



MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE TITULACIÓN

Modalidad Proyecto de Investigación y Desarrollo

Implementación de Medidas de Seguridad en Una Empresa Mediana

Autor: José Michael Vidal Montenegro

Guía: Roque Jacinto Hernández Bustos

Presentando como parte de los requisitos para el título de magister en ciberseguridad.

Guayaquil, 28 de febrero del 2024



PROPUESTA DE CLÁUSULA DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE TITULACIÓN

Yo, VIDAL MONTENEGRO, JOSÉ MICHAEL, autor del trabajo de titulación "Implementación de Medidas de Seguridad en Una Empresa Mediana", certifico que el ensayo reflexivo es una creación de mi autoría, por lo que sus contenidos son originales, de exclusiva responsabilidad de su autor y no infringen derechos de autor de terceras personas. Con lo cual, exoneró a la Universidad Casa Grande de reclamos o acciones legales.

VIDAL MONTENEGRO, JOSÉ MICHAEL
0951175090



VIDAL MONTENEGRO, JOSÉ MICHAEL en calidad de autor y titular del trabajo de titulación "Implementación de Medidas de Seguridad en Una Empresa Mediana" para optar por la **Maestría en Ciberseguridad**, autorizo a la Universidad Casa Grande para que realice la digitalización y publicación de este trabajo de titulación en su Repositorio Digital de acceso abierto, con fines estrictamente académicos, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Asimismo, autorizo a la Universidad Casa Grande a reproducir, distribuir, comunicar y poner a disposición del público mi documento de trabajo de titulación en formato físico o digital y en cualquier medio sin modificar su contenido, sin perjuicio del reconocimiento que deba hacer la Universidad sobre la autoría de dichos trabajos.

VIDAL MONTENEGRO, JOSÉ MICHAEL
0951175090

Introducción:

En el actual panorama digital, la ciberseguridad se ha convertido en un imperativo crítico para las organizaciones que buscan salvaguardar sus activos y datos frente a las crecientes amenazas cibernéticas. Este estudio se centra en la iniciativa estratégica llevada a cabo, compuesta por los proyectos clave que son: Plan de Contingencia, Plan de Contingencia ante lluvia, Url Filtering, Propuesta de actualización de AP por cobertura. Estos esfuerzos responden a la necesidad fundamental de establecer bases sólidas y fortalecer los cimientos para garantizar una infraestructura cibersegura y resistente.

Para este proyecto de titulación se llevaron a cabo cuatro mejoras específicas. Dos de estos proyectos se centraron en aspectos estratégicos, tales como la elaboración de planes de contingencia y épocas de lluvia. Los otros dos proyectos se enfocaron en aspectos técnicos, incluyendo la actualización de un punto de acceso y la implementación del URL Filtering.

Estos cuatro proyectos en desarrollo requirieron especialmente el conocimiento aportado por las siguientes asignaturas: Estrategias y Políticas Multilaterales para la Ciberseguridad, Gerencia, Operación y Planificación de la Ciberseguridad, Hacking Ético y Análisis del Ciberataque, Ciberseguridad Ubicua, Ciberseguridad en Entornos Industriales.

Desarrollo:

Estrategias y Políticas Multilaterales para la Ciberseguridad:

Esta asignatura me permitió estudiar las estrategias y políticas multilaterales me permitió entender las amenazas cibernéticas actuales a nivel global. Esto incluye no solo las tácticas y técnicas utilizadas por los ciberdelincuentes, sino también las vulnerabilidades comunes en sistemas y redes.

Las empresas necesitan un nivel alto de disponibilidad de la información, algunas requieren incluso un nivel incesante de la misma, sin esta disponibilidad resultaría difícil desempeñarse de manera eficaz. En caso de un desastre, la interrupción prolongada de los servicios de Tecnologías de Información puede llevar a pérdidas financieras significativas; perdiendo credibilidad y clientes, que repercuten en la mala imagen de la empresa. (Gómez 2019)

Gerencia, Operación y Planificación de la Ciberseguridad:

Esta materia me proporciono las herramientas necesarias para desarrollar políticas y procedimientos claros y efectivos en materia de ciberseguridad. Estos documentos definirán las responsabilidades de cada persona dentro de la organización, los pasos a seguir en caso de un incidente y las medidas de seguridad que deben implementarse para proteger los activos de la empresa

Hacking Ético:

Los conocimientos adquiridos en Hacking Ético me brindarán una comprensión profunda de las amenazas y vulnerabilidades en la gestión de direcciones IP, lo que me permitirá tomar decisiones efectivas al realizar la reserva de direcciones IP de toda la empresa por medio del DHCP.

Las tecnologías informáticas hoy en día están presentes de forma directa o indirecta en los más diversos aspectos de la sociedad; en el ámbito económico y comercial, las interacciones políticas, e incluso entre los distintos tipos de relaciones interpersonales. Esta presencia de la implementación de la informática, demanda de control y dominio de la información que genera y consume la sociedad contemporánea. (López 2017)

Análisis del Ciberataque, Ciberseguridad Ubicua:

Esta Materia me ayudo obtener información valiosa que me ayudo a tomar la decisión sobre la implementación del filtrado de URL como parte de tu estrategia de seguridad cibernética. Esto me permite proteger mejor los sistemas y datos contra las amenazas web y mejorar la postura de seguridad general de la organización.

Ciberseguridad en Entornos Industriales:

Esta asignatura me permitió evaluar los riesgos y tomar decisiones sobre la realización de reservas en dispositivos no usuales utilizados en el entorno laboral esto me permitió proteger adecuadamente los sistemas.

La utilización de tecnologías de sonorización, control y comunicación, hacen del sistema de fabricación una "fábrica de red inteligente", donde todas las actividades se controlan digitalmente. Esta situación hace que exista una gran dependencia entre el flujo de datos y la comunicación entre procesos, componentes y subsistemas, haciendo que la integridad de los datos y la integridad de los sistemas asuman dimensiones críticas, poniendo de manifiesto la relevancia de la seguridad en las comunicaciones en el entorno industrial. (Galván 2019)

Implementación:

Plan de contingencia y Plan de contingencia en época de lluvia:

Los primeros proyectos los cuales se plantearon fue el plan de Contingencia y Plan de contingencia para época de lluvia ya que no existía un plan de contingencia a seguir por si ocurría un evento negativo o evento inesperado, el plan de contingencia fue el primero en desarrollarse, el cual se enfoco en problemas que ocurrían con normalidad y problemas inesperados el plan de contingencia está dividido en áreas las cuales son los riesgos que podían ocurrir, las áreas prioritarias que pueden ser afectadas relacionadas, el escenario del problema, a quien se debe reportar dicho problema, su mitigación y pasos a seguir para solventar dichos problemas.

El plan de contingencia fue revisando y aprobado por parte de mi jefe del área de sistemas a cargo con el cual se realizaron pequeñas correcciones.

El Plan de contingencia de época de lluvia fue desarrollado enfocado en imprevistos de fenómenos naturales se desarrolló enfocándose en los puntos críticos de la empresa que pueden llegar a ser afectados por un fenómeno natural, el plan de contingencia está dividido en áreas las cuales son los riesgos que podían ocurrir, las áreas prioritarias que pueden ser afectadas relacionadas, el escenario del problema, a quien se debe reportar dicho problema, su mitigación y pasos a seguir para solventar dichos problemas.

El plan de contingencia fue revisado y aprobado por parte de mi jefe del área de sistemas el cual fue revisado también por el jefe de mantenimiento de la empresa ya que él nos brindó conocimiento de los puntos más críticos en las estructuras de la empresa.

Implementación de Url Filtering

El primer paso que se realizo fue la división de IP por áreas de la empresa, continuamos con la reserva de IP por medio del DHCP, al tener segmentadas las IP por áreas se hablo con el Proveedor del firmware el cual nos facilito una platilla con los diversos filtrados de URL que nos proporcionada el sistema

Propuesta de actualización de AP por cobertura:

El proyecto yo lo di a conocer por una insuficiente cobertura y mal selección de Ap instalado, en el área de garita de la empresa el problema se daba ya que el AP instalado es un AP de interior, al momento de tener subidas de temperatura o interferencia de lluvia comenzaba a fluctuar la conexión y daba problemas a los socios los cuales deben utilizar el wifi de la empresa para obtener un código QR, esta fluctuación causaba que el QR se generaba muy tarde y no permitía el acceso a la instalación, se realizaron estudios como el mapa de calor que nos mostro el radio del AP para exterior indicado por mi parte que cumple con el área necesaria y sin problemas de conexión, se realizaron toma de medidas de subida y bajada de la red para verificar si era suficiente para los socios al momento de ingresar a la instalación.

Conclusiones:

Los proyectos realizados, incluyendo el Plan de Contingencia y el Plan de Contingencia en Época de Lluvia, así como la Implementación de URL Filtering y la Propuesta de Actualización de AP por Cobertura, reflejan una mejora continua y la preparación ante situaciones adversas en la empresa. El desarrollo de los planes de contingencia proporcionó un plan estructurado y detallado para abordar tanto los problemas cotidianos como los imprevistos, con la participación del equipo de sistemas.

La implementación de URL Filtering y la propuesta de actualización de AP por cobertura son ejemplos de identificación de problemas específicos de infraestructura para mejorar la experiencia de los usuarios y garantizar un funcionamiento óptimo de los sistemas.

Al enfrentar los proyectos, me encontré con diversas limitaciones que desafiaron el progreso. Una de ellas fue la necesidad de obtener la aprobación de gerencia para llevar a cabo la actualización de equipos, lo que añadió una capa adicional de complejidad y tiempo al proceso. Otro de ellos fue el tiempo que tenía para completar el proyecto de URL Filtering ya que me encontraba en proceso de selección para una nueva empresa, Además, enfrente resistencia o falta de compromiso por parte de algunos miembros del personal para seguir los procedimientos de contingencia establecidos.

Sin embargo, a pesar de estas limitaciones, se demostró que con determinación y enfoque, es posible superar los obstáculos y llevar a cabo nuestros proyectos con éxito. A través de la colaboración y la dedicación.

La ejecución de estos proyectos ha sido una valiosa fuente de aprendizaje y crecimiento profesional para mí. A través de estas experiencias, he adquirido un conocimiento más profundo y una mayor experiencia, lo que ha fortalecido mi conjunto de habilidades.

Estoy seguro de que podré aplicar este aprendizaje en futuros desafíos, preparándome para abordar con éxito cualquier circunstancia que se presente.

Referencias

Marco López (2017) -Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas

Ferruzola Gómez (2019) Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit

Sánchez Galván (2019) -Ciberseguridad en la industria 4.0

Anexo 1: Asignaturas

<https://trusted-cadmium-85c.notion.site/a9b2950757144609971390640fb09392?v=f21389834674447d8987d0e4a48bed38&pvs=4>

Anexo 2: Propuesta

<https://trusted-cadmium-85c.notion.site/Propuesta-de-la-implementaci-n-de-medidas-de-seguridad-en-una-empresa-mediana-1365684ec62b4edb94f807e582522b54?pvs=4>

Anexo 3: Proyecto

<https://trusted-cadmium-85c.notion.site/Implementaci-n-de-medidas-de-seguridad-en-una-empresa-mediana-1a200f56a48c4b90b95e1c4b72de49be?pvs=4>