PROPUESTA DE SEGURIDAD PARA LA APLICACIÓN WEB SIRIUS ADM DE CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A E.S.P.

EDISON JAVIER ARION MENDOZA
JUAN CARLOS BALLESTEROS DURAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
SAN JOSÉ DE CÚCUTA, NORTE DE SANTANDER
2020

PROPUESTA DE SEGURIDAD PARA LA APLICACIÓN WEB SIRIUS ADM DE CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A E.S.P.

EDISON JAVIER ARIÓN MENDOZA
JUAN CARLOS BALLESTEROS DURAN

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Director de Proyecto:
YOLIMA ESTHER MERCADO PALENCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
SAN JOSÉ DE CÚCUTA, NORTE DE SANTANDER
2020

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Cúcuta, 20 de mayo de 2020

CONTENIDO

Pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

INTRODUCCIÓN

Hoy en día las organizaciones enfrentan grandes retos ante la competitividad que genera el entorno tecnológico, pero a su vez no deben perder de vista que la información es una parte fundamental para cumplir los objetivos y metas que se proponen. La información es importante ya que permite conocer al usuario y reducir las incertidumbres ayudando a la organización a tomar decisiones de valor administrativo, operacional, documental o histórico; pero a su vez el buen manejo de la información genera nuevos factores de competitividad, ya que está no solo depende de ofrecer productos a menor precio, si no lo que el usuario quiere: un servicio de calidad con una buena relación de costo beneficio. Las empresas de energía como **CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A. E.S.P. (CENS S.A. E.S.P.),** no son ajenas a todos estos riesgos y oportunidades que trae consigo la tecnología, sino que aún más están llamadas a ser pioneras e innovadoras en los servicios que prestan y además hacerlo teniendo en cuenta las necesidades no solo de sus clientes, sino también legales y normativas.

Una empresa de energía típica se dedica a prestar servicios de transmisión, comercialización y distribución; la Comercialización de energía es uno de los procesos más importantes de estas empresas ya que comprende desde la solicitud del servicio de energía hasta el recaudo, pasando por la toma de consumos y posterior facturación de ellos, esto es llamado ciclo de ingresos. CENS S.A. E.S.P, es una empresa de energía eléctrica que presta los servicios antes mencionados en los departamentos Norte de Santander, sur del Cesar y sur de Bolívar. Centrales eléctricas actualmente reconoce que la información es uno de sus activos más valiosos, ya que todos sus procesos organizacionales y en especial el proceso de facturación como parte importante del ciclo de aseguramiento de ingresos, tienen como entrada información confidencial de sus clientes, así como también las métricas de los dispositivos de medida (medidores de energía). Es por ello, que en este trabajo de grado se propone diseñar las políticas de seguridad basadas en las vulnerabilidades detectadas mediante la aplicación de metodologías de ethical hacking y el uso de herramientas de pentesting en un entorno controlado a la aplicación web Sirius ADM. Es decir, proponer una serie de normas, protocolos y reglamentos para proteger la seguridad de la aplicación web Sirius ADM teniendo en cuenta que dichas políticas deben adecuarse a las necesidades y recursos disponibles, ser holística, y contemplar los elementos claves en pro de salvaguardar la confidencialidad, integridad y disponibilidad de la información para minimizar o evitar los riesgos de que las amenazas se materialicen y produzcan daños tanto económicos, como de imagen para la empresa.

1. TITULO

PROPUESTA DE SEGURIDAD PARA LA APLICACIÓN WEB SIRIUS ADM DE CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A E.S.P.

2. PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

Los procesos de facturación como del equipo de control perdidas de CENS S.A. E.S.P realizan ordenes de trabajo o visitas a las instalaciones del cliente, en el caso del proceso de facturación para realizar la toma de lecturas o revisiones comerciales y para el equipo de control perdidas revisiones técnicas. Estas órdenes de trabajo se ejecutan o se diligencian en un aplicativo instalado en unas terminales portátiles que posteriormente transmiten la información vía online o por internet a la base de datos de la aplicación web Sirius ADM para que posteriormente sea transmitida al sistema comercial mediante una interfaz llamada Sirius-Cima. Pero para llevar a cabo la administración de la información relacionada con las órdenes de trabajo de la empresa se implementó una aplicación web de apoyo o complementaria llamada SIRIUS ADM, está tiene como objetivo principal servir de interface entre el sistema comercial y el servicio web llamado Sirius Server; Está aplicación permite además la administración de la programación de los dispositivos móviles, permitiendo asignar correrías de órdenes de trabajo, lectores o revisores a dichos equipos.

Como se observa la aplicación SIRIUS ADM administra información muy importante para CENS S.A. E.S.P. relacionada con la liquidación de la facturación de los usuarios, también información confidencial de los clientes como direcciones, nombres, seriales de los medidores entre otros. Al estar expuesta a transmitir y recibir información vía online o internet se expone a riesgos de ser atacada o saboteada con técnicas como: Hombre en el medio, Suplantación, Inyección SQL y Denegación de servicio entre otras; que permitirían capturar, modificar o eliminar datos sensibles como datos personales, resultados de Inspecciones o lecturas tomadas a los medidores que llevarían a alterar la facturación. Hasta el momento la aplicación web SIRIUS ADM no ha sido valorada en cuanto a seguridad informática se refiere.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo identificar las vulnerabilidades en el manejo de la información y los mecanismos a implementar para garantizar la seguridad de los datos contenidos en el aplicativo SIRIUS ADM de CENS S.A. E.S.P.?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar una propuesta de seguridad para la aplicación web SIRIUS ADM de CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A. E.S.P.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar las vulnerabilidades de la aplicación web SIRIUS ADM de CENS S.A. E.S.P con el fin de poder determinar controles.

- Determinar controles que minimicen las vulnerabilidades encontradas en la aplicación web SIRIUS ADM de CENS S.A. E.S.P

- Diseñar políticas de seguridad en la aplicación web SIRIUS ADM de CENS S.A. E.S.P. para su operación segura y oportuna.

4. JUSTIFICACIÓN

Ante los constantes avances tecnológicos, las empresas están sometidas a constantes cambios y a múltiples retos para mantener al día su información; y aunque cuentan con software cada vez más especializado, siempre existirán un sin número de riesgos que puedan causar pérdida de información. Pensando en las diversas razones y expectativas que tienen las empresas por proteger y salvaguardar su información, nace la necesidad de crear estándares y modelos aplicables a los sistemas de gestión de seguridad informática.

Hoy la aplicación web SIRIUS ADM es uno de los pilares más importantes en el proceso de facturación y por ende del ciclo de aseguramiento de ingresos de CENS S.A. E.S.P., debido a que genera los insumos principales para la liquidación del importe monetario que deben cancelar los usuarios por el servicio de energía. Está aplicación web está publicada en internet sin que se le haya realizado ningún tipo de revisión de seguridad exponiéndose a numerosos riesgos informáticos como suplantación, denegación de servicio, inyección SQL entre otros, por eso se hace necesario identificar las vulnerabilidades, diseñar controles y definir políticas de seguridad para dicha aplicación, debido a que con esto se minimiza o reduce el riesgo de que alguna de las amenazas se materialice; pues si esto ocurre el impacto que provocaría en CENS S.A. E.S.P., por no estar disponible la información almacenada en la aplicación web SIRIUS ADM sería muy alto a nivel operacional y económico y a nivel reputacional catastrófico.

Es por esta valoración e impacto de riesgos que se hace necesario realizar esta propuesta de seguridad para la aplicación web SIRIUS ADM, porque ayudaría a corto plazo a mantener y mejorar los niveles de disponibilidad de la aplicación, la satisfacción de los clientes, asegurar la facturación oportuna y se mantendrían los ingresos económicos para la empresa.

5. ALCANCE Y DELIMITACIÓN

ALCANCE

El alcance de este proyecto es identificar vulnerabilidades de la aplicación web SIRIUS ADM, diseñar controles y definir políticas de seguridad que ayuden a mantener la confidencialidad, integridad, disponibilidad y autenticidad de la información en la aplicación.

Este proyecto no contempla el desarrollo de los siguientes ítems:

- Identificación de las vulnerabilidades del sistema operativo de la granja de servidores del grupo empresarial EPM que alojan la aplicación web SIRIUS ADM, a la cual no se tiene acceso desde la filial CENS.

- Verificación de las vulnerabilidades de los dispositivos activos de red de la empresa.

- Las pruebas deberán ser realizadas en horarios no hábiles que no comprometan la operación de la empresa.

- La implementación de las políticas de seguridad debido a que requieren permisos, aprobaciones y trámites administrativos en el núcleo corporativo del grupo EPM (Medellín) al cual pertenece CENS S.A. E.S.P.

6. MARCO REFERENCIAL

6.1 ANTECEDENTES

En los años 60, los sistemas informáticos basados en la web se hacían más populares y en 1965 varios expertos en seguridad informática se reunieron en una de las primeras conferencias organizada por el COSUDE. Como resultado de esta conferencia se realizó una de las primeras peticiones para usar el pentesting como herramienta de seguridad. En 1967, en una nueva conferencia expertos como Willis Ware, Harol Petersen y Rein Tern de la Agencia de Seguridad Nacional (NSA) definieron un ataque contra un sistema computacional como “Penetración”. En escritos posteriores ellos expresaban que era necesario realizar pruebas deliberadas para comprobar la seguridad y además que en las entradas o salidas de los sistemas había mucha información que podría utilizarse por un programa de penetración para vulnerar los sistemas. Desde allí, muchos organismos gubernamentales como el Departamento de Defensa, la NSA y la CIA, contrataron a estos expertos para dirigir equipos en seguridad para realizar pruebas a sus sistemas. En los años siguientes, el uso del Pentesting como una herramienta para probar la seguridad de los sistemas sólo se volvería más refinada y sofisticada, hasta convertirse en la ciencia que hoy es.

6.2 MARCO TEÓRICO

Desde la época de Ware, Petersen y Tern hasta nuestros días, muchas personas se han dedicado a perfeccionar el arte de la seguridad informática, es por eso por lo que nos apoyaremos en los siguientes autores que han trabajado en temas similares a la temática de este documento:

Karina del Rocio Gaona Vázquez en su monografía de 2013 “Aplicación de la Metodología Magerit para el Análisis y Gestión de Riesgos de la Seguridad de la Información Aplicado a la Empresa Pesquera E Industrial Bravioto SA en La Ciudad de Machala”, realiza un análisis de riesgos basado en metodología MAGERIT y diseña un plan de seguridad que intenta llevar los riesgos a niveles aceptables para la empresa. Este proyecto nos sirve como ejemplo de la forma en que se deben clasificar los activos que componen el sistema de información Sirius ADM.

En 2014, Jhon Jairo Perafán Ruiz y Milred Caicedo Cuchimba, en su escrito “Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca”, realizan una detallada revisión de los sistemas de información de la universidad basada en riesgos que permitiría

identificar vulnerabilidades y sugerir o recomendar acciones para mitigarlos y a futuro definir un Sistema de Seguridad para la universidad; similar a Perafán y Caicedo, se decide documentar los activos que componen los sistemas de información para aplicar la metodología MAGERIT.

En el 2015, Alexandra Milena González Pombo, y Orlando Gómez Barboza, estudiantes de la Universidad Nacional Abierta y a Distancia (UNAD) en su monografía de grado "Identificar Vulnerabilidad y Diseñar Políticas de Seguridad para la Aplicación Web Sistema Integral De Registro Educación Permanente (Sirep) de la UNAD CCAV Cartagena" realizan la identificación de las vulnerabilidades en el aplicativo Sirep a través de herramientas de escaneo como Vega y Owasp Zed Attack Proxy, con el fin de reducir o eliminar los riesgos a los que se encuentra expuesto el aplicativo web. Además, está monografía realiza la clasificación de las vulnerabilidades a través del uso de la metodología Owasp (Open Web Application Security Project). Se Analizan y evalúan los posibles ataques al aplicativo SIREP usando el estándar Magerit para gestión de riesgos y por último se crean políticas de seguridad para el CCAV Cartagena. De igual forma que Alexandra, se decide para este proyecto aplicar pruebas de pentesting siguiendo la metodología Owasp, pero con otras herramientas de escaneo como Nessus y Acunetix.

6.3 MARCO CONCEPTUAL

6.3.1 Aplicaciones web. Una aplicación web es una herramienta o software alojada en un servidor web que mediante un navegador le permite al usuario final acceder a sus diferentes herramientas, estas herramientas se pueden acceder por medio de una intranet o por internet.

6.3.1.1 Tipos de aplicaciones web. Existen varias clasificaciones de aplicaciones Web bajo diferentes criterios, de entre los cuales se seleccionaron los dos más representativos: según la arquitectura del sistema y según la intención de la aplicación.

- **Según su Arquitectura.** Aunque existen múltiples alternativas a la hora de diseñar la arquitectura para una aplicación Web, todas ellas comparten unas características comunes derivadas del modelo cliente/servidor sobre el protocolo HTTP, pudiendo dividirse en tres grupos principales:

Cliente ligero (thin client). Este tipo de arquitecturas son las que menos potencia demandan del cliente, siendo ideales para aplicaciones Web que operan en Internet. El cliente consiste simplemente en un navegador con capacidad para

interpretar HTML y scripts de ejecución en el cliente ("client-side scripts" como JavaScript); esto implica que toda la carga de procesamiento cae del lado del servidor, es decir, toda la funcionalidad se ejecuta en el servidor, ejemplo paginas dinámicas en PHP, ASP entre otras[1].

Cliente pesado (thick client). En este caso, el cliente ejecuta una parte de la funcionalidad de la aplicación (lógica del negocio), por lo que se demanda de él más potencia y capacidad para ejecutar applets Java o controles ActiveX. Dentro de este apartado también se pueden incluir las aplicaciones Web que envían al cliente documentos XML para ser formateados en él con XSLT (toda la presentación cae del lado del cliente).

Reparto Web (Web delivery). En este tipo de aplicaciones se utilizan otros protocolos para la distribución de recursos además del protocolo HTTP, dando lugar a una arquitectura distribuida más rica, pero no necesariamente más compleja, porque se usan protocolos de objetos distribuidos como IIOP, DCOM o RMI. Este enfoque sólo es válido cuando los usuarios se conocen de antemano y pertenecen a la Intranet de la organización; e incluso en estas condiciones, hay que tener en cuenta las restricciones de seguridad y la infraestructura de comunicaciones de la organización.

- **Según su intencionalidad.** Las aplicaciones Web pueden agruparse en siete categorías según la intención para la que han sido creadas:

Informacionales o Documentales: son aquellas aplicaciones orientadas a difundir información. Entran en esta categoría: periódicos en línea, catálogos de productos, libros electrónicos en línea, etc.

Interactivas: son aquellas aplicaciones en donde el usuario proporciona información interactuando con la aplicación, por ejemplo: formularios de registro, presentación de información personalizada, juegos en línea, etc.

Transaccionales: se dice de las aplicaciones en donde se establecen relaciones

[1] TS TALENT GROUP. Qué son las Aplicaciones Web? Ventajas y Tipos de Desarrollo Web https://tstalent.net/site/es/noticias/117-que-son-las-aplicaciones-web-ventajas-y-tipos-de-desarrollo-web.html

con bases de datos, creando, eliminando y modificando datos. Ejemplo de ellas son la banca en línea, compras electrónicas, etc.

De flujo de trabajo: para controlar el desarrollo de alguna actividad o tarea como control de inventariado, monitorización de estados, etc.

Entornos de trabajo colaborativo: donde varios usuarios pueden trabajar sobre el mismo conjunto de datos recibiendo en tiempo real las modificaciones que realizan el resto de usuarios. Por ejemplo, sistemas de diseño distribuidos, herramientas de diseño colaborativo, etc.

Comunidades online: aquellas en las que un grupo de usuarios están comunicados e intercambian opiniones, información e incluso documentos entre sí. Ejemplos de este tipo de aplicaciones son los grupos Chat, mercados en línea, actuaciones en línea, foros, etc.

Portales Web: sitio desde donde se puede acceder a múltiples servicios ofertados a los usuarios con el fin de realizar trámites, solicitar servicios. Realizar pagos, etc[2].

6.3.2 Penetration test. Penetration test (Test de penetración), es el análisis de la seguridad de la infraestructura de redes y sistemas de información en busca de vulnerabilidades. Principalmente consiste en el intento de acceso a varios puntos de dichos sistemas mediante pruebas de intrusión que simulan las que se producen durante un ataque de una persona malintencionada. Su principal objetivo es infiltrarse en las instalaciones de una empresa y tratar de burlar toda la seguridad que esta tenga, para al final extraer toda la información valiosa y confidencial que se pueda. También se define Ethical hacking como un conjunto de metodologías y técnicas que permiten realizar una evaluación general de las debilidades de los sistemas informáticos ejecutando pruebas de intrusión en un entorno empresarial, que en resumen se refiere al proceso de someter la seguridad de una empresa a un ataque controlado para identificar las debilidades de sus sistemas, antes que un atacante real lo haga[3].

---

[2] SERGIO ESCRIBA. Todas las páginas web existentes para tu negocio: Tipos y clasificación. https://sergioescriba.com/tipos-clasificacion-paginas-web/

[3] IT GOVERNANCE BLOG ES. Qué es un test de penetración y para qué sirve. https://www.itgovernance.eu/blog/es/que-es-un-test-de-penetracion-y-para-que-sirve.

- **Importancia de un penetration test.** Los problemas de seguridad de los sistemas se presentan de muchas formas en nuestra sociedad y las empresas se encuentran cada vez más expuestas a ataques informáticos, por lo que ellas buscan tener mayor seguridad en sus sistemas de información y como consecuencia una buena imagen corporativa, pero el principal objetivo es evitar tener pérdidas económicas, como también de disponibilidad, integridad y confidencialidad de su información. Mediante la realización de un Test de penetración se contempla esta problemática y como resultado se cuida la seguridad de la información ya que los especialistas en esta rama no solo tratan de identificar e informar las debilidades, sino que también intentan explotarlas con el objetivo de validar los niveles de intrusión a los que se expone el sistema de información analizado. Por lo anterior se reducen los potenciales riesgos y su impacto, permitiendo el fortalecimiento de la seguridad de los sistemas de información y las redes de comunicaciones de las empresas.

  De acuerdo a lo anterior se definen políticas de seguridad que deben responder a tres interrogantes: ¿Contra qué hay que defenderse? ¿Por qué hay que defenderse? Y ¿Con qué podemos defendernos? las respuestas están basadas en los resultados de las pruebas de penetración que son un paso previo a los análisis de riesgos, enfocadas en comprobar y clasificar vulnerabilidades y el impacto que éstas tengan sobre las empresas.

  Por último, un Penetration Test deja al descubierto las debilidades que pudieran ser detectadas y explotadas por individuos no autorizados como: crackers y hackers y así hacer recomendaciones con base en las prioridades de la empresa que sirvan para mitigar y eliminar las deficiencias encontradas con el fin de reducir la probabilidad de que los riesgos puedan materializarse provocando la disminución de tiempo y esfuerzos requeridos para recuperase de ellos. Por todo lo anterior en necesario realizar un test de penetración en las Empresas para:

  - Identificar vulnerabilidades conocidas o desconocidas, antes que lo haga alguien con mala intención.

  - Evaluar cuál es el impacto real de una vulnerabilidad, mediante la realización de pruebas controladas.

  - Poner a prueba las políticas de seguridad existentes.

  - Estar preparado ante posibles ataques y construir planes de recuperación adecuados.

  - Evaluar fallas de seguridad en las aplicaciones por mala configuración.

- Proveer recomendaciones en base a los riesgos y debilidades detectadas.

- **Tipos de penetration test**. Existen varios tipos de pruebas de penetración, cada una puede simular diferentes escenarios y niveles de seguridad. Cada tipo representa un atacante con diferentes conocimientos y diferentes intenciones sobre la empresa víctima. Entre los tipos de penetration test más conocidos tenemos los siguientes:

  - **Penetration Test de Caja Negra:** En este tipo de Penetration test el consultor no recibe ningún tipo de información ni acceso autorizado al sistema o red que debe analizar, por lo que esto implica la realización de una evaluación de la seguridad sin conocimientos previos sobre la infraestructura objetivo. Se simula el ataque malicioso desde fuera de los límites de la empresa. Es típicamente el más rápido, pero no necesariamente el más efectivo, pues normalmente solo se escoge un escenario pudiendo generar un nivel de confianza excesivo

  - **Penetration Test de Caja Blanca:** El hacker tiene acceso a toda la información del sistema o red que debe analizar y la prueba de seguridad se realiza con total conocimiento de la infraestructura, como si fuera el administrador de red. Lo anterior produce una mayor probabilidad de detectar vulnerabilidades. En este tipo de pruebas se simula el peor de los casos para la empresa lo cual ofrece un importante nivel de confianza. La persona que realice la prueba de intrusión debe ser éticamente confiable.

  - **Penetration Test de Caja Gris:** Se refiere al caso en el que el hacker o atacante cuenta con solo una parte de la información y realiza pruebas para evaluar la seguridad y otras pruebas internas. Este tipo de Penetration Test examina el grado de acceso de las personas con información privilegiada dentro de la red.

- **Etapas que involucran un penetration test**. Se tienen siete etapas principales para el desarrollo de un Penetration Test que se citan a continuación:

  - **Definición del alcance:** Se trata de delimitar el test de penetración y establecer con la empresa reglas y políticas claras de hasta qué nivel se podrá llegar con las respectivas pruebas de intrusión.

- **Fase de recolección de información:** En esta fase se obtienen toda la información posible de la empresa disponible a través de internet y de las redes sociales de sus empleados, ejecución de scanners, etc. para hacernos una idea más clara de los sistemas y programas que usa la organización.

- **Fase de modelado de amenaza:** En este momento y a partir de la información recogida previamente, debemos pensar como hackers en cuál va a ser nuestra estrategia de intrusión. Cuáles serán los objetivos y de qué manera se pueden llegar a ellos. Puede ser que sobre la marcha se cambie la estrategia.

- **Fase de Análisis de vulnerabilidades:** En este punto debemos valorar la probabilidad de éxito de las estrategias de intrusión a través de la identificación proactiva de vulnerabilidades. Aquí es donde la experiencia, conocimiento y habilidad del pen-tester se pone a prueba para detectar el mayor número de vulnerabilidades que permitan llegar a los objetivos[4].

- **Fase de Explotación:** Una vez conseguido lo anterior, llega el momento de intentar conseguir acceso a los sistemas objeto de nuestra intrusión, para ello ejecutaremos programas llamados exploits contra las vulnerabilidades identificadas anteriormente o simplemente utilizaremos los usuarios y contraseñas obtenidas para ganar acceso a ellos.

- **Fase de Post-Explotación:** En esta fase se trata de conseguir el máximo nivel de privilegios e información de la red y a su vez el mayor número posible de ingresos a sistemas identificando información crítica.

- **Fase de Informe:** Finalmente se presenta el resultado de la auditoría al cliente, Es necesario redactar de forma tan sencilla que cualquier persona lo pueda entender, teniendo en cuenta que este informe no solo es para el personal de TI, sino para personal directivo que evaluara los riesgos y su respaldo en la implementación de controles que los eviten.

---

[4] CENTRO DE INVESTIGACION CIBERNETICA. Módulo Hacking Ético. https://www.cibe2000.com/hacking-etico

- **Actores de las pruebas de penetración.** Las pruebas de penetración pueden ser realizadas por un empleado interno calificado y entrenado o un proveedor de servicios calificado, estos deben ser expertos en sistemas informáticos y estar muy involucrados con el desarrollo de aplicaciones, la configuración y montaje de redes y los diferentes sistemas operativos como Windows, Unix, Solaris. Un pen-testing debe poseer varias competencias como la paciencia, la persistencia y la perseverancia debido al tiempo invertido y el nivel de concentración que requieren para realizar la mayoría de los ataques y obtener buenos resultados. Si se están realizando las pruebas de penetración con recursos internos estos recursos deben ser los más experimentados. Los individuos que realizan pruebas de penetración deben estar separados del ambiente que está siendo testeado y evitar ser "juez y parte". Por ejemplo, el administrador del servidor no debe realizar la prueba de penetración al firewall pues estaría sesgada por el pre-conocimiento que tiene. La mayoría de las veces son los hackers éticos los encargados de realizar las pruebas de penetración en las empresas debido a su conocimiento de las áreas de seguridad o relacionadas a ella. Estos están motivados en descubrir lo que un atacante malicioso puede ver en los sistemas o en la red, hay que recalcar que los hackers éticos no necesariamente son expertos en la implementación de los controles que pueden prevenir los ataques.

6.3.3 Hackers. Normalmente a las personas que son Hacker se les estigmatiza, sin saber si sus objetivos son altruistas o destructivos. Un hacker es una persona con altos conocimientos en ciencias computacionales y de comunicaciones, que, por eso mismo, pueden romper una contraseña y eso les permite obtener información confidencial de las organizaciones. Pero no todos los hackers son malos, ni tienen negras intenciones, gran parte de ellos se dedican a velar por la seguridad de los sistemas en las empresas y otros contribuyen a mejorar los softwares informando a los fabricantes vulnerabilidades, éstos se conocen como hackers éticos, es decir son profesionales en seguridad informática que realizan pruebas de penetración a una red o sistema en busca de debilidades o vulnerabilidades usando sus propios conocimientos y herramientas[5].

Sin embargo, un cracker se podría describir como alguien que utiliza sus habilidades para hacer mal, o para destruir. Estos tratan de infiltrarse a los sistemas para causar daño, buscan formas de bloquear medios o dispositivos de protección para la propagación de virus o para dejar fuera de servicio el sistema o la red, a esto último se le conoce como ataque de denegación de servicio (DoS).

---

[5] ENRIQUE ARRIOLS. Tipos de hackers según su conducta. https://tecnologia.uncomo.com/articulo/tipos-de-hackers-segun-su-conducta-49396.html

A veces son contratados para dañar la reputación de grandes empresas mientras que al mismo tiempo indisponen los procesos de negocio, comprometiendo la integridad de la información de las empresas. Por lo tanto, el cracker se distingue del hacker ético por sus acciones: los hackers son altruistas, mientras los crackers son destructivos. Las definiciones anteriores dan pie a que se pueda dividir a los hackers en tres grupos: Hacker de sombrero negro, sombrero blanco y sombrero gris.

- **Hacker de Sombrero Negro:** Estos se refieren a los crackers, quienes principalmente motivados por ensalzar su ego y obtener dinero utilizan sus habilidades con fines ilegales o inmorales. Un hacker de sombrero negro se aprovecha de las deficiencias de seguridad con el objetivo de robar o destruir información.

- **Hacker de Sombrero Blanco:** Se refiere a los hackers éticos quienes utilizan sus habilidades de hacking con objetivos defensivos y preventivos. Normalmente, los hackers de sombrero blanco son expertos de seguridad informática que se especializan en realizar pruebas de intrusión para localizar debilidades o vulnerabilidades e implementar controles a fin de asegurar los sistemas de información y demás infraestructura tecnológica de las empresas. Los hackers de sombrero blanco protegen las empresas de los hackers de sombrero negro.

- **Hacker de Sombrero Gris:** Son los que juegan a ser buenos y malos a la vez, suelen tener los conocimientos de un hacker de sombrero negro, con ellos penetran en sistemas y buscan vulnerabilidades y luego ofrecen sus servicios para aplicar controles a las vulnerabilidades que hallaron bajo un contrato.

6.3.4 Ethical Hacking. Se define como Ethical hacking la forma de explotar las deficiencias de seguridad encontradas en los sistemas de información valiéndose de un Test de penetración, que valida y evalúa su propia seguridad física y lógica, infraestructura de redes, servicios y aplicaciones web, bases de datos, servidores, etc. con la firme intención de ingresar y mostrar que un sistema es vulnerable, obteniendo información que ayuda a las empresas a tomar las medidas preventivas en contra de posibles ataques malintencionados.[6]

---

[6] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Ethical Hacking. https://www.cert.org.mx/historico/documento/index.html-id=7

El objetivo de un Hackeo Ético es realizar ataques de manera controlada, así como actividades del “modus operandi” de los ciber-delincuentes, esta forma de actuar tiene su base en el dicho de que "Para atrapar un ladrón, primero debes pensar como ladrón".

6.3.4.1 Tipos de Ethical Hacking. Los hackers éticos pueden usar gran variedad de métodos para violar la seguridad de una empresa durante un penetration test. Entre los métodos más comunes tenemos:

- **Forma Remota:** Representa un hacker ético elaborando un ataque a través de Internet, es decir, intenta romper o encontrar una vulnerabilidad desde afuera de los límites de las protecciones de la red, por ejemplo, en el firewall, el proxy o en el router.

- **Forma local:** Representa a alguien con acceso físico obteniendo acceso y privilegios adicionales no autorizados utilizando la red local. Para realizar este tipo de ataque el hacker ético debe ganar acceso directo a la red local, normalmente pudiendo infiltrarse a las instalaciones de las empresas.

- **Sustracción de Equipos:** Supone el robo de un computador corporativo. La Información de seguridad como usuarios, contraseñas, configuración de red y otras pueden ser obtenidos al robar una computadora portátil de un empleado.

- **Ingeniería Social:** Hoy en día es una de las técnicas más usadas, intenta validar la integridad de los empleados a través de llamadas o comunicaciones directas haciéndose pasar por alguien o en representación de alguna empresa que tenga relación con la organización. Con esto pueden obtener información que después es usada para hacer la intrusión.

- **Ingreso físico:** Es el intento de infiltrarse físicamente en las instalaciones. Un hacker ético que logra el acceso físico a la empresa puede desplegar por hardware un virus troyano, etc. directamente sobre los computadores conectados a la red.

6.3.4.2 Metodologías de Ethical Hacking. Dentro de las múltiples metodologías más relevantes de Ethical Hacking posibles hoy en día tenemos las siguientes:

- ***Osstmm*.** El Open-Source Security Testing Methodology Manual, propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura, estos niveles de seguridad se le denominan comúnmente Dimensiones de Seguridad y normalmente consiste en analizar los siguientes factores: visibilidad, acceso, confianza. autenticación, confidencialidad, privacidad, autorización, integridad, seguridad, alarma[7].

  Como parte de un trabajo secuencial la metodología OSSTMM consta de 6 ítems los cuales comprenden todo sistema actual, estos son:

  - ✓ Seguridad de la Información
  - ✓ Seguridad de los Procesos
  - ✓ Seguridad en las tecnologías de Internet
  - ✓ Seguridad en las comunicaciones
  - ✓ Seguridad inalámbrica
  - ✓ Seguridad Física

  Información adicional para la Auditoria.

  - ✓ Copias de informes anteriores de auditoría.
  - ✓ Documentación sobre la configuración hardware y software del sistema
  - ✓ El diagrama de red con la topología y el direccionamiento IP
  - ✓ Las Políticas, Normativa y Procedimientos de Seguridad relacionados
  - ✓ El Plan de Contingencia (BCP) y Recuperación de Desastres (DRP)
  - ✓ Datos de las personas o grupos responsables de la gestión, administración y operación del Sistema, así como del personal de Soporte y Mantenimiento
  - ✓ Datos de los proveedores de los equipos involucrados en la Auditoría, así como los términos, cláusulas, ámbito y fechas de los contratos de mantenimiento.
  - ✓ Manuales de Administración y Operación de los Sistemas de Información a auditar.

- ***Owasp.*** El proyecto abierto de seguridad de aplicaciones web (por sus siglas en inglés), es un proyecto de código abierto dedicado a determinar y combatir

---

[7] RAFAEL AUSEJO PRIETO. La metodología OSSTMM. http://www.ausejo.net/seguridad/osstmm.htm

las vulnerabilidades que hacen que el software sea inseguro. Se enfoca en la seguridad de los sistemas informáticos especialmente en las aplicaciones web, considerando las dimensiones de tecnología, procesos y personas a través de la creación de varias guías, metodologías y herramientas que son de distribución y uso gratuito. Se enfoca en el desarrollo seguro de aplicaciones web basadas en modelos de riesgos de amenazas. OWASP está estrechamente influenciada por marcos de referencia como COBIT y la norma ISO 17799, y todo lo escrito en la guía va en relación con el cumplimiento de estas buenas prácticas. Por lo anterior para una correcta implementación o interiorización requiere de un apoyo total y decidido de la alta gerencia y directivos de las empresas que tomen libremente la decisión de implementarla[8].

La metodología hoy por hoy presenta los siguientes diez puntos a ser evaluados en un sistema informático:

- ✓ A1-Inyección
- ✓ A2-Secuencia de Comandos en Sitios Cruzados (XSS).
- ✓ A3-Perdida de Autenticación de y Gestión de Sesiones.
- ✓ A4-Referencia Directa Insegura de Objetos.
- ✓ A5-Falsificación de Petición de Sitios Cruzados (CSRF).
- ✓ A6-Configuración Defectuosa de Seguridad.
- ✓ A7-Almacenamiento Criptográfico Inseguro.
- ✓ A8-Falla de restricción de acceso URL.
- ✓ A9-Protección Insuficiente de la Capa de Transporte.
- ✓ A10-Redirecciones y Destinos No Validos.

- ***Offensive Security.*** Esta metodología se basa en desarrollar estudios de seguridad y pruebas de penetración, utiliza métodos enfocados en la seguridad ofensiva y explotación de los indicadores de riesgos y vulnerabilidades. Dentro de las ventajas de utilizar esta metodología tenemos:

  - ✓ Explotación real de las plataformas
  - ✓ Enfoque altamente intrusivo
  - ✓ Se basa en resultados tangibles y no en estadísticas

[8] INFORMÁTICA, SEGURIDAD Y ALGO MÁS. OWASP. https://infow.wordpress.com/2010/12/16/owasp/

- ***Issaf*.** La metodología ISSAF está diseñada para evaluar la seguridad en redes de trabajo, sistemas operativos y control de aplicaciones y poder ofrecer recomendaciones que ayuden a minimizar los riesgos que afecten la continuidad del negocio[9].

  La Metodología se desarrollará en tres fases:

  A- Planificación y Preparación: En esta primera fase de pre-evaluación, se debe hacer reconocimiento actual de la empresa. Identificando las personas que intervienen en las pruebas, alcances del diagnóstico, cronograma de actividades, controles existentes, para lograr obtener una perspectiva completa de las vulnerabilidades presentadas y definir los puntos de partida de la evaluación.

  En esta etapa se pueden realizar actividades como:
  - ✓ Conocer el estado actual de la empresa.
  - ✓ Identificar las personas que intervienen en las pruebas.
  - ✓ Definir alcances del diagnóstico
  - ✓ Establecer cronograma de actividades
  - ✓ Indagar controles existentes

  B- Evaluación: Fase donde se ejecutan las pruebas que se presupuestaron en la fase "planificación y preparación", bajo algunas plantillas que permitan identificar y recolectar los factores internos o externos que estén afectando la empresa en cuanto al sistema de información.

  Estas actividades son:

  - ✓ Recopilar y analizar la información.
  - ✓ Mapeo de la Red.
  - ✓ Identificación de vulnerabilidades.
  - ✓ Penetración
  - ✓ Obtener acceso y nivel de privilegios
  - ✓ Enumeración de las vulnerabilidades detectadas.
  - ✓ Compromiso de usuarios remotos y del sitio
  - ✓ Mantenimiento de acceso.
  - ✓ Identificar rutas de ataque y posibles escenarios

  La figura 1 muestra las fases o etapas que se deben seguir para la aplicación de

---

[9] SEGURIDAD INFORMÁTICA. Metodología de test de intrusión ISSAF. http://insecuredata.blogspot.com/2009/04/metodologia-de-test-de-intrusion-issaf.html

la metodología de penetración ISSAF.

Figura 1. Metodología ISSAF

Fuente: Autores

C- Reportes, Limpieza y Destrucción de Objetos: Una vez concluido la fase de evaluación, se analiza para presentar los reportes de vulnerabilidades detectadas para presentar recomendaciones e informar inmediatamente al área para tomar las medidas correctivas del caso. El informe debe contener como mínimo:

- ✓ Resumen de gestión
- ✓ Alcance del proyecto
- ✓ Pruebas utilizadas
- ✓ Historial de fechas y tiempos de las pruebas.

6.3.5 Ataques a bases de datos. Hoy por hoy, las bases de datos son componentes fundamentales de cualquier aplicación con arquitectura Web, permitiendo que los sitios (sites) provean contenido dinámico. Debido a que mucha información considerada sensible o secreta puede ser almacenada en una base de datos, se tiene que considerar seriamente la protección de sus bases de datos o repositorios de información. Entre más acciones se tomen para incrementar la protección de la base de datos, menor será la probabilidad de que un atacante tenga

éxito, si lo lograse podría exponer o abusar de cualquier información allí almacenada. La mayoría de las veces un buen diseño del esquema de la base de datos y de la aplicación basta para lidiar con los mayores temores en cuanto a ciberseguridad se refiere. En este sentido, la información almacenada en los diferentes sistemas gestores de bases de datos es propensa a diferentes ataques que permitan acceder a dicha información, en donde se realiza una investigación de manera exhaustiva que permita identificar las vulnerabilidades que poseen los gestores o fallos en la seguridad del software y poder de esta forma atacar las bases de datos objetivo. Entre los ataques más comunes tenemos[10]:

- **Desbordamiento de buffer u overflow**. Esta vulnerabilidad se presenta por la inserción de gran cantidad de datos que supera a lo esperado por una aplicación, esto ocasiona la sobre escritura en la memoria en los espacios reservados en la memoria como lo son el stack que es donde se almacenan las variables locales, los argumentos de funciones y las funciones de retorno, y el heap que asigna la memoria dinámica que es requerida durante el tiempo de ejecución. Dentro de los ataques de desbordamiento de buffer podemos mencionar el más conocido stack overflow.

- **Sql injecction.** Estos ataques se realizan a través de la inserción de una consulta SQL oculta en una petición del cliente, dicho ataque tiene como finalidad cambiar la intensión real de la solicitud de acuerdo a lo que realice el atacante en las sentencias SQL directamente en la base de datos, el ataque que se realiza de forma exitosa puede obtener la derivación de la autenticación y la posible divulgación de información para facilitar la distribución de código malicioso a los usuarios. El atacante también puede realizar mediante la inyección SQL el descubrimiento de información llamado (information disclosure) modificando consultas para poder de esta forma acceder a registros u objetos de la base de datos, además puede realizar con este ataque la elevación de privilegios en donde se puede acceder a los identificadores de los usuarios más privilegiados y modificar dichas credenciales. La inyección de SQL también puede ocasionar la denegación del servicio por parte del atacante al modificar comandos SQL que generan diversas acciones destructivas como por ejemplo el bloqueo de servicios con comandos de parada y arranque de los sistemas, el borrado de datos o inyectar comandos que generen un alto cómputo en el motor de la base de datos y que el servicio no pueda responder en tiempos útiles a los usuarios.

[10] SHARPMIND SOFTWARE. los diez (10) tipos de vulnerabilidades de bases de datos más comunes. http://sharpmindsoftware.com/los-diez-10-tipos-de-vulnerabilidades-de-bases-de-datos-mas-comunes.b.aspx

- **Ataque de denegación de servicio DDOS**. Un ataque de denegación es donde varios equipos de cómputo se unen para atacar a un solo objetivo que puede ser un servidor, un sitio web o una base de datos con el objetivo de dejarla fuera de servicio para los usuarios que quieran ingresar, esto lo hace por medio de envíos de mensajes a tal punto que sobrecarga al sistema para que indisponga el servicio que brinda. Los ataques de denegación de servicio se pueden realizar de diferentes formas y comparten ciertas características en la implementación entre ellas tenemos:

    - Tienen un consumo alto de recursos de sistema,
    - Modificar la configuración de la información
    - Modificaciones de configuración de estado, por ejemplo, interrupción de sesiones TCP.
    - Interrupción de elementos físicos de red.
    - Interrupción de los medios que enlazan un servicio y la víctima, de manera que ya no pueda haber comunicación.

- **Cross-Site Scripting**. Es un tipo de ataque que obliga al sitio web ejecutar el código suministrado o ingresado por un atacante el cual se abrirá una vez que cargue el sitio o página web en el navegador del usuario. Este código está escrito en la mayoría de tecnologías que soporta los navegadores web como; JavaScript, flash, entre otros. Cuando un atacante consigue que el navegador del usuario ejecute este código, este se ejecutara dentro de la zona de seguridad del navegador el cual tiene unos privilegios como la lectura, escritura y transmisión de los datos sensibles del usuario. Hay dos tipos de ataques Cross-site Scripting, persistentes y no persistentes. Los ataques persistentes se hacen cuando el código es presentado al sitio web donde se almacena durante un periodo de tiempo. Los ataques no persistentes requieren que un usuario visite un enlace especialmente diseñado que incluye código malicioso. Al visitar este enlace, el código incrustado en la URL será repetido y ejecutado dentro del navegador web del usuario.

- **Robo por sniffing**. Este tipo de ataque se da cuando el atacante tiene un programa de sniffing en la red del usuario y puede interceptar el tráfico destinado al mismo, incluido su identificador de sesión. Es algo que ha dado mucho de qué hablar a causa de Firesheep, una extensión para Firefox que permite robar las sesiones de Facebook, Twitter y otras páginas web muy conocidas en redes inalámbricas públicas. La única forma de prevenir estos ataques es utilizando cifrado HTTPS en toda la página web.

6.3.6 Conceptos de seguridad informática. Los siguientes conceptos son necesarios para entender esta propuesta de seguridad:

- *Riesgo informático:* Puede definirse como la probabilidad de que ocurra un evento no deseado muchas veces impredecible, es decir, es la materialización de una amenaza o vulnerabilidad no tratada.

- *La Seguridad informática:* Es proteger la infraestructura tecnológica de hardware y software que soportan las tareas misionales de las empresas identificando vulnerabilidades o riesgos que puedan llegar a materializarse.

- *Seguridad de la información:* Es mucho más amplia que la seguridad informática pues además de la infraestructura se ocupa de otros factores como: las personas, procesos de negocio, seguridad perimetral, riesgos y continuidad del negocio.

- *Las políticas de seguridad de la información:* Son normas o lineamientos expedidas por la alta dirección de las organizaciones con el fin de prevenir, controlar y/o mitigar los riesgos a que está expuesta la información en todas sus fases creación, modificación, almacenamiento, etc. Está debe ser socializada con todo el personal de las organizaciones en todos los niveles de la estructura para asegurarse de que sea entendida, asimilada e interiorizada a fin de que sea más fácil su comprensión y especialmente su aplicación e implementación.

- *Ciclo de facturación:* Es la unidad de mayor de agrupamiento de clientes para los procesos de facturación. En SAC adicionalmente existen subgrupos como zona, municipio y sección (ésta es la menor).

- *Ruta:* Es equivalente al Numero_Instalacion (Codinstalacion) está compuesta por Sucursal, Sector, Zona y Correlativo Ruta.

- *Ordenes de trabajo:* En el proceso de lecturas equivale a las medidas o lecturas. Esto concepto cambia un poco para revisiones. Si un cliente tiene activa y reactiva tendrá dos órdenes de trabajo.

- *Correría:* Es el grupo de órdenes de trabajo que se cargan en una terminal como un grupo. Normalmente es el trabajo que realiza un lector en un día.

6.4 MARCO LEGAL

En Colombia, las siguientes leyes y decretos regulan la protección de la información, datos personales y en general el sector de las TIC's:

Ley 599 de 2000. El congreso de la Republica de Colombia con la promulgación de la Ley 599 de Julio 24 de 2000, “por la cual se expide el Código Penal” en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones en el artículo 192: Violación ilícita de comunicaciones, permitiendo que se diera inicio a la protección de los datos en Colombia.

Ley 1273 de 2009. Con el auge que ha tenido el internet y el rápido crecimiento de las tecnología web, ha llevado a la masificación del uso de aplicaciones WEB y por consiguiente el aumento de los delitos informáticos relacionados con ellas, llevando a que el Congreso de la Republica de Colombia sancionará en enero de 2009 la Ley 1273, "por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado 'De la Protección de la información y de los datos'– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" con el fin de establecer normatividad para combatir el cibercrimen. Con la creación de esta Ley se da un valor jurídico a la información, estableciendo las conductas criminales que tienen que ver con sistemas de cómputo y las nuevas tecnologías.

Ley 1581 de 2012. En octubre de 2012 el gobierno colombiano promulgó la Ley 1581, que en su artículo primero reza el objeto de la ley como ”La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.”. Estas normas amparan la disponibilidad, integridad, confiabilidad y seguridad de la información privilegiada (datos personales y datos estratégicos) tanto de los clientes del servicio de energía, como de CENS contenida en la aplicación Web SIRIUS ADM. Esta información corresponde a nombres, direcciones, teléfonos, correos de los clientes, así como características, codificación y ubicaciones de los ciberactivos eléctricos que pueden llegar a comprometer la seguridad de la infraestructura eléctrica de CENS.

6.5 MARCO CONTEXTUAL

Nombre de la empresa: Centrales Eléctricas del Norte de Santander S.A E.S.P., cuya sigla es CENS S.A E.S.P., es una empresa de servicios públicos mixta de nacionalidad colombiana, constituida como sociedad por acciones del tipo de las anónimas, sometida al régimen general de los servicios públicos domiciliarios y que ejerce sus actividades dentro del ámbito del derecho privado como empresario mercantil. La empresa como la conocemos hoy fue constituida el 16 de octubre de

1952 mediante Escritura Pública 3552 de la Notaría Octava de Bogotá y quedó configurada como filial del Grupo Empresarial EPM a partir del 19 de marzo de 2009.

CENS S.A E.S.P. está autorizada para prestar el servicio público domiciliario de energía eléctrica. Dentro de su objeto social, CENS S.A E.S.P. está autorizada para prestar el servicio público domiciliario de energía eléctrica y sus actividades complementarias de transmisión, distribución y comercialización, así como la comercialización y prestación de servicios de telecomunicaciones y las actividades que la complementen, de acuerdo con el marco legal regulatorio.

Estos servicios son prestados por la empresa en Cúcuta y su área metropolitana, Departamento Norte de Santander, sur del Departamento del Cesar y sur del Departamento de Bolívar, para lo cual cuenta con cuatro (4) regionales ubicadas en los municipios de Pamplona, Ocaña, Tibú y Aguachica y 39 localidades que atienden 47 municipios[11].

Reseña Histórica: La historia de la compañía inicia el 16 de junio de 1896 con la protocolización de la Escritura Pública 121 que crea la “Compañía de Alumbrado Eléctrico de Cúcuta”, quien a través de una planta hidroeléctrica de 220 kW de generación ubicada en "Los Colorados" suministra energía eléctrica a Cúcuta. Posteriormente, el 16 de octubre de 1952 y mediante Escritura Pública 3552 de la Notaría Octava de Bogotá, se constituye la empresa "Centrales Eléctricas de Cúcuta SA", la cual inició operaciones el 3 de enero de 1953 y posteriormente en 1955, cambió su razón social por "Centrales Eléctricas del Norte de Santander SA". En 1961 la electrificadora adquirió las Empresas de Energía Eléctrica de Pamplona y Ocaña, incorporando sus activos al sistema de electrificación departamental, con lo cual cumple su aspiración de atender la totalidad de municipios de Norte de Santander.

En el marco de la ley 142 de 1994, CENS se constituyó como Empresa de Servicios Públicos, siendo en ese entonces la Nación el principal accionista de la empresa con el 78,98% de las acciones y quedando a partir de esa fecha bajo la vigilancia y control de la Superintendencia de Servicios Públicos Domiciliarios. “La compañía inicia sus operaciones el 16 de junio de 1896”

En el primer trimestre de 2009 y mediante un proceso de enajenación de acciones de su propiedad, la Nación efectuó la venta de tres empresas distribuidoras y comercializadoras de energía eléctrica, entre las cuales se contaba CENS S.A. E.S.P, cuya subasta se efectuó por la totalidad del porcentaje de participación

[11] CENS S.A E.S.P. ¿Quiénes somos? http://www.cens.com.co/es-co/institucional/%C2%BFqui%C3%A9nessomos.aspx

accionaría de la Nación, quedando dicho paquete accionario en manos de EPM Inversiones S.A. Posteriormente, el 23 de julio de 2009, Empresas Públicas de Medellín E.S.P como accionista de EPM Inversiones, adquirió el 12,54% de las acciones de propiedad del Comité Departamental de Cafeteros, transacción con la cual el Grupo EPM pasó a ser el mayor accionista con una participación del 91,52%, convirtiendo a CENS en una filial del Grupo Empresarial[12].

Objeto social: La sociedad tendrá por objeto la prestación del servicio público domiciliario de energía eléctrica y sus actividades complementarias de transmisión, distribución y comercialización de energía eléctrica; presta los servicios de calibración e inspección de medidores, transformadores e instrumentación eléctrica; todos los servicios de telecomunicaciones, así como la comercialización y prestación de servicios o actividades de telecomunicaciones y actividades complementarias, de acuerdo con el marco legal y regulatorio.

Igualmente para lograr la realización de los fines que persigue la sociedad o que se relacionen con su existencia o funcionamiento, la empresa podrá celebrar y ejecutar cualesquiera actos y contratos, entre otros: prestar servicios de asesoría; consultoría; interventoría; intermediación; importar, exportar, comercializar y vender toda clase de bienes o servicios; recaudo; facturación; toma de lecturas; reparto de facturas; construir infraestructura; prestar toda clase de servicios técnicos, de administración, operación o mantenimiento de cualquier bien, contratos de leasing o cualquier otro contrato de carácter financiero que se requiera, contratos de riesgo compartido, y demás que resulten necesarios y convenientes para el ejercicio de su objeto social. Lo anterior de conformidad con las leyes vigentes[13].

Organigrama: La estructura administrativa de CENS está compuesta por: Gerencia General, Dos (2) Subgerencias, Cinco (5) Áreas, Tres (3) Unidades. Estas dependencias están operadas por 514 empleados de planta y aproximadamente 300 contratistas internos[14]. La figura 2 nos muestra la estructura administrativa actualmente aprobada por la junta directiva de CENS.

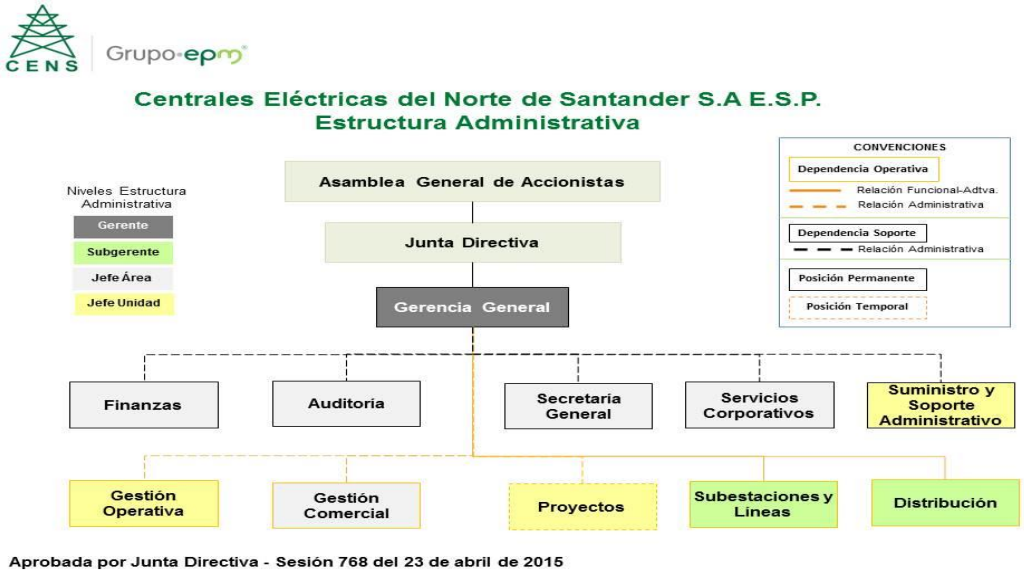
---

[12] CENS S.A E.S.P. Reseña histórica http://www.cens.com.co/es-co/institucional/rese%C3%B1ahist%C3%B3rica.aspx

[13] CENS S.A E.S.P. Objeto social http://www.cens.com.co/es-co/institucional/objetosocial.aspx

[14] CENS S.A E.S.P. Estructura administrativa http://www.cens.com.co/es-co/institucional/estructuraadministrativa.aspx

Figura 2. Estructura Administrativa



Fuente. https://www.cens.com.co/es-es/institucional/quienessomos.aspx

7. MARCO METODOLÓGICO

7.1 METODOLOGÍA DE INVESTIGACIÓN

Este proyecto se desarrolla basado en un enfoque de investigación de tipo aplicada en la cual se realizarán las actividades de recopilar, ordenar y analizar la información relacionada con la aplicación web SIRIUS ADM y servidor web para identificar las vulnerabilidades que presentan para así definir los controles y políticas de seguridad que minimicen los riesgos de que las amenazas se hagan efectivas.

7.2 METODOLOGÍA DE DESARROLLO

Para la ejecución de este proyecto se establecen las siguientes etapas:

Levantamiento de Información sobre CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A. E.S.P: En esta etapa se realizará un reconocimiento sobre CENS S.A E.S.P., empresa en la cual está implementada la aplicación, y en la que se ejecutará el análisis de vulnerabilidades. Dentro de los principales objetivos de esta etapa, se encuentra identificar la misión, visión y objetivos de la empresa. Luego se ahondará en la funcionalidad de la aplicación y específicamente, se buscará entender que procesos dentro de la empresa son soportados por la aplicación objetivo del análisis de vulnerabilidad. Esto permitirá enmarcar que tipo de información maneja la empresa a nivel general y también en la aplicación objetivo del trabajo.

Levantamiento de Activos de Información: En esta etapa se realizará un levantamiento de los activos de información que están asociados a la aplicación Web SIRIUS ADM. Los activos serán clasificados, se realizará una descripción de cada activo, se identificará su localización y quien es el propietario del activo. Posteriormente, se determinará el grado de seguridad de cada activo y se realizará la valoración respectiva, que permitirá obtener el grado de impacto de activo dentro del negocio según la metodología MAGERIT.

Elaboración Plan de Pruebas: Se realizará un plan de pruebas en donde se consignarán todas las pruebas a realizar sobre el servidor y aplicativo web SIRIUS ADM. Se realizarán tanto pruebas de seguridad como pruebas de control. Cada prueba será registrada en un formato en donde se especificará el objetivo, recursos y conclusiones de cada prueba.

Ejecución Plan de Pruebas: En esta etapa se realizará la ejecución del plan de pruebas elaborado en la etapa anterior. Cada prueba que se ejecute permitirá

obtener como resultado un hallazgo que será soportado mediante una evidencia. Se realizará una recopilación de los hallazgos que serán los insumos de la siguiente etapa.

Análisis de Riesgos, controles y recomendaciones: En esta etapa se tomarán como insumo los hallazgos y evidencias encontrados después de la ejecución del plan de pruebas. Serán analizados cada uno para realizar el análisis de los riesgos que pueden desencadenar, así como la elaboración de las recomendaciones que permitan posteriormente establecer los controles necesarios para la mitigación de los riesgos. Nota: Solamente se emitirán recomendaciones. No se realizará implementación de los controles que sean recomendados o sugeridos.

Definir y establecer la política de seguridad de la información y la ciberseguridad. En esta etapa se tomarán los resultados, recomendaciones y conclusiones de las anteriores etapas con el fin de englobar todos estos resultados y definir una buena política de seguridad de la información y la ciberseguridad.

8. IDENTIFICACIÓN DE VULNERABILIDADES

8.1 IDENTIFICACIÓN DE RIESGOS MEDIANTE MAGERIT

Para el desarrollo de este proyecto se utiliza la Metodología de Análisis de Riesgos de los Sistemas de Información – MAGERIT, diseñada y elaborada por el consejo Superior de Administración electrónica, la cual corresponde a un método formal para detectar riesgos y recomendar controles, medidas o salvaguardas para evitar dichos riesgos. A continuación, se aplica esta metodología para el análisis de la aplicación web SIRIUS ADM.

8.1.1 Identificación de Activos Informáticos

A continuación, en el cuadro 1 se presenta el inventario de los activos informáticos de Centrales Eléctricas del Norte de Santander S.A E.S.P. involucrados en el sistema web SIRIUS ADM. Estos activos se clasifican según la metodología MAGERIT en cuatro columnas, que presentan la categorización y clasificación del inventario de activos según la metodología y su equivalente para CENS. Allí encontramos lo siguiente:

- Código grupo de activo Magerit: Hace referencia a la clasificación de la familia de activos según lo expresado en los libros de la metodología Magerit. Por ejemplo: [files] ficheros o archivos, [www] sitios web, [sub] software subcontratado, [print] Impresoras, etc.

- Nombre Grupo de Activo: Hace referencia al nombre del grupo de activo, según la metodología MAGERIT.

- Código de activo CENS: Codificación nemotécnica empleada por CENS para identificar sus activos, inicia con un prefijo que identifica el tipo de activo seguida de una descripción del nombre. Ejemplo de está son “A_” para identificar archivos, “S_” identifica activos de tipo servicio, “SIS_” para identificar sistemas de información, etc.

- Nombre de activo CENS: Breve observación del activo, que permite detallar o describir el activo.

Cuadro 1. Activos de CENS Según Magerit

CATEGORÍA MAGERIT			
Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código activo CENS**	**Nombre activo CENS**
[D] Datos / Información			
[files]	Ficheros	[A_SYNAPSIS]	Contrato de prestación de soporte y mantenimiento del sistema comercial con el proveedor TIVIT-Synapsis
[files]	Ficheros	[A_EPM]	Contrato de prestación de soporte y mantenimiento del sistema Sirius con el proveedor Empresas Públicas de Medellín S.A. E.S.P.
[files]	Ficheros	[A_PRIMESTONE]	contrato de prestación de soporte y mantenimiento del sistema Primeread con el proveedor Primestone
[S] Servicios			
[www]	World wide web	[S_INTRANET]	Servicio de intranet
[email]	Correo electrónico.	[S_correo]	Manejo de correos electrónicos.
[SW] Software - Aplicaciones informáticas			
[sub]	desarrollo a medida (subcontratado)	[SIS_SIG]	Solución sistema de información geográfico
[sub]	desarrollo a medida (subcontratado)	[SIS_COMPRASE]	Solución para apoyar los procesos de validación y control de transacciones del mercado mayorista de energía
[sub]	desarrollo a medida (subcontratado)	[SIS_CU]	Solución que apoya el cálculo del costo unitario de la tarifa de energía del mercado regulado
[sub]	desarrollo a medida (subcontratado)	[SIS_SPARD]	Solución Spard
[sub]	desarrollo a medida (subcontratado)	[SIS_SCADA]	Solución Scada
[sub]	desarrollo a medida (subcontratado)	[SIS_CIMA]	Solución Comercial

Cuadro 1. (Continuación)

CATEGORÍA MAGERIT			
Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código activo CENS**	**Nombre activo CENS**
[sub]	desarrollo a medida (subcontratado)	[SIS_SIRIUS]	Solución móvil para lecturas y revisiones
[sub]	desarrollo a medida (subcontratado)	[SIS_MERC]	Solución gestión documental
[sub]	desarrollo a medida (subcontratado)	[SIS_SSE]	Solución seguridad electrónica
[sub]	desarrollo a medida (subcontratado)	[SIS_PRIME]	Solución para la toma de lecturas de fronteras comerciales
[sub]	desarrollo a medida (subcontratado)	[SIS_PPTO]	Solución para la gestión presupuestal
[sub]	desarrollo a medida (subcontratado)	[SIS_DIG]	Solución Digsilent
[sub]	desarrollo a medida (subcontratado).	[SIS_SAN]	Solución administración nómina
[sub]	desarrollo a medida (subcontratado)	[SIS_PM7]	Solución calidad de la potencia
[sub]	desarrollo a medida (subcontratado)	[SIS_LIT]	Solución Litisoft
[sub]	desarrollo a medida (subcontratado)	[SIS_DGT]	Solución Digiturno
[sub]	desarrollo a medida (subcontratado)	[SIS_POWER]	Solución Archivo digital
[Office]	Ofimática	[Office]	Office 365
[av]	Antivirus	[Antivirus]	Mcafee antivirus
[os]	sistema operativo	[SO]	Sistema operativo
[dbms]	sistema de gestión de bases de datos	[ORACLE]	Gestor de base de datos oracle
[HW] Equipamiento informático (hardware)			
[print]	medios de impresión	[IMP]	Impresoras

Cuadro 1. (Continuación)

CATEGORÍA MAGERIT			
Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo de acuerdo a CENS**	**Nombre activo de acuerdo a CENS**
[pc]	informática personal	[PC]	Computadores de escritorio y portátiles
[router]	encaminadores	[RT]	Router
[scan]	Escáneres	[SCN]	Escáner
[COM] Redes de comunicaciones			
[LAN]	red local	[LAN]	Red lan
[wifi]	red inalámbrica	[WIFI]	Red wifi
[Internet]	Internet	[IEX]	Internet
[PSTN]	red telefónica	[TEL]	Telefonía IP
[Media] Soportes de información			
[cd]	cederrón (CD-ROM)	[CD]	CD o DVD
[usb]	memorias USB	[USB]	Usb
[printed]	material impreso	[IMPRESO]	Impreso
[AUX] Equipamiento auxiliar			
[power]	fuentes de alimentación	[PTE]	Planta eléctrica
[L] Instalaciones			
[building]	Edificio	[E_entidad]	Instalación física de CENS
[P] Personal			
[ui]	usuarios internos	[GTI]	Gestor de TI
[ui]	usuarios internos	[CTI]	Coordinador de TI
[adm]	administradores de sistemas	[PTI]	Profesional de TI
[ui]	usuarios internos	[TTI]	Tecnólogo de TI
[ui]	usuarios internos	[TCTI]	Técnico de TI

Fuente: Autores

8.1.2 Valoración de los Activos

El siguiente paso en la metodología Magerit es la valoración de activos, para cada valoración conviene tomar en consideración la siguiente información:

- Dimensiones en las que el activo es relevante

- Estimación de la valoración en cada dimensión

Los criterios de valoración de los riesgos de los activos según su impacto se realizarán según lo indicado en el cuadro 2.

Cuadro 2. Criterios de Valoración

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

A continuación, se visualiza en el cuadro 3 la clasificación de los riesgos de los activos asociada a cada dimensión (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) para los activos asociados al sistema Sirius valorados según su impacto según la expresado en la metodología MAGERIT.

Cuadro 3. Valoración de Activos

CATEGORÍA MAGERIT			Dimensiones				
Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo CENS**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[D] Datos / Información							
[files]	Ficheros	[A_SYNAPSIS]	7	7	6	7	4
[files]	Ficheros	[A_EPM]	5	7	6	7	4
[files]	Ficheros	[A_PRIMESTONE]	5	7	6	7	4
[S] Servicios							
[www]	World wide web	[S_INTRANET]	7	5	6	6	6
[email]	Correo electrónico	[S_correo]	5	6	7	7	7
[SW] Software - Aplicaciones informáticas							
[sub]	desarrollo a medida (subcontratado)	[SIS_SIG]	5	5	7	6	5
[sub]	desarrollo a medida (subcontratado)	[SIS_COMPRASE]	4	7	7	5	5
[sub]	desarrollo a medida (subcontratado)	[SIS_CU]	4	7	7	5	5
[sub]	desarrollo a medida (subcontratado)	[SIS_SPARD]	7	6	8	6	6
[sub]	desarrollo a medida (subcontratado)	[SIS_SCADA]	8	8	8	8	8

Cuadro 3. (Continuación)

CATEGORÍA MAGERIT			Dimensiones				
Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo CENS**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[sub]	desarrollo a medida (subcontratado)	[SIS_CIMA]	8	8	8	8	8
[sub]	desarrollo a medida (subcontratado)	[SIS_SIRIUS]	7	6	7	6	6
[sub]	desarrollo a medida (subcontratado)	[SIS_MERC]	5	7	7	6	7
[sub]	desarrollo a medida (subcontratado)	[SIS_SSE]	5	6	6	5	5
[sub]	desarrollo a medida (subcontratado)	[SIS_PRIME]	7	7	7	6	6
[sub]	desarrollo a medida (subcontratado)	[SIS_PPTO]	5	6	6	6	5
[sub]	desarrollo a medida (subcontratado)	[SIS_DIG]	5	6	6	7	7
[sub]	desarrollo a medida (subcontratado)	[SIS_SAN]	7	8	8	7	7
[sub]	desarrollo a medida (subcontratado)	[SIS_PM7]	7	7	7	7	7
[sub]	desarrollo a medida (subcontratado)	[SIS_LIT]	5	6	7	6	6
[sub]	desarrollo a medida (subcontratado)	[SIS_DGT]	7	6	6	5	5
[sub]	desarrollo a medida (subcontratado)	[SIS_POWER]	6	7	7	6	6
[Office]	Ofimática	[Office]	5	7	2	7	7
[av]	Antivirus	[Antivirus]	7	7	2	7	7
[os]	sistema operativo	[SO]	7	7	2	7	7
[dbms]	sistema de gestión de bases de datos	[ORACLE]	8	7	8	8	8
[HW] Equipamiento informático (hardware)							
[print]	medios de impresión	[IMP]	6	2	6	6	4
[pc]	informática personal	[PC]	6	2	6	6	2
[router]	encaminadores	[RT]	7		8	8	2
[scan]	escáneres	[SCN]	6		6	6	2
[COM] Redes de comunicaciones							
[LAN]	red local	[LAN]	7	7	7	2	7
[wifi]	red inalámbrica	[WIFI]	5	7	7	2	7
[Internet]	Internet	[IEX]	7	7	7	2	7
[PSTN]	red telefónica	[TEL]	5	6	6	2	6
[Media] Soportes de información							
[cd]	cederrón (CD-ROM)	[CD]	4	7	7	2	2
[usb]	memorias USB	[USB]	4	7	7	2	2
[printed]	material impreso	[IMPRESO]	7	2	7	2	2
[AUX] Equipamiento auxiliar							
[power]	fuentes de alimentación	[PTE]	7	0	0	0	0

Cuadro 3. (Continuación)

CATEGORÍA MAGERIT			Dimensiones				
Código grupo de activo MAGERIT	**Nombre grupo de activo MAGERIT**	**Código Activo CENS**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[L] Instalaciones							
[building]	Edificio	[E_entidad]	7	3	3	3	3
[P] Personal							
[ui]	usuarios internos	[GTI]	7	8	8	8	2
[ui]	usuarios internos	[CTI]	7	8	8	8	2
[adm]	administradores de sistemas	[PTI]	7	7	8	8	2
[ui]	usuarios internos	[TTI]	6	7	7	7	2
[ui]	usuarios internos	[TCTI]	6	7	7	7	2

Fuente: Autores

8.1.3 Identificación de Amenazas

La identificación de amenazas se realiza haciendo un cruce entre cada activo y las posibles amenazas que lo puedan afectar, esto se muestra a continuación en el cuadro 4.

Cuadro 4. Amenazas

CATEGORÍA MAGERIT		
Código Activo CENS	**Nombre activo CENS**	**Amenazas**
[D] Datos / Información		
[A_SYNAPSIS]	Contrato de prestación de soporte y mantenimiento del sistema comercial con el proveedor TIVIT-Synapsis	[E.1] Errores de usuario [E.15] Alteración de la información [E.19] Fugas de información [A.19] Revelación de información [I.8]Fallos de servicios de comunicaciones
[A_EPM]	Contrato de prestación de soporte y mantenimiento del sistema Sirius con el proveedor Empresas Públicas de Medellín s.a. E.S.P.	[E.1] Errores de usuario [E.15] Alteración de la información [E.19] Fugas de información [A.19] Revelación de información [I.8]Fallos de servicios de comunicaciones.

Cuadro 4. (Continuación)

CATEGORÍA MAGERIT		
Código Activo CENS	**Nombre activo CENS**	**Amenazas**
[D] Datos / Información		
[A_SYNAPSIS]	Contrato de prestación de soporte y mantenimiento del sistema comercial con el proveedor TIVIT-Synapsis	[E.1] Errores de usuario [E.15] Alteración de la información [E.19] Fugas de información [A.19] Revelación de información [I.8]Fallos de servicios de comunicaciones
[A_EPM]	Contrato de prestación de soporte y mantenimiento del sistema Sirius con el proveedor Empresas Públicas de Medellín s.a. E.S.P.	[E.1] Errores de usuario [E.15] Alteración de la información [E.19] Fugas de información [A.19] Revelación de información [I.8]Fallos de servicios de comunicaciones.
[A_PRIMESTONE]	Contrato de prestación de soporte y mantenimiento del sistema Primeread con el proveedor Primestone	[E.1] Errores de usuario [E.15] Alteración de la información [E.19] Fugas de información [A.19] Revelación de información [I.8]Fallos de servicios de comunicaciones
[S] servicios		
[S_INTRANET]	Servicio de intranet	[A.11] Acceso no autorizado [A.5] Suplantación de identidad de usuario [I.8] Fallos de servicio de comunicaciones [E.2] Errores de administración
[S_correo]	Correo electrónico	[E.1] Errores de usuario [E.15] Alteración de la información [E.19] Fugas de información [A.19] Revelación de información [I.8]Fallos de servicios de comunicaciones [A.5] Suplantación de identidad de usuario

Cuadro 4. (Continuación)

CATEGORÍA MAGERIT		
Código Activo CENS	**Nombre activo CENS**	**Amenazas**
[SW] Software - Aplicaciones informáticas		
[SIS_SIG]	Solución sistema de información geográfico	[A.11] Acceso no autorizado [E.1] Errores de usuarios [I.5] Avería de origen físico o lógico [E.20] Vulnerabilidades de los programas (software) [I.8] Fallos de servicio de comunicaciones [E.21] Errores de mantenimiento/ actualización de programas (software) [A.5] Suplantación de la identificación del usuario
[SIS_COMPRASE]	Solución para apoyar los procesos de validación y control de transacciones del mercado mayorista de energía	
[SIS_CU]	Solución que apoya el cálculo del costo unitario de la tarifa de energía del mercado regulado	
[SIS_SPARD]	Solución Spard	
[SIS_SCADA]	Solución Scada	
Cuadro 4. (Continuación)		
[SIS_CIMA]	Solución Comercial	
[SIS_SIRIUS]	Solución móvil para lecturas y revisiones	
[SIS_MERC]	Solución gestión documental	
[SIS_SSE]	Solución seguridad electrónica	
[SIS_PRIME]	Solución para la toma de lecturas de fronteras comerciales	
[SIS_PPTO]	Solución para la gestión presupuestal	
[SIS_DIG]	Solución Digsilent	
[SIS_SAN]	Solución administración nómina	
[SIS_PM7]	Solución Calidad de la potencia	
[SIS_LIT]	Solución Litisoft	
[SIS_DGT]	Solución Digiturno	
[SIS_POWER]	Solución archivo digital	
[Office]	Office 365	[E.1] errores de los usuarios [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software) [A.8] Difusión de software dañino

Cuadro 4. (Continuación)

CATEGORÍA MAGERIT		
Código Activo CENS	**Nombre activo CENS**	**Amenazas**
[Antivirus]	Mcafee antivirus	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software)
[SO]	Sistema operativo	[I.5] Avería de origen físico o lógico [E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software) [A.7]Uso no previsto
[ORACLE]	Gestor de base de datos oracle	[E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software)
[HW] Equipamiento informático (hardware)		
[IMP]	Impresoras	[N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.1]Fuego [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.23]errores de mantenimiento/actualización de equipos(hardware) [A.11]Acceso no autorizado
[PC]	Computadores de escritorio y portátiles	[N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.1]Fuego [I.*]Desastres industriales [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.23]errores de mantenimiento/actualización de equipos(hardware) [E.24]Caída del sistema por agotamiento de recursos. [A.6]abuso de privilegios de acceso [A.7]Uso no previsto

Cuadro 4. (Continuación)

CATEGORÍA MAGERIT		
Código Activo CENS	**Nombre activo CENS**	**Amenazas**
[Antivirus]	Mcafee antivirus	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software)
[SO]	Sistema operativo	[I.5] Avería de origen físico o lógico [E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software) [A.7]Uso no previsto
[ORACLE]	Gestor de base de datos oracle	[E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software)
[HW] Equipamiento informático (hardware)		
[IMP]	Impresoras	[N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.1]Fuego [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.23]errores de mantenimiento/actualización de equipos(hardware) [A.11]Acceso no autorizado
[PC]	Computadores de escritorio y portátiles	[N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.1]Fuego [I.*]Desastres industriales [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.23]errores de mantenimiento/actualización de equipos(hardware) [E.24]Caída del sistema por agotamiento de recursos. [A.6]abuso de privilegios de acceso [A.7]Uso no previsto

Cuadro 4. (Continuación)

CATEGORÍA MAGERIT		
Código Activo CENS	**Nombre activo CENS**	**Amenazas**
[RT]	Router	[N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.3] Contaminación medioambiental [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [A.11] Acceso no autorizado.
[SCN]	Escanner	[N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.1] Fuego [I.*] Desastres industriales [I.5] Avería de origen físico o lógico [I.7] Condiciones inadecuadas de temperatura o humedad [E.23] errores de mantenimiento/actualización de equipos(hardware) [E.24] Caída del sistema por agotamiento de recursos [A.6]abuso de privilegios de acceso [A.7]Uso no previsto
[COM] Redes de comunicaciones		
[LAN]	Red lan	[I.8]Fallos de servicios de comunicaciones [E.9]Errores de re-encaminamiento [E.10] errores de secuencia [A.5] Suplantación de la identidad del usuario [A.9] Re-encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado
[WIFI]	Red wifi	[I.8]Fallos de servicios de comunicaciones [E.9]Errores de re-encaminamiento
[IEX]	Internet	[I.8] Fallo de servicios de comunicaciones [E.15] alteración de la información

Cuadro 4. (Continuación)

CATEGORÍA MAGERIT		
Código Activo CENS	**Nombre activo CENS**	**Amenazas**
[IEX]	Internet	[I.8] Fallo de servicios de comunicaciones [E.15] alteración de la información
[TEL]	Telefonía IP	N.1] Fuego [N.2]Daños por agua [I.8] Fallo en servicios de comunicaciones [E.9]errores de encaminamiento [E.15] alteración de la información [E.19] Fugas de información [A.7] Uso no previsto [A.9] Encaminamiento de mensajes [A.10] Alteración de frecuencia [A.12] Análisis de tráfico [A.14] Intercepción de información (escucha)
[Media] Soportes de información		
[CD]	CD o DVD	[N.1] Fuego [N.2]Daños por agua [E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información
[USB]	Usb	[N.1] Fuego [N.2]Daños por agua [E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información
[IMPRESO]	Impreso	[N.1] Fuego [N.2]Daños por agua [E.19] Fugas de información [A.19] Revelación de información
[AUX] Equipamiento auxiliar		
[PTE]	Planta eléctrica	[N.1] Fuego [N.2]Daños por agua [I.3] Contaminación medioambiental.

Cuadro 4. (Continuación)

CATEGORÍA MAGERIT		
Código Activo CENS	**Nombre activo CENS**	**Amenazas**
[I] instalaciones		
[E_entidad]	Instalación física de CENS	[A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.26] Ataque destructivo [I.1] Fuego [N.8] Desastres naturales. Fenómeno de origen volcánico [N.7] Desastres naturales. Fenómeno sísmico. [N.2] Daños por agua
[P] personal		
[GTI]	Gestor de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social
[CTI]	Coordinador de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social
[PTI]	Profesional de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social [A.29.2] Ataque desde el interior [E.4] Errores de configuración
[TTI]	Tecnólogo de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social [A.29.2] Ataque desde el interior
[TCTI]	Técnico de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social [A.29.2] Ataque desde el interior

Fuente: Autores

8.1.4 Caracterización y valoración de las amenazas

El objetivo de esta actividad es determinar la degradación del activo; el proceso consiste en evaluar el valor que pierde el activo (en porcentaje) en caso de que se materialice una amenaza.

Estas Amenazas se han tomado del catálogo de elementos que presenta la metodología MAGERIT en su libro II Versión 3.0

Para el desarrollo de esta actividad es necesario tener presente los rangos dados en el cuadro 5 de frecuencia o probabilidad de ocurrencia de cada amenaza.

Cuadro 5. Valoración Frecuencia de Amenazas

Valor Frecuencia			
Código	**Descripción**	**Observación**	**Valor**
MA	Muy Alto	Casi Seguro	5
A	Alto	Alto	4
M	Medio	Posible	3
B	Bajo	Poco Posible	2
MB	Muy Bajo	Siglos	1

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

Adicionalmente, se debe tener en cuenta los valores de degradación de cada amenaza mostrados en el cuadro 6, sugeridos por Magerit V.3 - Libro II.

Cuadro 6. Degradación de las Amenazas

Valor Degradación			
Código	**Descripción**	**Observación**	**Valor**
MA	Muy Alta	Desastroso	100%
A	Alta	Mayor	80%
M	Media	Moderado	50%
B	Baja	Menor	10%
MB	Muy Baja	Insignificante	1%

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

Como resultado de los anteriores, en el cuadro 7 se puede observar la valoración de amenazas y su impacto por cada activo en las dimensiones de disponibilidad, integridad, confiabilidad, autenticidad, trazabilidad y frecuencia.

Cuadro 7. Valoración de las Amenazas

Activo	Amenazas según Magerit	Valoración de Amenazas												Impacto				
		[F]		[D]		[I]		[C]		[A]		[T]		[D]	[I]	[C]	[A]	[T]
Contrato de prestación de soporte y mantenimiento del sistema comercial con el proveedor TIVIT-Synapsis.	. [E.1] Errores de usuario.	B	2	M	0.5	M	0.5	B	0.1	B	0.1	M	0.5	MB	MB	MB	MB	MB
	[E.15] Alteración de la información	B	2	M	0.5	M	0.5	B	0.1	A	0.8	M	0.5	MB	MB	MB	B	MB
	[E.19] Fugas de información	B	2	B	0.1	MB	0.01	A	0.8	MB	0.01	B	0.1	MB	MB	B	MB	MB
	[A.19] Revelación de información	B	2	B	0.1	MB	0.01	A	0.8	MB	0.01	B	0.1	MB	MB	B	MB	MB
	[I.8]Fallos de servicios de comunicaciones	B	2	B	0.1	M	0.5	B	0.1	M	0.5	B	0.1	MB	MB	MB	MB	MB
Contrato de prestación de soporte y mantenimiento del sistema Sirius con el proveedor Empresas Públicas de Medellín s.a. ESP.	[E.1] Errores de usuario	B	2	M	0.5	M	0.5	B	0.1	B	0.1	M	0.5	MB	MB	MB	MB	MB
	[E.15] Alteración de la información	B	2	M	0.5	M	0.5	B	0.1	A	0.8	M	0.5	MB	MB	MB	B	MB
	[E.19] Fugas de información	B	2	B	0.1	MB	0.01	A	0.8	MB	0.01	B	0.1	MB	MB	B	MB	MB
	[A.19] Revelación de información.	B	2	B	0.1	MB	0.01	A	0.8	MB	0.01	B	0.1	MB	MB	B	MB	MB
	[I.8]Fallos de servicios de comunicaciones	B	2	B	0.1	M	0.5	B	0.1	M	0.5	B	0.1	MB	MB	MB	MB	MB
Contrato de prestación de soporte y mantenimiento del sistema Primeread con el proveedor Primestone.	[E.1] Errores de usuario	B	2	M	0.5	M	0.5	B	0.1	B	0.1	M	0.5	MB	MB	MB	MB	MB
	[E.15] Alteración de la información	B	2	M	0.5	M	0.5	B	0.1	A	0.8	M	0.5	MB	MB	MB	B	MB
	[E.19] Fugas de información	B	2	B	0.1	MB	0.01	A	0.8	MB	0.01	B	0.1	MB	MB	B	MB	MB
	[A.19] Revelación de información	B	2	B	0.1	MB	0.01	A	0.8	MB	0.01	B	0.1	MB	MB	B	MB	MB
	[I.8]Fallos de servicios de comunicaciones.	B	2	B	0.1	M	0.5	B	0.1	M	0.5	B	0.1	MB	MB	MB	MB	MB

Cuadro 7. (Continuación)

Activo	Amenazas según Magerit	Valoración de Amenazas												Impacto				
		[F]		[D]		[I]		[C]		[A]		[T]		[D]	[I]	[C]	[A]	[T]
Servicio de intranet	[A.11] Acceso no autorizado	B	2	B	0.1	B	0.1	A	0.8	A	0.8	B	0.1	MB	MB	B	B	MB
	[A.5] Suplantación de identidad de usuario	B	2	B	0.1	M	0.5	M	0.5	A	0.8	B	0.1	MB	MB	MB	B	MB
	[I.8] Fallos de servicio de comunicaciones	M	3	MA	1	B	0.1	B	0.1	B	0.1	M	0.5	M	B	B	B	B
	[E.2] Errores de administración	M	3	A	0.8	B	0.1	B	0.1	B	0.1	MB	0.01	M	B	B	B	MB
Correo electrónico	[E.1] Errores de usuario	M	3	B	0.1	M	0.5	B	0.1	B	0.1	B	0.1	B	B	B	B	B
	[E.15] Alteración de la información	B	2	B	0.1	A	0.8	B	0.1	M	0.5	M	0.5	MB	B	MB	MB	MB
	[E.19] Fugas de información	B	2	B	0.1	B	0.1	A	0.8	B	0.1	M	0.5	MB	MB	B	MB	MB
	[A.19] Revelación de información	B	2	B	0.1	B	0.1	A	0.8	A	0.8	B	0.1	MB	MB	B	B	MB
	[I.8]Fallos de servicios de comunicaciones	M	3	M	0.5	B	0.1	B	0.1	B	0.1	B	0.1	B	B	B	B	B
	[A.5] Suplantación de identidad de usuario	B	2	B	0.1	A	0.8	A	0.8	A	0.8	M	0.5	MB	B	B	B	MB
Sistemas de información	[A.11] Acceso no autorizado	M	3	B	0.1	A	0.8	A	0.8	B	0.1	B	0.1	B	M	M	B	B
	[E.1] Errores de usuarios	M	3	M	0.5	M	0.5	B	0.1	B	0.1	B	0.1	B	B	B	B	B
	[I.5] Avería de origen físico o lógico	M	3	M	0.5	B	0.1	B	0.1	B	0.1	B	0.1	B	B	B	B	B
	[E.20] Vulnerabilidades de los programas (software)	B	2	B	0.1	A	0.8	A	0.8	M	0.5	B	0.1	MB	B	B	MB	MB
	[I.8] Fallos de servicio de comunicaciones	M	3	M	0.5	M	0.5	B	0.1	B	0.1	B	0.1	B	B	B	B	B
	[E.21] Errores de mantenimiento/ actualización de programas (software)	B	2	M	0.5	B	0.1	B	0.1	B	0.1	B	0.1	MB	MB	MB	MB	MB
	[A.5] Suplantación de la identificación del usuario	B	2	B	0.1	A	0.8	A	0.8	A	0.8	A	0.8	MB	B	B	B	B

Cuadro 7. (Continuación)

Activo	Amenazas según Magerit	Valoración de Amenazas												Impacto				
		[F]		[D]		[I]		[C]		[A]		[T]		[D]	[I]	[C]	[A]	[T]
Office 365	[A.10]Alteración de secuencia	MB	1	B	0.1	M	0.5	M	0.5	B	0.1	B	0.1	MB	MB	MB	MB	MB
	[A.11] Acceso no autorizado	MB	1	B	0.1	A	0.8	A	0.8	A	0.8	A	0.8	MB	MB	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario	MB	1	B	0.1	A	0.8	A	0.8	A	0.8	M	0.5	MB	MB	MB	MB	MB
	[A.9] [Re-]encaminamiento de mensajes	MB	1	B	0.1	M	0.5	B	0.1	B	0.1	B	0.1	MB	MB	MB	MB	MB
	[E.10] Errores de secuencia	MB	1	B	0.1	B	0.1	B	0.1	B	0.1	B	0.1	MB	MB	MB	MB	MB
	[E.9] Errores de [re-]encaminamiento	MB	1	B	0.1	B	0.1	B	0.1	B	0.1	B	0.1	MB	MB	MB	MB	MB
	[I.8] Fallo de servicios de comunicaciones	M	3	M	0.5	B	0.1	B	0.1	B	0.1	B	0.1	B	B	B	B	B
Mcafee antivirus	[E.8] Difusión de software dañino	M	3	M	0.5	M	0.5	M	0.5	M	0.5	B	0.1	B	B	B	B	B
	[E.20] Vulnerabilidades de los programas (software)	M	3	M	0.5	A	0.8	B	0.1	B	0.1	B	0.1	B	M	B	B	B
	[E.21] Errores de mantenimiento/ actualización de programas(software)	B	2	B	0.1	B	0.1	B	0.1	B	0.1	B	0.1	MB	MB	MB	MB	MB
Sistema operativo	[I.5] Avería de origen físico o lógico	M	3	M	0.5	B	0.1	B	0.1	B	0.1	B	0.1	B	B	B	B	B
	[E.1] Errores de los usuarios	M	3	M	0.5	B	0.1	B	0.1	B	0.1	B	0.1	B	B	B	B	B
	[E.8] Difusión de software dañino	M	3	M	0.5	M	0.5	A	0.8	M	0.5	B	0.1	B	B	M	B	B
	[E.20] Vulnerabilidades de los programas (software)	M	3	B	0.1	M	0.5	B	0.1	B	0.1	B	0.1	B	B	B	B	B
	[E.21] Errores de mantenimiento/actualización de programas(software)	B	2	M	0.5	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	MB	MB	MB	MB
	[A.7] Uso no previsto	B	2	M	0.5	M	0.5	MB	0.01	B	0.1	MB	0.01	MB	MB	MB	MB	MB

Cuadro 7. (Continuación)

Activo	Amenazas según Magerit	Valoración de Amenazas												Impacto				
		[F]		[D]		[I]		[C]		[A]		[T]		[D]	[I]	[C]	[A]	[T]
Gestor de base de datos Oracle	[E.20] Vulnerabilidades de los programas (software)	B	2	M	0.5	A	0.8	M	0.5	M	0.5	M	0.5	MB	B	MB	MB	MB
	[E.21] Errores de mantenimiento/ actualización de programas(software)	B	2	M	0.5	B	0.1	B	0.1	B	0.1	MB	0.01	MB	MB	MB	MB	MB
Impresoras	[N.1] Fuego	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.*]Desastres naturales	M	3	A	0.8	MB	0.01	MB	0.01	MB	0.01	MB	0.01	M	MB	MB	MB	MB
	[I.1]Fuego	B	2	A	0.8	MB	0.01	MB	0.01	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[I.5]Avería de origen físico o lógico	M	3	M	0.5	MB	0.01	MB	0.01	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[I.7]Condiciones inadecuadas de temperatura o humedad	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[E.23]errores de mantenimiento/actualización de equipos(hardware)	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.11]Acceso no autorizado	B	2	B	0.1	B	0.1	A	0.8	MB	0.01	MB	0.01	MB	MB	B	MB	MB
Computadores de escritorio y portátiles	[N.1] Fuego	B	2	M	0.5	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.*]Desastres naturales	M	3	B	0.1	MB	0.01	M	0.5	MB	0.01	MB	0.01	B	MB	B	MB	MB
	[I.1]Fuego	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[I.*]Desastres industriales	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[I.5]Avería de origen físico o lógico	A	4	M	0.5	MB	0.01	MB	0.01	MB	0.01	MB	0.01	M	B	B	B	B
	[I.7]Condiciones inadecuadas de temperatura o humedad	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[E.20] Vulnerabilidades de los programas (software)	B	2	M	0.5	A	0.8	M	0.5	M	0.5	M	0.5	MB	B	MB	MB	MB
	[E.21] Errores de manten. /actualiz. de programas (sw)	B	2	M	0.5	B	0.1	B	0.1	B	0.1	MB	0.01	MB	MB	MB	MB	MB

Cuadro 7. (Continuación)

Activo	Amenazas según Magerit	Valoración de Amenazas												Impacto				
		[F]		[D]		[I]		[C]		[A]		[T]		[D]	[I]	[C]	[A]	[T]
Gestor de base de datos Oracle	[E.23]errores de mantenimiento/actualización de equipos(hardware)	M	3	M	0.5	B	0.1	MB	0.01	MB	0.01	MB	0.01	B	B	MB	MB	MB
	[E.24]Caída del sistema por agotamiento de recursos	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.6]abuso de privilegios de acceso	M	3	B	0.1	A	0.8	A	0.8	M	0.5	M	0.5	B	M	M	B	B
	[A.7]Uso no previsto	M	3	B	0.1	M	0.5	A	0.8	M	0.5	B	0.1	B	B	M	B	B
Router	[N.1] Fuego	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.*]Desastres naturales	M	3	M	0.5	MB	0.01	B	0.1	MB	0.01	MB	0.01	B	MB	B	MB	MB
	[I.3] Contaminación medioambiental	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[I.5]Avería de origen físico o lógico	M	3	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[I.7]Condiciones inadecuadas de temperatura o humedad	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.11] Acceso no autorizado	M	3	B	0.1	A	0.8	M	0.5	M	0.5	M	0.5	B	M	B	B	B
Escanner	[N.1] Fuego	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.*]Desastres naturales	M	3	M	0.5	MB	0.01	MB	0.01	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[I.1]Fuego	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[I.*]Desastres industriales	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[I.5]Avería de origen físico o lógico	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[I.7]Condiciones inadecuadas de temperatura o humedad	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[E.23] errores de manten. / actualiz. de equipos (hw)	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB

Cuadro 7. (Continuación)

Activo	Amenazas según Magerit	Valoración de Amenazas												Impacto				
		[F]		[D]		[I]		[C]		[A]		[T]		[D]	[I]	[C]	[A]	[T]
Escanner	[E.24]Caída del sistema por agotamiento de recursos	B	2	M	0.5	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.6]abuso de privilegios de acceso	B	2	B	0.1	A	0.8	A	0.8	MB	0.01	M	0.5	MB	B	B	MB	MB
	[A.7]Uso no previsto	B	2	B	0.1	M	0.5	A	0.8	MB	0.01	M	0.5	MB	MB	B	MB	MB
Red lan	[I.8]Fallos de servicios de comunicaciones	M	3	M	0.5	M	0.5	B	0.1	MB	0.01	MB	0.01	B	B	B	MB	MB
	[E.9] Errores de re-encaminamiento	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[E.10] errores de secuencia	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.5] Suplantación de la identidad del usuario.	M	3	B	0.1	MB	0.01	M	0.5	M	0.5	B	0.1	B	MB	B	B	B
	[A.9] Re-encaminamiento de mensajes	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.10] Alteración de secuencia	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.11] Acceso no autorizado.	M	3	B	0.1	M	0.5	A	0.8	B	0.1	B	0.1	B	B	M	B	B
Red wifi	[I.8]Fallos de servicios de comunicaciones.	M	3	A	0.8	MB	0.01	B	0.1	MB	0.01	MB	0.01	M	MB	B	MB	MB
	[E.9]Errores de re-encaminamiento	B	2	M	0.5	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
Internet	[I.8] Fallo de servicios de comunicaciones	M	3	A	0.8	MB	0.01	B	0.1	MB	0.01	MB	0.01	M	MB	B	MB	MB
	[E.15] alteración de la información	M	3	M	0.5	MB	0.01	A	0.8	B	0.1	M	0.5	B	MB	M	B	B

Cuadro 7. (Continuación)

Activo	Amenazas según Magerit	Valoración de Amenazas												Impacto				
		[F]		[D]		[I]		[C]		[A]		[T]		[D]	[I]	[C]	[A]	[T]
Telefonía IP	[N.1] Fuego	B	2	B	0.1	MB	0.01	M	0.5	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[I.8] Fallo en servicios de comunicaciones	M	3	A	0.8	MB	0.01	B	0.1	MB	0.01	MB	0.01	M	MB	B	MB	MB
	[E.9]errores de encaminamiento.	B	2	B	0.1	MB	0.01	MB	0.01	B	0.1	MB	0.01	MB	MB	MB	MB	MB
	[E.15] alteración de la información	B	2	B	0.1	M	0.5	MB	0.01	B	0.1	B	0.1	MB	MB	MB	MB	MB
	[E.19] Fugas de información	M	3	B	0.1	MB	0.01	M	0.5	MB	0.01	MB	0.01	B	MB	B	MB	MB
	[A.7] Uso no previsto	B	2	B	0.1	M	0.5	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.9] Encaminamiento de mensajes	B	2	B	0.1	MB	0.01	MB	0.01	MB	0.01	B	0.1	MB	MB	MB	MB	MB
	[A.10] Alteración de frecuencia	B	2	B	0.1	MB	0.01	M	0.5	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[A.12] Análisis de tráfico.	M	3	M	0.5	B	0.1	A	0.8	MB	0.01	MB	0.01	B	B	M	MB	MB
	[A.14] Intercepción de información (escucha)	M	3	M	0.5	B	0.1	A	0.8	MB	0.01	MB	0.01	B	B	M	MB	MB
CD o DVD	[N.1] Fuego	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	B	0.1	MB	MB	MB	MB	MB
	[E.15] Alteración de la información	B	2	M	0.5	M	0.5	M	0.5	B	0.1	MB	0.01	MB	MB	MB	MB	MB
	[E.19] Fugas de información	M	3	B	0.1	B	0.1	M	0.5	MB	0.01	MB	0.01	B	B	B	MB	MB
	[A.15] Modificación de la información	B	2	B	0.1	M	0.5	B	0.1	B	0.1	MB	0.01	MB	MB	MB	MB	MB
	[A.19] Revelación de información	B	2	B	0.1	MB	0.01	A	0.8	MB	0.01	MB	0.01	MB	MB	B	MB	MB

Cuadro 7. (Continuación)

Activo	Amenazas según Magerit	Valoración de Amenazas												Impacto				
		[F]		[D]		[I]		[C]		[A]		[T]		[D]	[I]	[C]	[A]	[T]
Usb	[N.1] Fuego	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	B	0.1	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
	[E.15] Alteración de la información	M	3	M	0.5	B	0.1	MB	0.01	B	0.1	B	0.1	B	B	MB	B	B
	[E.19] Fugas de información	M	3	B	0.1	MB	0.01	A	0.8	MB	0.01	MB	0.01	B	MB	M	MB	MB
	[A.15] Modificación de la información	B	2	M	0.5	MB	0.01	A	0.8	B	0.1	MB	0.01	MB	MB	B	MB	MB
	[A.19] Revelación de información	M	3	B	0.1	MB	0.01	M	0.5	MB	0.01	MB	0.01	B	MB	B	MB	MB
Documentos impresos	[N.1] Fuego	B	2	A	0.8	MB	0.01	M	0.5	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	A	0.8	MB	0.01	M	0.5	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[E.19] Fugas de información	B	2	B	0.1	MB	0.01	A	0.8	MB	0.01	MB	0.01	MB	MB	B	MB	MB
	[A.19] Revelación de información	B	2	B	0.1	MB	0.01	M	0.5	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
Planta eléctrica	[N.1] Fuego	B	2	A	0.8	MB	0.01	MB	0.01	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[N.2]Daños por agua	B	2	A	0.8	MB	0.01	B	0.1	MB	0.01	B	0.1	B	MB	MB	MB	MB
	[I.3] Contaminación medioambiental	B	2	M	0.5	MB	0.01	MB	0.01	MB	0.01	MB	0.01	MB	MB	MB	MB	MB
Instalación física de CENS	[A.11] Acceso no autorizado	M	3	B	0.1	A	0.8	M	0.5	MB	0.01	MB	0.01	B	M	B	MB	MB
	[A.26] Ataque destructivo	M	3	A	0.8	MB	0.01	MB	0.01	MB	0.01	MB	0.01	M	MB	MB	MB	MB
	[I.1] Fuego	B	2	A	0.8	MB	0.01	B	0.1	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[N.8] Desastres naturales. Fenómeno de origen volcánico	B	2	A	0.8	MB	0.01	B	0.1	MB	0.01	MB	0.01	B	MB	MB	MB	MB
	[N.7] Desastres naturales. Fenómeno sísmico.	M	3	A	0.8	MB	0.01	B	0.1	MB	0.01	MB	0.01	M	MB	B	MB	MB
	[N.2] Daños por agua	B	2	M	0.5	MB	0.01	B	0.1	MB	0.01	MB	0.01	MB	MB	MB	MB	MB

Fuente: Autores

8.1.5 Causas de los riesgos y recursos afectados

En los siguientes subtítulos ilustraremos las posibles causas de los riesgos detectados en los recursos analizados por la metodología.

8.1.5.1 Información / Datos. *Información Sensible:* no se ha calificado el nivel de confidencialidad de la información para poder así establecer políticas de seguridad de acuerdo al nivel de confidencialidad de la información, lo que no garantiza la integridad de la información de las diferentes dependencias de la organización.

8.1.5.2 Software (SW). *Errores de configuración:* Aplicaciones con configuraciones básicas dejan expuesto a atacantes que conocen sus vulnerabilidades, amenazando la integridad y confidencialidad de la información manipuladas por ellas.

Inyección o instalación de código malicioso: Las aplicaciones software pueden ser atacadas por código malicioso por falta de actualización o por ser software obtenido ilegalmente.

Errores humanos: Errores en la lógica de programación o uso del software que pueden degenerar el comportamiento de los sistemas de información.

Usuarios sin restricciones: no posee políticas que asignen usuarios y contraseñas a los equipos usados por los empleados, lo que facilita el acceso directo a la información.

Actualizaciones de seguridad: la falta de actualización afecta la disponibilidad del sistema de la organización y presenta fallas en los procedimientos, dichas actualizaciones deben ser realizadas por los proveedores.

Ingeniería Social; Herramientas de Informática Forense: la organización está expuesta a que personal interno o externo use las herramientas para acceder a la información de la organización violando las políticas de seguridad de la información.

8.1.5.3 Hardware. Mal funcionamiento de equipos. la organización está expuesta ya que sus equipos al poseer problemas en su funcionamiento pueden causar perdida de información o indisponibilidad de los sistemas.

8.1.5.4 Servicios. Falla en los procesos y en la prestación de los servicios informáticos: se identifican fallas en los procesos del control interno. Además, se pueden presentar fallas en la prestación de servicios de los equipos de trabajo encargados de los servicios de red, comunicaciones y soporte.

8.1.5.5 Comunicaciones. Inyección de Comandos y de tráfico; Puertos No Administrados: por medio de la inyección de comandos se puede obtener información del servidor que sería una falla para el sistema de la organización además se pueden presentan ataques de denegación del servicio, fallas de seguridad y credenciales ya que los usuarios no poseen una política que permita configurar una contraseña segura.

8.1.5.6 Infraestructura. *Factores generados por el medio ambiente*: Los patrones climáticos son ejemplos de las amenazas del medio ambiente que pueden impactar los recursos, proyectos y rentabilidad.

Ingreso de personal no autorizado: Ingreso de personal no autorizado a las distintas áreas de control de la organización.

8.1.5.7 Personal. *Ingeniería Social*: El personal puede entregar información sensible sin conocimiento ya que desconoce el nivel de confidencialidad de dicha información, además los empleados no tienen políticas de acceso físico, ni lógico en la organización lo que representa un riesgo alto.

Factor Insiders: Estos se consideran como los agentes pertenecientes al interior de la organización que se encargan de atacar los sistemas informáticos. Estos por lo general en su mayoría son los mismos empleados de la organización lo cual representa una gran debilidad, ya que algunos empleados pueden cometer actos con intenciones lucrativas a través de la información, a esto se le denomina “Inside Trading”.

8.1.6 Probabilidad e impacto del riesgo

El cuadro 8 muestra la calificación del nivel de riesgo, valorado en términos de la probabilidad de ocurrencia y su impacto para CENS. Siendo el valor 1 Aceptable (verde), 2 tolerable (amarillo), 3 intolerable (naranja) y 4 el nivel de riesgo Extremo (rojo).

Cuadro 8. Probabilidad e impacto del riesgo

NR - Nivel de Riesgo						
Riesgo = Probabilidad * Impacto						
Probabilidad	**5**	**2**	3	4	4	4
	4	2	3	3	4	4
	3	2	2	3	4	4
	2	1	2	2	3	4
	1	1	1	2	**2**	3
		1	**2**	**3**	**5**	**8**
				Impacto		

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

En el cuadro 9, se puede observar el resultado de evaluar el impacto por su probabilidad de ocurrencia de cada amenaza para cada uno de los activos. En él, se puede observar que el nivel de riesgo para cada activo y amenazas asociadas es aceptable en su gran medida, seguido por el nivel de riesgo tolerable y muy pocos riesgos intolerables. No se presenta ningún nivel de riesgo extremo.

Cuadro 9. Probabilidad e impacto del riesgo

Activo	Amenazas según Magerit	IMPACTO																	
		[P]			[D]			[I]			[C]			[A]			[T]		
Contrato de prestación de soporte y mantenimiento del sistema comercial con el proveedor TIVIT-Synapsis	[E.1] Errores de usuario	B	2		MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.15] Alteración de la información	B	2		MB	1	1	MB	1	1	MB	1	1	B	2	2	MB	1	1
	[E.19] Fugas de información	B	2		MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[A.19] Revelación de información	B	2		MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[I.8]Fallos de servicios de comunicaciones	MB	1		MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
Contrato de prestación de soporte y mantenimiento del sistema Sirius con el proveedor Empresas Públicas de Medellín S.A. E.S.P	[E.1] Errores de usuario	B	2		MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.15] Alteración de la información	B	2		MB	1	1	MB	1	1	MB	1	1	B	2	2	MB	1	1
	[E.19] Fugas de información	B	2		MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[A.19] Revelación de información	B	2		MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[I.8]Fallos de servicios de comunicaciones	MB	1		MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
Contrato de prestación de soporte y mantenimiento del Sistema Primeread con el proveedor Primestone	[E.1] Errores de usuario	B	2		MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.15] Alteración de la información	B	2		MB	1	1	MB	1	1	MB	1	1	B	2	2	MB	1	1
	[E.19] Fugas de información	B	2		MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[A.19] Revelación de información	B	2		MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[I.8]Fallos de servicios de comunicaciones	MB	1		MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1

Activo	Amenazas según Magerit	IMPACTO																
		[P]		[D]			[I]			[C]			[A]			[T]		
Cuadro 9. (Continuación)																		
Servicio de intranet	[A.11] Acceso no autorizado	B	2	MB	1	1	MB	1	1	B	2	2	B	2	2	MB	1	1
	[A.5] Suplantación de identidad de usuario	M	3	MB	1	2	MB	1	2	MB	1	2	B	2	2	MB	1	2
	[I.8] Fallos de servicio de comunicaciones	M	3	M	3	3	B	2	2	B	2	2	B	2	2	B	2	2
	[E.2] Errores de administración	B	2	M	3	2	B	2	2	B	2	2	B	2	2	MB	1	1
Correo electrónico	[E.1] Errores de usuario	B	2	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2
	[E.15] Alteración de la información.	M	3	MB	1	2	B	2	2	MB	1	2	MB	1	2	MB	1	2
	[E.19] Fugas de información	B	2	MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[A.19] Revelación de información	B	2	MB	1	1	MB	1	1	B	2	2	B	2	2	MB	1	1
	[I.8]Fallos de servicios de comunicaciones	M	3	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2
	[A.5] Suplantación de identidad de usuario.	B	2	MB	1	1	B	2	2	B	2	2	B	2	2	MB	1	1
Sistemas de información	[A.11] Acceso no autorizado	B	2	B	2	2	M	3	2	M	3	2	B	2	2	B	2	2
	[E.1] Errores de usuarios	B	2	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2
	[I.5] Avería de origen físico o lógico	MB	1	B	2	1	B	2	1	B	2	1	B	2	1	B	2	1
	[E.20] Vulnerabilidades de los programas (software)	B	2	MB	1	1	B	2	2	B	2	2	MB	1	1	MB	1	1
	[I.8] Fallos de servicio de comunicaciones	M	3	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2
	[E.21] Errores de mantenimiento/ actualización de programas (software).	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.5] Suplantación de la identificación del usuario.	B	2	MB	1	1	B	2	2	B	2	2	B	2	2	B	2	2

Activo	Amenazas según Magerit	IMPACTO																	
		[P]		[D]			[I]			[C]			[A]			[T]			
Cuadro 9. (Continuación)																			
Office 365	[A.10] Alteración de secuencia	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.11] Acceso no autorizado	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.5] Suplantación de la identidad del usuario	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.9] [Re-]encaminamiento de mensajes	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.10] Errores de secuencia	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.9] Errores de [re-]encaminamiento	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.8] Fallo de servicios de comunicaciones	M	3	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2
Mcafee antivirus	[E.8] Difusión de software dañino	B	2	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2
	[E.20] Vulnerabilidades de los programas (software)	B	2	B	2	2	M	3	2	B	2	2	B	2	2	B	2	2
	[E.21] Errores de mantenimiento/ actualización de programas(software)	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
Sistema operativo	[I.5] Avería de origen físico o lógico	MB	1	B	2	1	B	2	1	B	2	1	B	2	1	B	2	1
	[E.1] Errores de los usuarios	B	2	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2
	[E.8] Difusión de software dañino	B	2	B	2	2	B	2	2	M	3	2	B	2	2	B	2	2
	[E.20] Vulnerabilidades de los programas (software)	A	4	B	2	3	B	2	3	B	2	3	B	2	3	B	2	3
	[E.21] Errores de mantenimiento/ actualización de programas(software)	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.7] Uso no previsto	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1

Activo	Amenazas según Magerit	IMPACTO																
		[P]		[D]			[I]			[C]			[A]			[T]		
Cuadro 9. (Continuación)																		
Gestor de base de datos Oracle	[E.20] Vulnerabilidades de los programas (software)	M	3	MB	1	2	B	2	2	MB	1	2	MB	1	2	MB	1	2
	[E.21] Errores de mantenimiento/ actualización de programas(software)	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
Impresoras	[N.1] Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.2]Daños por agua	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.*]Desastres naturales	B	2	M	3	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.1]Fuego	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.5]Avería de origen físico o lógico	MB	1	B	2	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.7]Condiciones inadecuadas de temperatura o humedad	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.23]errores de mantenimiento/actualización de equipos(hardware)	M	3	MB	1	2	MB	1	2	MB	1	2	MB	1	2	MB	1	2
	[A.11] Acceso no autorizado	B	2	MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
Computadores de escritorio y portátiles	[N.1] Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.2] Daños por agua	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.*] Desastres naturales	B	2	B	2	2	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[I.1] Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.*] Desastres industriales	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.5] Avería de origen físico o lógico	M	3	M	3	3	B	2	2	B	2	2	B	2	2	B	2	2
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.23] errores de mantenimiento/actualización de equipos(hardware)	B	2	B	2	2	B	2	2	MB	1	1	MB	1	1	MB	1	1

Activo	Amenazas según Magerit	IMPACTO																
		[P]		[D]			[I]			[C]			[A]			[T]		
	Cuadro 9. (Continuación)																	
	[E.24]Caída del sistema por agotamiento de recursos	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.6]abuso de privilegios de acceso	B	2	B	2	2	M	3	2	M	3	2	B	2	2	B	2	2
	[A.7]Uso no previsto	B	2	B	2	2	B	2	2	M	3	2	B	2	2	B	2	2
Router	[N.1] Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.2]Daños por agua	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.*]Desastres naturales	B	2	B	2	2	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[I.3]Contaminación medioambiental	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.5]Avería de origen físico o lógico	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.7]Condiciones inadecuadas de temperatura o humedad	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.11] Acceso no autorizado	MB	1	B	2	1	M	3	2	B	2	1	B	2	1	B	2	1
Escanner	[N.1] Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.2]Daños por agua	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.*]Desastres naturales	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.1]Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.*]Desastres industriales	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.5]Avería de origen físico o lógico	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.7]Condiciones inadecuadas de temperatura o humedad	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.23]errores de mantenimiento/actualización de equipos(hardware)	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.24]Caída del sistema por agotamiento de recursos	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1

Activo	Amenazas según Magerit	IMPACTO																
		[P]		[D]			[I]			[C]			[A]			[T]		
	Cuadro 9. (Continuación)																	
	[A.6]abuso de privilegios de acceso	B	2	MB	1	1	B	2	2	B	2	2	MB	1	1	MB	1	1
	[A.7]Uso no previsto	B	2	MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
Red LAN	[I.8]Fallos de servicios de comunicaciones	M	3	B	2	2	B	2	2	B	2	2	MB	1	2	MB	1	2
	[E.9]Errores de re-encaminamiento	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.10] errores de secuencia	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.5] Suplantación de la identidad del usuario	B	2	B	2	2	MB	1	1	B	2	2	B	2	2	B	2	2
	[A.9] Re-encaminamiento de mensajes	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.10] Alteración de secuencia	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.11] Acceso no autorizado	B	2	B	2	2	B	2	2	M	3	2	B	2	2	B	2	2
Red Wifi	[I.8]Fallos de servicios de comunicaciones	M	3	M	3	3	MB	1	2	B	2	2	MB	1	2	MB	1	2
	[E.9]Errores de re-encaminamiento	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
Internet	[I.8] Fallo de servicios de comunicaciones	M	3	M	3	3	MB	1	2	B	2	2	MB	1	2	MB	1	2
	[E.15] alteración de la información	MB	1	B	2	1	MB	1	1	M	3	2	B	2	1	B	2	1
Telefonía IP	[N.1] Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.2]Daños por agua	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.8] Fallo en servicios de comunicaciones	M	3	M	3	3	MB	1	2	B	2	2	MB	1	2	MB	1	2
	[E.9]errores de encaminamiento	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.15] alteración de la información	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1

Activo	Amenazas según Magerit	IMPACTO																	
		[P]		[D]			[I]			[C]			[A]			[T]			
	Cuadro 9. (Continuación)																		
	[E.19] Fugas de información	B	2	B	2	2	MB	1	1	B	2	2	MB	1	1	MB	1	1	
	[A.7] Uso no previsto	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[A.9] Encaminamiento de mensajes	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[A.10] Alteración de frecuencia.	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[A.12] Análisis de trafico	B	2	B	2	2	B	2	2	M	3	2	MB	1	1	MB	1	1	
	[A.14] Intercepción de información (escucha)	B	2	B	2	2	B	2	2	M	3	2	MB	1	1	MB	1	1	
CD o DVD	[N.1] Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[N.2]Daños por agua	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[E.15] Alteración de la información	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[E.19] Fugas de información	B	2	B	2	2	B	2	2	B	2	2	MB	1	1	MB	1	1	
	[A.15] Modificación de la información.	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[A.19] Revelación de información	MB	1	MB	1	1	MB	1	1	B	2	1	MB	1	1	MB	1	1	
Usb	[N.1] Fuego	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[N.2]Daños por agua	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	
	[E.15] Alteración de la información	B	2	B	2	2	B	2	2	MB	1	1	B	2	2	B	2	2	
	[E.19] Fugas de información	B	2	B	2	2	MB	1	1	M	3	2	MB	1	1	MB	1	1	
	[A.15] Modificación de la información.	MB	1	MB	1	1	MB	1	1	B	2	1	MB	1	1	MB	1	1	
	[A.19] Revelación de información	MB	1	B	2	1	MB	1	1	B	2	1	MB	1	1	MB	1	1	

Activo	Amenazas según Magerit	IMPACTO																
		[P]		[D]			[I]			[C]			[A]			[T]		
Cuadro 9. (Continuación)																		
Documentos impresos	[N.1] Fuego	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.2]Daños por agua	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[E.19] Fugas de información	B	2	MB	1	1	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[A.19] Revelación de información	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
Planta eléctrica	[N.1] Fuego	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.2]Daños por agua	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.3] Contaminación medioambiental	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
Instalación física de CENS	[A.11] Acceso no autorizado	B	2	B	2	2	M	3	2	B	2	2	MB	1	1	MB	1	1
	[A.26] Ataque destructivo.	MB	1	M	3	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[I.1] Fuego	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.8] Desastres naturales. Fenómeno de origen volcánico	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[N.7] Desastres naturales. Fenómeno sísmico.	B	2	M	3	2	MB	1	1	B	2	2	MB	1	1	MB	1	1
	[N.2] Daños por agua	B	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
Gestor de TI	[E.28.1] Enfermedad	M	3	M	3	3	MB	1	2	B	2	2	B	2	2	B	2	2
	[E.28.2]Huelga	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.29]Extorsión	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.30] Ingeniería social	M	3	MB	1	2	MB	1	2	MB	1	2	MB	1	2	MB	1	2
Coordinador de TI	[E.28.1] Enfermedad	M	3	M	3	3	MB	1	2	B	2	2	B	2	2	B	2	2
	[E.28.2]Huelga	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.29]Extorsión	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.30] Ingeniería social	M	3	MB	1	2	MB	1	2	MB	1	2	MB	1	2	MB	1	2

Activo	Amenazas según Magerit	IMPACTO																
		[P]		[D]			[I]			[C]			[A]			[T]		
Cuadro 9. (Continuación)																		
Profesional de TI	[E.28.1] Enfermedad	M	3	M	3	3	B	2	2	B	2	2	B	2	2	B	2	2
	[E.28.2]Huelga	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.29]Extorsión	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.30] Ingeniería social	M	3	MB	1	2	MB	1	2	MB	1	2	MB	1	2	MB	1	2
Tecnólogo de TI	[E.28.1] Enfermedad	M	3	M	3	3	MB	1	2	B	2	2	B	2	2	B	2	2
	[E.28.2]Huelga	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.29]Extorsión	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.30] Ingeniería social	M	3	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2
Técnico de TI	[E.28.1] Enfermedad	M	3	M	3	3	MB	1	2	B	2	2	B	2	2	B	2	2
	[E.28.2]Huelga	B	2	B	2	2	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.29]Extorsión	MB	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1	MB	1	1
	[A.30] Ingeniería social	M	3	B	2	2	B	2	2	B	2	2	B	2	2	B	2	2

Fuente: Autores

8.1.7 Plan de tratamiento de riesgos PTR

Una vez se haya realizado el análisis y cuantificado los riesgos se realiza el tratamiento del riesgo, que consiste en realizar la selección y aplicación de medidas con la finalidad de modificar los riesgos y poder minimizar los daños y aprovechar al máximo las ventajas que los mismos puedan generar. En el cuadro 10 se visualiza el plan de tratamiento de riesgos que contiene los riesgos y los controles asociados a ellos para tratar de reducirlos, modificarlos o eliminarlos.

Cuadro 10. Amenazas, causas y controles

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Portal web	[A.11] Acceso no autorizado. [A.5] Suplantación de identidad de usuario [I.8] Fallos de servicio de comunicaciones. [E.2] Errores de administración	Daño de equipos de comunicaciones por falta de mantenimiento.	Error de Configuración por parte del Administrador	Manejo incorrecto de contraseñas	Falta de definición del proceso de Gestión de Accesos	Acceso al portal mediante LDAP (Directorio Activo – contraseñas Robustas). Contrato de mantenimiento de Dispositivos de Comunicaciones. Personal Capacitado	Mitigar Transferir Mitigar
Sistemas de Información	[A.11] Acceso no autorizado. [E.1] Errores de usuarios [I.5] Avería de origen físico o lógico [E.20] Vulnerabilidades de los programas (software). [I.8] Fallos de servicio de	Daño de equipos de comunicaciones por falta de mantenimiento.	Error de Configuración por parte del Administrador Carencia de validaciones en operaciones de usuario. Fallas de	Falta de capacitación en el uso del software	Falta de definición del proceso de Gestión de Accesos	Acceso al portal mediante LDAP (Directorio Activo – contraseñas Robustas). Contrato de mantenimiento de Dispositivos de	Mitigar Transferir

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
	comunicaciones [E.21] Errores de mantenimiento/ actualización de programas (software) [A.5] Suplantación de la identificación del usuario		seguridad en la programación del sw. Pruebas de SW insuficientes			Comunicaciones. Pruebas de Penetración periódicas. Reentrenamientos periódicos en los roles de los sistemas de información.	 Mitigar Mitigar
Ofimática	[E.1] errores de los usuarios [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software) [A.8] Difusión de software dañino	Equipos sin antivirus o no actualizado.	Fallas de seguridad en los paquetes ofimáticos.	Falta de conocimiento del software legal y free.	Falta de definición de un procedimiento y validación de software legal.	-Instalación y aplicación de McAfee Aplication Control. -Liberación controlada de actualizaciones de seguridad mediante WSUS. -Actualización diaria de las definiciones de virus (.dat) a través de la consola de administración de McAfee	Mitigar Mitigar Mitigar
Antivirus	[E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software)	Equipos sin antivirus o no actualizado.		Falta de conocimiento en la configuración de las consolas de administración del antivirus	Carencia de soporte técnico del antivirus	Contrato de Soporte Técnico y Actualización del software antivirus McAfee. Revisión diaria de Equipos no gestionados desde la consola de McAfee.	Transferir Mitigar

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Cuadro 10. (Continuación)							
Sistema operativo	[I.5] Avería de origen físico o lógico [E.1] Errores de los usuarios [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento/ actualización de programas(software) [A.7]Uso no previsto		Bugs de Seguridad del SO	Errores de configuración. Instalación de SW dañino	Carencia de Soporte técnico	Contrato de Soporte Técnico y Actualización del software Microsoft. McAfee Aplication Control	Transferir Eliminar
Impresoras	[N.1] Fuego [N.2]Daños por agua N.*]Desastres naturales [I.1]Fuego [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [E.23]errores de mantenimiento/actualización de equipos(hardware) [A.11]Acceso no autorizado.	Falta de Mantenimiento periódico	Driver incompatible con el SO		Instalaciones locativas deficientes Carencia de pólizas de seguros.	Contrato de Mantenimiento de Hardware (Equipos, Impresoras y Scanners) Póliza Global de Seguros contra todo riesgo	Mitigar Transferir

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Cuadro 10. (Continuación)							
Computadores de Escritorio y portátiles	[N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.1]Fuego [I.*]Desastres industriales. [I.5]Avería de origen físico o lógico. [I.7]Condiciones inadecuadas de temperatura o humedad. [E.23]errores de mantenimiento/actualización de equipos(hardware) [E.24]Caída del sistema por agotamiento de recursos [A.6]abuso de privilegios de acceso. [A.7]Uso no previsto	Falta de Mantenimiento periódico	Falta de actualizaciones de seguridad.	Instalación de programas dañinos	Carencia de pólizas de seguros. Carencia de políticas de uso seguro de equipos.	Contrato de Mantenimiento de Hardware (Equipos, Impresoras y Scanners) Póliza Global de Seguros contra todo riesgo. Bloqueo de ejecución de medios extraíbles según perfil de usuario.	Mitigar Transferir Mitigar

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Cuadro 10. (Continuación)							
Scanner	N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.1]Fuego [I.*]Desastres industriales [I.5]Avería de origen físico o lógico. [I.7]Condiciones inadecuadas de temperatura o humedad [E.23]errores de mantenimiento/actualización de equipos(hardware). [E.24]Caída del sistema por agotamiento de recursos [A.6]abuso de privilegios de acceso [A.7]Uso no previsto	Falta de Mantenimiento periódico	Driver incompatible con el SO		Instalaciones locativas deficientes. Carencia de pólizas de seguros.	Contrato de Mantenimiento de Hardware (Equipos, Impresoras y Scanners) Póliza Global de Seguros contra todo riesgo	Mitigar Transferir

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Cuadro 10. (Continuación)							
Router	[N.1] Fuego [N.2]Daños por agua [N.*]Desastres naturales [I.3] Contaminación medioambiental [I.5]Avería de origen físico o lógico [I.7]Condiciones inadecuadas de temperatura o humedad [A.11] Acceso no autorizado.	Daño de equipos de comunicaciones por falta de mantenimiento.	Error de Configuración por parte del Administrador	Falta de capacitación en la configuración del dispositivo	Falta de Soporte Técnico especializado	Contrato de mantenimiento de Dispositivos de Comunicaciones. Equipos y módulos de Contingencia.	Transferir Mitigar
Telefonía IP	[N.1] Fuego [N.2]Daños por agua [I.8]Fallo en servicios de comunicaciones [E.9]errores de encaminamiento [E.15] alteración de la información [E.19] Fugas de información [A.7] Uso no previsto [A.9] Encaminamiento de mensajes. [A.10] Alteración de frecuencia [A.12] Análisis de trafico [A.14] Intercepción de información.	Por descarga electica o corto circuito	Error de Configuración por parte del Administrador	Daño de equipos por mal uso de los equipos. Direccionamiento erróneo de IP's	Mala calidad de los equipos en busca de economía.	Cronogramas de Mantenimiento preventivo. Sistemas de detección de Incendios Control de Subneteo IP para la red de telefonía. Capacitación en uso de los teléfonos IP	Mitigar Mitigar Mitigar Mitigar

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Cuadro 10. (Continuación)							
Red WIFI	[I.8]Fallos de servicios de comunicaciones [E.9]Errores de re-encaminamiento	Por descarga electica o corto circuito Falta de mantenimiento		Direccionamiento erróneo de IP's		Contrato de mantenimiento de Dispositivos de Comunicaciones. Control de Subneteo IP para la red WIFI	Transferir Mitigar
Red LAN	[I.8]Fallos de servicios de comunicaciones [E.9]Errores de re-encaminamiento [E.10] errores de secuencia [A.5] Suplantación de la identidad del usuario [A.9] Re-encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado	Fallas en los canales de comunicación. Falla de los equipos de comunicaciones.	Firmware de los equipos no actualizados	Errores en la configuración de los equipos.	Carencia de un plan de capacitación para los administradores de la red.	Contrato de mantenimiento de Dispositivos de Comunicaciones. Canales de Contingencia Activo-Activo Pruebas de Penetración periódicas.	Transferir Mitigar Mitigar
Internet	[I.8] Fallo de servicios de comunicaciones [E.15] alteración de la información	Fallas en los canales de comunicación. Falla de los equipos de comunicaciones.	Uso de Navegadores antiguos y no actualizados.	Inconsciencia del uso seguro de internet.	-Falta de políticas claras sobre el uso seguro de internet para la empresa. -Carencia de plan de internet de contingencia.	Canales de Contingencia Activo-Activo Plan de Internet de Contingencia	Mitigar Mitigar

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Cuadro 10. (Continuación)							
Sistema de video-Vigilancia y seguridad electrónica.	[N.1] Fuego [N.2]Daños por agua [I.3] Contaminación medioambiental [I.7] condiciones inadecuadas de temperatura o humedad	Por descarga electica o corto circuito Falta de mantenimiento		Errores en la configuración de los sistemas y equipos.	Equipos Inadecuados para el ambiente donde se instalan	Contrato de Servicio de Monitoreo permanente de las sedes de CENS.	Transferir
Planta eléctrica	[N.1] Fuego [N.2]Daños por agua [I.3] Contaminación medioambiental	Falta de Mantenimiento		Configuración errada.	Carencia de contrato de mantenimiento periódico.	Revisión periódica del estado de la Planta.	Mitigar
CD o DVD	[N.1] Fuego [N.2]Daños por agua [E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información.	Falta de mantenimiento	Drivers antiguos	Asignación inadecuada de permisos de uso.	Lineamiento de uso de dispositivos de grabación.	Bloqueo de ejecución de medios extraíbles según perfil de usuario.	Mitigar
Usb	[N.1] Fuego [N.2]Daños por agua [E.15] Alteración de la información [E.19] Fugas de información [A.15] Modificación de la información [A.19] Revelación de información	Falta de mantenimiento	Drivers antiguos	Asignación inadecuada de permisos de uso.	Lineamiento de uso de dispositivos de grabación.	Bloqueo de ejecución de medios extraíbles según perfil de usuario.	Mitigar

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Cuadro 10. (Continuación)							
TIVIT-Synapsis	[E.1] Errores de usuario [E.15] Alteración de la información [E.19] Fugas de información [A.19] Revelación de información [I.8]Fallos de servicios de comunicaciones.	Por descarga electica o corto circuito Falta de mantenimiento			Carencia de cláusulas de confidencialidad de la información en los contratos.	Pólizas de Cumplimiento, Responsabilidad Civil. ANS Acuerdo de Confidencialidad	Transferir Mitigar Mitigar
EPM S.A. E.S.P.	[E.1] Errores de usuario [E.15] Alteración de la información [E.19] Fugas de información [A.19] Revelación de información [I.8]Fallos de servicios de comunicaciones.	Por descarga electica o corto circuito Falta de mantenimiento			Carencia de cláusulas de confidencialidad de la información en los contratos.	Pólizas de Cumplimiento, Responsabilidad Civil. ANS Acuerdo de Confidencialidad	Transferir Mitigar Mitigar
Gestor de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social			-Carencia de hábitos de vida saludable. -Falta de capacitación en seguridad informática	Falta de seguimiento a enfermedades profesionales Carencia de Estudio de Seguridad.	Sistema de Seguridad y Salud en el Trabajo. Sistema de Gestión de Calidad (procesos, procedimientos, guías, instructivos)	Mitigar Mitigar

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
Cuadro 10. (Continuación)							
Coordinador de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social			Carencia de hábitos de vida saludable. Falta de capacitación en seguridad informática	Falta de seguimiento a enfermedades profesionales Carencia de Estudio de Seguridad.	Sistema de Seguridad y Salud en el Trabajo. Sistema de Gestión de Calidad (procesos, procedimientos, guías, instructivos)	Mitigar Mitigar
Profesional de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social [A.29.2] Ataque desde el interior [E.4] Errores de configuración			Carencia de hábitos de vida saludable. Falta de capacitación en seguridad informática	Falta de seguimiento a enfermedades profesionales Carencia de Estudio de Seguridad.	Sistema de Seguridad y Salud en el Trabajo. Sistema de Gestión de Calidad (procesos, procedimientos, guías, instructivos)	Mitigar Mitigar
Tecnólogo de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30] Ingeniería social [A.29.2] Ataque desde el interior			Carencia de hábitos de vida saludable. Falta de capacitación en seguridad informátic	Falta de seguimiento a enfermedades profesionales Carencia	Sistema de Seguridad y Salud en el Trabajo. Sistema de Gestión de Calidad (procesos, procedimientos, guías, instructivos)	Mitigar Mitigar

Activos	Amenazas	HW	SW	TH	ORG	Controles	Tratamiento
				a	de Estudio de Seguridad. Acceso innecesario de información privilegiad.		
Técnico de TI	[E.28.1] Enfermedad [E.28.2]Huelga [A.29]Extorsión [A.30]Ingeniería social [A.29.2] Ataque desde el interior			Carencia de hábitos de vida saludable. Falta de capacitación en seguridad informática	Falta de seguimiento a enfermedades profesionales. Carencia de Estudio de Seguridad. Acceso innecesario de información privilegiada.	Sistema de Seguridad y Salud en el Trabajo. Sistema de Gestión de Calidad (procesos, procedimientos, guías, instructivos)	Mitigar Mitigar

Fuente: Autores

8.2. PENTEST DE LA APLICACIÓN Y SERVIDOR WEB

En los siguientes apartados se desarrollarán las fases de un pentest controlado a la aplicación web SIRIUS ADM utilizando la herramienta Acunetix.

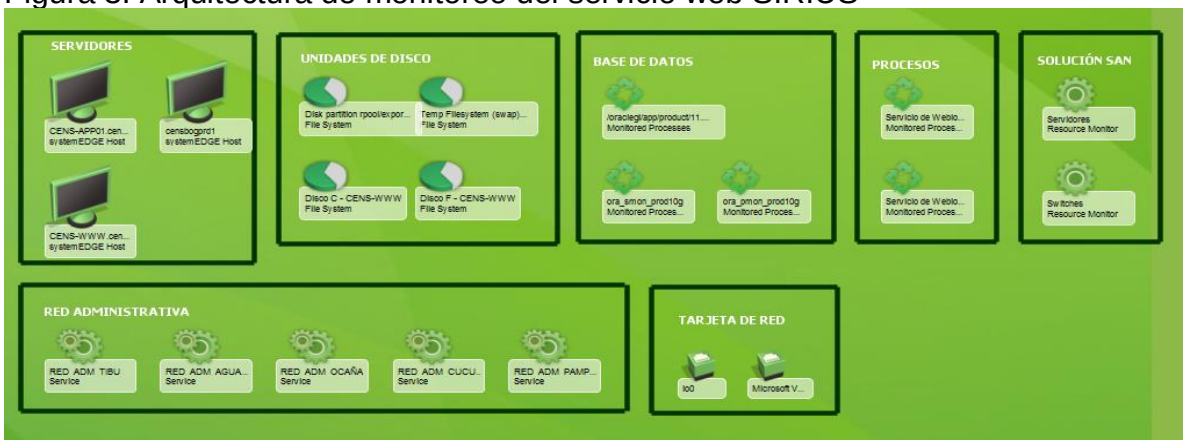
8.2.1 Contexto

La aplicación web SIRIUS ADM es utilizada para la administración y ejecución de tareas relacionadas con la toma de lecturas, revisiones comerciales y revisiones técnicas en CENS SA ESP. La aplicación consta de 4 módulos a saber:

- Sirius ADM
- Sirius Server
- Sirius Lectura
- Sirius Revisión

La aplicación web SIRIUS ADM por ser una aplicación critica para CENS, es monitoreada por componentes con la herramienta CA SPECTRUM para medir su disponibilidad y poder detectar a tiempo cualquier tipo de anomalía que degrade o indisponga la aplicación, en la figura 3 se puede observar los componentes relacionados con el servicio web SIRIUS.

Figura 3. Arquitectura de monitoreo del servicio web SIRIUS



Fuente: Los Autores

Debido a la salida a producción de la nueva versión del servicio web para la solución de movilidad encargado de la toma de lecturas de energía (SIRIUS), se requiere realizar un análisis de vulnerabilidades, con el fin de mitigar los riesgos encontrados

y que puedan ocasionar un incidente de seguridad de la información para la organización.

8.2.2 Reglas definidas

Advertencia: La información contenida en este documento es confidencial. Se autoriza su uso exclusivamente a CENS. Toda reproducción parcial o completa, distribución a terceros o modificaciones al documento no autorizados se encuentra totalmente prohibida.

Niveles de las vulnerabilidades: en cuanto al análisis de la aplicación web Sirius ADM se realizará con la solución de software Acunetix el cual clasifica las vulnerabilidades en cuatro niveles, Alto, Medio, Bajo e informativo, siendo el primer nivel (Alto) el de riesgo más crítico y al cual se le debe dar prioridad en su remediación o mitigación, en cuanto al análisis del servidor web se realizará con la solución Nessus que clasifica las vulnerabilidades en 5 niveles, Critico, Alto, medio, bajo e informativo.

Objetivo: Analizar y evaluar las vulnerabilidades de la aplicación web Sirius ADM el ambiente de pruebas, las cuales puedan afectar la confidencialidad, integridad y/o disponibilidad de la información.

Escenario: La identificación y evaluación de vulnerabilidades de la aplicación web Sirius ADM como la del servidor web se realiza desde un servidor de la red corporativa de la organización, con el software especializado Acunetix y Nessus, además, se tienen conocimiento de la URL donde esta implementada la aplicación web Sirius ADM y servidor web en ambiente de pruebas.

8.2.3 Recolección de información aplicación web SIRIUS ADM

A continuación, vemos en el cuadro 11 información general relativa al activo informático estudiado, “aplicación web Sirius ADM”:

Cuadro 11. Activo de información evaluado

Nombre del Activo	Tipo de Activo	URL	Ambiente
Sirius ADM	Aplicación WEB	https://10.46.2.24:8444/WsSiriusServer60/api/SiriusRest/	Pruebas

Fuente. Los Autores

Una vez realizada la primera revisión de auditoria se encontró que los puertos TCP 135, 139, 443, 445, 1720, 1801, 1863, 2030, 2103, 2105, 2107, 3389, 5555, 8081, 8443, 9090, 49152, 49153, 49154, 49155 y 49167 se encontraban abiertos tal y como se observa en la figura 4.

Figura 4. Estado de puertos según escaneo con NMAP

Fuente: Los Autores

8.2.4 Identificación de vulnerabilidades de la aplicación web

A continuación, se describe el resumen de las vulnerabilidades encontradas en la aplicación web Sirius ADM, están clasificadas por severidad, que puede ser Alta, Media, Bajo o Informativa y por tipo.

8.2.4.1 Vulnerabilidades clasificadas por Severidad. A continuación, en el Cuadro 12 se puede visualizar el resultado de las vulnerabilidades detectadas por nivel de severidad, en donde se aprecia que no se encontró ninguna vulnerabilidad con severidad alta, con severidad media dos, con severidad baja dos y seis de tipo informativa.

Cuadro 12. Vulnerabilidades por nivel de severidad

Severidad	Cantidad
Alta	0
Media	2
Baja	2
Informativa	6
Total	10

Fuente: Los Autores

El score base CVSS versión 3, es un sistema de puntuación estándar para la evaluación cuantitativa de vulnerabilidades y de esta forma priorizar su remediación o mitigación. En el cuadro 13 se observa los 4 tipos de vulnerabilidades encontradas, RC4 Cipher suites detected, The POODLE attack (SSLv3 supported), Clickjacking: X-Frame-Options header missing y Possible sensitive directories.

Cuadro 13. Score de vulnerabilidades según CVSS

Tipo de Vulnerabilidad	Severidad	Score CVSS	Cantidad
RC4 Cipher suites detected	Media	9.1	1
The POODLE attack (SSLv3 supported)	Media	3.1	1
Clickjacking: X-Frame-Options header missing	Baja	6.8	2
Possible sensitive directories	Baja	7.5	6
		Total	10

Fuente: Los Autores

8.2.4.2 Vulnerabilidad RC4 cipher suites detected. Cifrado débil de la suite RC4 detectado.

Identificación: CWE-310, CVE-2013-2566

Impacto: Medio, afecta principalmente la confidencialidad de la información.

Posibilidad de ocurrencia: Medio. Existen herramientas de software automatizadas para detectar este tipo de vulnerabilidad y obtener información en texto plano.

Riesgo: Medio.

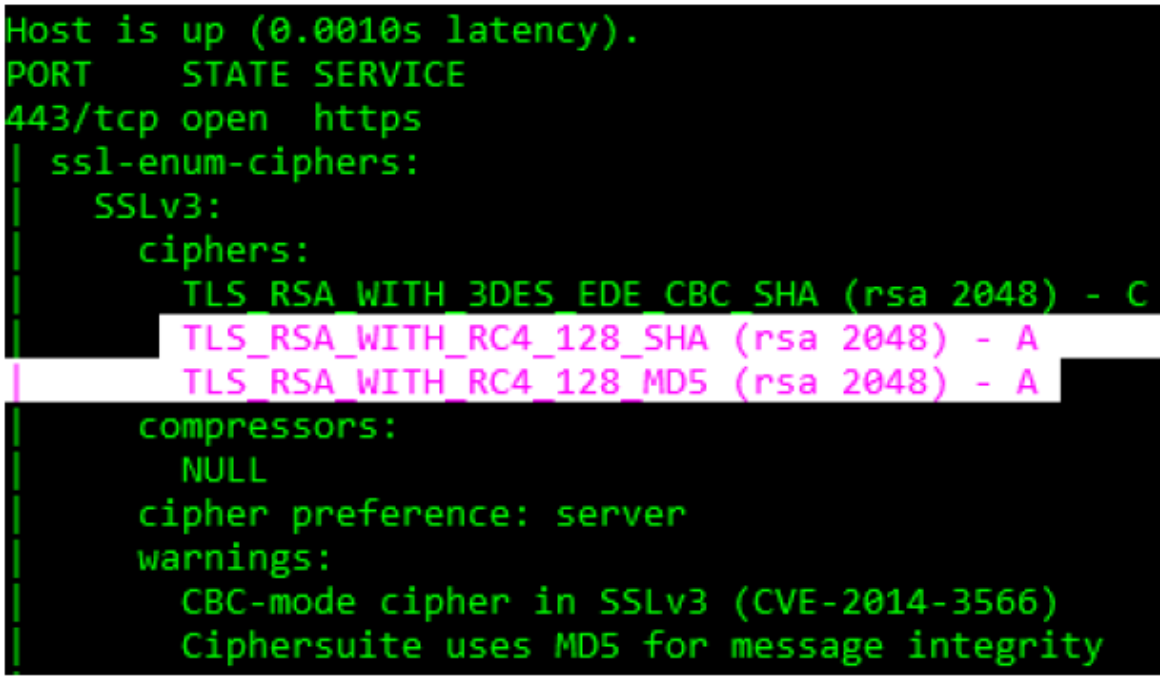
Descripción: El servidor Web usa un cifrado débil con el algoritmo RC4 sobre SSL3 y TLS1. Un caso de un ataque fue propuesto por Alfardan, Bernstein, Paterson,

Poettering y Schuldt que utilizaba nuevos sesgos estadísticos descubiertos en la clave RC4 para recuperar partes del texto en claro con un gran número de cifrados TLS. Un ataque de sesgo de doble byte en RC4 en TLS y SSL que requiere 13 × 220 cifrados para romper RC4 se dio a conocer el 8 de julio de 2013.

Verificación o Prueba de Concepto (PoC): Se detectaron los siguientes cifrados tipo RC4, que se puede observar en la figura 5.:

- TLS_RSA_WITH_RC4_128_SHA (rsa 2048)-A
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048)-A

Figura 5. Tipo de cifrado detectado RC4

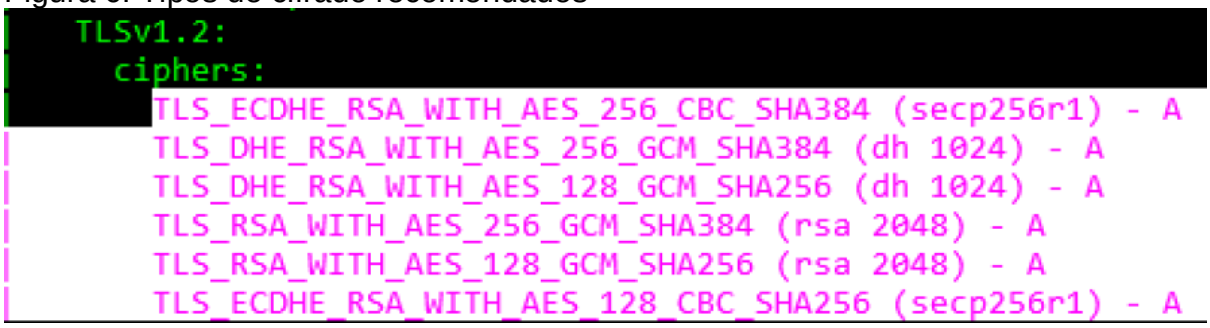


Fuente: los Autores

Recomendación/Mitigación: Se recomienda usar algunos de los siguientes cifrados sobre TLSv1.2, que pueden ser observados en la figura 6:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) – A
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) – A
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) – A
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) – A
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) – A
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) – A

Figura 6. Tipos de cifrado recomendados



Fuente: los Autores

8.2.4.3 The POODLE attack (SSLv3 supported). Padding Oracle On Downgraded Legacy Encryption, esta vulnerabilidad se aprovecha de la utilización del protocolo SSLv3.

Severidad: Media.

Identificación: CWE-16, CVE-2014-3566

Impacto: Medio, afecta principalmente la confidencialidad de la información. Posibilidad de ocurrencia: Medio. Existen herramientas de software automatizadas para detectar este tipo de vulnerabilidad y obtener información en texto plano.

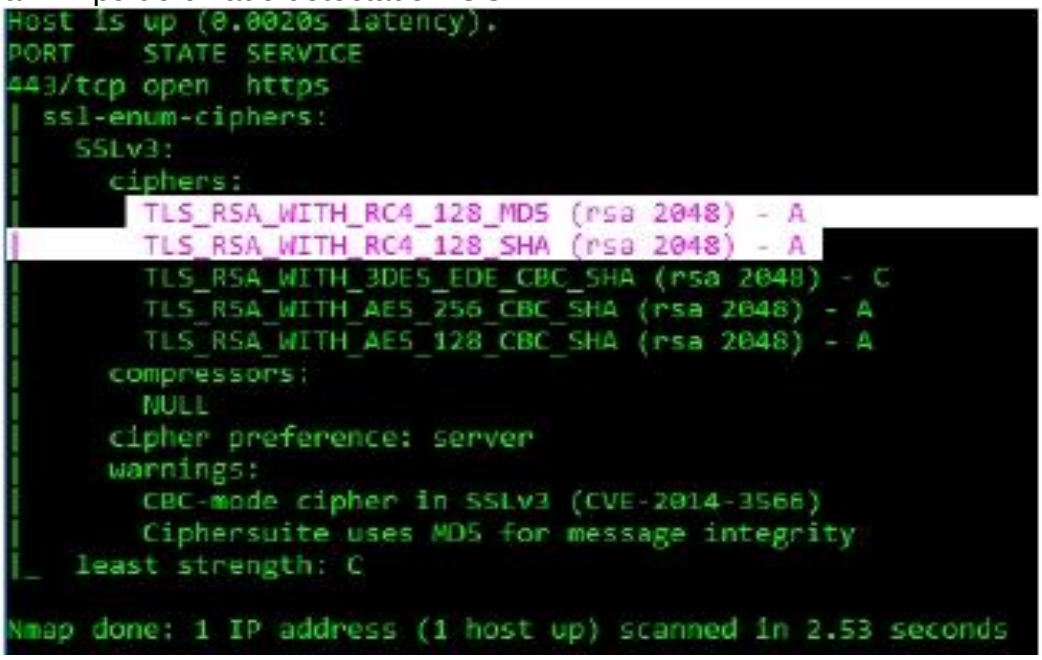
Riesgo: Medio.

Descripción: El servidor Web usa SSL versión 3 y el modo de cifrado CBC, y este tiene una vulnerabilidad conocida identificada con el CVE-2014-3566 lo que permitirá materializar el ataque de Poodle que es de tipo Hombre en el Medio (Man-in-the-middle) para capturar información confidencial en texto plano.

Prueba de concepto: Se detectaron los siguientes cifrados, mostrados en la figura 7:

- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) – A
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048) – A

Figura 7. Tipo de cifrado detectado POODLE

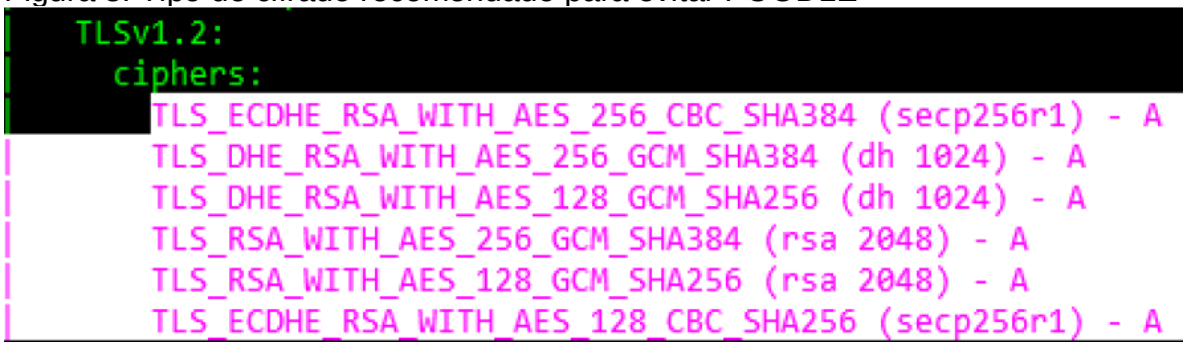


Fuente: Los Autores

Recomendación/Mitigación: En la figura 8 se pueden observar algunos de los siguientes protocolos de cifrado sobre TLSv1.2 que se recomienda usar:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) – A
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) – A
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) – A
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) – A
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) – A
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) – A

Figura 8. Tipo de cifrado recomendado para evitar POODLE



Fuente: los autores

8.2.4.4 Possible sensitive directories. Posible información sensible en directorio.

Severidad: Bajo

Impacto: Este directorio puede exponer información confidencial que podría ayudar a un usuario malintencionado a preparar ataques más avanzados.

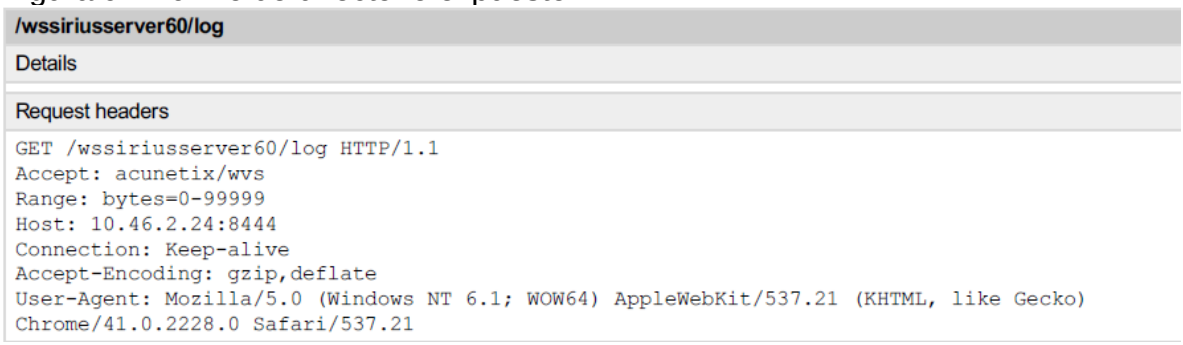
Posibilidad de ocurrencia: Informativo. Existen herramientas de software automatizadas para detectar este tipo de vulnerabilidad y obtener información de tipo sensible.

Riesgo: Bajo

Descripción: Se ha encontrado un directorio sensible el cual se puede observar en la figura 9. Este directorio no está vinculado directamente desde el sitio web. Recursos sensibles como directorios de copia de seguridad, volcados de base de datos, páginas de administración, directorios temporales, podrían ayudar a un atacante a aprender más sobre su objetivo.

Prueba de concepto: Ítem afectado:

Figura 9. Archivo de directorio expuesto



Fuente: los autores

Recomendación: Restringir el acceso a este directorio o eliminarlo del sitio web.

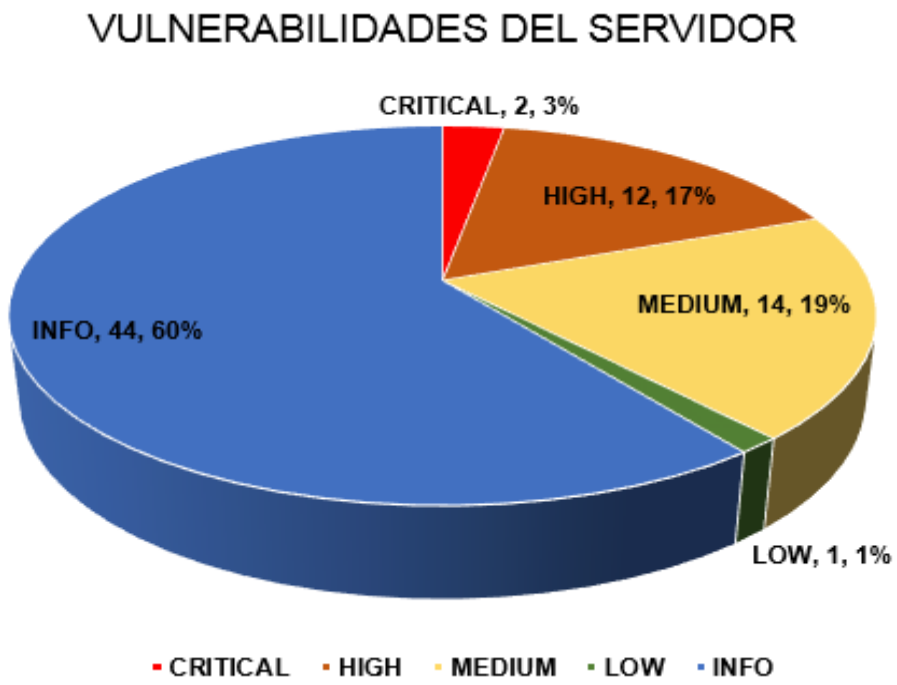
8.2.4.5 Conclusión de la identificación de vulnerabilidades de la aplicación web. Se puede concluir que el servicio Web tiene un nivel de riesgo aceptable para CENS, ya que no tiene vulnerabilidades conocidas de severidad alta y las de severidad media aplican para el servidor Web y no tienen una posibilidad de ocurrencia o impacto alto si se llegan a materializar. Sin embargo, se recomienda

verificar las vulnerabilidades con cifrado débil sobre el protocolo SSL y TLS para evitar la materialización de un riesgo sobre la infraestructura de TI. Además, se recomienda verificar si es necesario tener abiertos todos los puertos que se evidencian en el escaneo de lo contrario cerrarlos o filtrarlos.

8.2.5. Identificación de vulnerabilidades del servidor web

En el servidor web se ejecutó el software Nessus para identificar las vulnerabilidades, en la figura 10 se observa que la mayor cantidad de vulnerabilidades son de tipo informativa, pero se encontraron dos vulnerabilidades críticas y doce altas las cuales se deben analizar y buscar una rápido solución, por otra parte, se evidencia que vulnerabilidades de tipo medio catorce y de tipo bajo una sola.

Figura 10. Vulnerabilidades del servidor web



Fuente: los autores

A continuación, se enuncian las vulnerabilidades de tipo crítico y alto. En el cuadro 14 se describen y se da una posible solución a las vulnerabilidades de tipo crítico y altas, las dos de tipo crítico están relacionadas con PHP y en las de tipo alto están relacionadas con PHP y el Apache.

Cuadro 14. Vulnerabilidades críticas y altas

Vulnerabilidad/Solución	Cantidad
Critical	2
PHP 5.3.x < 5.3.15 Multiple Vulnerabilities	1
Upgrade to PHP version 5.3.15 or later.	
PHP Unsupported Version Detection	1
Upgrade to a version of PHP that is currently supported.	
High	13
Oracle WebLogic Server CVE-2015-4852 Remote Code Execution Vulnerability	1
Update to WebLogic Server version 10.3.6.0 and Apply Patch	
Apache 2.2.x < 2.2.28 Multiple Vulnerabilities	1
Upgrade to Apache version 2.2.29 or later. Note that version 2.2.28 was never officially released.	
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	1
Upgrade to Apache version 2.2.33-dev / 2.4.26 or later.	
Apache 2.2.x < 2.2.34 Multiple Vulnerabilities	1
Upgrade to Apache version 2.2.34 or later.	
PHP < 5.3.11 Multiple Vulnerabilities	1
Upgrade to PHP version 5.3.11 or later.	
PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	1
Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.	
PHP < 5.3.9 Multiple Vulnerabilities	1
Upgrade to PHP version 5.3.9 or later.	
PHP 5.3.x < 5.3.13 CGI Query String Code Execution	1
Upgrade to PHP version 5.3.13 or later. A 'mod_rewrite' workaround is available as well.	
PHP 5.3.x < 5.3.14 Multiple Vulnerabilities	1
Upgrade to PHP version 5.3.14 or later.	
PHP 5.3.x < 5.3.22 Multiple Vulnerabilities	1
Upgrade to PHP version 5.3.22 or later.	
PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities	1
Upgrade to PHP version 5.3.28 or later.	
PHP 5.3.x < 5.3.29 Multiple Vulnerabilities	1
Upgrade to PHP version 5.3.29 or later.	
Unsupported Web Server Detection	1
Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.	

Fuente: los autores

8.2.5.1 Multiple Vulnerabilities 60085 - PHP 5.3.x < 5.3.15. El servidor web utiliza una versión de PHP que se ve afectada por múltiples vulnerabilidades.

Según el diagnóstico, la versión de PHP instalada en el servidor es 5.3.x anterior a 5.3.15, y es, por lo tanto, potencialmente afectados por las siguientes vulnerabilidades:

- Existe una vulnerabilidad de desbordamiento no especificada en la función '_php_stream_scandir' en el archivo 'main / streams / streams.c '. (CVE-2012-2688).

- Existe un error no especificado que puede permitir que la restricción 'open_basedir' se omita. (CVE-2012-3365)

CVE-2012-3365: La funcionalidad SQLite en PHP anterior a la 5.3.15 permite a los atacantes remotos eludir el mecanismo de protección open_basedir a través de vectores no especificados.

CVE-2012-2688: Vulnerabilidad no especificada en la función _php_stream_scandir en la implementación de flujo en PHP antes de 5.3.15 y 5.4.x antes de 5.4.5 tiene un impacto desconocido y vectores de ataque remotos, relacionados con un "desbordamiento".

8.2.5.2 PHP Unsupported Version Detection (58987). El host remoto contiene una versión no compatible de un lenguaje de scripting de aplicación web. Según la versión instalada en el servidor, la instalación de PHP en el ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto, como resultado, es probable que contenga vulnerabilidades de seguridad.

9. CONTROLES SE SEGURIDAD

9.1 RC4 CIPHER SUITES DETECTED

Esta vulnerabilidad, Cifrado débil de la suite RC4 es identificada dentro de la lista de debilidades que comúnmente afectan a las aplicaciones como CWE-310 el cual corresponde a la categoría de inconvenientes criptográficos. Dentro de la lista de vulnerabilidades y exposiciones comunes de la seguridad de información se identifica como CVE-2013-2566 el cual describe la vulnerabilidad como un inconveniente del algoritmo RCA sobre los protocolos TLS y SSL ya que dicho algoritmo tiene muchos sesgos de un solo byte permitiendo a los delincuentes informáticos recuperar texto plano mediante análisis estadístico del texto cifrado en una gran cantidad de sesiones que utilizan el mismo texto plano.[15] Esta vulnerabilidad tiene una severidad media, un riesgo medio y una posibilidad de ocurrencia media por lo cual no se debe perder de vista o darla como una vulnerabilidad sin importancia.

En el cuadro 15 mostrado a continuación, se describen los productos que tienen esta vulnerabilidad.

Cuadro 15. Productos con vulnerabilidad de Cifrado débil de la suite RC4

#	Product Type	Vendor	Product
1	Application	Apple	Safari
2	Application	Google	Chrome
3	Application	IBM	Websphere Application Server
4	Application	Jboss	Jboss Enterprise Application Server
5	Application	Microsoft	IE
6	Application	Microsoft	IIS
7	Application	Mozilla	Firefox
8	Application	Opera	Opera Browser
9	Application	Oracle	Glassfish
10	Application	Oracle	Sparc-opl Service Processor
11	Application	SUN	Glassfish Enterprise Server

Fuente: https://www.cvedetails.com/cve/CVE-2013-2566/

[15] Acunetix, https://www.acunetix.com/vulnerabilities/web/rc4-cipher-suites-detected/

A continuación, se recomiendan acciones para controlar la vulnerabilidad.

Desactivar SSL 2.0 y SSL 3.0. SSL 2.0 fue la primera versión de SSL publicada públicamente en 1995. Esta versión de SSL contenía una serie de problemas de seguridad que llevaron a la introducción de SSL 3.0. SSL 3.0 fue lanzado en 1996 con un completo rediseño del protocolo. Debido a los problemas presentados en SSL2.0, el protocolo no es seguro de usar y debe estar completamente deshabilitado. Debido a la vulnerabilidad de POODLE (Padding Oracle On Downgraded Legacy. Encryption), SSL 3.0 tampoco es seguro de usar y se debe deshabilitar para evitar que un atacante recupere el texto plano de las conexiones seguras.

Deshabilitando TLS 1.0 y 1.1. A menos que sea necesario admitir navegadores heredados, TLS 1.0 y 1.1 también deberían estar deshabilitados. PCI DSS especifica que TLS 1.0 ya no se puede usar a partir del 30 de junio de 2018, y también sugiere enfáticamente deshabilitar TLS 1.1; ya que estos protocolos pueden verse afectados por vulnerabilidades como FREAK, POODLE, BEAST y CRIME.

Los cifrados débiles como DES y RC4 deben estar desactivados. El DES se puede romper en unas pocas horas, mientras que RC4 se ha encontrado que es más débil de lo que se pensaba anteriormente. Si bien se recomendó el uso de RC4 para mitigar los ataques de BESTIA en el pasado, dado los últimos ataques en el cifrado RC4.

Configuración: Dependiendo de su caso de uso empresarial (por ejemplo, la necesidad de ser compatible con los navegadores heredados y los requisitos reglamentarios), es posible que deba optar por configuraciones de conjuntos de cifrado ligeramente diferentes. El generador de configuración SSL de Mozilla se puede usar para obtener una configuración TLS óptima en función de sus requisitos utilizando diferentes "perfiles" de navegador (perfiles modernos, intermedios y antiguos).

El siguiente es un desglose del perfil moderno (clientes compatibles más antiguos: Firefox 27, Chrome 30, Internet Explorer 11 en Windows 7, Edge, Opera 17, Safari 9, Android 5.0 y Java 8)

Dependiendo del servidor web en cuestión (por ejemplo, Servidor HTTP Apache, Nginx…), la sintaxis de habilitar / deshabilitar los protocolos TLS y los conjuntos de cifrado TLS compatibles variará ligeramente.

Servidor HTTP Apache:

Enable TLSv1.2, disable SSLv3.0, TLSv1.0 and TLSv1.1 SSLProtocol all -SSLv3

-TLSv1 -TLSv1.1 # Enable modern TLS cipher suites SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256 # The order of cipher suites matters SSLHonorCipherOrder on # Disable TLS compression SSLCompression off # Necessary for Perfect Forward Secrecy (PFS) SSLSessionTickets off

La cadena proporciona el cifrado más sólido en los navegadores modernos y los clientes TLS / SSL (AES en Galois Counter Mode solo se admite en TLS 1.2). Además, la cadena también proporciona Perfect Forward Secrecy si tanto el servidor como el cliente TLS / SSL tienen soporte (SSLSessionTickets debe estar off para que esto funcione en el servidor HTTP Apache).

9.2 THE POODLE ATTACK (SSLV3 SUPPORTED)

El protocolo SSL 3.0, tal como se utiliza en OpenSSL a través de 1.0.1i y otros productos, utiliza un relleno CBC no determinista, lo que facilita que los atacantes de man-in-the-middle obtengan datos de texto claro mediante un ataque oráculo de relleno, también conocido como "POODLE". "

El ataque Padding Oracle On Downgraded Legacy Encryption (POODLE) se publicó en octubre de 2014 y aprovecha dos factores. El primero es el hecho de que algunos servidores / clientes siguen siendo compatibles con SSL 3.0 para la interoperabilidad y compatibilidad con sistemas heredados, y el segundo factor es una vulnerabilidad que existe en SSL v3.0 que está relacionada con el Bloqueo de bloques.

El Cliente inicia Handshake y envía la lista de las versiones SSL / TLS compatibles. Un atacante intercepta el tráfico, realiza un ataque Man-in-The-Middle (MiTM) y se hace pasar por el Servidor hasta que el Cliente acepte degradar la conexión al SSL 3.0 vulnerable.

Ahora que la conexión entre el Cliente y el Servidor se establece en una versión SSL vulnerable, el atacante puede realizar el ataque POODLE real. La vulnerabilidad existe en el modo Cipher Block Chaining. Dado que los cifrados en bloque tienen una longitud fija, si los datos en el último bloque no son múltiplos de su tamaño, entonces se agrega relleno para llenar el espacio adicional. Uno de los problemas es que el servidor ignora el valor de relleno y comprueba solo si la longitud del relleno es correcta, así como el Código de autenticación de mensaje

(MAC) del texto plano. Eso significa que el receptor (Servidor) no puede verificar si el valor de relleno se ha modificado.

Un atacante puede descifrar el valor de texto simple de un bloque cifrado modificando los bytes de relleno y luego viendo la respuesta correspondiente del servidor. Se requieren un máximo de 256 solicitudes SSL 3.0 para descifrar un solo byte.

Esto significa que una vez cada 256 solicitudes, el servidor aceptará el valor modificado. El atacante no necesita conocer el método de cifrado o la clave para realizar este ataque. Usando herramientas automatizadas, un atacante puede recuperar el carácter de texto simple por carácter. Esto podría ser fácilmente una contraseña, una cookie, una sesión u otros datos confidenciales.

A continuación, se enumeran algunas recomendaciones para prevenir esta vulnerabilidad.

- Deshabilite completamente SSL3.0 en el servidor (Recomendado).

- Actualice el navegador (cliente) a la última versión o, si por alguna razón necesita usar una versión anterior, asegúrese de desactivar los protocolos SSL 2.0 y SSL 3.0. La mayoría de los navegadores / servidores actualizados utilizan TLS_FALLBACK_SCSV . Si un cliente solicita una versión del protocolo TLS que es más baja que la más alta admitida por el servidor (y el cliente), el servidor identificará el respaldo descendente intencional y eliminará la conexión.

- Algunas implementaciones de TLS 1.0 / 1.1 también son vulnerables a POODLE, ya que aceptan una estructura de relleno incorrecta después del descifrado.

- Se descubrió un error en el protocolo de criptografía Secure Socket Layer (SSL) v 3.0, también conocido como SSL v 3.0 (SSLv3). Los sistemas y aplicaciones que utilizan SSL v 3.0 con cifrado de cifrado en bloque (CBC) están en riesgo. Esta falla fue descubierta por investigadores en Google y describieron cómo esta falla puede ser explotada por un método que llamaron ataque Padding Oracle On Downgraded Legacy Encryption (POODLE).

- Si bien el protocolo SSLv3 es defectuoso, los certificados SSL y su clave privada están bien. Los certificados SSL no se ven afectados y no es necesario reemplazarlos.

- SSLv3 es un protocolo anterior que se introdujo alrededor de 1995 y ha sido reemplazado por Transport Layer Security (TLS), TLS v 1.0, TLS v 1.1 y TLS v 1.2. Aunque SSLv3 es antiguo, todavía es compatible con la mayoría de los navegadores de Internet, servidores y sistemas que utilizan OpenSSL. En la mayoría de los casos, los sistemas que admiten TLS retrocederán o bajarán a

SSLv3 según sea necesario. Cuando falla una conexión segura, la mayoría de los servidores bajarán a un protocolo más antiguo como SSLv3.

- Un posible escenario de ataque es cuando un atacante controla la red entre la computadora cliente y el servidor. Podrían manipular el protocolo de enlace utilizado por el protocolo de criptografía para forzar al servidor a una llamada "danza de degradación de protocolo". La idea es lograr que los sistemas involucrados usen el protocolo SSLv3 más antiguo para asegurar la transmisión de datos. Luego, los atacantes podrían explotar el error con el ataque del hombre en el medio (MITM) para comprometer las cookies seguras, lo que podría llevar a un ladrón de información o al acceso y control ilegal de las cuentas de la víctima.

- Actualmente no hay una solución para esta vulnerabilidad en SSLv3, la falla es fundamental para el protocolo de SSLv3. La solución es deshabilitar el uso de SSLV3 y SSLv2 de los browers si es posible o usar una versión de navegador con SSLv3 eliminado. Los investigadores también recomiendan aplicar parches a los servidores y dispositivos con TLS_FALLBACK_SCSV, una extensión de protocolo que evita que los atacantes MITM puedan forzar una degradación del protocolo.

9.3 POSSIBLE SENSITIVE DIRECTORIES

Esta vulnerabilidad, Posible información sensible en directorio es identificada dentro de la lista de debilidades que comúnmente afectan a las aplicaciones como CWE-200 el cual corresponde a la categoría de exposición de información.

La información ya sea que:

- se considera sensible dentro de la funcionalidad propia del producto, como un mensaje privado; o
- proporciona información sobre el producto o su entorno que podría ser útil en un ataque pero que normalmente no está disponible para el atacante, como la ruta de instalación de un producto que es accesible de forma remota.

Son resultantes muchas exposiciones de información (p. Ej., Error de script PHP que revela la ruta completa del programa), pero también pueden ser primarias (p. Ej., Discrepancias de tiempo en la criptografía). Hay muchos tipos diferentes de problemas que involucran exposiciones de información. Su gravedad puede variar ampliamente según el tipo de información que se revela.

El control que se debe aplicar es restringir el acceso a este tipo de directorios o

eliminarlo del sitio web y crear límites de confianza.

9.4 PHP 5.3.X < 5.3.15 MULTIPLE VULNERABILITIES - 60085. El control que se recomienda para mitigar esta vulnerabilidad es actualizar a la versión de PHP 5.3.15 o posterior.

9.5 PHP UNSUPPORTED VERSION DETECTION - 58987. El control que se recomienda para mitigar esta vulnerabilidad es actualizar la versión de PHP a una versión que este soportada.

10. POLÍTICA DE SEGURIDAD

La Junta Directiva de CENS en reunión del 27 de abril de 2017 sesión 791, aprobó por unanimidad la política de seguridad de la información y la ciberseguridad en los siguientes términos: “CENS se compromete a proteger la información, los activos críticos y ciberactivos que posee, con el fin de contar con información integra, completa y con los niveles de confidencialidad requeridos para la toma de decisiones, la operación segura y la respuesta oportuna a incidentes o ataques sobre sus activos críticos y ciberactivos, de forma que se garantice la continuidad en la prestación de los servicios.”[16]

10.1 LINEAMIENTOS

Para CENS, los lineamientos son directrices que ayudan al cumplimiento de las políticas. En lo sucesivo se impartirán algunos lineamientos para los procesos de nivel 2: Diseño del Servicio, Desarrollo del Servicio y Operación del Servicio que conforman el macro-proceso de Tecnología de Información (nivel 1).

10.1.1 Lineamientos para el proceso “diseño del servicio”

Diseño del servicio es un proceso de nivel 2, que está compuesto por los procesos de nivel 3: Gestión de Disponibilidad, Gestión de Catalogo, Gestión de Niveles de Servicio y Gestión de Seguridad del Servicio de TI. Los Lineamientos actúan en los procesos de más bajo nivel ayudando a la consolidación de la política.

10.1.1.1 Gestión de la disponibilidad. El proceso de gestión de la disponibilidad debe propender porque los servicios de TI estén disponibles y funcionen en el marco de las condiciones establecidas en los Acuerdos de Nivel de Servicio (ANS) con los clientes de TI; para lo cual se definen anualmente las metas del indicador de disponibilidad de los servicios de TI prestados con infraestructura propia de CENS, las cuales velan por mantener niveles adecuados de estabilidad, calidad y confiabilidad, contribuyendo con ello a la eficiencia operativa en los procesos.

[16] CENS S.A E.S.P. Política De Seguridad. www.cens.com.co

10.1.1.2 Gestión de catálogo y niveles de servicio. El proceso de gestión del catálogo de servicios deberá definir, estructurar y mantener actualizada la información de los servicios de TI. De esta forma se facilita la comunicación con los diferentes actores de la organización, al disponer de una versión única y consistente de la oferta de servicios disponibles, suministrando información de las características, funcionalidad, condiciones, niveles de servicio y restricciones para su utilización.

10.1.1.3 Gestión de seguridad del servicio de TI. Protección de información, activos críticos y ciberactivos: La información, los activos críticos y ciberactivos objeto de protección, deben ser valorados mediante las metodologías definidas en el Sistema de Gestión de Seguridad de la Información y ciberseguridad, e implementar los controles necesarios para realizar una operación segura y confiable y contar con información integra y completa, con los niveles de confidencialidad requeridos para la toma de decisiones.

Mantenimiento del inventario de activos críticos y ciberactivos: Las dependencias responsables por la administración, operación y mantenimiento de los activos críticos y ciberactivos, deben mantener actualizado el inventario de éstos, a través de las metodologías definidas en el Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

Respuesta oportuna a incidentes o ataques: Las dependencias responsables por gestionar los incidentes de seguridad y ciberataques, deben monitorear permanentemente, con el fin de detectar y anticiparse a la ocurrencia de los mismos (ciber inteligencia). Frente a la ocurrencia del incidente o ataque, se debe realizar con celeridad la contención, erradicación y las operaciones de respuesta, defensa y recuperación (ciber defensa) a las que haya lugar, involucrando a los actores internos y externos que sean requeridos.

Continuidad del negocio y resiliencia: La Empresa implementa mecanismos de prevención, atención y recuperación en la gestión de Seguridad de la Información y Ciberseguridad, con el fin garantizar la continuidad en la prestación de los servicios en el nivel predefinido como aceptable, después de un incidente de seguridad o ciberataque. Dichos mecanismos propenden por aumentar la capacidad de adaptación y respuesta de la Empresa, de manera oportuna, salvaguardando los intereses propios y de los grupos de interés, mitigando los efectos sobre los objetivos estratégicos de la organización.

Competencia y concienciación: La Empresa debe desarrollar estrategias de sensibilización, capacitación y entrenamiento permanente para los empleados y contratistas, con el objetivo de crear conciencia sobre la necesidad de proteger el conocimiento y los datos de la empresa y para que en sus actuaciones no afecten el desempeño de la seguridad de la información y la ciberseguridad.

10.1.2 Lineamientos para el proceso “desarrollo del servicio”

En el nivel 3 del proceso Desarrollo del Servicio, se encuentran los procesos de Gestion de Cambios y Gestión de la configuración, que se encargan de mantener actualizadas la base de datos de configuración y el registro pormenorizado de los cambios a los servicios prestados por TI.

10.1.2.1 Gestión de Cambios. El proceso gestión de cambios debe velar porque los cambios realizados a los servicios de TI sean registrados, evaluados, autorizados, priorizados, planeados, probados, implementados, documentados y revisados de manera controlada. De esta forma se pretende minimizar el efecto adverso de los cambios en la calidad y continuidad de los servicios de TI.

10.1.2.2 Gestión de la Configuración. El proceso de gestión de la configuración debe identificar y registrar todos los ítems de configuración (IC) que hacen parte de un servicio de TI y sus relaciones. Estos ítems de configuración son almacenados en el repositorio centralizado o Base de datos de Configuración (CMDB), haciendo uso de las plantillas y procedimientos establecidos, para la planeación y evaluación del impacto de los cambios que pueden afectar la disponibilidad de los servicios de TI.

10.1.3 Lineamientos para el proceso “operación del servicio”

A continuación, se enumeran lineamientos para los procesos de gestión de Incidentes, Atención de Solicitudes y Gestión de problemas, que soportan el hacer diario de la mesa de servicios de TI.

10.1.3.1 Gestión de incidentes. La gestión de incidentes debe restablecer los servicios de TI lo más rápido posible, analizando cada falla y aplicando guías de solución, teniendo en cuenta los Acuerdos de Niveles de Servicio (ANS) establecidos con los clientes para minimizar el impacto en las operaciones del negocio.

10.1.3.2 Atención de solicitudes. La atención de solicitudes debe gestionar las solicitudes de servicio de los usuarios, aplicando procedimientos establecidos y teniendo en cuenta los Acuerdos de Niveles de Servicio (ANS) pactados con los clientes.

10.1.3.3 Gestión de problemas. La gestión de problemas deber buscar la causa raíz de los incidentes repetitivos o de alto impacto, a través de la gestión reactiva o proactiva de problemas, para prevenir la aparición de incidentes y reducir el impacto de una falla crítica.

11. LINEAMIENTOS DE SEGURIDAD PARA LA APLICACIÓN WEB SIRIUS ADM

11.1 ALCANCE

Este documento es una propuesta de controles, normas o lineamientos de seguridad, que pretenden mantener la confidencialidad, integridad y disponibilidad de la información para la aplicación web SIRIUS ADM, que abarca los principales componentes de la solución como: Talento Humano, Infraestructura y Software.

11.2 REVISIONES Y MODIFICACIONES

Esta política debe ser dinámica y como mínimo se debe revisar y actualizar anualmente, para evitar que caiga en desuso y obsolescencia. Además, será responsabilidad del gestor de equipo de Tecnología de Información su coordinación y actualización, por ende, cualquier cambio, corrección o recomendación se comunicará a él, para su respectiva autorización o aprobación y posterior publicación y socialización a toda la empresa.

11.3 LINEAMIENTOS PARA EL TALENTO HUMANO

Tanto la empresa, como los funcionarios deben trabajar de la mano en pro de la seguridad informática. Por tanto, se debe:

11.3.1 Por parte de CENS

El área de gestión humana como representante de CENS, se debe responsabilizar de:

- Aplicar procesos de selección que garanticen que las personas asignadas al equipo de Tecnología de Información tengan el conocimiento, aptitudes y competencias necesarias para desempeñarse en los cargos. Siendo especialmente críticos los cargos del administrador de servidores, gestor de comunicaciones y DBA, se deberá realizar un estudio de seguridad mayor al del resto de los funcionarios en concordancia a los recursos que administrarán.

- Así mismo, debe asignar los recursos para actualización de conocimiento, cierre de brechas, formación y adiestramiento que requieran los funcionarios de TI para el ejercicio de sus funciones.

11.3.2 Por los funcionarios

Los funcionarios también deben participar activamente y comprometerse con la seguridad de la aplicación y para ello:

- Los funcionarios de CENS deben actuar de forma responsable y segura en el manejo y operación de la aplicación web Sirius ADM.

- Los usuarios del sistema SIRIUS ADM, deben cambiar su contraseña cada 30 días y aplicar las recomendaciones de complejidad dadas por tecnología de Información (longitud mayor a 6 caracteres, uso de mayúsculas, minúsculas, números y caracteres especiales legibles).

- Los usuarios no deben compartir por ningún motivo sus credenciales de acceso al sistema de información SIRIUS ADM, so pena de hacerse responsable de las acciones malintencionadas o no que hagan con sus privilegios y acceso a la aplicación.

- Ningún usuario del sistema SIRIUS ADM está autorizado para extraer la información de la base de datos mediante el uso de programas y/o software que no esté autorizado por Tecnología de Información.

- Ningún funcionario puede compartir la información del sistema SIRIUS ADM, sin previa autorización escrita de algún directivo de CENS.

11.4 LINEAMIENTOS PARA LA ADMINISTRACIÓN DE LA INFRAESTRUCTURA

La infraestructura de hardware es uno de los pilares más críticos de cualquier sistema de información, por lo cual se debe tener especial cuidado en su correcta gestión y administración. A continuación, se recomiendan lineamientos para la:

11.4.1 Administración de servidores

Para una gestión segura de los servidores que usa la aplicación web SIRIUS ADM, se recomienda:

- Los servidores deben instalarse en ubicaciones con acceso físico restringido, limpios, con aire acondicionado, con fuentes de energía reguladas y adicionalmente, se deben aplicar medidas de control para el ingreso como cámaras de video, biometría, etc.

- Administrar los privilegios y accesos sobre los servidores sobre la premisa de "otorgar el menor privilegio posible", con el fin de que no puedan ser escalados o usados permisos otorgados innecesariamente, para vulnerar los servidores.

- Los softwares como sistemas operativos, antivirus, etc. Instalados en el servidor deben estar licenciados legalmente, y deben ser actualizados periódicamente con el fin de evitar brechas de seguridad, en especial el sistema operativo.

- Se deben desactivar los usuarios, servicios y puertos que no se requieran para la operación de los servicios prestados por los servidores. Así mismo, se deben cambiar las contraseñas por defecto de los usuarios del sistema operativo.

- Se deberán configurar los accesos de red de acuerdo con los servicios habilitados en el servidor; esta configuración debe ir de la mano con los lineamientos de configuración y administración de sistemas firewall-UTM.

- Se debe mantener un documento actualizado con los parámetros de seguridad y configuraciones de los servicios habilitados en el servidor.

- Se deben revisar periódicamente los logs de auditoria habilitados en los servidores, con el fin de prevenir o actuar a tiempo en caso de acciones indeseadas.

- Se recomienda hacer mantenimientos periódicos al hardware de los servidores por lo menos dos veces al año, para evitar que se deterioren más rápidamente por factores como el polvo y la humedad.

- Se debe mantener una política de copias de seguridad o respaldo acordada con los clientes del sistema, que garantice la menor pérdida de información posible en caso de un siniestro. Por ejemplo: copia full mensual e incremental semanal.

- Se debe monitorear constantemente el estado de los servicios y aplicaciones que los servidores habilitan.

11.4.2 Administración de bases de datos

La mayor parte de las fugas de información y fraudes suelen suceder por una débil o inadecuada gestión en la administración de bases de datos, por lo cual:

- Se debe mantener un documento actualizado con los parámetros de instalación, configuración y seguridad de las bases de datos donde están instaladas las aplicaciones.

- Se deben cambiar las contraseñas por defecto de los usuarios de base de datos durante los procesos de instalación de instancias o habilitación de servicios y desactivar los usuarios administradores de la base de datos.

- Se debe tratar al máximo de instalar los procesos “listener” o de escucha de las bases de datos en puertos de escucha diferentes a los puertos por defecto (ej. Oracle 1521, MySQL 3306, Sql Server 1433).

- El o los DBA’s deben tener creados usuarios nombrados que los identifiquen plenamente con los privilegios suficientes y evitar el uso de los usuarios de las bases de datos (SYS, SYSTEM, ROOT, etc.) con el fin de mantener la trazabilidad de las transacciones realizadas a nivel de base de datos.

- Se deben crear usuarios de base de datos solo si es estrictamente necesario y velar porque se otorguen los mínimos privilegios requeridos, con el fin de que no puedan ser usados para vulnerar las aplicaciones y bases de datos.

- Se debe monitorear constantemente la salud de las bases de datos y las aplicaciones habilitadas para detectar comportamientos y eventos anómalos. Así como también para observar o detectar la necesidad de aplicar “parches” de seguridad.

- Se debe mantener una política de copias de seguridad o respaldo acordada con los clientes del sistema, que garantice la menor pérdida de información posible en caso de un siniestro. Por ejemplo: copia full semanal e incremental diaria.

- Se deben revisar periódicamente los logs de auditoria habilitados en las bases de datos, con el fin de prevenir o actuar a tiempo en caso de acciones indeseadas.

11.4.3 Administración de dispositivos de redes y comunicaciones

La red de datos es uno de los componentes de la infraestructura más grande y vulnerable por su muti-localización, al contrario de otros componentes como los servidores o las bases de datos, debido a esto:

- Se debe mantener actualizados los sistemas operativos de los dispositivos activos como switches, routers, firewalls, utm's, etc.

- Se debe realizar y mantener en un sitio seguro o en la nube, copias periódicas de los sistemas operativos y las configuraciones de cada dispositivo activo que conforme la red.

- Se deben cambiar las contraseñas por defecto en los dispositivos administrables y/o utilizar una contraseña maestra que solo sea conocida por el administrador de redes y comunicaciones.

- Los dispositivos de red se deben instalar en sitios seguros, restringidos, bien ventilados, protegidos del polvo y la humedad, para evitar un rápido deterioro y/o una mala operación.

- Se debe programar y realizar mantenimientos periódicos con el fin de retardar su obsolescencia o prevenir fallas en su operación.

- Se debe revisar periódicamente el cableado de datos para evitar interceptaciones, suplantación o fugas de información.

- Se debe segmentar la red para contener fácilmente eventos que puedan degradar o indisponer la red de datos.

- Se deben implementar en lo posible listas de control de acceso (ACL), que permitan o rechacen la conexión de dispositivos a la red.

- Se deben bloquear o deshabilitar los puntos de la red cableada que no estén en uso, especialmente en áreas de acceso público con el fin de prevenir conexiones fraudulentas.

- Se deben emplear en lo posible para la transmisión de datos protocolos criptográficos y seguros como HTTPS, TLS, SSH.

- Se debe configurar para las conexiones con otras redes o subredes expuestas a internet un área desmilitarizada (DMZ) para proteger la red principal de ataques.

11.5 LINEAMIENTOS DE CODIFICACIÓN SEGURA

Durante la etapa de codificación del ciclo de desarrollo de aplicaciones, es necesario tener en cuenta ciertas verificaciones o estilos de programación, con el fin de propiciar errores que resultan en vulnerabilidades de seguridad.

Aunque es cierto que, con la evolución de los lenguajes de programación, realizan chequeos de memoria, verificación de tamaños de arreglos, verificación de tipos y límites de variables; aun el programador es responsable de realizar ciertas verificaciones y de implementar ciertos controles de seguridad.

Para el desarrollo de estos lineamientos, se tuvieron en cuenta las vulnerabilidades más comunes enunciados por organizaciones como OWASP, CERT y SANS, y para cada uno de éstas se propone su solución en los lenguajes de programación Java y .Net (C#) los cuales son los permitidos o aceptados por el grupo empresarial EPM.

11.5.1 Validación de parámetros y saneamiento de data

Las principales vulnerabilidades en la seguridad de aplicaciones web corresponden al ingreso de datos y parámetros, por lo cual es indispensable asegurar las entradas de datos a las aplicaciones:

11.5.1.1 Sanear entradas de usuario. Se deben limpiar las entradas para evitar ser sujeto de ataques como SQL Injection, XML Injection y XPath Inhjection.

Sql Injection: Una vulnerabilidad de SQL Injection ocurre cuando un query de SQL es modificado de manera mal intencionado.

Un código con este problema se ve de la siguiente forma:

```
String sqlString = "SELECT * FROM db_user WHERE username = '" + username +
"' AND password = '" + pwd + "'";

Statement stmt = connection.createStatement();
ResultSet rs = stmt.executeQuery(sqlString);
```

En Java, se debe corregir usando PreparedStatement de la siguiente manera:

```
String sqlString = "select * from db_user where username=? and password=?";
PreparedStatement stmt = connection.prepareStatement(sqlString);
stmt.setString(1, username);
stmt.setString(2, pwd);
ResultSet rs = stmt.executeQuery();
```

En .Net (C#), se debe corregir de la siguiente forma:

```
String cmdStr = "select * from db_user where username=@user and password=@pass";

   using (SqlConnection conn = new SqlConnection(connStr))
      using (SqlCommand cmd = new SqlCommand(cmdStr, conn))
         {
             // add parameters
             cmd.Parameters.AddWithValue("@user", username);
             cmd.Parameters.AddWithValue("@pass", pwd);

             conn.Open();
             cmd.ExecuteQuery();
         };
```

XML Injection: Una vulnerabilidad de XML Injection ocurre cuando es posible modificar una estructura de XML, la cual muchas veces es utilizada para ejecutar comandos, intercambio y almacenamiento de información.

Un código con este problema se ve de la siguiente forma:

```
String xmlString;
xmlString = "<item>\n<description>Widget</description>\n" + "<price>500.0</price>\n" +
"<quantity>" + quantity + "</quantity></item>";
...
```

En Java, se deben verificar los parámetros antes de construir el XML:

```
if (!Pattern.matches("[0-9]+", quantity)) {
}
String xmlString = "<item>\n<description>Widget</description>\n" + "<price>500</price>\n" +
"<quantity>" + quantity + "</quantity></item>";
```

En .Net (C#), se debe corregir de la siguiente forma:

```
Regex number = new Regex("[0-9]+");
if (!numberIsMatch(quantity)) {
}
String xmlString = "<item>\n<description>Widget</description>\n" + "<price>500</price>\n" +
"<quantity>" + quantity + "</quantity></item>";
```

XPath Injection: XPath es un lenguaje utilizado para realizar búsquedas en archivos XML. Al igual que SQL, es vulnerable a una inyección de código XML para manipular las búsquedas. Para evitar este tipo de ataque en ambos lenguajes se recomienda verificar que no contenga caracteres tales como: < > / ‘ = “ ?.

Validación de Parámetros: El uso de parámetros no validados corresponde el foco más amplio de vulnerabilidades existentes en las aplicaciones. Si los parámetros no son validados, la aplicación puede entrar en un estado no previsto y puede incurrir en problemas de seguridad.

En ambos lenguajes de programación se deben validar parámetros tanto en el front-

end, como en el back-end, con el fin de evitar que los atacantes sobrepasen los controles implementados en el front end.

Se recomienda utilizar siempre expresiones regulares para la validación de parámetros, tal como se mostró en la sección anterior.

También se recomienda que los parámetros que son diferentes a string puedan ser validados a través de una conversión de string al tipo de datos que se quiera validar, dicha conversión generará una excepción en el caso que sea un formato inválido:

En Java:

```
try
{
int i = Int32.Parse(<parámetro>);
. . .
}
catch( FormatException)
{
. . .
}
```

En .Net (C#):

```
try
{
int i = Integer.parseInt(<parámetro>);
. . .
}
catch( NumberFormatException )
{
. . .
}
```

11.5.1.2 Normalización de cadenas de caracteres (strings). Los Strings corresponden a la mayoría de entradas realizadas por los usuarios a las aplicaciones, y su manipulación constituye la mayor fuente de vulnerabilidades de las aplicaciones. Sin embargo, cuando se realiza la validación de parámetros, no se tienen en cuenta las diferentes codificaciones usadas y la verificación puede ser evadida.
Es necesario entonces normalizar las cadenas de caracteres para luego realizar las verificaciones necesarias.

En Java:

```
String s = "hola mundo";
// Normalizar
s = Normalizer.normalize(s, Form.NFKC);
// Validar
....
```

En .Net (C#):

```
String s = "hola mundo";
// Normalizar
s = s.Normalize(NormalizationForm.FormKC);
// Validar
....
```

11.5.1.3 Declaración e inicialización de variables. Cuando se utilizan variables estáticas, muchas veces no se tiene en cuenta que la referencia de éstas realiza un llamado del constructor de la clase. Lo anterior puede ser un problema en el caso que se utilice un constructor para la inicialización de variables y generar ciclos o abrazos mortales cuando se realiza la invocación de objetos.

El siguiente código representa un error de este tipo:

```
public class Cycle {
private int balance;
private static Cycle c = new Cycle();
private static int deposit = 1000;

public Cycle() {
        balance = deposit - 10; // Subtract processing fee
}
```

En este ejemplo, la clase Cycle posee un atributo estático c, que llama al constructor de la clase. Sin embargo, esta inicialización se realiza antes de la inicialización del parámetro deposit, por lo que un llamado de c.deposit no daría como resultado el valor 990.

Es por esto que se deben inicializar todas las variables estáticas al final de las demás variables y tener en cuenta las dependencias de inicialización.

11.5.2 Saneamiento de salida a usuarios

Las salidas controladas también deben ser cuidadas meticulosamente a fin de no dar más información que la requerida a un usuario final y generar logs de detalles

técnicos para las áreas de soporte.

11.5.2.1 Tener en cuenta el manejo de excepciones. Los manejos de excepciones en el código se deben manejar con la sentencia try…catch, con lo que se pretende sacar de un estado de error a la ejecución de código en un momento determinado.

Sin embargo, muchas veces cuando se presentan excepciones, los programadores ignoran las causas del error y no permiten recuperarse del estado de error.

```
try {
        //...
}
catch (IOException ioe) {
        //Imprimir Stack Trace
}
```

El código anterior no permite al usuario recuperarse de una acción inválida, además le puede entregar información sensible sobre el funcionamiento y/o arquitectura de la aplicación.

Por esta razón, se recomienda que el manejo de errores se realice con excepciones propias de la aplicación y manejarlo en los componentes de la capa de presentación de la aplicación, tal como se muestra a continuación:

```
try {
        //...
}
catch (IOException ioe) {
        throw new MyApplicationException(ioe);
}

//Manejo de Errores
try {
        //...
}
catch (MyApplicationException e) {
        //Registrar el error.
        //Solicitar una acción de recuperación del error.
}
```

No se recomienda imprimir la traza de error (stacktrace) para ser visualizada por el usuario, sino realizar registro de los errores y desplegar un código de error propio de la aplicación.

11.5.2.2 Restaurar el estado de la aplicación en caso de error. En el código anterior se puede observar un error en el caso que la verificación de parámetros falle en el método getVolumePackage, el objeto Dimensions quedará en un estado inválido cuando se realice un nuevo llamado.

Una solución tanto en Java y C# se recomienda utilizar la cláusula finally:

```
...
} catch (Throwable t) {
        return -1;
} finally {
        //Regresar al estado normal
        length -= PADDING;
        width -= PADDING;
        height -= PADDING;
}
```

11.5.2.3 Verificar apuntadores a null. Siempre se debe verificar las referencias a objetos con el fin de verificar que no sean nulos y provocar comportamientos inesperados en la aplicación.

Sin embargo, no se debe realizar esta verificación mediante el manejo de excepciones (Java: NullPointerException / C#: NullReferenceException), ya que no es posible determinar la variable afectada, tal como se muestra a continuación:

```
boolean isName(string s) {
try {
        String names[] = s.split(" ");
        if (names.length != 2) {
                return false;
        }
        return (isCapitalized(names[0]) && isCapitalized(names[1]));
        }
        //Java
        catch (NullPointerException e) {
                return false;
        }
        //C#
        catch (NullReferenceException e) {
                return false;
        }

}
```

Se recomienda que siempre se realice la verificación del apuntador con la palabra null. En este caso el código debe verse así:

```
boolean isName(string s) {
        if (s==null) {
                return false;
        }

        String names[] = s.split(" ");
        if (names.length != 2) {
                return false;
        }
        return (isCapitalized(names[0]) && isCapitalized(names[1]));
}
```

11.5.2.4 Autenticación. La autenticación es una parte vital en las aplicaciones, ya que limita las acciones de los usuarios y protege la información crítica o privilegiada. Durante el desarrollo de las aplicaciones se tiende a crear modelos de autenticación propios, inyectando problemas de autenticación ya solucionados por modelos existentes en el mercado.

Para una correcta autenticación se debe tener en cuenta las siguientes consideraciones:

- Dividir la aplicación en módulos.
- La Autenticación debe realizarse sobre un canal seguro (cifrado).
- Los tokens o cookies de autenticación deben almacenarse en el lado cliente de forma cifrada.
- Verificar la identidad del usuario durante intervalos de tiempo, y forzar la expiración de sesión durante un periodo de inactividad.

Una solución adecuada para C# (utilizando propiamente ASP) es permitir la autenticación de Windows con el directorio activo, y para Java se recomienda utilizar el API JAAS.

11.5.2.5 Autorización. Al igual que la Autenticación, la Autorización es muy necesaria en el momento de diseñar y desarrollar una aplicación ya que esta permite verificar y controlar las acciones de los usuarios contra la información administrada por la aplicación.

También es necesario tener en cuenta una serie de recomendaciones a la hora de diseñar una aplicación con un esquema de autorización fuerte:

- Dividir la aplicación en módulos de acuerdo con los privilegios de los usuarios.
- Verificar la identidad del usuario cada vez que se vaya a realizar una acción.
- Proteger las reglas de control de acceso ante problemas de integridad y disponibilidad.

Para solucionar los problemas de Autorización se recomienda que para .Net se

utilice autorización de Windows mediante los grupos del Directorio Activo y en Java se recomienda utilizar la librería de JAAS.

11.5.3 Uso de información sensible en el código

Durante el diseño y desarrollo de aplicaciones es usual conectar diferentes componentes las cuales, la mayoría de las veces se requiere credenciales para su acceso. Debido a lo anterior los programadores codifican las credenciales para facilitar el acceso, impidiendo su parametrización.

Dicho comportamiento provoca un serio problema de seguridad, ya que la información sensible codificada en las aplicaciones es fácil de extraer, ya sea mediante análisis de código binario o análisis del segmento de memoria usado por el programa.

Lo anterior no solo ocurre con contraseñas, sino también con cadenas de conexión y llaves de criptografía.

Para solucionar este problema se recomienda que todos estos tipos de información se almacenen en archivos independientes, y estos se protejan a nivel de sistema operativo.

11.5.4 Serialización

La serialización es usada en .Net y Java con el fin transportar los objetos a otros componentes, procesos y/o servidores. La serialización es posible gracias a la herencia de la interfaz ISerializable en ambos lenguajes, y se permite elegir los atributos en cada clase que se pueden serializar.

Durante la serialización se deben tener en cuenta los siguientes aspectos:

11.5.4.1 No serializar atributos con información sensible. Cuando se serializan los objetos, estos se guardan o se transforman en una secuencia de bytes que puede ser utilizado para recuperar el estado del objeto más adelante. Debido a esto, es posible tanto leer información privilegiada cuando viaja por red, o cuando se almacena en archivos o bases de datos.

Es por esto que se recomienda no serializar dichos atributos o cifrarlos tal como se muestra en la sección criptografía.

En Java, para no serializar un atributo se debe utilizar la palabra transient:

```
public class Employee implements Serializable {
    private string name;
    private transient double annualSalary;
. . .
}
```

También se puede recurrir a cifrar el atributo sensible, sin embargo, esta aproximación requiere previamente un intercambio de llaves si se requiere compartir el objeto.

En el caso de .Net, se debe especificar los atributos que no son serializables, o al igual mantener estos atributos cifrados:

```
[Serializable]
public class Employee {
    private string name;
    [NonSerialized] private double annualSalary;
. . .
}
```

11.5.4.2 Realice verificaciones de los atributos al deserializar. Cuando se recuperen los objetos de una serialización, no se puede asumir su estado adecuado. Por esta razón es necesario verificar el tipo de atributos al igual como si fuera un parámetro.

En el caso de Java, en un objeto serializable se debe implementar los métodos writeObject y readObject y realizar las verificaciones con expresiones regulares en el método de lectura:

```
public class Employee implements Serializable {
    private String name;
    private double annualSalary;
. . .

    private void writeObject(java.io.ObjectOutputStream oos)
            throws IOException {
       ObjectOutputStream.PutFields fields = oos.putFields();
       fields.put(“name”, name);
       fields.put(“salary”, cifrar(annualSalary));
       oos.writeFields();
    }

    private void readObject(java.io.ObjectInputStream ois)
           throws IOException, ClassNotFoundException {
       ObjectInputStream.GetField fields = ois.readFields();

       String tempName = fields.get(“name”, null);
       <verificar tempName>
       name = tempName;

       double tempSalary = descifrar(fields.get(“salary”, 0));
       <verificar tempSalary>
       annualSalary = tempSalary;
    }
}
```

En el caso de .Net se debe crear una serialización personalizada implementando el método GetObjectData y un constructor para la deserialización del objeto.

```
[Serializable]
public class Employee : ISerializable {
    private string name;
    private double annualSalary;
. . .
    public Employee(SerializationInfo serInfo, StreamingContext streamContext) {
        string tempname = serInfo.GetString(“name”);
        <verificar tempName>
        name = tempName;

        double tempSalary = descifrar(serInfo.GetString(“salary”));
        <verificar tempSalary>
        annualSalary = tempSalary;
    }

     public void GetObjectData(SerializationInfo serInfo, StreamingContext streamContext)
     {
        serInfo.AddValue("name", name);
        serInfo.AddValue("salary ", cifrar(annualSalary));
     }
}
```

11.5.5 Criptografía

El uso de controles criptográficos es indispensable para el intercambio de información con otros sistemas o en caso de cualquier comunicación entre dos puntos.

11.5.5.1 Uso de algoritmos conocidos. Cuando se requiere manejar información sensible, los programadores piensan en mecanismos para ocultar dicha información. Algunos inexpertos intentan idear algoritmos propios que intentan mantener la confidencialidad de la información.

Esta práctica no es adecuada, ya que dichos algoritmos no han sido sometidos a estudios rigurosos y pueden ser objeto de los atacantes y ser fácilmente vulnerado.

En este caso se recomienda utilizar los algoritmos de criptografía de uso público, ya que estos son sometidos a pruebas constantes y son probados por matemáticos expertos en la materia.

Para realizar cifrado se recomienda los siguientes algoritmos y tamaños de llave:

- Llave simétrica: AES-128, AES-192 o AES-256.
- Llave asimétrica: RSA-2048.

En Java, se recomienda utilizar las siguientes librerías de criptografía, para llaves simétricas:

```
public byte[] encrypt(byte[] key, byte[] textplain) {
       KeyGenerator kgen = KeyGenerator.getInstance("AES");
       kgen.init(key.length); // Generar una llave de 128

       // Generar la llave
       SecretKey skey = kgen.generateKey();
       byte[] raw = skey.getEncoded();

       //Copiar la llave
       for (int i=0; i < raw.length; i++) {
          key[i] = raw[i];
       }

       SecretKeySpec skeySpec = new SecretKeySpec(key, "AES");
       // Iniciar el algoritmo
       Cipher cipher = Cipher.getInstance("AES");
       cipher.init(Cipher.ENCRYPT_MODE, skeySpec);
       return cipher.doFinal(textplain);
}

public byte[] decrypt(byte[] key, byte[] textcipher) {
        SecretKeySpec skeySpec = new SecretKeySpec(key, "AES");
        Cipher cipher = Cipher.getInstance("AES");
        cipher.init(Cipher.DECRYPT_MODE, skeySpec);

        return cipher.doFinal(textcipher);
}
```

En el caso de cifrado de llave asimétrica, se propone lo siguiente:

```
private Key publicKey;
private Key privateKey;

public void generateKeys() {
        KeyPairGenerator kpg = KeyPairGenerator.getInstance("RSA");
        kpg.initialize(2048);
        KeyPair kp = kpg.genKeyPair();
        publicKey = kp.getPublic();
        privateKey = kp.getPrivate();
}

public byte[] encrypt(byte[] textplain) {
        Cipher cipher = Cipher.getInstance("RSA");
        cipher.init(Cipher.ENCRYPT_MODE, publicKey);
        return cipher.doFinal(textplain);
}

public byte[] decrypt(byte[] textcipher) {
        Cipher cipher = Cipher.getInstance("RSA");
        cipher.init(Cipher.DECRYPT_MODE, privateKey);
        return cipher.doFinal(textcipher);
}
```

Para .Net se puede tomar el siguiente ejemplo para el cifrado con llave simétrica:

```
using System;
using System.IO;
using System.Security.Cryptography;
class RijndaelMemoryExample {
private static RijndaelManaged aesAlg = new RijndaelManaged();

public RijndaelManaged() {
        aesAlg.KeySize = 256;
        aesAlg. GenerateKey();
        aesAlg. GenerateIV();
}

public byte[] encrypt(string textplain) {
        ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key, aesAlg.IV);
        MemoryStream msEncrypt = new MemoryStream();
        using (CryptoStream csEncrypt = new CryptoStream(msEncrypt, encryptor,
                    CryptoStreamMode.Write)) {
                using (StreamWriter swEncrypt = new StreamWriter(csEncrypt)) {
                        swEncrypt.Write(textplain);
                }
        }
        return msEncrypt.ToArray();
}

public string decrypt(byte[] textcipher) {
        string plaintext = null;
        ICryptoTransform decryptor = aesAlg.CreateDecryptor(aesAlg.Key, aesAlg.IV);
                using (MemoryStream msDecrypt = new MemoryStream(textcipher)) {
                        using (CryptoStream csDecrypt = new CryptoStream(msDecrypt,
                            decryptor, CryptoStreamMode.Read)) {
                                using (StreamReader srDecrypt = new
                                    StreamReader(csDecrypt)) {
                                        plaintext = srDecrypt.ReadToEnd();
                                }
                        }
                }
        return plaintext;
}
```

En el caso de cifrado con llave asimétrica se puede utilizar lo siguiente:

```
using System;
using System.Security.Cryptography;
using System.Text;

class RSAExample {
private static RSACryptoServiceProvider RSA = new RSACryptoServiceProvider();

public byte[] encrypt(byte[] textplain) {
        byte[] encryptedData = null;
        try {
                RSACryptoServiceProvider nRSA = new RSACryptoServiceProvider();
                nRSA. ImportParameters(RSA. ExportParameters(false));
                encryptedData = RSA.Encrypt(textplain, false);
        } catch (CryptographicException e) {
                ...
                return null;
        }
}

public byte[] decrypt(byte[] textcipher) {
        byte[] decryptedData = null;
        try {
                RSACryptoServiceProvider nRSA = new RSACryptoServiceProvider();
                nRSA. ImportParameters(RSA. ExportParameters(true));
                decryptedData = RSA.Decrypt(textcipher, false);
        } catch (CryptographicException e) {
                ...
                return null;
        }
}
```

11.5.5.2 Uso de algoritmos de hash con 'Salt'. Cuando se utilizan algoritmos de hash dentro de la programación de software, la mayoría de las veces se utiliza para ofuscar información sensible como contraseñas, números de tarjetas de crédito y entre otros creyendo que así que protegen su confidencialidad.

Sin embargo, el uso de "Hashing" no garantiza la seguridad de la información, ya que, conociendo el algoritmo utilizado, el resultado puede ser reversado si es usado un algoritmo vulnerable, encontrar el resultado mediante tablas de valores pre calculados, o encontrar colisiones.

Se recomienda siempre agregar un "Salt", que no es más que un valor aleatorio para agregar un cierto grado de dificulta, y además se realicen varias pasadas del algoritmo de hash.

Adicionalmente, se recomienda utilizar los algoritmos SHA-256 o SHA-512, que son mucho más robustos y están soportados más allá del 2013.

Para el caso de Java se recomienda el siguiente código:

```
import java.security.*;

public byte[] getHash(int iterationNb, String password, byte[] salt) throws
NoSuchAlgorithmException {
       MessageDigest digest = MessageDigest.getInstance("SHA-256");
       digest.reset();
       digest.update(salt);
       byte[] input = digest.digest(password.getBytes("UTF-8"));
       for (int i = 0; i < iterationNb; i++) {
           digest.reset();
           input = digest.digest(input);
       }
       return input;
   }
```

Para .Net el código debería ser el siguiente:

```
using System;
using System.Security.Cryptography;

public byte[] getHash(int iterationNb, string password, byte[] salt) {
       SHA256Managed digest = new SHA256Managed();
       digest.Clear();
       byte[] plainTextBytes = Encoding.UTF8.GetBytes(plainText);

       byte[] plainTextWithSaltBytes =
                new byte[plainTextBytes.Length + salt.Length];

       for (int i=0; i < plainTextBytes.Length; i++)
            plainTextWithSaltBytes[i] = plainTextBytes[i];

       for (int i=0; i < salt.Length; i++)
            plainTextWithSaltBytes[plainTextBytes.Length + i] = salt [i];

       byte[] input = digest.ComputeHash(plainTextWithSaltBytes);
       for (int i = 0; i < iterationNb; i++) {
           digest.Clear();
           input = digest.ComputeHash(input);
       }
       return input;
   }
```

11.5.6 Concurrencia. En sistemas de información que permiten el ingreso de múltiples usuarios y principalmente en sistemas transaccionales, es necesario controlar el estado de la información con el fin de mostrar siempre un estado consistente y evitar tomar decisiones con información que puede ser actualizada por otros usuarios.
Para solucionar este problema, los programadores deben identificar los objetos o recursos que pueden ser objeto a acceso concurrente dentro del sistema de información, y tener en cuenta los siguientes lineamientos de programación:

En Java se recomienda el uso del atributo synchronized, el cual le especifica al lenguaje que el atributo o método debe ser excluyente en su acceso (solo un thread de ejecución a la vez puede leer o escribir el objeto), tal como se muestra en el siguiente código:

```
public class SynchronizedCounter {
    private int c = 0;

    public synchronized void increment() {
        c++;
    }

    public synchronized void decrement() {
        c--;
    }

    public synchronized int value() {
        return c;
    }
}
```

En el caso anterior, la declaración de synchronized garantiza que cada thread de ejecución vea un estado consistente cuando realiza el llamado del método value. El uso de métodos synchronized, hace que sea controlado a nivel de clase, es decir solo se puede llamar un método a la vez.

También es posible realizar un control de concurrencia sobre un objeto o atributo particular usando un bloque synchronized, sin embargo, este no se puede utilizar sobre atributos nativos (int, double, long, etc):

```
public int foo() {
     synchronized(<atributo>) {
        ...
        //Operaciones con atributo
        //Otras operaciones
        ...
     }
}
```

Para el caso de .Net se usa el bloque lock, el cual es similar al synchronized:

```
public int foo() {
     lock (<atributo>) {
        ...
        //Operaciones con atributo
        //Otras operaciones
        ...
     }
}
```

12. CONCLUSIONES

Con el desarrollo del presente proyecto se pudo analizar, evidenciar y detectar vulnerabilidades de seguridad a nivel físico y lógico para la aplicación web SIRIUS, de lo cual se concluye lo siguiente:

- Se identificaron los activos críticos de la aplicación web SIRIUS ADM mediante la adecuada clasificación, asignación del nivel de criticidad y evaluación de cada uno de sus riesgos. Además, se sugieren los controles que se pueden aplicar para prevenir y remediar vulnerabilidades y amenazas detectadas en el análisis de riesgos realizado mediante la aplicación de la metodología de riesgos MAGERIT. Esta práctica arrojo resultados útiles, coherentes y confiables en la identificación de los riesgos asociados a los activos que utiliza la aplicación web Sirius ADM y reveló la importancia de algunos que inicialmente no la tenían para CENS.

- Se determinó con base en los resultados del análisis de los activos mediante la metodología MAGERIT, los riesgos y se realizaron los controles plasmados en el plan de tratamiento de riesgos, que consistió en relacionar las amenazas, las causas y controles para cada uno de los vectores de riesgo permitiendo así reducirlos, modificarlos o eliminarlos. Adicionalmente, se indicaron los controles para las vulnerabilidades detectadas en el pentesting realizado con el software NESSUS a la aplicación web SIRIUS ADM.

- Como resultado del análisis de riesgos mediante MAGERIT y las pruebas de penetración, podemos concluir que la aplicación web SIRIUS ADM funciona en un ambiente medianamente seguro dando un parte de tranquilidad a CENS. Sin embargo, esto no quiere decir que su seguridad es infranqueable, por eso para mantener el mínimo riesgo posible se definieron lineamientos de seguridad que aseguren integridad, confidencialidad y disponibilidad de la información para la aplicación Sirius ADM; Estos lineamientos pueden ser extrapolados a otras aplicaciones web que se implementen en CENS.

13. RECOMENDACIONES

- Al finalizar este proyecto, los autores recomiendan implementar los lineamientos de seguridad propuestos en este trabajo de grado sobre la aplicación web SIRIUS ADM, ya que esto ayudara a reducir los niveles de riesgo sobre dicho sistema de información y preservar el activo más importante para la empresa hoy en día, según lo evidenciado en el análisis de riesgos y las pruebas de penetración.

- Se recomienda realizar periódicamente (al menos una vez al año) un análisis de riesgos que servirá para mantener actualizados los lineamientos de seguridad basados en las amenazas más importantes del momento, debido a que constantemente proliferan nuevos eventos que pueden comprometer la información.

- Es recomendado documentar, caracterizar e implementar el proceso de seguridad informática en CENS, porque ayudará con su puesta en marcha a velar por la integridad, autenticidad, confiabilidad y no repudio de la información. Esto a su vez podría tomarse como uno de los primeros pasos para obtener una certificación en las normas ISO 27000.

- Se recomienda realizar planes de formación, socialización y sensibilización a todas las dependencias de CENS SA ESP, para que interioricen los riesgos a que están sujetas los sistemas informáticos y así acaten los lineamientos impartidos por el área informática con el objetivo de mitigar los impactos negativos que puedan provocar la materialización de alguno de los riesgos.

BIBLIOGRAFÍA

ACUNETIX. RC4 cipher suites detected [en línea]. Disponible en: https://www.acunetix.com/vulnerabilities/web/rc4-cipher-suites-detected/

ARRIOLS, Enrique. Tipos de hackers según su conducta. [en línea]. Disponible en: https://tecnologia.uncomo.com/articulo/tipos-de-hackers-segun-su-conducta-49396.html

CAICEDO CUCHIMBA, Mildred y PERAFÁN RUÍZ, Jhon Jairo. Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca. Popayán. Universidad Nacional Abierta y a Distancia. Especialización en Seguridad Informática. Escuela de Ciencias Básicas, Tecnología e Ingeniería, 2014. [en línea]. [Consulta realizada en junio del 2018]. Disponible en: https://repository.unad.edu.co/bitstream/10596 /2655/3/76327474.pdf

CENS S.A E.S.P. ¿Quiénes somos? [en línea]. Disponible en: http://www.cens.com.co/es-co/institucional/%C2%BFqui%C3%A9nessomos.aspx

CENTRO DE INVESTIGACION CIBERNETICA. Módulo Hacking Ético. [en línea]. Disponible en: https://www.cibe2000.com/hacking-etico

COLOMBIA. SENADO DE LA REPUBLICA. Ley 599 de 2000. [en línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

COLOMBIA. SENADO DE LA REPUBLICA. Ley 1273 de 2009. [en línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. SENADO DE LA REPUBLICA. Ley 1581 de 2012. [en línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Examen de penetración. [en línea]. Disponible en: https://es.wikipedia.org/wiki/Examen_de_penetraci%C3%B3n

GAONA VÁSQUEZ, Karina del Rocío. Aplicación de la Metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información Aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la Ciudad de Machala. Cuenca. Universidad Politécnica Salesiana. Ingeniería de Sistemas. Facultad de Ingenierías. 2013. [En Línea]. [Consulta realizada en junio del 2018]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

GONZÁLEZ POMBO, Alexandra y GÓMEZ BARBOZA, Orlando. Identificar vulnerabilidad y diseñar políticas de seguridad para la aplicación web sistema integral de registro educación permanente (sirep) de la unad ccav cartagena. Cartagena. Universidad Nacional Abierta y a Distancia. Especialización en Seguridad Informática. Escuela de Ciencias Básicas, Tecnología e Ingeniería, 2015. [en línea]. [Consulta realizada en junio del 2018]. Disponible en: http://repository.unad.edu.co/handle/10596/5345

ICONTEC. Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana, 2009

ICONTEC, Norma Técnica Colombiana, 1486, presentación de tesis, trabajo de grado y otros trabajos de investigación.

ICONTEC, Norma Técnica Colombiana, 5613, referencias bibliográficas contenido, forma y estructura.

INFORMÁTICA, SEGURIDAD Y ALGO MÁS. OWASP. [en línea]. Disponible en: https://infow.wordpress.com/2010/12/16/owasp/

IT GOVERNANCE BLOG ES. Qué es un test de penetración y para qué sirve. [en línea]. Disponible en: https://www.itgovernance.eu/blog/es/que-es-un-test-de-penetracion-y-para-que-sirve.

MATEU, CARLES. Desarrollo de Aplicaciones Web. [en línea]. Disponible en: http://libros.metabiblioteca.org/bitstream/001/591/1/004%20Desarrollo%20de%20aplicaciones%20web.pdf

PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información. [En línea]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VCmVZhZRVJQ

PRIETO, Rafael Ausejo. La metodología OSSTMM. [en línea]. Disponible en: http://www.ausejo.net/seguridad/osstmm.htm

RAMIREZ MONTAÑEZ, Jorge Enrique. Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de pamplona - norte de santander. Pamplona. Universidad Nacional Abierta y a Distancia. Especialización en Seguridad Informática. Escuela de Ciencias Básicas, Tecnología e Ingeniería, 2015. [en línea]. [Consulta realizada en junio del 2018]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3415/1/88030934.pdf

SEGURIDAD INFORMÁTICA. Metodología de test de intrusión ISSAF. [En línea]. Disponible en: http://insecuredata.blogspot.com/2009/04/metodologia-de-test-de-intrusion-issaf.html

SHARPMIND SOFTWARE. los diez (10) tipos de vulnerabilidades de bases de datos más comunes. [En línea]. Disponible en: http://sharpmindsoftware.com/ los-diez-10-tipos-de-vulnerabilidades-de-bases-de-datos-mas-comunes.b.aspx

TS TALENT GROUP. Qué son las Aplicaciones Web? Ventajas y Tipos de Desarrollo Web. [En línea]. Disponible en: https://tstalent.net/site/es/noticias/117-que-son-las-aplicaciones-web-ventajas-y-tipos-de-desarrollo-web.html

UNAD. GONZALEZ, Y. C. (2013). fundamentos de seguridad de la información. Bogota: datateca UNAD.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. Ethical Hacking. [en línea]. Disponible en: https://www.cert.org.mx/historico/documento/index.html-id=7

OWASP. Una Guía para Construir Aplicaciones y Servicios Web Seguros. [en línea]. Disponible en: https://www.owasp.org/images/b/.../OWASP_Development_Guide_2.0.1_Spanish.pdf

ANEXOS

Anexo A. Autorización para realizar el proyecto

CENS grupo epm	CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A. E.S.P. SISTEMA DE GESTIÓN

6430 201600015563

Cúcuta, 18 de octubre de 2016

INGENIERA MARTHA LILIANA HERNANDEZ CORONA
PROFESIONAL P3 - ÁREA SERVICIOS CORPORATIVOS
GESTORA EQUIPO DE TRABAJO TECNOLOGÍA DE INFORMACIÓN
Av. 6 #5N-220 Barrio Sevilla
Teléfono: 5824444 Ext. 2200
CÚCUTA

Asunto:Aprobación de Proyecto de Grado

Cordial Saludo,

Por medio de la presente solicitamos nos autorice realizar en CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A. E.S.P el proyecto de grado de la especialización en seguridad informática que estamos cursando en la Universidad Nacional Abierta y a Distancia - UNAD.

El título del proyecto de grado que realizaremos es "PROPUESTA DE SEGURIDAD PARA LA APLICACIÓN WEB SIRIUS ADM DE CENTRALES ELÉCTRICAS DEL NORTE DE SANTANDER S.A E.S.P.".

El proyecto de grado lo realizaremos en horario no laboral y con recursos propios, sin exponer a ningún riesgo la información y la infraestructura de la aplicación web SIRIUS ADM. Al finalizar el proyecto entregaremos un documento con la propuesta de seguridad para la aplicación web SIRIUS ADM.

Atentamente,

PROFESIONAL P2 SERVICIOS CORPORATIVOS
SOLUCIONES INFORMÁTICAS

PROFESIONAL P1 SERVICIOS CORPORATIVOS
SOLUCIONES INFORMÁTICAS

Aprobado,

PROFESIONAL P3 SERVICIOS CORPORATIVOS
TECNOLOGÍA DE INFORMACIÓN

Transcriptor: Edison Javier Arión Mendoza
Revisado por: Martha Liliana Hernández Corona