IDENTIFICACIÓN DE VULNERABILIDADES DE SEGURIDAD EN EL CONTROL DE ACCESO AL SISTEMA DE GESTIÓN DOCUMENTAL, MEDIANTE PRUEBAS DE TESTEO DE RED EN LA EMPRESA INGELEC S.A.S

HENRY ALDEMAR GUERRERO ERAZO
LORENA ALEXANDRA LASSO GARCES
PAOLA ALEXANDRA LEGARDA MUÑOZ

Proyecto de Investigación

Asesor
Harold Emilio Cabrera Meza
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERÍA
INGENIERIA DE SISTEMAS
PASTO
2015

Nota de aceptación:

Firma presidente del jurado

Firma del jurado

Firma del jurado

San Juan de Pasto 10 de Marzo de 2015

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

El proyecto de investigación busca la realización de pruebas de testeo a la red de datos para el diagnóstico de vulnerabilidades en el control de acceso al Sistema de Gestión Documental de la empresa INGELEC S.A.S, de acuerdo al dictamen revelado se ejecuta la evaluación y su impacto, con lo anterior se formaliza un planteamiento de estrategias de mitigación de riesgos encontrados para la prevención y fortalecimiento de la seguridad en el control de acceso del Sistema de Gestión Documental.

Se empleó la aplicación de software libre OpenVAS (Sistema Abierto para Evaluación de Vulnerabilidades), el cual permite evidenciar la seguridad y las vulnerabilidades existentes en los sistemas de información.

ABSTRACT

The research project aims at testing a data network for the diagnosis of vulnerabilities in the Document Management System Access Control of the Company INGELEC SAS, according to the revealed opinion the assessment and its impact is executed, with the above an approach to risk mitigation strategies found for the prevention and strengthening the security in the Document Management System access Control is formalized.

Free software application Open Vas (Open Vulnerability Assessment System), was used which allows to demonstrate the safety and existing vulnerabilities in information systems

1. INTRODUCCIÓN

La información es el activo más importante de las organizaciones, para lo cual las personas encargadas de la seguridad de los sistemas informáticos, deben establecer procedimientos y herramientas eficientes para el envío de datos de una forma segura.

La seguridad de la información es una responsabilidad y compromiso misional de gran relevancia intrínseca de las organizaciones según sea la actividad económica a la que se dedican: públicas, privadas o de cualquier otra naturaleza, razón por la cual se debe adoptar los mecanismos esenciales para la protección de la información y no estar expuesta a ataques informáticos. La proyección de la seguridad en una empresa crea certidumbre y viabilidad.

La insensibilidad en los controles y uso inadecuado de la información en las organizaciones ocasiona que tengan mayor probabilidad a ser vulnerados sus sistemas. Los delincuentes informáticos no solo atacan grandes empresas, regularmente son atacadas pequeñas empresas por personal interno que las constituyen.

Para lograr la mitigación de los riesgos de seguridad presentes en una organización es imperiosa la ejecución de pruebas de testeo a la red de datos y lograr diagnosticar las vulnerabilidades existentes en los sistemas de información, efectuando la evaluación de las mismas y el planteamiento de estrategias de mitigación de los riesgos hallados para la prevención y mejora de la seguridad en el control de acceso fundamentado en los estándares actuales (ISO/IEC 27002).

2. ASPECTOS GENERALES

2.1 TITULO

Identificación de vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental, mediante pruebas de testeo de red en la empresa INGELEC S.A.S

2.2 DEFINICIÓN DEL PROBLEMA

La información es un recurso que, como el resto de los activos, tiene valor para INGELEC S.A.S y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los servicios prestados por el servidor de gestión documental, minimizando los riesgos de daño y contribuyendo de esta manera, a un mejor desempeño en sus procesos que contribuya a la calidad del servicio de energía.

En el servidor de gestión documental, se maneja información clasificada en financiera, comercial, reportes al SUI (Sistema Único de Información de Servicios Públicos), correspondencia interna y externa, la cual es de vital importancia, ya que si es expuesta a terceros se ve afectada en los tres pilares de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

INGELEC S.A.S no tiene implementada estrategias de mitigación de riesgos en el Sistema de Gestión de Seguridad de la Información, para hacer análisis, control y optimización demandadas por la ISO/IEC 27002, logrando atenuar los riesgos relacionados con la seguridad informática. Existen varios tipos de amenazas que ponen en riesgo los servicios prestados por el sistema de gestión documental, lo cual podría causar daños en los procesos de producción y administrativos de la empresa.

2.3 JUSTIFICACIÓN

De acuerdo a la Ley 1581 de 2012 y el Decreto 1377 de 2013, las entidades públicas y empresas privadas están obligadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas. Por esta razón es importante que el sistema de gestión documental - SGD de la empresa INGELEC que contiene información financiera, comercial, de reportes al SUI (Sistema Único de Información de Servicios Públicos), correspondencia interna y externa, sea un sistema vital para la empresa el cual se obliga a ser protegido.

Al aplicar un reconocimiento de vulnerabilidades al SGD permitirá evaluar sus condiciones de seguridad lo cual permitirá plantear un plan de mitigación de vulnerabilidades que a presente y futuro mantenga un sistema de gestión de la información confiable, íntegra y disponible que además prevendrá los riesgos a los cuales estaría expuesto.

2.4 OBJETIVOS

2.4.1 objetivo general

Identificar vulnerabilidades de seguridad en el control de acceso al sistema de gestión documental (SGD), mediante pruebas de testeo de red en la empresa INGELEC S.A.S.

2.4.2 objetivos específicos

- Realizar pruebas de testeo a la red de datos que permita diagnosticar las vulnerabilidades en el control de acceso al sistema de gestión documental de la empresa INGELEC S.A.S.

- Evaluar las vulnerabilidades encontradas de acuerdo a los riesgos detectados en las pruebas de testeo de red y su impacto en el SGD.

- Plantear estrategias de mitigación de los riesgos encontrados para prevenir y fortalecer la seguridad en el control de acceso del SGD.

3. MARCO REFERENCIAL

3.1 MARCO LEGAL

3.1.1 Legislación de Seguridad Informática en Colombia

3.1.1.1 Ley 1581 de 2012 y el Decreto 1377 de 2013 [1]

La Ley 1581 de 2012 y el Decreto 1377 de 2013, sentencian disposiciones para la protección de información personal almacenada en una base de datos donde se efectué procedimientos de agregar, eliminar, modificar y actualizar por parte de empresas del sector público y privado.

Dicha Ley exige a las empresas públicas y privadas examinar la utilización de los datos personales depositados en los sistemas de información y modificar las políticas de seguridad de la información con las herramientas tecnológicas apropiadas debido al auge de los flujos de información en la actualidad.

El decreto 1377 de 2013, facilita el acatamiento de la Ley 1581 regulando aspectos concernientes al manejo de la información personal.

3.1.1.1.1 Propósito de la ley 1581 de 2012 y el Decreto 1377 de 2013[2]

El Decreto 1377 tiene como objetivo facilitar la implementación y el cumplimiento de la Ley 1581 reglamentando aspectos relacionados con la autorización del titular

[1]CONGRESO DE LA REPÚBLICA. Diario Oficial No. 48.587 de 18 de octubre de 2012.Ley estatutaria 1581 de 2012. Disponible en: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html/>

[2]Certicámara. La Ley obliga a todas las entidades públicas y empresas. Disponible en: <https://web.certicamara.com/productos-y-servicios/consultor%C3%ADa-en-protección-datos-personales/ >

de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros.

3.1.2 Ley 594 de 2000[3]

El Sistema de Información de Gestión Documental se rige en la Ley 594 de 2000, (Ley General de Archivos) que reglamenta la administración de la documentación en Colombia, se aplica en las tres ramas del poder público. El fin es alcanzar el tratamiento integral y mejorar la gestión de archivos. Comprendiendo el ciclo de la documentación desde la producción, el trámite y la disposición final para su preservación o supresión.

3.1.3 INGELEC S.A.S

La Empresa: INGELEC S.A.S nace en Septiembre de 1.998 en la Ciudad de Santiago de Cali, ante la necesidad de búsqueda de oportunidad laboral que aplique la Profesión de su Gerente y los conocimientos adquiridos con anterioridad en algunas Empresas donde se desempeñó como funcionario.

Inicialmente la Empresa contó con una vinculación directa en el área de telecomunicaciones, participando en proyectos de ampliación de redes telefónicas y comercialización de productos de telefonía. De igual manera, cuando no hubo la suficiente oferta en este campo, situación común en la época de surgimiento de la Empresa en la ciudad de Cali, se iniciaron contactos con distribuidores de materiales eléctricos; a quienes se asesoraba en diferentes proyectos de construcción de electrificación urbana y rural. Sin embargo, pese a grandes

[3]CONGRESO DE LA REPÚBLICA. Diario Oficial 44084 del 14 de julio de 2000. Ley 594 de 2000. Disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4275>

esfuerzos, la crisis de esta Ciudad motivó el desplazamiento hacia la Ciudad de Pasto en el año 2.000, donde se empezó de inmediato a recibir ofertas para la elaboración de planos eléctricos, construcciones de redes eléctricas de media y baja tensión.

Una vez radicada la Empresa en la Ciudad de Pasto, se comienza a fortalecer el campo de redes eléctricas; área en la cual, la experiencia de su Gerente en otras ciudades y su formación académica, motivó a varios de los clientes a seleccionar a INGELEC S.A.S, para el desarrollo y ejecución de los proyectos, destacándose por la entrega a tiempo de las obras y calidad en los servicios.

Desde entonces, la Empresa se dedica a la búsqueda de oferta y a la ejecución de contratos para la construcción de redes eléctricas, construcción de sistemas de cableado estructurados, Ejecución de actividades de control de pérdidas y la Administración, Operación y Mantenimiento de Centrales Hidroeléctricas y/o Sistemas de Bombeo.

En el mes de Agosto de 2010, se realiza el cambio de Empresa Unipersonal a Sociedad por Acciones Simplificada, cambio la razón social de INGELEC E.U. a INGELEC S.A.S.; ampliando de esta manera las opciones de mercado nacional e internacional.

Actualmente la Empresa se encuentra bien posicionada en el mercado local, funcionando dos sedes en la ciudad de Pasto, ubicadas en la carrera 44ª No. 16ª-42 de la Urbanización Calatrava y en la carrera 5E No. 17-42 del Barrio Lorenzo de Aldana y la Bodega ubicada en el Corregimiento de Obonuco.

ESTRUCTURA ORGANIZACIONAL INGELEC S.A.S

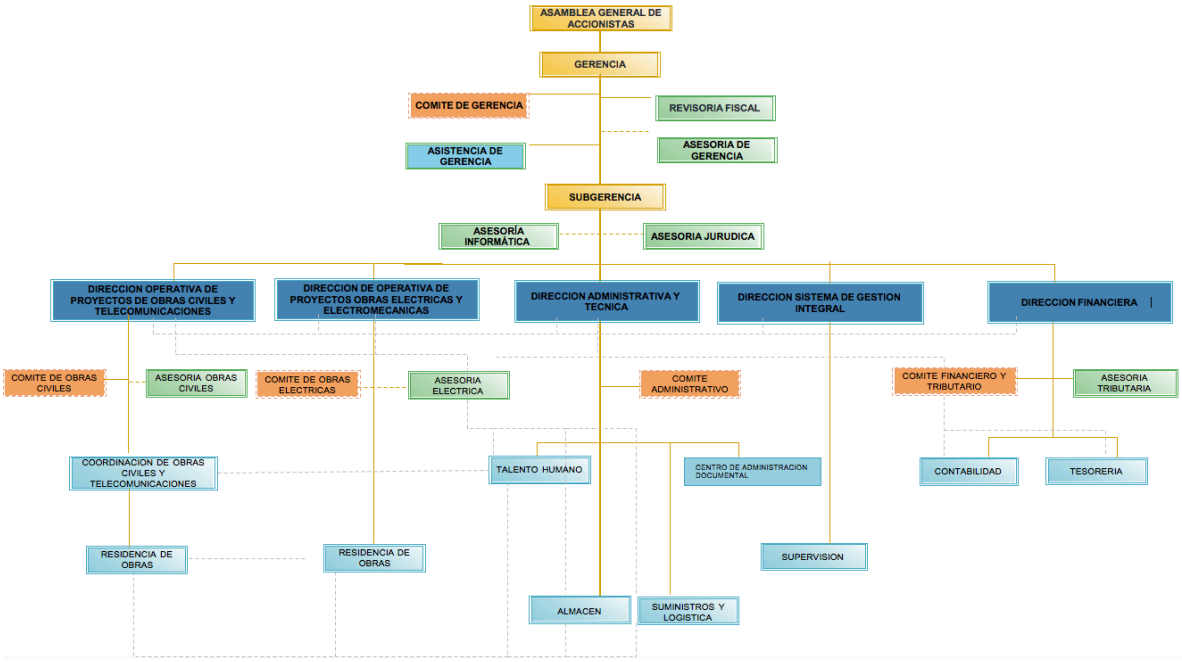

Figura 1. Estructura organizacional (Fuente: Empresa INGELEC S.A.S)

3.2 MARCO TEORICO

3.2.1 Seguridad informática[4]

La seguridad informática es el área del conocimiento que se encarga de trazar las pautas, los procedimientos, métodos y técnicas con el fin de lograr un sistema de información auténtico y confidencial. Protege contra posibles riesgos, amenazas, vulnerabilidades originados por la inadecuada utilización de tecnologías de información.

Las organizaciones deben establecer políticas de seguridad estableciendo mecanismos de protección y obstruir todos los medios de acceso que generen amenazas al sistema de la información.

La seguridad informática está orientada en salvaguardar el sistema computacional, aplicando normas, protocolos, herramientas para reducir perjuicios en el software, bases de datos y toda la información empresarial teniendo como objetivos:

- Conservar la integridad, disponibilidad, confidencialidad, autenticidad y no repudio de la información.

- Preservar los activos informáticos de la empresa, como la infraestructura tecnológica (hardware, software), mediante el uso de estrategias apropiadas, la seguridad informática apoya a la empresa en el desarrollo de sus metas, protegiendo los bienes materiales e inmateriales.

- Proteger los sistemas informáticos para impedir grandes pérdidas de información lo cual influye en el cumplimiento la misión empresarial.

[4]AGUILERA, Purificación. Seguridad informática. Editex, 2010. p.9

- Los directivos de las empresas deberían agregar a los objetivos empresariales la seguridad informática como una herramienta para controlar y mitigar los riesgos.

- Se entiende por seguridad informática la característica de cualquier sistema informático, que hace que esté libre de todo peligro, daño o riesgo. Como no hay sistema infalible, se trata de que el sistema sea lo más fiable posible.

3.2.2 Sistema de Información de Gestión Documental

El Sistema de Información de Gestión Documental utiliza el software Docunet que opera bajo el sistema operativo Windows, con un motor de base de datos Oracle/ SQL Server, un repositorio para el acceso a archivos compartidos, permite realizar tareas como: radicación, digitalización, adhesión de archivos tipo procesador de palabras, hojas de cálculo, presentación de ideas, correo electrónico, comunicación en línea con las dependencias existentes en la Electrificadora INGELEC S.A.S, categorización, almacenamiento, consultas y preservación de documentación electrónica creados por las áreas administrativas. En el Centro de Gestión Documental se encuentran los archivos centrales e históricos de la empresa. Para el cumplimiento de las actividades el Sistema de Información de Gestión Documental debe regirse bajo las normas sistemáticas y legales vigentes en Colombia.

3.2.2.1 Aplicación Docunet[5]

Es una aplicación para el trámite de documentos electrónicos, posee una propiedad especial en comparación a otras aplicaciones comerciales, está sustentada en la reglamentación del Archivo General de la Nación promulgado en la Ley 594 del 2.000, esta es de empleo imprescindible para empresas gubernativas.

Docunet tiene varias herramientas y técnicas de almacenamiento de información, que se adaptan de manera eficaz a los procedimientos de las empresas sin importar su naturaleza y dimensión. Docunet es un software privado.

Todos los archivos son accesibles por medio de un repositorio el cual utiliza el protocolo vía SMB con restricción de accesos.

Consta de un programa cliente que se conecta a un servidor de aplicación, tiene una base de datos, la aplicación gestiona conexión con la base de datos y el repositorio lo cual puede estar en un mismo servidor o en servidores separados.

Requisitos del sistema

- Sistema operativo: Windows 2000 Server y superiores, Windows XP y superiores
- Procesador: Pentium, Celeron, Core 2 Dúo, Centrino, Athlon, Durón.
- Memoria RAM: superior a 256 MB.
- Disco duro: superior a 10 GB.
- Navegador de Internet: Mozilla Firefox, Google Chrome, Safari, Ópera, Internet Explorer.

[5]INNOVA. Docunet Solución de Gestión Documental. [En línea]. Citado[07/08/2014]Disponible en: <http://www.guiadesolucionestic.com/sistemas-de-informacion/gestion-documental/administracion-y-gestion-electronica-de-documentos/569--docunet>

- Adobe Acrobat Reader 7 en adelante.
- Bases de datos Oracle, SQL Server.

Propiedades, Funciones y Servicios.

- Realización y levantamiento de tablas de retención y valoración documental.

- Digitalización, radicación, búsqueda de imágenes, archivos, videos, presentaciones.

- Módulos de atención al cliente: manipulación de información interna y externa.

- Sistematización de técnicas de registro, posibilita impartir la designación de tareas a los funcionarios encargados en cada una de las áreas de la empresa.

Reconocimiento de carácter óptico.

- Permite comprender la cronología, lugar y recorrido de los documentos existente en la empresa.

- Diversos repositorios de archivos e imágenes.

- Organización de documentos para permitir su búsqueda y verificación.

- Librerías.

Arquitectura del servidor SGD

Ejecuta las solicitudes de varias terminales para transmitir información y brindar servicios.

La topología lógica presta servicios de archivos a un cliente/servidor, en el caso de los servidores del Sistema de Gestión Documental se comunican con un cliente de base de datos, con un cliente de aplicaciones y con cliente RDP (Protocolo de Escritorio Remoto), los cuales se encuentran en una red LAN (Red de Área Local)

La estructura de red de datos utilizada en el proyecto de investigación está conformada por:

- Un gabinete o concentrador donde se encuentra organizado los switchs, enrutadores, patch panels.

- Los servidores donde se encuentra almacenado los servicios que prestan los sistemas de información.

- Los switchs son dispositivos que trabajan en capa dos (Enlace) del Modelo OSI, resuelve inconvenientes de rendimiento (ancho de banda), se usan para conectar diversas terminales dentro de una misma una red.

- Los routers son dispositivos que trabajan en capa tres (Red) del Modelo OSI, su función es interconectar distintas redes donde se examina los datos a exportar y los empaqueta para enviarlos a otra red. Son administrables y poseen servicios de firewall.

- Un cortafuego está catalogado como un dispositivo de protección, el cual se encarga de realizar filtros de paquetes mediante una secuencia de órdenes y juicios precisados por el administrador del sistema.

- Un firewall suele ser un aparato particularmente creado para ejercer esta labor, también es un software que se monta en un host conectado en red por medio de la cual ejecuta filtrado de información con anterioridad a la asignación a los hosts que integran la red. En cada host en el software instalado usualmente contiene un Firewall que efectúa un filtrado propio.

- Los Routers Firewall son aparatos electrónicos cuya función es proteger la red y los recursos compartidos de accesos no autorizados.

- Patch panel´s son organizadores de cables.

- Servidor Proxy. Opera como mediador, en el cual el servidor que recoge una solicitud no sabe quién es el usuario que envía dicha petición.

- Servidor de Base de Datos. Presta servicios de almacenaje y funcionalidad de la base de datos a usuarios.

- Servidores Dedicados. Destinado a un solo sistema de información.

- Servidores de Archivos. Manejan el almacenamiento de la información, normalizan y vigilan la accesibilidad a los recursos y operan como una fracción del sistema operativo de la red.

- Servidor de Aplicaciones. Suministra servicios de aplicación a los terminales de usuarios.

3.2.3 Vulnerabilidad

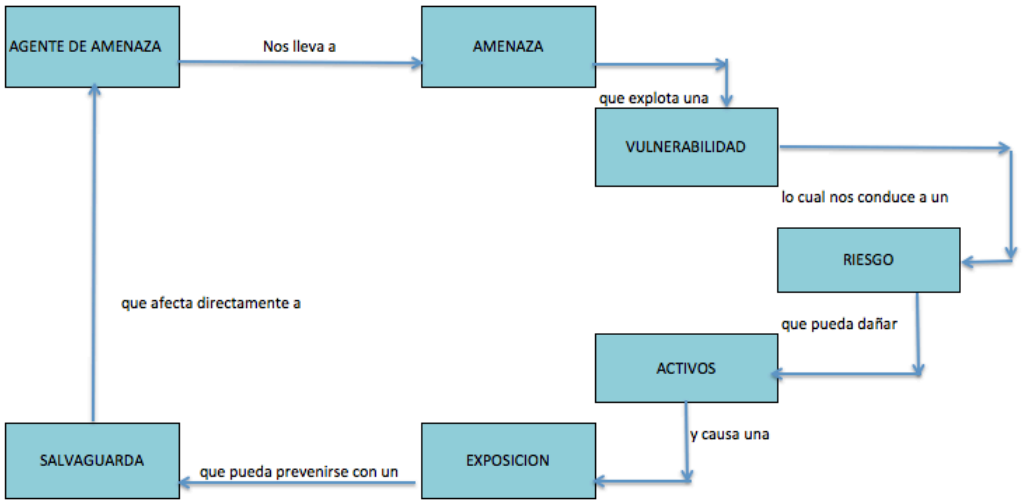

Figura 2. Ciclo de la Vulnerabilidad (Fuente: Esta investigación)

Es la materialización de una amenaza premeditada o accidental en un sistema informático provocando pérdida y hurto de información. Las vulnerabilidades surgen desde el esquema e implementación de los sistemas, errores de programación, las técnicas de seguridad y los mecanismos de control interno.

Las vulnerabilidades se originan por protecciones incorrectas o escasas en la parte física y lógica o reglamentarias presentes en los sistemas informáticos.

Las vulnerabilidades cuando son aprovechadas repercuten en fallas de seguridad que afectan al sistema de información de la empresa, las cuales se derivan de problemas en la fabricación de software, error humano en el uso de los sistemas, centralizar la seguridad en un solo recurso, carencia en el cumplimiento de las políticas, falta en la administración de los activos informáticos, fallas en la adjudicación de perfiles y permisos, deficiencia en planes de mitigación, ausencia

de capacitación del personal, hardware y software obsoletos, falta de sensibilización de la seguridad y trabajo en equipo.

3.2.3.1 Diagnóstico de vulnerabilidades[6]

Es el proceso por el cual se detectan vulnerabilidades informáticas en una organización, antes que un atacante pueda explotar estos problemas en la seguridad. El resultado de esta prueba si la seguridad está conforme a las políticas.

3.2.3.2 Evaluación de vulnerabilidades[7]

Permite medir la seguridad de los sistemas y la eficiencia de los controles implementados de ahí la importancia de la evaluación para mantener la confidencialidad, disponibilidad e integridad de la información.

Esta evaluación se puede realizar usando herramientas automatizadas las cuales generan una lista de vulnerabilidades encontradas y las medidas correctivas, además la cuantificación del impacto potencial de las amenazas identificadas en los activos.

3.2.3.3 Categorización de Vulnerabilidades

3.2.3.3.1 Riesgo

El riesgo es la eventualidad de que se realice o no una amenaza valiéndose de una vulnerabilidad generando pérdidas y deterioros en la información.

---

[6]OPENWARE, Attaka.Plataforma para la gestión y el diagnóstico de vulnerabilidades. En:ZMA IT SOLUTIONS. [En línea]. Citado[08/08/2014]. Disponible en: (http://www.zma.com.ar/contenidos/images/image/Attaka/Documentos/Attaka-%20Folleto.pdf)

[7]ISSA. Gestión de Vulnerabilidades: no es simple, pero no tiene por qué resultar difícil. 2014. [En línea]. Citado[07/11/2014]. Disponible: <http://www.issachile.cl/Vulnerability_Management_I>

Riesgos son las violaciones y amenazas a los sistemas de información.

- **Tipos de riesgos**[8]

  - **Riesgos de Integridad.** Interface del usuario, procesamiento, procesamiento de errores, interface, administración de cambios, información.

  - **Riesgos de Relación**. Utilización pertinente de la información originada por una aplicación.

  - **Riesgos de Utilidad.** Se orientan en tres modelos de riesgos: pueden afrontarse antes de la ocurrencia de falencias mediante el direccionamiento de sistemas, métodos para la recuperación y reparación empleadas para disminuir las fallas de los sistemas, copias de seguridad y planes de mitigación para el control de riesgos.

  - **Riesgos en la infraestructura.** Hace alusión a que las empresas no tienen una infraestructura tecnológica eficaz para sobrellevar las carencias que se presenten en tiempo presente y futuro. Se presentan en los procesos: planeación organizacional, definición de las aplicaciones, administración de seguridad, operaciones de red y computacionales, administración de sistemas de bases de datos, información / negocio.

  - **Riesgos de Seguridad General.** Son los requerimientos para el bosquejo de la seguridad y minimización del riesgo: riesgo eléctrico, incendio, radiación, mecánicos.

[8] BASC.2013.Riesgos Informáticos. [En línea]. Citado[09/11/2014]. Disponible en: <http://basc-costarica.com/site/wp-content/uploads/2013/04/riesgosinformatica.pdf >

3.2.3.4 Análisis de vulnerabilidades

El análisis enfoca su fin en reconocer vulnerabilidades con mayor relevancia en un sistema de información (distribución de dispositivos, servidores, programas). El producto obtenido es una relación de vulnerabilidades detalladas y ofrecimiento de estrategias de solución. El análisis de vulnerabilidades se cimienta en el uso de instrumentos automatizados e incorpora mapeo de la red para localizar puertos abiertos, mapeo de vulnerabilidades en equipos, servidores, programas, redes.

3.2.3.5 Técnica para el análisis de vulnerabilidades

Con el propósito de detallar los riesgos a que se ven expuestos los activos de un sistema de información y optimización de la seguridad. El análisis de vulnerabilidades se integra con el análisis de riesgos comprendiendo las siguientes tareas:

- Identificación de la Infraestructura**.** Se reconoce los dispositivos físicos y lógicos con que cuenta la red y establecer las vulnerabilidades en: programas, hosts, servidores, Routers.

- Pruebas. Se efectúa una relación de servicios activos de acuerdo a su utilidad y la confiabilidad de los datos almacenados. A través del empleo de herramientas de pentesting se identifica componentes activos que se encuentran en la red, mediante una dirección IP para localizar las vulnerabilidades existentes en el software y prevenir percances de seguridad.

- Disposiciones de Prevención. Realizadas las pruebas se apropiará las disposiciones de prevención aptas para su cumplimiento, para evitar consecuencias desfavorables en el suministro de los servicios, entre estas se puede destacar:

- Precisar horas de prueba. bajo tráfico y horas de no asistencia del servicio. Ejecutar análisis de riesgos cualitativo en las pruebas: análisis en la no existencia de activos cruciales disponibles, valorar el cumplimiento y el impacto. Adoptar disposiciones de posibles eventualidades: determinar tácticas de contingencia para activos graves, comprometer el administrador de la seguridad.

- Efectuar copias de seguridad de la información de los activos cruciales. Almacenar en archivos tangibles y electrónicos las estructuras de los hosts implicados. Ejecutar registro de las prestaciones en la realización de pruebas, periodos de réplica desmesurados y sucesos o percances de seguridad. Comunicar a la oficina de sistemas la elaboración de pruebas.

- Registrar el tránsito de la red, uso de fracciones cruciales, requisitos de error, uso de unidades centrales de procesamiento en servidores cruciales. Notificar a los directivos de la empresa.

- Ejecución de pruebas de vulnerabilidades. Se determina el tiempo de duración de las pruebas, se tiene herramientas que permiten detallar de forma automática los componentes de la red, se pueden hacer pruebas a nivel interno o externo.

3.2.4 Pruebas de penetración[9]

Es una labor realizada por profesionales en seguridad informática que buscan evidenciar que un sistema informático es vulnerable, accediendo por medio de ataques vigilados desde la parte interna o externa de la empresa. Se procura imitar las tareas de un hacker, explorando métodos para eludir controles, reconocer y obtener zonas críticas del área de los sistemas de la información.

Las pruebas de penetración se definen en dos clases: formales e informales, las formales se dirigen a comprobar falencias en las estrategias de seguridad, sujetas a técnicas que afectan los datos susceptibles de la empresa, las informales están encaminadas por propósitos tecnológicos de la estructura de los sistemas de información.

El informe de una prueba de penetración define los pasos del desarrollo de la tarea para llegar y acceder a la estructura de los sistemas de información. Además registra cómo se usaron las inconsistencias de las aplicaciones o defectos en la distribución del hardware para el acceso no permitido al área de los sistemas de información.

Pruebas de penetración llamadas también pentesting o hacking ético facilitan reconocer vulnerabilidades en un medio informático, permite evaluar el riesgo y estimar los procedimientos de seguridad actuales en la empresa, muestra donde falla la seguridad o es escasa y se pude utilizar para justificar la necesidad de una actualización, un mayor presupuesto para seguridad o para validar la valoración de los riesgos. Tiene como objetivos:[10]

---

[9]CANO, Jeimy J.1996. Auditoría de Seguridad, Evaluación de Seguridad y Pruebas de Penetración: tres paradigmas en la Seguridad Informática. P.71. [En línea]. Citado[07/08/2014]. Disponible:<http://www.derechotecnologico.com/estrado/estrado003.html >

[10]AREITIO BERTOLÍN, Javier. 2009.Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red. p. 38. [En línea]. Citado[07/08/2014]. Disponible en: <http://www.redeweb.com/_txt/653/36.pdf>

- Averiguar la cantidad de información libre y abierta de la red de la empresa.

- Identificar el sistema de información a comprobar.

- Establecer la probabilidad de alterar un procedimiento del sistema informático.

- Determinar el grado de seguridad de los controles que estén establecidos: cortafuegos, antivirus, filtración de documentos, técnicas de localización y precaución de intromisiones.

- Reconocer si el plan de seguridad en el Sistema de Gestión Documental empleado en una empresa es apropiado.

- Conocer si los funcionarios logran arriesgar la seguridad de los equipos informáticos.

3.2.4.1Tipos pruebas de penetración[11]

- Ataques externos.

- Ataques internos.

- Ataques a infraestructura hurtada.

- Ataque para diagnosticar el ingreso físico.

[11]Ibid p.40

- Ataque omitiendo la autenticación.

- Ataque confundiendo y gobernando las mentes de los usuarios.

Tabla 1. Etapas pruebas de penetración[12] (Fuente: Areitio Bertolin)

ETAPAS PRUEBAS DE PENETRACION	
ETAPA	DESCRIPCION
RECOLECCIÓN DE INFORMACIÓN	Se pretende recolectar gran volumen de información oficial.
EXAMINAR EQUIPAMIENTO INFORMÁTICO	Para este caso fueron usadas: • Querying System (sistema de consulta), y documentación DNS. • Se emplea: TraceRoute (marca el trayecto de la red), Transmisión de sector Sistema de Nombre de Dominio (brindan información de los hosts existentes en el sector y de la dirección IP). • Rastreo de puertos. El mapeo ofrece información sobre que puertos percibe un host. Todo puerto abierto es muy vulnerable.
ANALIZAR LOS EQUIPOS	Se aplican herramientas de escaneo de puertos y fingerprinting para adquirir información acerca de la versión y sistema operativo que están montados.
EXAMINAR LOS PROGRAMAS	Aplicando estudio útil, ordenado, ejecutando ataques contra la confirmación de la identidad de un individuo, permisos, información, condición última de los procedimientos y los usuarios

[12]Ibid.p.40-42

3.2.5 Técnicas de intrusión

Es una agrupación de acciones cuya finalidad es vulnerar la seguridad de los sistemas de información. Dichas prácticas además de conocerlas los delincuentes informáticos, es necesario que los profesionales de la seguridad de información también las conozcan, con el objetivo de brindar protección y salvaguardar los sistemas de información de forma efectiva y precisa.

Reconocer las inseguridades del sistema de información es labor significativa tanto para el delincuente informático como para el que lo protege; no debe eliminarse una vulnerabilidad si desde el inicio se ignora su presencia.

- Escaneo de Puertos: El mapeo de puertos se basa en identificar los puertos abiertos con el fin de analizarlos internamente en uno o varios hosts que integran una red. El escaneo de puertos es utilizado para optimizar las funciones de seguridad y utilidad de las redes, de igual forma se logra transformar en una acción peligrosa que se usa para averiguar zonas críticas sensibles y violentar el ingreso al sistema de información.

Los sistemas informáticos pueden presentar puertos abiertos que son omitidos por los profesionales de seguridad, ocasionado que los puertos no sean supervisados y la información circule por medio de estos desprovistos de controles de seguridad, produciendo una vulnerabilidad del sistema de información, Lo anterior es producto de errores en la configuración de los procedimientos de seguridad, en los cortafuegos por defecto se dejan diversos puertos abiertos, y los encargados de la administración de los cortafuegos omiten analizar cuidadosamente la configuración para identificar todos los puertos utilizables .

Cuando los puertos TCP/IP (interfaces de transmisión no físicas para conmutación de datos y servicios en una red) se encuentran abiertos son atractivos para los

atacantes los cuales pueden ejecutar pruebas de intrusión y vulnerar la seguridad de una red. Una técnica usual para revelar los puertos abiertos es el sondeo con el objetivo de evaluar los servicios aprovechables en una red, para identificar puertos vulnerables se remite una sucesión de paquetes deficientes a una dirección IP inexistente en la red, estos son filtrados por el firewall el cual los obstruye y no accede a enrutarlos, cuando no se efectúa el filtrado faculta el paso de los paquetes los cuales no es factible enrutarlos y al no poder enrutarlo apropiadamente, el firewall envía avisos de error ICMP (Protocolo de Mensajes de Control de Internet: accede gestionar y notificar errores de los hosts de una red más no permite su modificación) mostrando que los paquetes no se filtraron.

- Normas y filtros: Las normas de filtrado son una sucesión de situaciones que un funcionario, host, o conjunto de datos deben cumplir apoyado en las políticas de seguridad del sistema de información de la empresa para lograr ingreso a una terminal mediante los puertos protegidos por un procedimiento de protección (Cortafuegos).

3.2.5.1 Herramientas penetración

Tabla 2. Herramientas de penetración (Fuente: Secutatis Information Security)

	Nmap (herramienta de código abierto que ejecuta mapeo de puertos)	OpenVas (Sistema Abierto para Evaluación de Vulnerabilidades)
Tipo de Prueba	Sondeo Ping	Escaneo y análisis de vulnerabilidades de hosts
Objetivo	Escanear puertos de los hosts determinando si se encuentran abiertos, cerrados o custodiados	Permite analizar de forma automática un terminal o servidor desde la parte interna o externa a través de un equipo remoto.

3.2.6 Mitigación De Riesgos[13].

Metodología para minimizar riesgos. Se fundamenta en prevalecer, valorar y efectuar los controles adecuados de reducción de riesgos sugeridos por el tratamiento de estimación del riesgo.

Opciones de resolución para mitigar el riesgo:

1. Aceptar el riesgo. Admitir el riesgo latente y seguir trabajando, o establecer controles para aminorar el riesgo a un estado admisible.

2. Prevenir el riesgo. Suprimir el origen y/o secuela del riesgo.

3. Disminuir el riesgo: Restringir el riesgo con el establecimiento de controles que disminuyen el efecto perjudicial de una amenaza que aprovecha una debilidad.

Opciones de tratamiento del riesgo: mitigación

La mitigación del riesgo se refiere a una de dos opciones:

• Disminuir la desvalorización ocasionada por una amenaza.

• Aminorar la posibilidad de que una amenaza se realice.

En los casos anteriores se debe aumentar u optimizar el grupo de protecciones.

Proteger los recursos de los sistemas de información de INGELEC S.A.S y la tecnología utilizada para su procesamiento, frente a amenazas, internas o

[13] COMISIÓN INTERAMERICANA DE TELECOMUNICACIONES. 2009. Gestión de riesgos de seguridad. [En línea]. Citado[07/08/2014]. Disponible en: <http://www.oas.org/en/citel/infocitel/2009/septiembre/seguridad_e.asp>

externas, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

3.2.7 Control de acceso a la red[14]

El Control de Acceso a la Red tiene como finalidad controlar el acceso de los usuarios a la red, verificar que todos los dispositivos que se conectan a las redes de una organización cumplan las políticas de seguridad establecidas para prevenir amenazas como la entrada de virus, salida de información, etc.

3.2.8 Red de datos[15]

Conjunto de dos o más puntos los cuales se encuentra enlazados entre sí mediante un medio físico, estos puntos están en la capacidad de enviar y recibir información, como es el caso de un computador o de una impresora.

3.2.9 Estándar ISO 27002 para la evaluación de seguridad

Para la valoración de los riesgos de seguridad de la información se utilizan diversos procedimientos de evaluación, la manejada por el estándar ISO 27002 constituye una variedad de controles diferenciados en 11 Dominios, 39 Objetivos de Control y 133 Controles, lo anterior permite efectuar un análisis íntegro del Sistema de Gestión Documental posibilitando la formulación de estrategias de mitigación de riesgos. Posteriormente se indica la estructura de la norma nombrando los dominios, objetivos de control y controles empleados en el proyecto de investigación

[14]SECUTATIS INFORMATION SECURITY. [En línea]. Citado[28/10/2014]. Control de acceso a la red. Disponible en: http://www.secutatis.com/?page_id=62
[15]FOROUZAN. Comunicación de datos. 2007

- **Control de Acceso**

Requisitos de negocio para el control de acceso

- Política de Control de Acceso.

Gestión del acceso a los usuarios

- Registro de usuarios.
- Gestión de contraseñas para usuarios.

Responsabilidad de los usuarios

- Uso de contraseñas.
- Equipo de usuario desatendido.

Control de Acceso a la Red

- Autenticación de usuarios para conexiones externas.
- Identificación de los equipos en las redes.
- Protección de los puertos de configuración y diagnóstico remoto.
- Separación en las Redes.
- Control de Conexiones a las Redes.
- Control del Enrutamiento en la Red.

Control de acceso al sistema operativo

- Procedimientos de registro de inicio seguro.
- Identificación y autenticación de usuarios.
- Sistema de gestión de contraseñas.
- Uso de las utilidades del sistema.

Control de acceso a las aplicaciones y a la información

- Aislamiento de sistemas sensibles.

Computación móvil y trabajo remoto

- Trabajo remoto.

4. DISEÑO METODOLOGICO

En esta etapa se desarrolla los aspectos relacionados con el tipo de investigación a efectuar, la muestra con la cual se trabajará, las herramientas y el procedimiento para la identificación de las vulnerabilidades en el Sistema de Gestión Documental en INGELEC S.A.S mediante testeo de red.

4.1 TIPO DE INVESTIGACIÓN

El tipo de investigación empleado es de tipo exploratorio al sistema de cómputo (plataforma informática), se realizará un proceso de análisis el cual buscará encontrar vulnerabilidades en el Sistema de Gestión Documental, y aplicada porque a partir de los hallazgos se propone una solución de acuerdo a los conceptos, normas y técnicas de la seguridad informática.

4.2 POBLACIÓN

La población está constituida por los sistemas, servidores y estaciones de la INGELEC S.A.S, (remitirse a la Figura 1 Estructura organizacional).

4.3 INSTRUMENTOS.

- **Fuentes primarias:**

Son aquellas que brindan una demostración o certeza acerca del tema de estudio, este tipo de fuentes ofrecen una visión del suceso en específico, transmitiendo ideas nuevas, admitiendo apreciación de la sociedad.

Posee información nueva o inédita en base a la experiencia, que ha sido por primera vez transmitida y que no ha sido editada, deducida o valorada por otro autor. Es el resultado de una investigación o de una función especialmente novedosa.

- Pruebas de pentesting

Pruebas de penetración llamadas también pentesting o hacking ético las cuales se las puede realizar de forma remota o local donde facilitan reconocer vulnerabilidades en un medio informático, permite evaluar el riesgo y estimar los procedimientos de seguridad actuales en la empresa, muestra donde falla la seguridad o es escasa y se puede utilizar para justificar la necesidad de una actualización, un mayor presupuesto para seguridad o para validar la valoración de los riesgos.

Las pruebas de penetración se definen en dos clases: formales e informales, las formales se dirigen a comprobar falencias en las estrategias de seguridad, sujetas a técnicas que afectan los datos susceptibles de la empresa, las informales están encaminadas por propósitos tecnológicos de la estructura de los sistemas de información.

- **Fuentes Secundarias:**

Este tipo de fuentes abarcan información estructurada, formalizada, donde muestra resultados de estudios, o textos originales primarios, son utilizadas para

ratificar hallazgos del estudio, extender el contenido de la información de una fuente primaria y para proyectar los estudios realizados.

Esta clase de fuente es creada normalmente por alguna persona que no posee contacto directo con el suceso o argumento.

- Internet
- Artículos
- Libros
- Documentación empresarial

Se utilizará estos medios para constituir los elementos teórico-prácticos necesarios para el desarrollo del proyecto.

5. PRUEBAS DE PENETRACIÓN

TOPOLOGIA DE RED

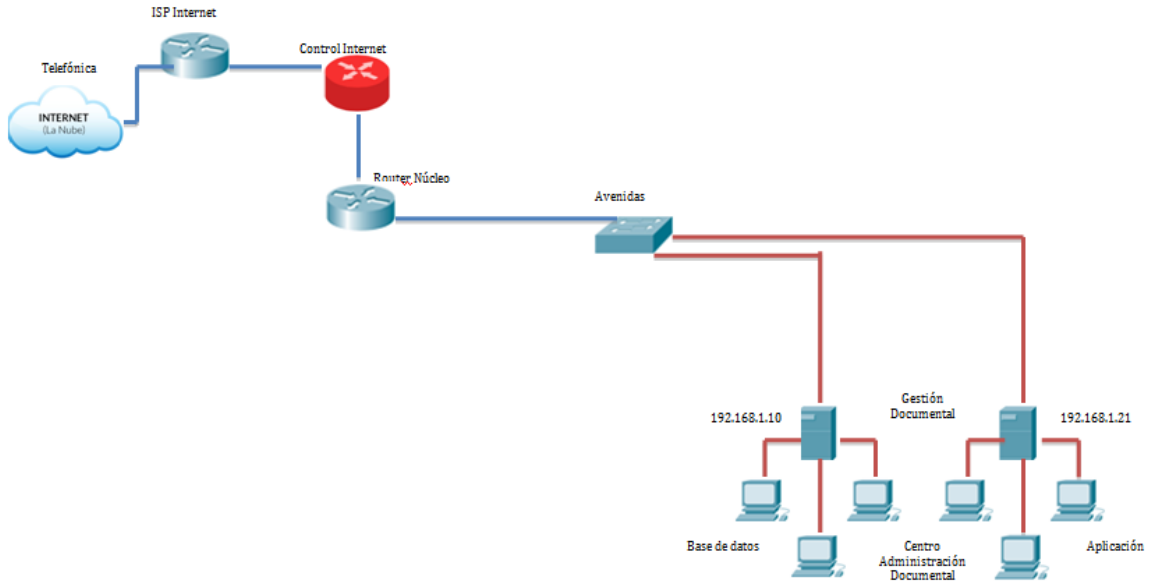

Figura 3: Topología de la red 192.168.0.0/22 (Fuente: Esta investigación)

En la red 192.168.0.0/22 el objeto de estudio se enfoca en los servidores del Centro de Administración Documental los cuales se identifican con las direcciones IP 192.168.1.10 y 192.168.1.21, estos se encuentran ubicados en el cuarto de comunicaciones (lugar donde se encuentra la infraestructura de conexión de la red para controlar el acceso físico no autorizado) de INGELEC S.A.S.

Topología física: La Empresa telefónica presta el servicio de Internet a través de un ISP (Proveedor Servicio de Internet) el cual recoge las solicitudes del router para posteriormente enviarlas al router de control acceso Internet (para realizar filtrado de paquetes e impedir el ingreso a sitios web no autorizados), la información va al router núcleo (dispositivo para interconexión que permite la

distribución y acceso de datos a las demás áreas de la red LAN), luego esta va al switch Avenidas, a través de fibra óptica a los servidores para el envío de paquetes según las peticiones requeridas por medio de las terminales.

La topología lógica presta servicios de archivos a un cliente/servidor, en el caso de los servidores del Sistema de Gestión Documental se comunican con un cliente de base de datos, con un cliente de aplicaciones y con cliente RDP (Protocolo de Escritorio Remoto), los cuales se encuentran en una red LAN (Red de Área Local)

Tabla 3. Pruebas y Resultados (Fuente: Esta investigación)

Etapa	Proceso	Resultados	Evidencias
Escaneo de la red.	En la red 192.168.0.0/22 de INGELEC S.A.S, se ejecutó escaneo de la red con la herramienta Nmap para detectar los puertos abiertos y los servicios activos de las máquinas que estén en funcionamiento.	El resultado del mapeo indicó 36 direcciones IP activas, correspondientes a los host disponibles.	Anexo A EV1
		192.168.0.1 Router Microtik servicios activos: ftp, ssh, telnet, domain, http, bandwidth-test	Anexo A EV2 EV3
		192.168.0.2 Router Cisco que tiene servicios activos: telnet, ssh, http, https	Anexo A EV4 EV5
		192.168.0.5 impresora hp LaserJet 4250 servicios activos: ftp, telnet, http, ssl/http, printer, jetdirect , tcpwrapped	Anexo A EV6 EV7
		192.168.0.11 equipo UNIX servicios activos: ssh, http	Anexo A EV8 EV9
		192.168.0.109 equipo Windows 7 Professional servicios activos: msrpc, netbios-ssn, microsoft-ds	Anexo A EV10 EV11
		192.168.0.210 equipo Windows servicios activos: msrpc, netbios-	Anexo A EV12 EV13

		ssn, microsoft-ds, globe, ms-wbt-server, cslistener	
		192.168.0.231 equipo Windows 7 servicios activos: http, msrpc, netbios-ssn, https, ms-wbt-server	Anexo A EV14 EV15 EV16
		192.168.0.250 Windows Server 2008 servicios activos: http, msrpc, netbios-ssn, ssl/http vmware-auth, oracle-tns, ssl/globe, ms-wbt-server, afs3-callback, ajp13, jdwp, cce4x	Anexo A EV17 EV18 EV19
		192.168.1.8 Windows Server 2008 servicios activos: ftp, http, msrpc, netbios-ssn, ssl/http, oracle-tns, mysql, ms-wbt-server, ajp13	Anexo A EV20 EV21 EV22
		192.168.1.10 Windows Server 2012 servicios activos: domain, http, kerberos-sec, msrpc, netbios-ssn, ldap, kpasswd, ncacn_http, tcpwrapped, oracle-tns, ms-wbt-server.	Anexo A EV23 EV24 EV25

		192.168.1.21 Windows Server 2008 servicios activos: domain, kerberos-sec, msrpc, netbios-ssn, ldap, kpasswd5, ncacn_http, tcpwrapped, ms-wbt-server, ajp13	Anexo A EV26 EV27 EV28
		192.168.1.23 Windows Server 2008 servicios activos: Ftp, domain, msrpc, netbios-ssn, ms-wbt-server, http	Anexo A EV29 EV30
		192.168.1.18 Windows Server 2008 servicios activos: msrpc, netbios-ssn, ms-wbt-server, http	Anexo A EV31 EV32
		192.168.1.25 servidor UNIX servicios activos: ssh, rpcbind, vcn-http, vnc, x11	Anexo A EV33 EV34
Identificación del objetivo.	De acuerdo a los servicios y al sistema operativo.	Servidor: 192.168.1.10 Servidor: 192.168.1.21	Anexo A EV35 EV36
Identificación de vulnerabilidades.	Se ejecutó la aplicación OpenVas en los servidores objetivos: • 192.168.1.10	192.168.1.10 se encontraron 11 vulnerabilidades (1 alta, 5 medias y 5 bajas).	Anexo B EV1
		192.168.1.21 se	Anexo B

	• 192.168.1.21	encontraron 10 vulnerabilidades (1 alta, 5 medias y 4 bajas).	EV5

5.1 RESULTADOS TEST DE PENETRACIÓN

Tabla 4. Resultados (Fuente: Esta investigación)

Servidor	Vulnerabilidad detectada	Nivel de la vulnerabilidad	Identificación vulnerabilidad	Solución
192.168.1.10	Microsoft RDP vulnerabilidad de divulgación en el Servidor de información privado.	Alta	CVE-2005-1794	• Las opciones de soluciones generales son para actualizar a una nueva versión, como desactivar las respectivas características, retirando el producto o sustituir el producto por otro. • Una solución consiste en conectar sólo a los servicios de terminal en una red confiable. • Microsoft terminal Server utilizando el protocolo de escritorio remoto (RDP) almacena una clave privada RSA y lo utiliza en firmar

				un certificado, que permite a atacantes remotos falsificar las claves públicas de los servidores legítimos, y llevar a cabo un ataque hombre en el medio. • Este sistema es propenso de la vulnerabilidad de divulgación de la información.
192.168.1.10	NVT: Detección del servicio Windows SharePoint	Baja	CVE-2011-0653	• El anfitrión remoto ejecuta Windows SharePoint Services.Productos y tecnologías de SharePoint de Microsoft incluyen la colaboración basada en navegador y una plataforma de gestión de documentos. • Estos pueden ser usados para alojar sitios web que el acceso y espacios de trabajo compartidos documento.

192.168.1.10	Detección de la versión de Oracle	Baja	CVE-2012-1675	• La detección de la versión instalada de Oracle. Este script envía 'CONNECT_DATA = (COMANDO = VERSION)' comando a través tnslsnr Oracle, una interfaz de red a la base de datos Oracle remota y tratar de conseguir la versión de la responce, y establece el resultado en KB.
192.168.1.21	Apache Tomcat servlet/JSP contenedor predeterminados de archivos.	Alta	CVE-2003-0045	• Eliminar archivos predeterminado, ejemplo JSP y servlets de Tomcat • Contenedor servlet / JSP. Estos archivos deben ser removidos, ya que pueden ayudar a un atacante adivinar la versión exacta de Apache Tomcat que se está ejecutando en este host y puede proporcionar otra información útil. • Se encontró que los siguientes

				archivos por defecto como: /tomcat-docs/index.html, en ciertos sistemas Windows puede permitir a los atacantes remotos provocar una denegación de servicio a través de una petición JSP.
192.168.1.21	Detección de protocolo de escritorio remoto de Microsoft	Baja	CVE-2012-2526	• La aplicación Remote Desktop Protocol (RDP) de Microsoft Windows XP SP3 no procesa correctamente los paquetes en la memoria, lo que permite a atacantes remotos ejecutar código arbitrario mediante el envío de paquetes RDP artesanales que desencadenan el acceso a un objeto eliminado, también conocido como "Vulnerabilidad remota protocolo de escritorio."

192.168.1.10 192.168.1.21	DCE Enumeración de Servicios	Media	CVE-2004-0716	• Filtrar el tráfico entrante a este puerto. • Desbordamiento de buffer en el demonio de DCE (DECD) permite a atacantes remotos ejecutar código arbitrario mediante una petición con una pequeña longitud de los fragmentos y una cantidad de datos • Computing Environment (DCE) Servicios Distribuidos en ejecución en el host remoto se pueden enumerar mediante la conexión en el puerto 135 y hacer las consultas pertinentes. Un atacante puede utilizar este hecho para obtener más conocimientos sobre el host remoto.

192.168.1.10 192.168.1.21	TCP Marcas de Tiempo	Media	CVE-2005-0356	• Permite atacantes remotos provocar una denegación de servicio (pérdida de conexión) a través de un paquete falsificado.
192.168.1.10 192.168.1.21	LDAP permite bases nulos	Media	CVE-2009-3862	• Deshabilitar consultas BASE NULL en el servidor LDAP • Permite a atacantes remotos provocar una denegación de servicio (bloqueo del sistema) a través de una solicitud de búsqueda con un valor NULL DN base.
192.168.1.10 192.168.1.21	Solicitud de búsqueda Uso de LDAP para recuperar información de servicios de directorio de NT	Media	CVE-2013-3868	• Si no se requiere compatibilidad anterior a Windows 2000, cambie a Windows 2000 la compatibilidad de la siguiente manera: - Cmd.exe inicio -Ejecutar el comando: net localgroup "Pre-Windows 2000 Compatible Access 'todos / eliminar

				- Reiniciar el host remoto • Microsoft servicio de directorio ligero de Active Directory (AD LDS) en Windows Vista SP2, Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1 y Windows 8 y servicios de Active Directory en Windows Server 2008 SP2 y R2 SP1 y Server 2012 permite a atacantes remotos provocar una denegación de servicio (interrupción LDAP directory-servicio) a través de una consulta LDAP diseñado, también conocido como "Vulnerabilidad remota AnonymousDoS"
192.168.1.10 192.168.1.21	Microsoft DNS servidor de nombre de host interno de detección de divulgación	Baja	CVE-2009-4022	• Vulnerabilidad no especificada en ISC BIND 9.0.x través 9.3.x, 9.4 antes de 9.4.3-P4, 9,5 antes de 9.5.2-

				P1, 9.6 antes de 9.6.1-P2, y 9.7 beta antes 9.7.0b3, con validación DNSSEC habilitada y comprobar deshabilitado (CD), permite a atacantes remotos realizar ataques de envenenamiento de caché DNS mediante la recepción de una consulta recursiva cliente y el envío de una respuesta que contiene una sección adicional con datos manipulados, que no se maneja adecuadamente cuando la respuesta se procesa", al mismo tiempo que solicitan registros DNSSEC (DO), "aka 20438 Bug.
192.168.1.10 192.168.1.21	NTP leer las variables	Baja	CVE-2013-5211	• Un servidor NTP (Netword time protocol) está escuchando en este puerto

6. USO DE LA NORMA ISO 27002 PARA CLASIFICAR LOS RIESGOS DETECTADOS EN EL TEST DE PENETRACIÓN

6.1. Descripción de la metodología aplicada

Para el desarrollo del proyecto de investigación se empleó como punto de referencia el estándar ISO IEC 27002, este estándar muestra una variedad de controles que evalúan de forma significativa los riesgos asociados a la seguridad de la información, enfatizando que para esta investigación se analiza las vulnerabilidades en el Sistema de Gestión Documental en la empresa INGELEC S.A.S. Se aplica el dominio que se muestra en el numeral 3.2.10. el cual permite verificar la seguridad de dicho sistema, el análisis de riesgos se establece al seleccionar los objetivos de control y los controles a ser evaluados, la medición realizada se fundamenta en los siguientes porcentajes de cumplimiento: de menos del 50% de cumplimiento del control se consideran riesgos de vulnerabilidad latentes y de más del 50% los riesgos se consideran de manejo adecuado y no manifiestan existencia de vulnerabilidades significativas para la seguridad de la información.

6.2 Evaluación de la seguridad en el Sistema de Gestión Documental

Para ejecutar la evaluación de la seguridad en el Sistema de Gestión Documental se toma el dominio explicado en el numeral 3.2.10 de este documento y se procede a realizar las listas de chequeo para cada dominio y objetivos seleccionados que evalúan las vulnerabilidades.

Se observa a continuación la medición del control para cada uno de los controles inspeccionados.

Tabla 5. Valoración de los controles (Fuente: Esta investigación)

ALTO LEVE	SIN RIESGO
ALTO MODERADO	RIESGO MUY BAJO
ALTO CRÍTICO	RIESGO BAJO
MEDIO LEVE	RIESGO MEDIO BAJO
MEDIO MODERADO	RIESGO MEDIO
MEDIO CRÍTICO	RIESGO MEDIO ALTO
BAJO LEVE	RIESGO ALTO BAJO
BAJO MODERADO	RIESGO ALTO MEDIO
BAJO CRÍTICO	RIESGO MUY ALTO

En la tabla 3 se muestra los tipos de vulnerabilidades encontradas de acuerdo al porcentaje de cumplimiento del control en la empresa que se define en: ALTO cumplimiento entre el 100% y el 70%, MEDIO cumplimiento entre el 69% y 50% y BAJO cumplimiento de menos del 50% para este caso se consideran vulnerabilidades de ALTO RIESGO ya que el incumplimiento del control da camino para una potencial vulnerabilidad.

A continuación se presentan las listas de chequeo para la verificación del cumplimiento de los controles, como se observa cada riesgo se clasifica como un R (riesgo) y cada lista de chequeo se clasifica como un LC (lista de chequeo), dentro de un dominio D.

Las listas de chequeo contienen: objetivo de control y control evaluados, la medición del cumplimiento del control (Alto, Medio y Bajo) y el impacto por no cumplimiento (Leve, Moderado y Crítico) con la relación de estas dos variables se mide el % de cumplimiento del control y al final de la lista de chequeo se observa y de acuerdo al número de controles examinados en la organización el porcentaje de cumplimiento del dominio. Las tablas presentadas a continuación son las aplicadas dentro de la empresa y los valores incluidos son el resultado del proceso de verificación.

Tabla 6. Lista de chequeo. Requisitos de negocio para el control de acceso (Fuente: Esta investigación)

D1	11. CONTROL DE ACCESOS							
LC 1	11.1. Requisitos de negocio para el control de acceso	Cumplimiento Objetivo Control			Impacto por no cumplimiento			
11.1.1 Política de Control de Acceso		Alto	Medio	Bajo	leve	Moderado	Crítico	% Cumplimiento del Control
R1	Las políticas de control de acceso son desarrolladas y revisadas basadas en los requerimientos de seguridad del negocio?	1			1			100
R2	Los controles de acceso tanto físico como lógico son tenidos en cuenta en las políticas de control de acceso?	1				1		100
R3	Tanto a los usuarios como a los proveedores de servicios se les dio una clara declaración de los requisitos de la empresa en cuanto a control de acceso?	1				1		100
	% cumplimiento objetivo	100						

Tabla 7. Lista de chequeo Gestión del acceso a los usuarios (Fuente: Esta investigación)

LC 2	11.2.Gestión del acceso a los usuarios	Cumplimiento Objetivo Control			Impacto por no cumplimiento			
	11.2.1 Registro de usuarios	Alto	Medio	Bajo	leve	Moderado	Crítico	% Cumplimiento del Control
R4	Existen procedimientos para el registro y cancelación de usuarios para el acceso a todos los sistemas y servicios de la información?	1				1		100
	% cumplimiento objetivo	100						
	11.2.2 Gestión de privilegios	Alto	Medio	Bajo	leve	Moderado	Crítico	% Cumplimiento del Control
R5	Se restringe y controla la asignación y el uso de privilegios a los usuarios?	1					1	100
R6	Se identifica usuarios y sus privilegios de acceso, sistema operativo, sistema de gestión de bases de datos y aplicaciones?		1			1		50
	% cumplimiento objetivo	75						

11.2.3 Gestión de contraseñas para usuarios		Alto	Medio	Bajo	leve	Moderado	Crítico	% Cumplimiento del Control
R7	Existe un procedimiento para la asignación de contraseñas a usuarios?	1				1		100
% cumplimiento objetivo		**100**						

Tabla 6. Lista de chequeo Responsabilidad de los usuarios (Fuente: Esta investigación)

LC 3	11.3. Responsabilidad de los usuarios	Cumplimiento Objetivo Control			Impacto por no cumplimiento			
11.3.1 Uso de contraseñas		Alto	Medio	Bajo	leve	Moderado	Crítico	% Cumplimiento del Control
R8	Se exige a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas?	1				1		100
% cumplimiento objetivo		**100**						
11.3.2 Equipo de usuario desatendido		Alto	Medio	Bajo	leve	Moderado	Crítico	% Cumplimiento del Control

R9	Existen procedimientos de seguridad para proteger los equipos desatendidos, así como sobre las responsabilidades en la implementación de dicha protección?			1		1		1
	% cumplimiento objetivo	**1**						

Tabla 8. Lista de chequeo Control de acceso a las redes (Fuente: Esta investigación)

LC 4	**11.4. Control de acceso a las redes**	**Cumplimiento Objetivo Control**			**Impacto por no cumplimiento**			
11.4.2 Autenticación de usuarios para conexiones externas		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R10	Son utilizados mecanismos apropiados de autenticación para controlar el acceso remoto de los usuarios?		1			1		50
	% cumplimiento objetivo	**50**						
11.4.3 identificación de los equipos en las redes		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R11	La identificación automática es considerada para autenticar conexiones desde equipos y	1				1		100

	direcciones específicas?							
% cumplimiento objetivo		**100**						
11.4.4 Protección de los puertos de configuración y diagnostico remoto		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R12	Los accesos físicos y lógicos a puertos de diagnóstico están apropiadamente controlados y protegidos por mecanismos de seguridad?			1		1		1
% cumplimiento objetivo		**1**						
11.4.5 Separación de la red		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R13	Los grupos de servicios de información, usuarios y sistemas de información son segregados en la red?	1			1			100
R14	La red (desde donde asociados de negocios o terceros necesitan acceder a los sistemas de información) es segregada utilizando mecanismos de seguridad perimetral como firewalls?	1				1		100

R15	En la segregación de la red son hechas las consideraciones para separar las redes wireless en internas y privadas?	1				1		100
	% cumplimiento objetivo	**100**						
	11.4.6 Control de Conexiones a las Redes	**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R16	Existe una política de control de acceso que verifique conexiones provenientes de redes compartidas, especialmente aquellas que se extienden más allá de los límites de la organización?			1		1		1
	% cumplimiento objetivo	**1**						
	11.4.7 Control del enrutamiento de la red	**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R17	Existen políticas de control de acceso que establezcan los controles que deben ser realizados a los ruteos implementados en la red?			1		1		1
R18	Los controles de ruteo, están basados en mecanismos de identificación positiva de origen y			1		1		1

	destino?							
% cumplimiento objetivo		**1**						

Tabla 9. Control de acceso al sistema operativo (Fuente: Esta investigación)

LC 5	**11.5. Control de acceso al sistema operativo**	**Cumplimiento Objetivo Control**			**Impacto por no cumplimiento**			
11.5.1 Procedimientos de registro de inicio seguro		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R19	Existe controles para el acceso a los sistemas operativos mediante un procedimiento de registro de inicio seguro?			1		1		1
% cumplimiento objetivo		**1**						
11.5.2 Identificación y autenticación de usuarios		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R20	Existe una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario de inicio seguro ?.		1			1		50

R21	Los usuarios poseen un identificador único (ID del usuario) únicamente para su uso personal?	1				1		100
	% cumplimiento objetivo	**75**						
11.5.3 Sistema de gestión de contraseñas		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R22	Los sistemas para la gestión de contraseñas son interactivos y aseguran la calidad de dichas contraseñas?.	1			1			100
	% cumplimiento objetivo	**100**						
11.5.4 Uso de las utilidades del sistema		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	**% Cumplimiento del Control**
R23	Se restringe y controla el uso de programas utilitarios que pueden perjudicar los controles del sistema y de la aplicación?	1					1	100

Tabla 10. Control de acceso a las aplicaciones y a la información (Fuente: Esta investigación)

LC6	**11.6. Control de acceso a las aplicaciones y a la información**	**Cumplimiento Objetivo Control**			**Impacto por no cumplimiento**			**% Cumplimiento del Control**
11.6.2 Aislamiento de sistemas sensibles		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	

R24	Existe un entorno informático dedicado (aislados) para los sistemas sensibles.			1	1			1
% cumplimiento objetivo		**1**						

Tabla 11. Control de acceso a las aplicaciones y a la información (Fuente: Esta investigación)

LC7	**11.7. Computación móvil y trabajo remoto**	**Cumplimiento Objetivo Control**			**Impacto por no cumplimiento**			**% Cumplimiento del Control**
11.7.2 Trabajo remoto		**Alto**	**Medio**	**Bajo**	**leve**	**Moderado**	**Crítico**	
R25	Existen implementados procedimientos para las actividades de trabajo remoto?	1					1	100
% cumplimiento objetivo		**100**						

- Evaluación del cumplimiento

A continuación se muestra el dominio (D) evaluado, el porcentaje de cumplimiento de los objetivos de control (OC) en el dominio y en qué porcentaje lo cumple empresa, con esto se determina los riesgos y las potenciales vulnerabilidades de la seguridad en el Sistema de Gestión Documental, es primordial tener presente los porcentajes de cumplimiento determinados para evaluar los riesgos obtenidos en las listas de chequeo anteriores.

Tabla 12. Dominio control de acceso Porcentaje de cumplimiento por objetivo de control (Fuente: Esta investigación)

D1	11. CONTROL DE ACCESO	
OC1	11.1. Requisitos de negocio para el control de acceso	**% cumplimiento del control**
11.1.1 Política de Control de Acceso		**100**
OC2	11.2.Gestión del acceso a los usuarios	**% cumplimiento del control**
11.2.1 Registro de usuarios		**100**
11.2.2 Gestión de privilegios		**75**
11.2.3 Gestión de contraseñas para usuarios		**100**
OC3	11.3. Responsabilidad de los usuarios	**% cumplimiento del control**
11.3.1 Uso de contraseñas		**100**
11.3.2 Equipo de usuario desatendido		**1**
OC4	11.4. Control de acceso a las redes	**% cumplimiento del control**
11.4.2 Autenticación de usuarios para conexiones externas		**50**
11.4.3 Identificación de los equipos en las redes		**100**
11.4.4 Protección de los puertos de configuración y diagnostico remoto		**1**
11.4.5 Separación de la red		**100**
11.4.6 Control de Conexiones a las Redes		**1**
11.4.7 Control del enrutamiento de la red		**1**
OC5	11.5. Control de acceso al sistema operativo	**% cumplimiento del control**

11.5.1 Procedimientos de registro de inicio seguro		**1**
11.5.2 Identificación y autenticación de usuarios		**75**
11.5.3 Sistema de gestión de contraseñas		**100**
11.5.4 Uso de las utilidades del sistema		**100**
OC6	11.6. Control de acceso a las aplicaciones y a la información	**% cumplimiento del control**
11.6.2 Control del enrutamiento de la red		**1**
OC7	11.7. Computación móvil y trabajo remoto	**% cumplimiento del control**
11.7.2 Trabajo remoto		**100**

- **Nivel del Riesgo**

Es importante determinar el nivel del riesgo a partir del porcentaje de cumplimiento del control, dentro del objetivo de control a continuación se hace la clasificación del riesgo de acuerdo al nivel de obtenido en la lista de chequeo y que indica una falla de seguridad dentro de la organización que da lugar a un revisión de una potencial vulnerabilidad en el Sistema de Gestión Documental de la empresa, a continuación se muestra el nivel del riesgo obtenido para cada uno de los controles analizados, esto permite posteriormente clasificar los riesgos y determinar la matriz de riesgo que proporciona información de los controles vulnerables:

Tabla 13. Nivel del Riesgo (Fuente: Esta investigación)

	Resultado del control evaluado	Nivel del Riesgo
R1	Las políticas de control de acceso si son desarrolladas y revisadas basadas en los requerimientos de seguridad del negocio.	ALTO LEVE
R2	Los controles de acceso tanto físico como lógico si son tenidos en cuenta en las políticas de control de acceso.	RIESGO MUY BAJO
R3	Tanto a los usuarios como a los proveedores de servicios si se les dio una clara declaración de los requisitos de la empresa en cuanto a control de acceso.	RIESGO MUY BAJO
R4	Se observa que si existen procedimientos para el registro y cancelación de usuarios y para el acceso a todos los sistemas y servicios de la información	RIESGO MUY BAJO
R5	Hay restricción y control en la asignación y el uso de privilegios a los usuarios.	RIESGO BAJO
R6	Se observa que hay identificación mediana de usuarios y sus privilegios de acceso, sistema operativo, sistema de gestión de bases de datos y aplicaciones	RIESGO MEDIO
R7	Se evidencia la existencia de un procedimiento para la asignación de contraseñas a usuarios.	RIESGO MUY BAJO
R8	Se observa que hay un control a los usuarios para que cumplan con las buenas prácticas de seguridad en la selección y el uso de las contraseñas.	RIESGO MUY BAJO

R9	Se evidencia que los procedimientos de seguridad para proteger los equipos desatendidos, así como las responsabilidades en la implementación de dicha protección no son muy adecuados.	**RIESGO ALTO MEDIO**
R10	Se evidencia la utilización mediana de mecanismos apropiados de autenticación para controlar el acceso remoto de los usuarios.	**RIESGO MEDIO**
R11	La identificación automática si es considerada para autenticar conexiones desde equipos y direcciones específicas.	**RIESGO MUY BAJO**
R12	Los accesos físicos y lógicos a puertos de diagnóstico no están apropiadamente controlados y protegidos por mecanismos de seguridad.	**RIESGO ALTO MEDIO**
R13	Los grupos de servicios de información, usuarios y sistemas de información son segregados en la red.	**ALTO LEVE**
R14	La red es segregada y utiliza mecanismos de seguridad perimetral como firewalls.	**RIESGO MUY BAJO**
R15	En la segregación de la red son hechas las consideraciones para separar las redes Wireless en internas y privadas.	**RIESGO MUY BAJO**
R16	No existe una política de control de acceso que verifique conexiones provenientes de redes compartidas.	**RIESGO ALTO MEDIO**
R17	No existen políticas de control de acceso que establezcan los controles que deben ser realizados a los ruteos implementados en la red.	**RIESGO ALTO MEDIO**

R18	Los controles de ruteo no están basados en mecanismos de identificación positiva de origen y destino.	**RIESGO ALTO MEDIO**
R19	No existen controles para el acceso a los sistemas operativos mediante un procedimiento de registro de inicio seguro.	**RIESGO ALTO MEDIO**
R20	Existe una técnica medianamente apropiada de autenticación para comprobar la identidad declarada de un usuario inicio seguro.	**RIESGO MEDIO**
R21	Se muestra que los usuarios poseen un identificador único para su uso personal.	**RIESGO MUY BAJO**
R22	Los sistemas para la gestión de contraseñas si son interactivos y aseguran la calidad de las contraseñas.	**ALTO LEVE**
R23	Existe restricción y control en el uso de programas utilitarios que pueden perjudicar los controles del sistema y de la aplicación.	**RIESGO BAJO**
R24	No existe un entorno informático dedicado (aislados) para los sistemas sensibles.	**RIESGO ALTO BAJO**
R25	Si hay implementados procedimientos para las actividades de trabajo remoto.	**RIESGO BAJO**

- **Clasificación de los riesgos detectados**

Una vez aplicadas las listas de chequeo se puede determinar la matriz de riesgo donde se observa en que riesgo se encuentran las comunicaciones de la organización de acuerdo a los dominios relacionados a las comunicaciones aplicadas para el estudio:

Tabla 14. Matriz de riesgos (Fuente: Esta investigación)

	leve	Moderado	Crítico
Alto	R1,R13,R22	R2,R3,R4,R7,R8,R11,R14,R15,R19,R21	R5,R23,R25
Medio		R6,R10,R20	
Bajo	R24	R9,R12,R16,R17,R18,R19	

De acuerdo a las listas de chequeo se comprueba el porcentaje de cumplimiento del control y el impacto de cumplimiento, para el caso de investigación se tiene que los riesgos que se clasificaron en color verde son controles que cumplen un porcentaje de cumplimiento mayor al 70% que indica una seguridad alta en la protección de las vulnerabilidades del Sistema de Gestión Documental; los riesgos que se clasifican en color amarillo son controles que cumplen medianamente los aspectos de seguridad indicando que deben ser revisados para su mejoramiento y por último los riesgos clasificados en la zona roja muestra que existen riesgos latentes que pueden generar vulnerabilidades peligrosas.

7. CONJETURAS FINALES DE LA EVALUACIÓN DE LA SEGURIDAD EN EL SISTEMA DE GESTIÓN DOCUMENTAL DE INGELEC

Con las evaluaciones de seguridad realizadas en el numeral 4.1 de la presente investigación se obtuvieron los riesgos detectados en la tabla 11 matriz de riesgo, los cuales se analizarán para proponer unas estrategias de seguridad, cabe mencionar que los riesgos a ser tratados son los que están en las clasificación: bajo – leve, bajo – moderado; bajo – crítico; estos niveles representan menos del 50% de cumplimiento del control de seguridad evaluado y para la seguridad del Sistema de Gestión Documental.

Para los riesgos que se sitúan en los niveles, medio – bajo, medio – moderado y medio crítico que se sitúan entre el 50% y 70% de cumplimiento en un rango aceptable de cumplimiento del control de seguridad son tenidos en cuenta ya que presentan algún tipo de vulnerabilidad y se hacen las recomendaciones necesarias para que se mejore de manera satisfactoria su cumplimiento.

Se presenta la siguiente tabla que muestra el resumen general de los resultados obtenidos de las evaluaciones realizadas a los objetivos de control de comunicaciones basados en el dominio del estándar ISO 27002.

Tabla 15. Resumen de Objetivos de control, riesgo detectado y evidencia relacionada (Fuente: Esta investigación)

DOMINIO	OBJETIVO DE CONTROL	RIESGO	DESCRIPCION DEL FALLO O VULNERABILIDAD DETECTADA	EVIDENCIA RELACIONADA
D1	OC2	R6	Se observa que hay identificación mediana de usuarios y sus privilegios de acceso, sistema operativo, sistema de gestión de bases de datos y aplicaciones.	Anexo B EV6
D1	OC3	R9	Se evidencia que los procedimientos de seguridad para proteger los equipos desatendidos, así como las responsabilidades en la implementación de dicha protección no son muy adecuados.	Anexo B EV7
D1	OC4	R10	Se evidencia la utilización mediana de mecanismos apropiados de autenticación para controlar el acceso remoto de los usuarios.	Anexo B EV2
D1	OC4	R12	Los accesos físicos y lógicos a puertos de diagnóstico no están apropiadamente controlados y protegidos por mecanismos de seguridad.	Anexo B EV3
D1	OC4	R16	No existe una política de control de acceso que verifique conexiones provenientes de redes	Anexo B EV4

			compartidas.	
D1	OC4	R17	No existen políticas de control de acceso que establezcan los controles que deben ser realizados a los ruteos implementados en la red.	Anexo A EV1
D1	OC4	R18	Los controles de ruteo no están basados en mecanismos de identificación positiva de origen y destino.	Anexo A EV2 EV3 EV4
D1	OC5	R19	No existen controles para el acceso a los sistemas operativos mediante un procedimiento de registro de inicio seguro.	Anexo A EV13
D1	OC5	R20	Existe una técnica medianamente apropiada de autenticación para comprobar la identidad declarada de un usuario inicio seguro.	Anexo A EV7
D1	OC6	R24	No existe un entorno informático dedicado (aislados) para los sistemas sensibles.	Anexo A EV19 EV22 EV25

8. ESTRATEGIAS DE MITIGACIÓN PARA VULNERABILIDADES DETECTADAS EN EL SISTEMA DE GESTION DOCUMENTAL DE INGELEC

Es importante que los principios de la seguridad sean parte de la cultura empresarial, para esto se manifiesta un compromiso de parte de las máximas autoridades de INGELEC S.A.S y de los titulares de diferentes áreas empresariales para la difusión, consolidación y cumplimiento de las presentes estrategias.

Tabla 16. Estrategias de seguridad recomendadas (Fuente: Esta investigación)

DOMINIO	OBJETIVO DE CONTROL	RIESGO	CONTROL A IMPLEMENTAR	ESTRATEGIA DE MITIGACION
D1	OC2	R6	Se debe restringir y controlar la asignación y el uso de privilegios.	"Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado deben controlar la asignación de privilegios a través de un proceso formal de autorización. Se recomienda tener en cuenta los siguientes elementos: a) Se deben identificar los usuarios y sus privilegios de acceso asociados con cada producto del sistema, como: sistema operativo, sistema de gestión de bases de datos y aplicaciones; b) se deben asignar los privilegios a los usuarios sobre los principios de

				necesidad-de-uso y evento-por-evento, es decir, el requisito mínimo para su función, solo cuando se necesario; c) se debe conservar un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se deberían otorgar hasta que el proceso de autorización este completo; d) es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios; e) se recomienda promover también el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios; f) los privilegios se deben asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal del negocio."[16]
D1	OC3	R9	Los usuarios deben asegurarse de que los equipos desatendidos tengan protección apropiada.	"Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de seguridad para proteger los equipos

[16] NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002. p.92.

				desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre: a) terminar las sesiones activas cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña; b) realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión (es decir, no solo apagar el interruptor de la pantalla del computador o terminal); c) cuando no están en uso, asegurar los computadores personales o los terminales contra el uso no autorizado mediante una clave de bloqueo o un control equivalente como, por ejemplo, el acceso por contraseña."[17]

[17]Ibid, p.96.

D1	OC4	R10	Se debe emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	"Los procedimientos y controles de devolución de marcación, por ejemplo empleando módems de retorno de marcación, pueden suministrar protección contra conexiones no deseadas o no autorizadas a los servicios de procesamiento de información de la organización. Este tipo de control autentica a los usuarios tratando de establecer una conexión con una red de la organización desde sitios remotos."[18]
D1	OC4	R12	El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado.	"Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o de red, que no se requieren específicamente para la funcionalidad del negocio, se deberían inhabilitar o retirar. Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico Un ejemplo de un procedimiento de

[18]Ibid, p-99.

				soporte es garantizar que los puertos de diagnóstico y configuración solo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/software que requiere el acceso."[19]
D1	OC4	R16	Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio establecidos.	"Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según se requiera a través de la política de control de acceso de la organización. La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace (Gateway) de red que filtren el tráfico por medio de tablas o reglas predefinidas. Los siguientes son algunos ejemplos de aplicaciones a las cuales se deberían aplicar restricciones: 1) mensajería. por ejemplo, el correo electrónico 2) transferencia de archivos 3) acceso interactivo 4) acceso a las aplicaciones es conveniente tomar en consideración el enlace

[19]Ibid, p100.

				de los derechos de acceso a la red con algunas horas del día o fechas. Información adicional. La política de control del acceso puede exigir la incorporación de controles para restringir la capacidad de conexión de los usuarios a redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización."[20]
D1	OC4	R17 Y R18	Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones de la organización.	"Los controles de enrutamiento se deberían basar en mecanismos de verificación para las direcciones fuente/ destino válidos. Las puertas de enlace (Gateway) de seguridad se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes interna y externa, si se emplean tecnologías proxy y/o de traducción de dirección de red. Los requisitos para el control del enrutamiento en la red se deberían basar en

[20]Ibid, p102.

				la política de control de acceso."[21]
D1	OC5	R19	El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.	"El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos: a) no mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente; b) mostrar una advertencia de notificación general indicando que solo deberían tener acceso al computador los usuarios autorizados; c) no suministrar mensajes de ayuda durante el procedimiento de registro de inicio que

[21] Ibid, p103

				ayuden a un usuario no autorizado; d) validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar que parte de los datos es correcta o incorrecta; e) limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos, y considerar: 1) registrar intentos exitosos y fallidos; 2) forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización específica; 3) desconectar las conexiones de enlaces de datos; 4) enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio; 5) establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege;

				f) limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación; g) mostrar la siguiente información al terminar un registro de inicio exitoso: 1) fecha y hora del registro de inicio exitoso previo; 2) detalles de los intentos fallidos de registro de inicio desde el último registro exitoso; h) no mostrar la contraseña que se introduce o considerar esconder tos caracteres mediante símbolos; i) no transmitir contraseñas en texto claro en la red."[22]
D1	OC5	R20	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	"Se debería aplicar a todos los tipos de usuarios (incluyendo el personal de soporte único, operadores, administradores de red. programadores de sistemas y administradores de bases de datos). Los identificadores de usuario (ID) se deberían utilizar para rastrear las actividades de la persona

[22]Ibid. P.104

				responsable. Las actividades de usuarios regulares no se deberían realizar desde cuentas privilegiadas. Solo se deberían permitir los identificadores (ID) de usuario genéricos para uso de un individuo si existen funciones accesibles o si no es necesario rastrear las acciones ejecutadas por el 'identificador (por ejemplo el acceso de solo lectura), o cuando no hay controles establecidos por ejemplo cuando la contraseña para un identificador genérico solo se emite para un personal a la vez y el registro de tal caso).”[23]
D1	OC6	R24	Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	“Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles: a) la sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del dueño de la aplicación b) cuando una aplicación se ha de ejecutar en un entorno compartido, los

[23] Ibid. p.105

				sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el dueño de la aplicación sensible. Los sistemas de aplicación son lo suficientemente sensibles a la pérdida potencial que requieren manejo especial. La sensibilidad puede indicarle el sistema de aplicación se debería: a) ejecutarse en un computador dedicado, o b) únicamente debería compartir recursos con sistemas de aplicaciones confiables. El aislamiento se puede lograr utilizando métodos físicos o lógicos”[24]

[24]Ibid. P.109.

9. CONCLUSIONES

En el presente trabajo y la investigación desarrollada para llevar a cabo las pruebas de testeo para la red de datos que soporta los procesos de información de la Empresa INGELEC S.A.S., se identificó las vulnerabilidades que en adelante la empresa deberá atender para mitigar los riesgos conexos a estas, como caso específico se debe fortalecer los niveles de detección de intrusos, para ello se implementará sistemas de detección al alcance de la empresa; estos sistemas habrán de fortalecerse con un esquema de segmentación de la red, el cual luego de las pruebas se evidencia que la Empresa no lo tiene implementado, esquema que tendrá intrínseco la administración y gestión de los puertos de los dispositivos de comunicación como de los servidores, que luego de la verificación se demostró que no se tenía el óptimo manejo de este aspecto.

En el desarrollo del trabajo, se demuestra que el sistema actual que soporta la empresa INGELEC S.A.S presenta vulnerabilidades que se evidenciaron de una manera óptima con el uso de la aplicación *Open Vas* la cual es muy eficiente en el proceso de análisis de vulnerabilidades y que permite realizar pruebas de intrusión, realizando un escaneo de puertos; permitiendo así la visualización de la infraestructura de red y las deficiencias de la misma.

Por otra parte se hizo uso de los métodos de hacker ético para el análisis íntegro de la infraestructura del Sistema de Información Documental, protocolos y aplicaciones utilizadas en la empresa INGELEC S.A.S. permitiendo identificar como corroboración las vulnerabilidades mencionadas y reportar a la empresa de manera que esta información permita tomar medidas sin poner en riesgo la integridad del sistema para su corrección.

En la investigación presente se adoptó el ***dominio 11***. "*Control de Acceso con los objetivos de control y controles"* usados del estándar (ISO/IEC 27002) con la metodología de listas de chequeo las cuales permitieron realizar una evaluación que determinó el nivel del riesgo, para realizar una clasificación obteniendo los resultados como hallazgos que permitieron formular las estrategias de mitigación de vulnerabilidades para la empresa INGELEC S.A.S.

En cuanto a la implementación de estrategias para tener el sistema de información de la Empresa INGELEC S.A.S y los sistemas conexos en un nivel óptimo de seguridad, es fundamental tener identificado las vulnerabilidades, sus ocurrencias y el impacto dado; que permitirán con una adecuado empoderamiento de la dirección de la empresa y la clara identificación de estas, realizar un manejo adecuado de los controles sugeridos en este documento, de manera rutinaria y con una asignación documentada de los responsables que los ejecutarán, permitiendo tener evaluación permanente, que direccionará la mejora en los casos de más alto impacto a la ocurrencia de una vulnerabilidad, mitigando estas para un desarrollo funcional y óptimo de los sistemas que son parte del software de gestión documental Docunet de la empresa INGELEC.S.A.S.

10. RECOMENDACIONES

Impedir el acceso no autorizado al sistema de información documental.

Controlar la seguridad en la conexión entre la Intranet y otras redes públicas o privadas.

Registrar y revisar eventos y actividades criticas llevadas a cabo por los usuarios en el sistema.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Impedir el acceso no autorizado al sistema de información documental de la empresa.

Gestionar por parte del administrador del sistema de información la seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, de acuerdo al procedimiento establecido.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Definir controles para garantizar la seguridad de la infraestructura de comunicaciones y los servicios conectados en al sistema de información, contra el acceso no autorizado.

Aplicar políticas en la red, en el firewall se debe definir los perfiles de usuarios como: el administrador tiene un perfil con todos los permisos mientras que los usuarios solo tienen acceso a las aplicaciones de acuerdo a los roles asignados.

Definir y documentar los perímetros de seguridad que sean convenientes, que se implementen mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

Implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto. Dichos controles se deben implementar en los “gateways”.

Limitar y controlar la asignación y uso de privilegios, debido a que el uso inadecuado resulta frecuentemente siendo el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente, tarea que debe ser ejecutada por cada administrador o responsable de los sistemas de información.

Se recomienda a los encargados de la seguridad en la empresa INGELEC S.A.S, implementar las estrategias formuladas en este documento para alcanzar mejores prácticas, controlar y minimizar los riesgos.

11. BIBLIOGRAFIA

AGUILERA, P. Seguridad informática. Editex, 2010. p.9-10,15-16

AREITIO BERTOLÍN, J. 2009.Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red. p. 38-42. Recuperado de: http://www.redeweb.com/_txt/653/36.pdf

BASC. Riesgos Informáticos. 2013. Recuperado de: http://basc-costarica.com/site/wp-content/uploads/2013/04/riesgosinformatica.pdf

CANO, Jeimy J. Auditoría de Seguridad, Evaluación de Seguridad y Pruebas de Penetración: tres paradigmas en la Seguridad Informática. 1996. P. 71. Recuperado de: http://www.derechotecnologico.com/estrado/estrado003.html

CERTICÁMARA. La Ley obliga a todas las entidades públicas y empresas. Recuperado de: https://web.certicamara.com/productos-y-servicios/consultor%C3%ADa-en-protección-datos-personales/

CONGRESO DE LA REPÚBLICA. Ley 594 de 2000. . Diario Oficial 44084 del 14 de julio de 2000. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4275

CONGRESO DE LA REPÚBLICA. Ley estatutaria 1581 de 2012. Diario Oficial No. 48.587 de 18 de octubre de 2012.Ley estatutaria 1581 de 2012. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html/

FOROUZAN. Comunicación de datos. 2007

INNOVA. Docunet Solución de Gestión Documental. Recuperado de: http://www.guiadesolucionestic.com/sistemas-de-informacion/gestion-documental/administracion-y-gestion-electronica-de-documentos/569--docunet

ISSA. Gestión de Vulnerabilidades: no es simple, pero no tiene por qué resultar difícil. 2014. Recuperado de: <http://www.issachile.cl/Vulnerability_Management_I>

Norma Técnica Colombiana NTC-ISO/IEC 27002. P.92,109.

OPENWARE. Attaka Plataforma para la gestión y el diagnóstico de vulnerabilidades. Recuperado de: http://www.zma.com.ar/contenidos/images/image/Attaka/Documentos/Attaka-%20Folleto.pdf

SECUTATIS INFORMATION SECURITY. Control de acceso a la red. Recuperado de: <http://www.secutatis.com/?page_id=62>

12. ANEXOS

Los anexos del proyecto se encuentran almacenados en la carpeta “Anexos” que acompaña este documento.