,32 % del total de las amenazas.

- Las amenazas y los riesgos de tipo "Servicios Internos" fueron las de menor presencia con el 4,6 % dentro de un total de 48 amenazas.

- El riesgo con mayor número de vulnerabilidades identificadas corresponde a "Posible error humano en la protección de la Información debido al insuficiente conocimiento y aceptación de las responsabilidades con la seguridad informática.", con un total de 4 y se encuentra bajo el activo personas.

- Se identificaron un total de 76 vulnerabilidades para los 48 riesgos identificados, presentando un promedio 1,58 % .vulnerabilidades por cada riesgo identificado.

C. 5 Control del Riesgo

Luego de identificar y clasificar los riesgos inherentes en esta etapa se determinan los controles que actualmente se tienen para mitigar los riesgos, con el fin de evaluar su efectividad y la reducción del impacto en caso que el riesgo

se materialice. Finalmente para obtener y clasificar los riesgos residuales para ubicarlos en el mapa de calor, para los que se tipifique en los niveles "EXTREMO" y "ALTO", se deberá gestionar su tratamiento a través del diseño de planes de seguridad.

En la fase de medición, se identificaron en total 48 riesgos inherentes; en la actualidad el 89,58 % de estos tiene aplicación de controles para tratar de mitigarlos; dichos controles son evaluados por cada uno de los riesgo para determinar su efectividad. Luego de la evaluación de efectividad de los riesgos por cada uno de los activos se pudo ultimar lo siguiente:

- **Software [SW].** Para este activo se disminuyeron aquellos riesgos tipificados en el nivel EXTREMO, pasando de 3 a 0 y los riesgos tipificados en el nivel ALTO se mantuvieron en 5.

- El control “Contrato de Mantenimiento y Desarrollo”, es el que presenta mayor efectividad, reduciendo la probabilidad de materialización de la amenaza y pasando de un nivel del riesgo “Posible falta de integridad en el ingreso de la información al sistema” de extremo a medio.

- El 25 % de los controles que se aplicados a este activo corresponden a un tipo de control preventivo.

- Un total de 7 riesgos residuales tipificados en el nivel alto, se incluyen en el diseño de planes de seguridad.

- La amenaza “Errores de mantenimiento / actualización de programas”, cuyo riesgo paso de nivel alto a nivel medio, esto gracias al control que actualmente se aplica para mitigarlo. Pero para dicho riesgo sino se realiza un adecuado monitoreo puede llegar a generar nuevas amenazas y vulnerabilidades puesto que los sistemas operativos de los servidores del SIM caducaron.

- **Servicios Internos [SI].** Los servicios internos son el activo que presenta el menor número de riesgos identificados, luego de aplicar los controles estos se mantienen en los mismo niveles de medición del riesgo (Alto y Bajo), lo que indica que dichos controles no está siendo lo suficiente efectivos para mitigarlos.

- El riesgo identificado como “Posible afectación de la disponibilidad de los servicios por errores de mantenimiento y actualización”, presenta un nivel del riesgo alto, por lo cual se incluye en el diseño de planes de seguridad.

- Este es uno de los activos más variables en la gestión del riesgo, puesto que se depende indirectamente de la administración de riesgos de los demás sistemas de información de la entidad.

- **Hardware [HW].** Se logró identificar 6 riesgos inherentes para este activo, clasificados en los niveles Bajo y Alto, en donde el 33,33 % del total de los riesgos corresponden al nivel Alto, porcentaje relativamente bajo teniendo en cuenta la importancia de dicho activo para desempeño del sistema.

- Los riesgos inherentes identificados en los niveles altos, luego de aplicarles controles, se logró en uno de ellos reducir su impacto en la materialización de la amenaza quedando en un nivel bajo, mientas que para el otro se logró reducir la probabilidad de ocurrencia dejándolo en el nivel bajo.

- Es el primero de dos activos donde se alcanzó reducir los riesgos inherentes a los niveles medios y bajos, dichos niveles son aceptados por la el grupo SIM, claro está, que se deben monitorear constantemente para mantenerlos al margen o bien mitigarlos.

- El 83,33 % de los controles son de ejecutados con el tipo de control preventivo, es por ello que su probabilidad de ocurrencia de amenaza se encuentra categorizada en improbable con el valor 1 como “Nunca se ha materializado la amenaza pero no se descarta su ocurrencia”.

- **Datos / Información [D].** Para este activo se identificaron un total de 8 riesgos, siendo el segundo activo junto con el de personas el de mayor numero de riesgos identificados.

- Junto con el activo de software, los datos fueron los de mayor identificación de riesgos inherentes con el 37,5 % en el nivel extremo, pero luego de aplicar los controles correspondientes para cada uno de ellos se logró mitigar su probabilidad de ocurrencia, reduciendo su nivel a alto y medio.

- De un total de 8 riesgos identificados, solo el 12,5 % va ser parte del proceso de tratamiento a través del diseño de planes de seguridad.

- Dentro de todos los activos, el riesgo “Posible fuga de la información sensible”, fue el que presento la mayor calificación de probabilidad de ocurrencia de la amenaza (INMINENTE). Luego de aplicar los controles se logró reducir su probabilidad a (IMPROBABLE), es decir este riesgo quedo categorizado en el nivel MEDIO indicando que el control aplicado fue un 80% efectivo, porque aun si se llegase a presentar, su impacto está catalogado en nivel 3, pudiendo afectar algunas operaciones del SIM.

- **Servicios Subcontratados [SE].** Este activo no se tuvo en cuenta en el análisis de riesgos, puesto que la entidad manifiesta que las posibles amenazas expuestas a este activo no aplican ya que no se tiene ninguna dependencia de algún tercero debido a que el SIM es el único sistema de información de la entidad vigente y desde su inicio adquirieron todos los derechos y los códigos fuentes, lo que permite no tener ninguna filiación sobre este.

- **Personas [P].** Se logró identificar 8 riesgos inherentes para este activo, clasificados en los niveles Extremo, Medio y Alto, en donde el 62,5 % del total de los riesgos corresponden al nivel Alto y Extremo, porcentaje relativamente alto teniendo en cuenta la importancia de dicho activo para desempeño del sistema.

- El 100 % de los controles utilizados en este activo cuentan con evidencia física electrónica, aun cuando esto es muy bueno, este porcentaje contrasta con el 42,68 %, 1puesto que dichos controles se encuentran parcialmente desactualizados.

- Luego de la ejecución de los controles, se logró reducir el nivel de los riesgos Extremos y Altos, a niveles aceptables para el SIM. Únicamente para este activo se tomaran tres riesgos ya que en este momento cumplen con los niveles de aceptación del riesgo.

- Aun cuando el riesgo “Posible fallo en las operaciones del sistema por indisponibilidad de personal”, que inicialmente se encontró en un nivel Extremo, luego de los controles fue catalogado en nivel Medio; sin embrago se debe realizar un monitoreo continuo sobre este ya que se están modificando el manual de funciones de la entidad impactando directamente las operaciones de los funcionarios del SIM.

- **Redes de Comunicación [COM].** Este activo dentro del análisis presenta 2 riesgos inherentes Altos, al revisar la aplicación de los controles, estos indican que los riesgos fueron clasificados en niveles de aceptación del SIM, para lo cual se diría que ninguno de ellos haría parte del proceso de tratamiento a través del diseño de planes de seguridad, pero esto no es de todo cierto, ya que el riesgo “Posible denegación de servicio por ausencia de pistas de auditoria”, no cuenta con controles para mitigar su probabilidad de ocurrencia. Este riesgo presento un nivel Medio, ya que su probabilidad de ocurrencia es Baja (1), pero su impacto puede llegar a ser considerable y es por ello que será parte de los planes de seguridad.

- A pesar que este activo no presenta riesgos residuales Extremos y Altos, los actuales niveles de los riesgos se podrían disminuir mucho más si se logra disminuir el 75 % de los controles de tipo correctivo a preventivo.

- La gran fortaleza que presentan los controles para este activo son sus recursos, ya que la entidad dentro de sus planes de invención, cuentan con un alto porcentaje en los recursos para este tipo de activo, esto se ve reflejado en la matriz de análisis de riesgos.

- **Instalaciones [L].** Para este activo se identificaron un total de 7 riesgos de los cuales 2 (inherentes) de ellos se encontraron en el nivel Alto, pero luego de aplicar los controles correspondientes se logró mitigar su nivel de severidad, quedando en los niveles aceptables para el SIM, por lo cual para este activo no se tendrá planes de seguridad.

- En los últimos años sobre este activo la entidad ha ejecutado gran cantidad de recursos, es por ello que el 100 % de sus controles ahora son de tipo preventivo, permitiendo con ello reducir aún más los niveles de severidad del riesgo.

- En cuanto a la seguridad física de las instalaciones de la entidad, dada la envergadura de la misma; se cuenta con sistema robusto de seguridad perimetral, al igual que seguridad privada y seguridad policial.

- La efectividad de los controles para este riesgo es alta puesto que para los 7 controles identificados, puesto que sus niveles de severidad se encuentran en Bajo, siendo este activo uno del mejor control de riesgo.

El 12,5 % del total de los riesgos inherentes no cuentan con controles, impidiendo dar cumplimiento al objetivo de control y por consiguiente mitigar los riesgos, teniendo en cuenta la aceptación del riesgo del sistema de información misional SIM, estos de igual manera se deberá gestionar su tratamiento a través del diseño de planes de seguridad.

A continuación se en listan los riesgos que harán parte del proceso de tratamiento a través del diseño de planes de seguridad:

1. Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios. [SW].

2. Posible suplantación de usuarios por falta de protección de contraseñas. [SW].

3. Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de las mismas en el sistema de información. [SW].

4. Posible afectación de la confidencialidad e integridad de la información por suplantación de usuario. [SW].

5. Posible afectación en la disponibilidad e integridad del sistema por la manipulación de la configuración. [SW].

6. Posible afectación de la disponibilidad de los servicios por errores de mantenimiento y actualización. [SI].

7. Posible afectación de la confidencialidad de la información. [D].

8. Posible uso no previsto por parte de los usuarios por ausencia de políticas para el uso de los recursos. [P].

9. Posible afectación en equipos o archivos por uso incorrecto de hardware y software [P]

10. Posible afectación a la confidencialidad, integridad o disponibilidad de los sistemas por extorsión o presión mediante amenazas [P]

C.6 Conclusiones

Con la información obtenida con la realización del análisis y gestión de riesgos, se logró obtener una visión general de cada uno de los activos de información del sistema de información misional SIM, adicionalmente se alcanzó identificar los riesgos que afectan al SIM, así como sus controles y la efectividad de los mismos, el cual servirá como parte del insumo necesario para el diseño del plan de seguridad información del SIM.

Dentro de la información obtenida se pudo llegar a concluir algunas cosas puntuales:

- Aunque los contratos de mantenimiento y desarrollo son los controles que presentan mayor efectividad, al no mantener una adecuada y constante contratación de dichos servicios, estos pueden llevar a incrementar el número de riesgos identificados para cada activo en los que se ve involucrado.

- Se debe actualizar el sistema operativo del servidor de aplicaciones y base de datos, puesto que en este momento aún están soportados con Windows server 2013; sistema operativo que caduco en el primer semestre del año pasado, quedando sin soporte, sin actualizaciones y expuesto a vulnerabilidades.

- Se deben definir procedimientos para el manejo de información sensible, teniendo en cuenta la confidencialidad, integridad y el no repudio.

- Se pudo evidenciar que la mayor regularidad en los recursos dispuestos para los controles están focalizados en los activos de hardware y redes de comunicación con un 100% de disponibilidad, razón por la cual para estos dominios no se gestionar su tratamiento, pero de igual manera deben continuar su monitoreo.

- Los recursos para la ejecución de los controles tiene una regularidad alta, ya que solo en el 8,33 % de los casos se presenta insuficiencia de recursos.

- Aun cuando el 50% de los controles se encuentra debidamente documentados, este porcentaje sigue siendo bajo ya que el deber ser es que dicha documentación debe estar documentada al 100 %, para tener por lo menos la evidencia del control en medio físico.

- En la actualidad la entidad se encuentra en renovación de personal (concurso de méritos), este impacta directamente al sistema de información misional, ampliando la posibilidad de ocurrencia de riesgos que se encuentran “controlados”. Uno de ellos es “Posible afectación de la disponibilidad e integridad de la información por errores de usuario”; en este caso se debe tener un plan de contingencia junto con la administración para ampliar las campañas de capacitación al momento del ingreso masivo de personal nuevo a la entidad. Posible riesgo EXTREMO.

- La seguridad perimetral es uno de pilares de la entidad, esto se ve reflejado en la efectividad de sus controles. Tal vez su falencia se encuentra en la ausencia de un plan de continuidad del negocio, que hasta el momento se encuentra en los planes de la entidad, pero dada la robustez de la misma se debe contar con un presupuesto muy alto para logar este cometido. En cuanto a este tema la entidad se tuvo al margen, prefiriendo no entregar información al respecto y solicitando no presentar propuesta ni comentarios del tema.

Anexo D. Lista de chequeo

D.1 Lista de chequeo para Evaluación y tratamiento del riesgo

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Evaluación y tratamiento del riesgo						
Evaluación de los Riesgos de Seguridad	La evaluación de riesgos debería identificar, cuantificar y priorizar los riesgos frente a los criterios para la aceptación del riesgo y los objetivos pertinentes para el sistema de información. Es conveniente realizar periódicamente las evaluaciones de riesgos para abordar los cambios en los requisitos de seguridad.	¿Se tiene una metodología de análisis de riesgos definida que permita identificar, analizar y tratar los riesgos asociados con el SIM?	No	No se tiene una definida pero se realizó una con el MECI pero no enfocada a seguridad de la información.	0%	25%
		¿Cuándo se hizo el último análisis de riesgos o revisión independiente de la aplicación?	Si	A Finales de diciembre del 2013.	50%	

Fuente: autores

D.2 Lista de chequeo para el dominio de políticas de seguridad

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Políticas de seguridad de la información						
Orientación de la dirección para la gestión de la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	¿Cuenta con una política de seguridad informática aprobada por la dirección y enfocada a proteger la Confidencialidad, disponibilidad e integridad de la información?	Si	Sin comentarios	100%	83%
		¿Cómo y con qué frecuencia son comunicadas las políticas de seguridad informática a empleados, subcontratistas, temporales y/o estudiantes en práctica?	N/A	No existe una programación para comunicar las políticas. Estas se comunican eventualmente	50%	
	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	¿Son actualizadas las políticas de seguridad informática?	Si		100%	

Fuente: autores

D.3 Lista de chequeo para el dominio Seguridad de los recursos humanos

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Seguridad de los recursos humanos						
Antes de asumir el empleo	Se recomienda realizar la verificación de antecedentes en todos los candidatos al empleo, contratistas, y usuarios de terceras partes de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.	¿Cuenta con políticas, estándares y procedimientos para la selección del personal?	Si	Sin Comentarios	100%	70%
		¿Qué tipo de verificaciones se realizan a los empleados?	Si	Antecedentes penales y disciplinario	100%	
		¿Cada cuánto actualiza las hojas de vida de los funcionarios, y las verificaciones realizadas?	Si	Cuando se requiere. Anualmente se pide actualización	100%	
		¿Se realizan verificaciones adicionales para el personal (Ej. Visitas domiciliarias)?	No	Sin Comentarios	100%	
		¿Firman los empleados un convenio de no divulgación o acuerdo de confidencialidad?	Si	Sin Comentarios	100%	
Durante la ejecución del empleo	Se recomienda que exista un proceso disciplinario formal para empleados que han perpetrado una violación a la seguridad.	¿Se establecen medidas disciplinarias para las personas que no cumplen con las políticas de seguridad?	Si	Sin Comentarios	100%	
	Se recomienda que todos los empleados de la organización y, donde sea relevante, contratistas y usuarios de terceras partes reciban formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, relevantes para su función laboral.	¿Tiene un programa formal de capacitación y sensibilización de seguridad relacionada con el sistema de información misional?	Si	Si pero el programa está incompleto.	50%	
		¿Por qué medios y con qué frecuencia se realiza la concientización de seguridad informática?	Si	Correos y medio audiovisual. Se realiza esporádicamente.	50%	
		¿En el programa de capacitación y concientización incluye los contratistas, temporales y/o estudiantes en práctica?	No	Sin Comentarios	0%	
		¿Cómo le da seguimiento o mide la efectividad del programa de capacitación y concientización de seguridad informática?	No	Sin Comentarios	0%	

Fuente: autores

D.4 Lista de chequeo para el dominio de gestión de activos

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Gestión de activos						
Responsabilidad por los activos	Todos los activos sean claramente identificados y es conveniente que se realice y mantenga un inventario de los activos importantes.	¿Mantiene un inventario de hardware, software, información, activos físicos y recursos en donde se procesa la información del Sistema de información misional?	Si	Sin comentarios	100%	32%
		¿Con qué frecuencia se revisa y actualiza el inventario de activos?	N/A	Anualmente se realiza una revisión.	100%	
Clasificación de la información	Se recomienda que la información se clasifique en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.	¿Cuenta con un esquema de clasificación de la información, en términos de su valor utilizado en el sistema misional?	No	Sin comentarios	0%	
		¿Cuáles son los procedimientos para etiquetar (identificar) los informes?	N/A	No existe procedimiento.	0%	
Manejo de medios	Se recomienda que existan procedimientos implementados para la gestión de los medios removibles.	¿Tiene procedimientos para la autorización, instalación y administración controlada de medios removibles que puedan utilizarse para copiar información del Sistema de información misional?	No	Por el modelo de negocio de sistema de información, se hace necesario la utilización de medios removibles.	50%	
		¿Están configurados todos los servidores y estaciones de trabajo para prevenir un *boot up* desde algún dispositivo periférico?	No	Sin comentarios	0%	
		¿Cuáles son los procedimientos para proteger la información confidencial que se almacena en medios de almacenamiento removibles?	N/A	No existen procedimientos	0%	
	Se recomienda eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.	¿Cuenta con procedimientos de borrado y reutilización de medios?	Si	Sin comentarios	100%	
		¿Está cifrada (encrypted) toda la información digital en tránsito?	No	Sin comentarios	0%	
		¿ Cuál es el esquema de cifrado utilizado y servicio de transporte de los medios físicos en tránsito que contienen información confidencial del Sistema de información misional	N/A	No existen esquemas de cifrado para el sistema	0%	

Fuente: autores

D.5 Lista de chequeo para el dominio control de accesos

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Control De Acceso						
Requisitos del negocio para control de acceso	Se recomienda establecer, documentar y revisar una política de control de acceso, basada en requisitos de negocio y seguridad para el acceso.	Existe una política de control de accesos?	No	Sin comentarios	0%	67%
		¿Están todos los funcionarios de planta, temporales y subcontratistas identificados por un nombre de usuario único (User ID)?	Si	Sin comentarios	100%	
		¿En qué casos usan cuentas de usuario (User ID) compartidas?	N/A	Sin comentarios	100%	
		¿Se desactivan los nombres de usuario (User ID) después de un período de inactividad?.	Si	Sin comentarios	100%	
		¿Se usan cuentas con altos privilegios (genéricos o de administración) para la operación de las aplicaciones o recursos que procesan información del Sistema de información misional?	Si	Sin comentarios	100%	
		¿Cómo se controlan las cuentas con altos privilegios usadas en sistemas operativos, bases de datos o que utilizan los procesos automatizados?	N/A	actualmente no se controlan las cuentas con privilegios altos	0%	
		¿Qué controles están implementados para verificar el acceso a los sistemas, bases de datos, redes o plataformas (Ejemplo: declaraciones de responsabilidad, audit trails, revisión de logs, etc.)?	N/A	revisión de logs	100%	
		¿Se encuentra autorizado, protegido y controlado el acceso a archivos del sistema	No	Sin comentarios	0%	
		¿Cómo es protegida la integridad de los archivos críticos del sistema?	Si	Sin comentarios	100%	
Gestión de acceso de usuarios	Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.	¿Existe módulo, menú u opción para la administración de usuarios (User IDs), contraseñas y los derechos de acceso?	Si	Sin comentarios	100%	
Gestión de acceso de usuarios	Se recomienda restringir y controlar la asignación y uso de privilegios.	¿Existe un procedimiento para otorgar, modificar y/o revocar derechos de acceso?	No	Sin comentarios	0%	

D5. (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Gestión de acceso de usuarios	Se recomienda restringir y controlar la asignación y uso de privilegios.	¿Están documentadas las solicitudes para otorgar, modificar y/o revocar derechos de acceso?	No	Sin comentarios	0%	67%
		¿Quién es responsable y cuánto tiempo se requiere para que el administrador de seguridad elimine o cambie los derechos de acceso a los sistemas después de que se le notifica de un retiro o cambio de funciones de los funcionarios?	N/A	El responsable de la administración es el grupo SIM, este se realiza por demanda cada vez que se solicita por el jefe de la dependencia.	0%	
	Se recomienda que la dirección revise los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.	¿Qué procedimiento siguen los gerentes/directivos para revisar y verificar los derechos de acceso de sus funcionarios y cada cuanto lo ejecutan?	No	No existen procedimientos	0%	
Gestión de acceso de usuarios	Se recomienda restringir y controlar la asignación y uso de privilegios.	¿Existe un procedimiento para otorgar, modificar y/o revocar derechos de acceso?	No	Sin comentarios	0%	
		¿Están documentadas las solicitudes para otorgar, modificar y/o revocar derechos de acceso?	No	Sin comentarios	0%	
		¿Quién es responsable y cuánto tiempo se requiere para que el administrador de seguridad elimine o cambie los derechos de acceso a los sistemas después de que se le notifica de un retiro o cambio de funciones de los funcionarios?	N/A	El responsable de la administración es el grupo SIM, este se realiza por demanda cada vez que se solicita por el jefe de la dependencia.	0%	
	Se recomienda que la dirección revise los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.	¿Qué procedimiento siguen los gerentes/directivos para revisar y verificar los derechos de acceso de sus funcionarios y cada cuanto lo ejecutan?	No	No existen procedimientos	0%	

D5. (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Control De Acceso						
Responsabilidades de los usuarios	Se recomienda exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.	¿Cuáles son las reglas mínimas de construcción de las contraseñas?	Si	Sin comentarios	100%	67%
		¿Se visualiza en pantalla el texto real de las contraseñas cuando se digitan?	No	Sin comentarios	100%	
	Se recomienda al menos los siguientes parámetros: -mínimo ocho (8) caracteres, -usar letras y números, -cambiarla con frecuencia, al menos cada 60 días,	Existe un estándar de contraseñas?	Si	Sin comentarios	100%	
		¿Las contraseña se deshabilita después de un número específico de intentos fallidos continuos de conexión? Si es así, ¿cuántos?	Si	Sin comentarios	100%	
		¿Se les obliga a los usuarios a cambiar periódicamente las contraseñas? Si es así, ¿con qué frecuencia?	Si	Sin comentarios	100%	
Control de acceso a sistemas y aplicaciones	Se recomienda que todos los usuarios tengan un identificador único para su uso personal exclusivo, y se recomienda elegir una técnica de autenticación adecuada para sustentar la identidad alegada por un usuario.	¿Se garantiza que cada usuario tenga su propia cuenta de acceso a través de esquema de identificación individual	Si	Sin comentarios	100%	
		¿La aplicación usa servicios compartidos de autenticación (active directory, LDAP, siteminder, single-sign-on, etc.)?	Si	LDAP	100%	
		¿La aplicación bloquea automáticamente las cuentas de usuario que no han tenido actividad en más de 60 días?	No	Sin comentarios	0%	

D.5. (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Control De Acceso						
Control de acceso a sistemas y aplicaciones	Se recomienda que el acceso al código fuente de programas sea restringido.	¿Cómo es controlado el código fuente?	N/A	un funcionario	0%	67%
		¿Se cuenta con un sistema automático para el control de versiones y quien es el responsable?	Si	Sin comentarios	100%	
		¿Cuenta con procedimientos y controles tienen para el paso de versiones a producción?	Si	Sin comentarios	100%	
		¿El software en operación está catalogado?	Si	Sin comentarios	100%	
		¿Las versiones de los programas de producción corresponden a las versiones de programas fuentes catalogadas?	Si	Sin comentarios	100%	

Fuente: autores

D.6 Lista de chequeo para dominio de criptografía

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Criptografía						
Controles criptográficos	Se recomienda desarrollar una política sobre el empleo de controles criptográficos y establecer una gestión de claves para dar soporte al empleo de técnicas criptográficas.	¿La aplicación desarrollada utiliza algoritmos de cifrado (encryption)?	No	Sin comentarios	0%	67%
		¿La aplicación usa certificados digitales o soluciones asimétricas de cifrado (public key technology)?	Si	Sin comentarios	100%	
		¿Cómo se protegen los archivos de configuración, seguridad y contraseñas de usuarios durante el almacenamiento (ejemplo: cifrado, control de acceso, etc.)?	Si	Control de accesos	100%	

Fuente: autores

D.7 Lista de chequeo para dominio de seguridad física y del entorno

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Seguridad física y del entorno						
Áreas seguras	Se recomienda diseñar y aplicar medios de protección física contra daños por incendio, inundación, terremoto, explosión, disturbios civiles, y otras formas de desastre natural o artificial.	¿Están protegidas las instalaciones con sistemas de alarma o de detección de humo y fuego?	Si	Sin comentarios	100%	100%
		¿Están los sistemas contra incendio o alarmas conectados a la central de bomberos o a las autoridades correspondientes?	Si	Sin comentarios	100%	
		¿Están protegidas las instalaciones por sistemas automáticos de supresión de fuego (rociadores/gas inerte)?	Si	Sin comentarios	100%	
		¿Tiene un generador de energía eléctrica de respaldo y por cuanto tiempo soporta la operación?	Si	Soporta un máximo de 3 horas	100%	
Equipos	Se recomienda que el equipamiento se ubique o se proteja para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	¿Existe techo o pisos falsos que puedan ser usados para acceder sin autorización a los centros de datos, cuartos de servidores y/o comunicaciones?	No	Sin comentarios	100%	
		¿Las paredes del exterior de los centros de datos, cuartos de servidores y/o comunicaciones están construidas del piso al techo?	Si	Sin comentarios	100%	
		¿El centro de datos (data center) está identificado desde el exterior?	No	Sin comentarios	100%	
		¿Qué controles de accesos existentes en el centro de cómputo?	Si	Sin comentarios	100%	

D.7 (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Seguridad física y del entorno						
Equipos	Se recomienda que el equipamiento se ubique o se proteja para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	¿El centro de datos (data center) tiene controles de temperatura y humedad?	Si	Sin comentarios	100%	
		¿Se cuenta con un respaldo de fuente de poder (UPS) para los sistemas de cómputo. Cuál es su capacidad de respaldo en minutos?	Si	Sin comentarios	100%	
		¿Están asegurados los racks de las conexiones telefónicas y de los cables de datos?	Si	Sin comentarios	100%	
		¿Quién tiene acceso a los racks de conexiones telefónicas y datos y cómo se autoriza el acceso?	Si	Sin comentarios	100%	
Equipos	Se recomienda que todo aquel equipamiento que contenga medios de almacenamiento se revise para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobre escrito con seguridad antes de su disposición.	¿Se tienen los procedimientos y controles para desechar y/o reutilizar los equipos de cómputo?	Si	Sin comentarios	100%	100%

Fuente: autores

D.8 Lista de chequeo para el dominio de seguridad de las operaciones

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Seguridad de las operaciones						
Procedimientos operacionales y responsabilidades	Se recomienda controlar los cambios en los sistemas e instalaciones de procesamiento de información.	¿Se cuenta con un procedimiento para control de cambios en los servidores y sistemas de procesamiento?	No	Sin comentarios	0%	69%
		¿Se cuenta con el procedimiento de soporte a producción y cambios de emergencia de software en producción?	No	Sin comentarios	0%	
		¿Cómo mantiene informado a los funcionarios de los cambios críticos que puedan tener un impacto en la prestación del servicio del sistema misional?	Si	Con anterioridad se informa por medio del correo institucional o medio audiovisual.	100%	
	Se recomienda supervisar y adaptar el uso de recursos, así como proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	¿Qué alarmas se han implementado para monitorear el estado de la infraestructura tecnológica, que permitan identificar y corregir las fallas oportunamente?	Si	Los responsables de cada recurso tecnológico a cargo, deben monitorizar continuamente a través de software especializado.	100%	
	Se recomienda que los recursos para desarrollo, prueba y producción se separen para reducir los riesgos de acceso no autorizado o los cambios al sistema operacional.	¿Está el ambiente de sistemas en producción segregado, física o lógicamente, de los ambientes de desarrollo de software y realización de pruebas?	Si	Sin comentarios	100%	
		¿Cómo se protege la información confidencial contra acceso no autorizado en los sistemas de producción, prueba y desarrollo?	Si	Se manejan perfiles de acceso dependiendo de los privilegios a la información	100%	
Procedimientos operacionales y responsabilidades	Se recomienda que los recursos para desarrollo, prueba y producción se separen para reducir los riesgos de acceso no autorizado o los cambios al sistema operacional.	¿Está el ambiente de sistemas en producción segregado, física o lógicamente, de los ambientes de desarrollo de software y realización de pruebas?	Si	Sin comentarios	100%	

D.8 (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje cumplimiento
Seguridad de las operaciones						
Procedimientos operacionales y responsabilidades		¿Cómo se protege la información confidencial contra acceso no autorizado en los sistemas de producción, prueba y desarrollo?	Si	Se manejan perfiles de acceso dependiendo de los privilegios a la información	100%	69 %
Protección contra códigos maliciosos	Se recomienda implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto a procedimientos adecuados para concientizar a los usuarios.	¿Qué productos antivirus tienen instalados los equipos personales, portátiles y servidores de la organización	Si	Sin comentarios	100%	
		¿Los usuarios pueden deshabilitar o anular el software y/o actualizaciones del antivirus?	No	Sin comentarios	100%	
Copias de respaldo	Se recomienda hacer regularmente copias de seguridad informática y del software y probarse regularmente acorde con la política de respaldo.	¿Se tiene procedimiento para hacer copias de respaldo (backups) de la información del Sistema de información misional?	Si	Sin comentarios	100%	
		¿Con qué frecuencia se realizan estos respaldos (backups)?	Si	Se realiza un backup semanal	100%	
		¿Con qué frecuencia prueba su sistema de respaldo (backups) para verificar que la información se puede recuperar?		No se realizan pruebas al sistema de respaldo	0%	
		¿Se mantienen los respaldos fuera de sus instalaciones?. Si es así, ¿cubre el contrato o acuerdo de nivel de servicio con el proveedor externo de almacenamiento las responsabilidades de seguridad (incluyendo los controles de acceso físico) y las responsabilidades civiles?	Si	Dentro del contrato se estipulan las responsabilidades penales y civiles	100%	
		¿Conforme los respaldos (backups) llegan a la terminación de su vida programada, ¿se destruyen o se vuelven a utilizar los medios?	N/A	Pasan la bodega de la entidad y se conservan para mantener memoria historica de la entidad	100%	

D.8 (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Seguridad de las operaciones						
Registro y seguimiento	Se recomienda que la grabación de registros de auditoría de actividades de usuario, excepciones, y eventos de seguridad informática sean producidas y guardadas durante un período acordado para ayudar en futuras investigaciones y en la supervisión del control de acceso.	¿Se generan bitácoras (logs) o pruebas de auditoría (audit trails) para todos los sistemas que almacenan o procesan información del Sistema de información misional?	Si	Sin comentarios	100%	69%
		¿Están protegidas las bitácoras (logs) contra acceso o modificación no autorizada?	Si	Sin comentarios	100%	
		¿Las pruebas de auditoría (audit trails) reportan todos los intentos de violaciones al sistema de seguridad, todos los eventos significativos relacionados con seguridad?	No	Sin comentarios	0%	
		¿Cuenta con un procedimiento para revisar las bitácoras de (logs)?	No	Sin comentarios	0%	
		¿La revisión de bitácoras de (logs)? es automática o manual, cada cuento se realiza, quienes realizan la revisión, y que acciones se toman sobre los eventos detectados?	N/A	Manual; se revisa cada vez que se requiere alguna información	50%	
	Se recomienda que los relojes de todos los sistemas de procesamiento de información relevantes estén sincronizados con una fuente de horario confiable acordada.	¿Cuál es el procedimiento para sincronizar todos los relojes de los servidores y dispositivos usados en la prestación del servicio contratado por el Sistema de información misional?	N/A	No existe un procedimiento establecido	0%	
Gestión de la vulnerabilidad técnica	Se recomienda obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluarse la exposición de la organización a tales vulnerabilidades, y tomar medidas apropiadas para gestionar el riesgo asociado.	¿Existe un proceso para la liberación de parches (Service Packs) y actualizaciones (Updates) de configuración para solucionar problemas de seguridad de los sistemas operativos y aplicaciones que procesan información del Sistema de información misional?	Si	Sin comentarios	100%	
		¿Se hacen escaneos periódicos del tráfico de la red y de los componentes de la red/dominio para asegurarse de que no existan vulnerabilidades?	No	Sin comentarios	0%	

Fuente: Autores

D.9 Lista de chequeo para el dominio Seguridad en las comunicaciones

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Seguridad de las comunicaciones						
Gestión de la seguridad de las redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Se cuenta con controles de conectividad LAN y WAN?	Si	Sin comentarios	100%	100%
	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Se tienen ANS en caso de caídas de canales de comunicaciones?	Si	Sin comentarios	100%	
	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	La red se encuentra segmentada, de tal forma que se pueda identificar servicios?	Si	Sin comentarios	100%	
Transferencia de información	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	Se cuenta con políticas y procedimientos para las transferencias de información relacionadas con el sistema de información misional?	Si	Sin comentarios	100%	

Fuente: autores

D.10 Lista de chequeo para el dominio adquisición, desarrollo y mantenimiento

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Adquisición, desarrollo y mantenimiento de sistemas						
Requisitos de seguridad de los sistemas de información	Se recomienda que las declaraciones de requisitos de negocio para nuevos sistemas de información, o mejoras a sistemas de información existentes especifiquen los requisitos para controles de seguridad.	¿Desarrolla sistemas de información o aplicaciones que son integradas al Sistema de información misional?	Si	Sin comentarios	100%	73%
		¿Cuáles son los requerimientos de seguridad que se solicitan para el desarrollo de software?	Si	Sin comentarios	100%	
		¿Se hace validación de los datos de entrada para detectar y reducir el riesgo de errores y prevenir ataques estándar, incluyendo desbordamiento de pila (buffer overflow) e inyección de código (code injection)? • ¿Esto se incluye en la metodología de desarrollo de software?	Si	Sin comentarios	100%	
		¿Tiene procedimientos para la revisión de código fuente? ¿En qué parte del ciclo de vida se ejecuta la revisión?	Si	se hace revisión pero no se tienen procedimientos establecidos	100%	
		¿Cómo protegen las herramientas de desarrollo o utilitarios para prevenir acceso no autorizado en producción?	Si	Sin comentarios	100%	
		¿La información se encuentra en una misma base de datos o servidor común? Si es así, ¿Cómo se mantiene segregada la información?	No	Sin comentarios	100%	
		Si la información del Sistema de información misional está almacenada en una base de datos, proporcione los siguientes detalles: • Tipo de base de datos y número de versión, • Si la información tiene controles de restricción acceso y/o actualización, • Si la información está almacenada en una base de datos en forma cifrada (encrypted).	Si	BD Ocalcle 10g Tiene controles de perfiles de Acceso La Información no está cifrada	100%	

D.10. (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Adquisición, desarrollo y mantenimiento de sistemas						
Seguridad en los procesos de desarrollo y de soporte	Se debe asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	Se supervisa y hace seguimiento de la actividad de desarrollo de sistemas contratados externamente?	Si	Sin comentarios	100%	
Datos de prueba	Se recomienda que los datos de prueba sean seleccionados cuidadosamente, protegidos y controlados.	¿Es usada una base de datos confidenciales vigentes del Sistema de información misional para pruebas fuera del ambiente de producción?	Si	Sin comentarios	0%	
		¿Qué controles se tienen para usar información confidencial sin enmascarar fuera del ambiente de producción?	No	Sin comentarios	0%	
		¿Cuál es el procedimiento que asegura borrar la información de producción usada en los ambientes de prueba o desarrollo?	N/A	N existe procedimiento	0%	

Fuente: autores

D.11 Lista de chequeo para el dominio de relación con proveedores

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Relaciones Con Los Proveedores						
Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	¿Cuántos subcontratistas tiene contratados para el servicio con el Sistema de información misional?	N/A	Un contratista	100%	86%
		¿Firman los terceros un convenio de no divulgación o acuerdo de confidencialidad?	Si	cada vez que se realiza un contrato se firma el acuerdo de confidencialidad	100%	

D.11. (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Relaciones Con Los Proveedores						
Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	¿Que servicios prestan los subcontratistas existentes?	N/A	Mantenimiento y garantia del sistema	100%	86%
		¿Qué tipo de información confidencial del Sistema de informacion misional comparte con los subcontratistas?	N/A	El contratista accede a toda la información registrada en la base de datos pero del ambiente de pruebas	100%	
		¿Qué requerimientos de seguridad informática les solicita a los subcontratistas con los que comparte información confidencial?	N/A	Cambio periodico de la clave de acceso a la red de la entidad	100%	
		¿Está cifrada la información confidencial que se intercambia del Sistema de informacion misional o con los subcontratistas?	No	Sin comentarios	0%	
Gestión de la prestación de servicios de proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Si	Sin comentarios	100%	

Fuente: autores

D.12 Lista de chequeo para el dominio de gestión de incidentes de seguridad de la información

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Gestión de incidentes de seguridad de la información						
Gestión de incidentes y mejoras en la seguridad de la información	Se recomienda que existan mecanismos establecidos para permitir que los tipos, volúmenes y costos de los incidentes de seguridad informática sean cuantificados y supervisados.	¿Existe un procedimiento para reportar, registrar, investigar y escalar incidentes de seguridad informática?	No	Sin comentarios	0%	75%
		¿Existe una lista de contactos del Sistema de información misional con nombres, números de teléfono y siempre disponible para permitir una rápida escalación de incidentes?	Si	existe la lista pero no siempre existe disponibilidad de personal para el escalamiento de los incidentes	100%	

D.12. (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Gestión de incidentes de seguridad de la información						
Gestión de incidentes y mejoras en la seguridad de la información	Se recomienda que existan mecanismos establecidos para permitir que los tipos, volúmenes y costos de los incidentes de seguridad informática sean cuantificados y supervisados.	¿Se toman en cuenta las lecciones aprendidas para futuros incidentes de seguridad?	Si	Sin comentarios	100%	75%
		¿Se sensibiliza a los funcionarios sobre la importancia de reportar incidentes de seguridad?	Si	Sin comentarios	100%	

Fuente: autores

D.13 Lista de chequeo para el dominio Cumplimiento

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Cumplimiento						
Cumplimiento de requisitos legales y contractuales	Se recomienda que todos los requisitos estatutarios, reguladores, y contractuales relevantes y el enfoque de la organización para cumplir estos requisitos sean definidos explícitamente, documentados, y mantenidos al día para cada sistema de información y para la organización.	¿Qué requisitos estatutarios, reguladores y contractuales relevantes aplican para el sistema de información misional?	Si	Ley 743 Ley decreto 262 Ley 200 del 1995	100%	33%
		¿Se ha evaluado el cumplimiento de los requerimientos (Normatividad) que aplican para el servicio contratado por el Sistema de información misional?	Si	Sin comentarios	100%	

D.13. (Continuación)

Requerimiento	Evaluación	Preguntas	Respuesta Corta	Detalles/ Comentarios	Valor	Porcentaje de cumplimiento
Cumplimiento						
Revisiones de seguridad de la información	Se recomienda que el enfoque de la organización hacia la gestión de la seguridad informática y su implementación sea revisado independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.	¿Se hacen auditorías para verificar el cumplimiento de las políticas de seguridad informática aplicadas al sistema misional?	No	Sin comentarios	0%	
		¿Se le da tratamiento a las oportunidades de mejora detectadas?	No	Sin comentarios	0%	
	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	¿Se realizan revisiones periódicas del cumplimiento de procedimientos del alcance de SIM?	No	Sin comentarios	0%	
	Revisión del cumplimiento técnico	Se revisa periódicamente para determinar el cumplimiento con las políticas y normas de seguridad información?	No	Sin comentarios	0%	

Fuente: Autores

Anexo F. Matriz de Riesgos

F.1 Identificación de activos tipo software

Nombre Activo:	*Software - [SW]*
Base de datos Oracle, Aplicación, S.O Servidores, Sistema Operativo de Servidores	

Fuente: autores

F.2 Identificación de riesgos inherentes de activos de software del SIM

Descripción de la amenaza	Aplica / no aplica	Código	Vulnerabilidades identificadas	Riesgo	Probabilidad de materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Abuso de privilegios de acceso	Aplica	BD-1	SW - Asignación errada de los derechos de acceso SW - Ausencia de mecanismos de identificación y autenticación de usuario	Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios	5	3	4	5	Extremo
Errores del administrador	Aplica	BD-2	ORG - Ausencia de procedimiento de control de cambios ORG - Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Posible fallo en el funcionamiento de la base de datos por error del administrador	2	3	4	5	Alto
Caída del sistema por agotamiento de recursos	Aplica	BD-3	ORG - Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Posible pérdida de disponibilidad de almacenamiento del sistema por falta de recursos	3	2	1	2	Medio
Suplantación de la entidad del usuario	Aplica	BD-4	SW - Tablas de contraseñas sin protección	Posible suplantación de usuarios por falta de protección de contraseñas	2	3	4	4	Alto

F.2. (Continuación)

Descripción de la amenaza	Aplica / no aplica	Código	Vulnerabilidades identificadas	Riesgo	Probabilidad de materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Errores de los usuarios	Aplica	APP-2	SW - Interfaz de usuario compleja SW - Configuración incorrecta de parámetros SW - Habilitación de servicios innecesarios	Posible falta de integridad en el ingreso de la información al sistema	4	2	3	3	Extremo
Explotación de Vulnerabilidades de los programas (sw)	Aplica	APP-3	Vulnerabilidades sobre el sistema operativo del servidor de aplicaciones SW - Configuración incorrecta de parámetros	Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de las mismas en el sistema de información	2	4	3	4	Alto
Abuso de privilegios de acceso	Aplica	APP-5	SW - Configuración incorrecta de parámetros SW - Asignación errada de los derechos de acceso	Posible afectación de la integridad de la configuración del sistema por abuso de privilegios	1	2	1	2	Bajo
Errores de mantenimiento / actualización de programas (sw)	Aplica	APP-6	SW - Ausencia de control de cambios eficaz	Posible afectación en la disponibilidad del sistema por actualización de servicios de la aplicación	3	3	3	2	Alto

F.2. (Continuación)

Descripción de la amenaza	Aplica / no aplica	Código	Vulnerabilidades identificadas	Riesgo	Probabilidad de materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Suplantación de la identidad del usuario	Aplica	APP-8	RH - Falta de conciencia acerca de la seguridad	Posible afectación de la confidencialidad e integridad de la información por suplantación de usuario	4	2	3	3	Extremo
Manipulación de la configuración	Aplica	APP-9	SW - Configuración incorrecta de parámetros	Posible afectación en la disponibilidad e integridad del sistema por la manipulación de la configuración.	1	3	3	5	Medio
Denegación de servicio	Aplica	APP-12	SW - Software nuevo o inmaduro SW - Ausencia o insuficiencia de pruebas de software	Posible denegación de servicio por errores en el software	3	3	3	2	Alto

Fuente: autores

F.3 Identificación de riesgo residual para los activos de software del SIM

Cód.	Riesgo	*Control*	*Tipo de control*	*Frecuencia*	*Ejecución*	*Complejidad*	*Documentación*	*Evidencia*	*Desviación*	*Recursos*	*Valor residual probabilidad*	*Valor impacto Residual*	*Riesgo residual*
BD-1	Posible afectación de la integridad y disponibilidad de la información por abuso de privilegios	Asignación de ID únicos de usuarios y roles	Preventivo	Continuo	Automático	Simple	Documentado	Ninguna	Sin desviaciones	Suficientes	2	4	Alto
BD-2	Posible fallo en el funcionamiento de la base de datos por error del administrador	Rollback a los cambios realizados	Correctivo	Esporádico	Manual	Moderado	Sin documentar	Informal	Sin desviaciones	Regulares	2	2	Bajo
BD-3	Posible pérdida de disponibilidad de almacenamiento del sistema por falta de recursos	Liberación de espacio de almacenamiento	Correctivo	Esporádico	Manual	Moderado	Sin documentar	Ninguna	Sin desviaciones	Regulares	3	1	Bajo
BD-4	Posible suplantación de usuarios por falta de protección de contraseñas	No hay controles	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	2	4	Alto
APP-2	Posible falta de integridad en el ingreso de la información al sistema	Contrato de Mantenimiento y Desarrollo	Preventivo	Continuo	Mixto	Complejo	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	2	3	Medio

F.3. (Continuación)

Cód.	Riesgo	*Control*	*Tipo de control*	*Frecuencia*	*Ejecución*	*Complejidad*	*Documentación*	*Evidencia*	*Desviación*	*Recursos*	*Valor residual probabilidad*	*Valor impacto Residual*	*Riesgo residual*
APP-3	Posible explotación de vulnerabilidades técnicas debido a deficiencias en la detección o remediación de las mismas en	No hay controles	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	2	4	Alto
APP-5	Posible afectación de la integridad de la configuración del sistema por abuso de privilegios	Matriz de roles y perfiles	Preventivo	Continuo	Manual	Simple	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	2	Bajo
APP-6	Posible afectación en la disponibilidad del sistema por actualización	Control de cambios y versionamiento de Software	Preventivo	Continuo	Mixto	Moderado	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	1	3	Medio
APP-8	Posible afectación de la confidencialidad e integridad de la	Sensibilización en seguridad de la información	Preventivo	Esporádico	Manual	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones no resueltas	Insuficientes	3	3	Alto
APP-9	Posible afectación en la disponibilidad e integridad del sistema por la	No hay controles	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1	4	Medio
APP-12	Posible denegación de servicio por errores en el software	Contrato de Mantenimiento y Desarrollo	Preventivo	Continuo	Mixto	Complejo	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	1	3	Medio

Fuente: autores

F.4. Identificación de activos tipo Servicios

Nombre Activo:	***Servicios Internos- [SI]***
Directorio Activo, Gestion documental, Web Service SIM-SIRI, Web Service SIM-SIAF	

Fuente: autores

F.5 Identificación de riesgos inherentes de activos de tipo servicio del SIM

Descripción de la amenaza	**Aplica / no aplica**	**Código**	***Vulnerabilidades identificadas***	***Riesgo***	**Probabilidad de materialización de la amenaza**	***Impacto***			***Nivel de riesgo inherente***
						Operacional	***Reputacional***	***Legal***	
Caída del servicio por agotamiento de recursos	Aplica	S-1	ORG - Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información SW - Ausencia de gestión de capacidad	Posible afectación de la disponibilidad de los servicios utilizados por el SIM	2	3	3	1	Bajo
Errores de mantenimiento / actualización de programas (sw)	Aplica	S-2	SW - Ausencia de control de cambios eficaz ORG - Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Posible afectación de la disponibilidad de los servicios por errores de mantenimiento y actualización	3	3	3	2	Alto

Fuente: autores

F.6. Identificación de riesgos residuales de activos de tipo servicio del SIM

Cod.	*RIESGO*	*Controles*	*Tipo de control*	*Frecuencia*	*Ejecución*	*Complejidad*	*Documentación*	*Evidencia*	*Desviación*	*Recursos*	*Valor Probabilidad Residual*	*Valor Impacto Residual*	*Riesgo Residual*
S-1	Posible afectación de la disponibilidad de los servicios utilizados por el SIM	Gestión de capacidad	Correctivo	Esporádico	Mixto	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	2	1	Bajo
S-2	Posible afectación de la disponibilidad de los servicios por errores de mantenimiento y actualización	Contrato de Mantenimiento	Preventivo	Periódico	Manual	Moderado	Documentado	Informal	Con desviaciones resueltas	Suficientes	3	3	Alto

Fuente: autores

F.7 Identificación de activos tipo Hardware

Nombre Activo:	*Hardware - [HW]*
Servidores, PCs de los usuarios	

Fuente: autores

F.8 Identificación de riesgos inherentes de activos de tipo hardware del SIM

Descripción de la amenaza	Aplica / No Aplica	Código	*vulnerabilidades identificadas*	Riesgo	probabilidad materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Errores de mantenimiento / actualización de equipos (hw)	Aplica	HW-1	HW - Ausencia de un eficiente control de cambios en la configuración	Posible afectación de la disponibilidad del servicio por errores de mantenimiento	1	3	3	1	Bajo

F.8. (Continuación)

Descripción de la amenaza	Aplica / No Aplica	Código	*vulnerabilidades identificadas*	Riesgo	probabilidad de materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Caída del sistema por agotamiento de recursos	Aplica	HW-2	HW - Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Posible afectación de la disponibilidad de los equipos por agotamiento de recursos	1	3	2	2	Bajo
Robo	Aplica	HW-3	HW - Almacenamiento sin protección	Posible pérdida trazabilidad de no saber quién accede a qué datos y qué hace con ellos por la manipulación de registros	3	3	3	3	Alto
[D] Avería origen físico.	Aplica	HW-5	HW - Defectos de fabrica	Posible Fallo en el funcionamiento en el servidor	1	3	3	1	Bajo
[D] Corte del suministro eléctrico	Aplica	HW-6	HW - Susceptibilidad a las variaciones de voltaje Falta de respaldo eléctrico	Posible interrupción del servicio por corte de suministro eléctrico	3	4	3	2	Alto
Condiciones de temperatura y/o humedad,	Aplica	HW-7	HW - Susceptibilidad a las variaciones de temperatura	Posible daño en equipos por exceso de calor, exceso de frío, exceso de humedad	1	3	2	1	Bajo

Fuente: autores

F.9 Identificación de riesgos residuales de activos de tipo hardware del SIM

Cod.	*Riesgo*	*Controles*	*Tipo de control*	*Frecuencia*	*Ejecución*	*Complejidad*	*Documentación*	*Evidencia*	*Desviación*	*Recursos*	*Valor probabilidad residual*	*Valor impacto residual*	*Riesgo residual*
Hw-1	Posible afectación de la disponibilidad del servicio por errores de mantenimiento	Procedimiento de control de cambios	Preventivo	Periódico	Manual	Moderado	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	2	2	Bajo
Hw-2	Posible afectación de la disponibilidad de los equipos por agotamiento de recursos	Contrato de mantenimiento	Preventivo	Continuo	Manual	Complejo	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	2	2	Bajo
Hw-3	Posible pérdida trazabilidad de no saber quién accede a qué datos y qué hace con ellos por la manipulación de registros	Campañas sobre la seguridad de la información	Correctivo	Periódico	Mixto	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	1	Bajo
Hw-5	Posible fallo en el funcionamiento en el servidor	Contratos de mantenimientos al hardware	Preventivo	Continuo	Manual	Complejo	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	2	2	Bajo
Hw-6	Posible interrupción del servicio por corte de suministro eléctrico	Ups y planta eléctrica	Preventivo	Periódico	Manual	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	3	3	Medio
Hw-7	Posible daño en equipos por exceso de calor, exceso de frío, exceso de humedad	Contratos de mantenimientos al hardware	Preventivo	Periódico	Manual	Complejo	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	2	2	Bajo

Fuente: autores

F.10 Identificación de activos de tipo Datos

Nombre Activo:	*Datos / Información - [D]*
Información Interna de los Procesos Misionales.	

Fuente: autores

F.11 Identificación de riesgos inherentes de activos de tipo Datos del SIM

Descripción de la amenaza	**Aplica / no aplica**	**Código**	***Vulnerabilidades identificadas***	***Riesgo***	**Probabilidad materialización de la amenaza**	***Impacto***			***Nivel de riesgo inherente***
						Operacional	***Reputacional***	***Legal***	
Modificación de la información	Aplica	D-1	La información se puede modificar dependiendo de la configuración del perfil de usuario	Posible afectación de la integridad por modificación de la información	2	3	3	2	Medio
Robo	Aplica	D-2	La información del sistema se puede descargar por todos los usuarios ORG - Ausencia de procedimiento formal para la autorización de la información disponible al público No hay bloqueos de medios extraíbles	Posible fuga de la información sensible	5	1	4	3	Extremo
Corrupción de la información	No aplica	D-3	RH - Falta de conciencia acerca de la seguridad SW - Configuración incorrecta de parámetros	Posible afectación de la integridad por corrupción de la información	N/A	N/A	N/A	N/A	N/A
Errores de los usuarios	Aplica	D-4	RH - Uso incorrecto de software y hardware SW - Interfaz de usuario compleja Falta de capacitación de los funcionarios	Posible afectación de la disponibilidad e integridad de la información por errores de usuario	4	3	3	2	Medio

F.11. (Continuación)

Descripción de la amenaza	Aplica / no aplica	Código	*Vulnerabilidades identificadas*	*Riesgo*	Probabilidad de materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Divulgación de información	Aplica	D-5	RH - Entrenamiento insuficiente en seguridad ORG - Ausencia de procesos disciplinarios definidos	Posible afectación de la confidencialidad de la información	4	4	3	4	Extremo
Introducción de falsa información	Aplica	D-6	RH - Falta de conciencia acerca de la seguridad RH - Entrenamiento insuficiente en seguridad ORG - Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Posible afectación de la integridad por introducción de la información					
Destrucción de información	Aplica	D-7	SW - Ausencia de copias de respaldo	Posible afectación de la disponibilidad e integridad de la información por destrucción de información	2	2	2	2	Bajo
Espionaje Remoto	Aplica	D-8	RED - Líneas de comunicación sin protección	Posible afectación de la confidencialidad de la información por espionaje remoto	2	3	3	3	Medio

Fuente: autores

F.12. Identificación de riesgos residuales de activos de tipo Datos del SIM

Cod.	*Riesgo*	*Controles*	*Tipo de control*	*Frecuencia*	*Ejecución*	*Complejidad*	*Documentación*	*Evidencia*	*Desviación*	*Recursos*	*Valor residual probabilidad*	*Valor residual impacto*	*Riesgo residual*
D-1	Posible afectación de la integridad por modificación de la información	Estructuración de la matriz de roles y perfiles	Preventivo	Esporádico	Manual	Moderado	Documentado	Física	Con desviaciones resueltas	Regulares	1	3	Medio
D-2	Posible fuga de la información sensible	Articulación de funcionalidades con el módulo de seguridad	Detectivo	Esporádico	Manual	Moderado	Parcialmente / desactualizado	Informal	Con desviaciones resueltas	Insuficientes	1	3	Medio
D-3	Posible afectación de la integridad por corrupción de la información	Campañas sobre la seguridad de la información	Preventivo	Esporádico	Mixto	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	3	Medio
D-4	Posible afectación de la disponibilidad e integridad de la información por errores de usuario	Campañas periódicas de capacitación	Preventivo	Periódico	Mixto	Moderado	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	2	3	Medio
D-5	Posible afectación de la confidencialidad de la información	Circulares internas de la entidad	Preventivo	Continuo	Mixto	Moderado	Documentado	Física / electrónica	Con desviaciones resueltas	Suficientes	2	4	Alto
D-6	Posible afectación de la integridad por introducción de la información	Campañas sobre la seguridad de la información	Preventivo	Esporádico	Mixto	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	2	Bajo
D-7	Posible afectación de la disponibilidad e integridad de la información por destrucción de información	Contrato de backups	Preventivo	Esporádico	Mixto	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	2	Bajo

Fuente: autores

F.13 Identificación de activos de tipo Personal

Nombre Activo:	*Personal - [P]*
usuarios SIM, Servidores PGN	

Fuente: autores

F.14. Identificación de riesgos inherentes de activos de tipo Personal del SIM

Descripción de la amenaza	**Aplica / no aplica**	**Código**	***Vulnerabilidades identificadas***	***Riesgos***	**Probabilidad materialización de la amenaza**	***Impacto***			***Nivel de riesgo inherente***
						Operacional	***Reputacional***	***Legal***	
Indisponibilidad del personal	Aplica	P-1	RH - Ausencia del personal ORG - Ausencia de autorización de los recursos de procesamiento de la información ORG - Ausencia de resolución de adopción del grupo de apoyo al sistema de información	Posible fallo en las operaciones del sistema por indisponibilidad de personal	5	4	3	3	Extremo
Errores de los usuarios	Aplica	P-2	RH - Entrenamiento insuficiente en seguridad RH - Ausencia de mecanismos de monitoreo SW - Asignación errada de los derechos de acceso ORG - Ausencia de procedimientos de identificación y valoración de riesgos ORG - Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Posible error humano en la protección de la Información debido al insuficiente conocimiento y aceptación de las responsabilidades con la seguridad informática.	3	3	2	2	Medio
Uso no previsto	Aplica	P-3	ORG - Ausencia de procedimiento formal para el registro y retiro de usuarios	Posible uso no previsto por parte de los usuarios por ausencia de políticas para el uso de los recursos	3	3	3	3	Alto

F.14. (Continuación)

Descripción de la amenaza	Aplica / no aplic	Código	Vulnerabilidades identificadas	*Riesgos*	Probabilidad de materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Destrucción de información	Aplica	P-4	RH - Uso incorrecto de software y hardware	Posible afectación en equipos o archivos por uso incorrecto de hardware y software	1	3	4	4	Medio
Robo	Aplica	P-5	RH - Trabajo no supervisado del personal externo o de limpieza RH - Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería SW - Asignación errada de los derechos de acceso	Posible robo de equipos e información por falta de supervisión de personal	4	2	3	3	Extremo
Extorsión o presión mediante amenazas, Afectación a la confidencialidad, integridad o disponibilidad de los sistemas de información	Aplica	P-6	RH - Ausencia de mecanismos de monitoreo	Posible afectación a la confidencialidad, integridad o disponibilidad de los sistemas por extorsión o presión mediante amenazas	2	4	3	4	Alto
Ingeniería social o abuso de la buena fe, Obtención de información	Aplica	P-7	RH - Falta de conciencia acerca de la seguridad RH - Entrenamiento insuficiente en seguridad	Posible obtención de información mediante ingeniería social o abuso de la buena fe	3	2	2	3	Medio
Deficiencias en la organización	Aplica	P-8	RH - Falta de conciencia acerca de la seguridad ORG - Ausencia de la resolución de adopción de las políticas de seguridad de la información.	Posible deficiencia en el tratamiento de la Información al interior de la entidad debido a la falta de una coordinación encargada de velar por la seguridad informática.	3	2	4	3	Alto

Fuente: autores

F.15 Identificación de riesgos residuales de activos de tipo Personal del SIM

Cód.	*Riesgos*	*Controles*	*Tipo de control*	*Frecuencia*	*Ejecución*	*Complejidad*	*Documentación*	*Evidencia*	*Desviación*	*Recursos*	*Valor Probabilidad Residual*	*Valor Impacto Residual*	*Riesgo residual*
P-1	Posible fallo en las operaciones del sistema por indisponibilidad de personal	Circulares internas y manual de funciones haciendo alusión al uso obligatorio del Sistema	Preventivo	Continuo	Manual	Simple	Documentado	Física / electrónica	Con desviaciones resueltas	Suficientes	1	3	Medio
P-2	Posible error humano en la protección de la Información debido al insuficiente conocimiento y aceptación de las responsabilidades con la seguridad informática.	Estructuración de la Matriz de Roles y Perfiles	Correctivo	Esporádico	Manual	Complejo	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	3	1	Bajo
P-3	Posible uso no previsto por parte de los usuarios por ausencia de políticas para el uso de los recursos	No existe control	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	3	3	Alto
P-4	Posible afectación en equipos o archivos por uso incorrecto de hardware y software	Configuraciones de equipos según tipo de usuario	Preventivo	Periódico	Mixto	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	4	Medio

F.15. (Continuación)

Cód.	Riesgos	Controles	Tipo de control	Frecuencia	Ejecución	Complejidad	Documentación	Evidencia	Desviación	Recursos	Valor Probabilidad Residual	Valor Impacto Residual	Riesgo residual
P-5	Posible robo de equipos e información por falta de supervisión de personal	Controles de Acceso, cámaras de seguridad y Políticas para uso de correo	Preventivo	Continuo	Mixto	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	3	Medio
P-6	Posible afectación a la confidencialidad, integridad o disponibilidad de los sistemas por extorsión o presión mediante amenazas	Manual de funciones de la entidad y Decreto 262 de 2000, Ley 734 2002	Preventivo	Continuo	Mixto	Moderado	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	1	4	Medio
P-7	Posible obtención de información mediante ingeniería social o abuso de la buena fe	Jornadas extenporaneas en seguridad Informática	Preventivo	Esporádico	Mixto	Moderado	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	1	2	Bajo
P-8	Posible deficiencia en el tratamiento de la Información al interior de la entidad debido a la falta de una coordinación encargada de velar por la seguridad informática.	Solicitudes a la alta direccion acerca del tema	Correctivo	Continuo	Mixto	Complejo	Documentado	Física / electrónica	Con desviaciones resueltas	Suficientes	3	1	Bajo

Fuente: autores

F.16 Identificación de activos de tipo Redes de comunicaciones

Nombre Activo:	***Redes de Comunicaciones - [COM]***
Canales de comunicación	

Fuente: autores

F.17 Identificación de riesgos inherentes de tipo Redes de comunicaciones

Descripción de la amenaza	**Aplica / no aplica**	**Código**	***Vulnerabilidades identificadas***	***Riesgos***	**Probabilidad de materialización de la amenaza**	**Impacto**			**Nivel de riesgo inherente**
						Operacional	**Reputacional**	**Legal**	
Denegación de servicio	Aplica	COM-1	RED - Ausencia de identificación y autentificación de emisor y receptor	Posible denegación de servicio por ausencia de pistas de auditoria	1	4	3	3	Medio
Errores de [re-]encaminamiento	No aplica	COM-2	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Análisis de tráfico	Aplica	COM-3	RED - Tráfico sensible sin protección	Posible Alteración o afectación de la configuración del sistema	1	4	2	2	Medio
Caída del sistema por agotamiento de recursos	Aplica	COM-4	ORG - Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Posible pérdida de almacenamiento por falta de recursos	3	3	3	3	Alto
[D] Corte del suministro eléctrico, interrupción del servicio	Aplica	COM-5	RED - Punto único de falla	Posible interrupción del servicio por corte de suministro eléctrico	3	4	3	2	Alto

F.17. (Continuación)

Descripción de la amenaza	Aplica / no aplica	Código	*Vulnerabilidades identificadas*	*Riesgos*	Probabilidad de materialización de la amenaza	Impacto			Nivel de riesgo inherente
						Operacional	Reputacional	Legal	
Vulnerabilidades de los programas (sw)	Aplica	COM-6	Vulnerabilidades sobre el sistema operativo del servidor de aplicaciones RED - Líneas de comunicación sin protección	Posible explotación de vulnerabilidades técnicas	1	4	2	4	Medio

Fuente: autores

F.18 Identificación de riesgos residuales de tipo Redes de comunicaciones

Cod.	Riesgos	Controles	Tipo de control	Frecuencia	Ejecución	Complejidad	Documentación	Evidencia	Desviación	Recursos	Valor probabilidad residual	Valor Impacto residual	Riesgo residual
Com-1	Posible denegación de servicio por ausencia de pistas de auditoria	No hay controles	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1	3	Medio
Com-2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Com-3	Posible alteración o afectación de la configuración del sistema	Procedimiento para la revisión de trafico	Correctivo	Esporádico	Manual	Complejo	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	2	Bajo
Com-4	Posible pérdida de almacenamiento por falta de recursos	Liberación de espacio de almacenamiento	Preventivo	Esporádico	Manual	Moderado	Sin documentar	Ninguna	Sin desviaciones	Regulares	2	3	Medio

F.18. (Continuación)

Cod.	Riesgos	Controles	Tipo de control	Frecuencia	Ejecución	Complejidad	Documentación	Evidencia	Desviación	Recursos	Valor probabilidad residual	Valor Impacto residual	Riesgo residual
Com-5	Posible interrupción del servicio por corte de suministro eléctrico	Ups y planta eléctrica	Correctivo	Esporádico	Manual	Moderado	Parcialmente / desactualizado	Física / electrónica	Con desviaciones resueltas	Regulares	1	2	Bajo
Com-6	Posible explotación de vulnerabilidades técnicas	Firewall, antivirus	Correctivo	Continuo	Mixto	Moderado	Parcialmente / desactualizado	Física / electrónica	Sin desviaciones	Regulares	1	1	Bajo

Fuente: autores

F.19 Identificación de activos tipo instalaciones

Nombre Activo:	Instalaciones / Infraestructura Física - [L]
Instalaciones de la procuraduría, Data Center	

Fuente: autores

F.20 Identificación de riesgos inherentes para activos tipo instalaciones

Descripción de la amenaza	Aplica / no aplica	Código	*Vulnerabilidades identificadas*	*Riesgos*	Probabilidad de materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Fallo de identificación y autenticación, acceso no autorizado equipos, aplicaciones, archivos	Aplica	L-1	Lug - uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Acceso no autorizado a las instalaciones físicas	1	5	3	5	Medio

F.20. (Continuación)

Descripción de la amenaza	Aplica / no aplica	Código	*Vulnerabilidades identificadas*	*Riesgos*	Probabilidad de materialización de la amenaza	*Impacto*			*Nivel de riesgo inherente*
						Operacional	*Reputacional*	*Legal*	
Ataque destructivo,disponibilidad de equipos, soportes o archivos	Aplica	L-2	Lug - ausencia de protección física de la edificación, puertas y ventanas	Posible afectación de la disponibilidad del sistema	1	3	2	2	Bajo
Ocupación enemiga instalaciones, perdida de equipos, soportes o archivos	Aplica	L-3	Org - ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad Org - ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Posible alteración o afectación de la integridad y disponibilidad	1	4	3	3	Medio
[d] fuego, daño a equipos, archivos o documentos	Aplica	L-4	Org - ausencia de planes de continuidad	Posible afectación en equipos o archivos	1	4	5	5	Alto
[d] al agua, daño a equipos, archivos o documentos	Aplica	L-5	Org - ausencia de planes de continuidad	Posible afectación en equipos o archivos	1	4	5	5	Alto
[d] a desastres industriales, daño equipos o archivos (muy poco probable)	Aplica	L-6	Org - ausencia de procedimientos para el manejo de información clasificada	Posible afectación de la disponibilidad del sistema	1	4	4	4	Medio
[d] desastre natural, daño a equipos, archivos o documentos	Aplica	L-8	Org - ausencia de planes de continuidad	Posible afectación de disponibilidad	1	4	3	2	Medio

Fuente: autores

F.21 Identificación de riesgos residuales para activos tipo instalaciones

Cod.	*Riesgos*	*Controles*	*Tipo de control*	*Frecuencia*	*Ejecucion*	*Complejidad*	*Documentacion*	*Evidencia*	*Desviación*	*Recursos*	Valor probabilidad residual	Valor Impacto residual	*Riesgo residual*
L-1	Acceso no autorizado a las instalaciones físicas	Controles de acceso y cámaras de seguridad	Preventivo	Continuo	Mixto	Simple	Documentado	Física / electrónica	Con desviaciones resueltas	Suficientes	1	1	Bajo
L-2	Posible afectación de la disponibilidad del sistema	Contrato de seguridad privada a instalaciones y seguridad policial	Preventivo	Continuo	Mixto	Complejo	Documentado	Física / electrónica	Con desviaciones resueltas	Suficientes	1	1	Bajo
L-3	Posible alteración o afectación de la integridad y disponibilidad	Seguridad policial	Preventivo	Continuo	Mixto	Complejo	Documentado	Física / electrónica	Sin desviaciones	Suficientes	1	1	Bajo
L-4	Posible afectación en equipos o archivos	Sistemas antifuego	Preventivo	Continuo	Mixto	Complejo	Documentado	Física / electrónica	Sin desviaciones	Insuficientes	1	1	Bajo
L-5	Posible afectación en equipos o archivos	Data center de respaldo	Preventivo	Continuo	Mixto	Complejo	Documentado	Física / electrónica	Sin desviaciones	Insuficientes	1	1	Bajo
L-6	Posible afectación de la disponibilidad del sistema	Sgc	Preventivo	Continuo	Mixto	Complejo	Documentado	Física / electrónica	Con desviaciones resueltas	Regulares	1	1	Bajo
L-8	**Posible afectación de disponibilidad**	Seguridad policial	Preventivo	Continuo	Mixto	Complejo	Documentado	Física / electrónica	Con desviaciones resueltas	Suficientes	1	1	Bajo

Fuente: autores