RESUMEN ANALÍTICO ESPECIALIZADO – RAE

1. Información General	
Tema	Diseño de políticas de seguridad para la aplicación web SIRIUS ADM de CENS S.A. E.S.P.
Título	Propuesta de seguridad para la aplicación web SIRIUS ADM de Centrales Eléctricas Del Norte De Santander S.A E.S.P.
Autores	Edison Javier Arión Mendoza Juan Carlos Ballesteros Durán
Director	Yolima Esther Mercado Palencia
Fuente Bibliográfica	Se referencian 26 fuentes bibliográficas, entre las más importantes tenemos: • 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 • 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
Año	2020.
Resumen	La aplicación web SIRIUS ADM de CENS S.A. E.S.P., es un sistema que apoya uno de los procesos principales de la electrificadora como es la Facturación de Clientes. El sistema se encarga de gestionar la información de los clientes, a través de ordenes de trabajo, que recolectan la información técnica y comercial en campo para ser transferida al sistema comercial mediante una interfaz.

	Este proyecto tiene como objetivo principal desarrollar una propuesta de seguridad para la aplicación web SIRIUS ADM, basados en la identificación de vulnerabilidades, identificación y valoración de riesgos utilizando la metodología MAGERIT y finalizando con la generación de lineamientos o reglas de negocio (políticas). Lo anterior con el objetivo de mitigar los riesgos, desarrollar controles y definir salvaguardas que mantengan la integridad, confiabilidad y disponibilidad de la información que reposa en la aplicación web Sirius ADM.
Palabras Claves	Activo, amenaza, auditoría, backup, cifrado, contraseña, impacto, Magerit, plan, política, riesgo, salvaguarda, seguridad, vulnerabilidad.
Contenidos	Problema Objetivos Justificación Alcance y delimitación Marco referencial Marco metodológico Identificación de vulnerabilidades Controles se seguridad Política de seguridad Lineamientos de seguridad para la aplicación web SIRIUS ADM Conclusiones Recomendaciones

2. Descripción del problema de investigación

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.

3. Objetivos

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.

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. Metodología

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.

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.
- *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.
- *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.
- *Ejecución Plan de Pruebas:* En esta etapa se realizará la ejecución del plan de pruebas elaborado en la etapa anterior.

- *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.
- *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.

5. Referentes teóricos

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. Referentes conceptuales

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.

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 lo anterior, es necesario realizar una prueba 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. 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.

7. Resultados

Como resultado del análisis de riesgos mediante MAGERIT y las pruebas de penetración realizadas con el software Nessus y Acunetix podemos concluir que la aplicación web SIRIUS ADM funciona en un ambiente medianamente seguro dando un parte de tranquilidad a CENS pues se pudieron detectar y evidenciar los verdaderos niveles de severidad de los riesgos que pueden impactar el servicio web Sirius ADM, tanto a nivel físico como lógico y sus posibles salvaguardas. Esto ha contribuido de manera positiva a CENS, ya que el análisis de vulnerabilidades junto a la identificación de riesgos logró identificar oportunidades de mejora en los procesos y subprocesos de “Tecnología de Información”, que materializados en los lineamientos recomendados ayudaran a mantener la confiabilidad, disponibilidad, integridad y trazabilidad de la información de CENS.

Los resultados de este análisis de riesgos pueden ser tomados para extrapolarlos a otros sistemas de información web con que cuente CENS y poder reducir o mitigar los riesgos de los activos informáticos de la empresa y así dar un gran paso en la definición de su sistema de Seguridad de la Información con miras a futuro de una posible certificación en ISO 27000.

8. Conclusiones

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.