MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE TITULACIÓN

Modalidad Proyecto de Investigación y Desarrollo

Propuesta De Implementación - Plan De Mejoras En Ciberseguridad A Un Hospital De La Red Integral De Salud

Autor: Jonathan Enrique Gaibor Jiménez

Guía: Roque Jacinto Hernández Bustos

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

Guayaquil, 3 de marzo del 2024

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

Yo, GAIBOR JIMÉNEZ, JONATHAN ENRIQUE, autor del trabajo de titulación “Propuesta De Implementación - Plan De Mejoras En Ciberseguridad A Un Hospital De La Red Integral De Salud”, 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, exonero a la Universidad Casa Grande de reclamos o acciones legales.

Firmado electrónicamente por:
JONATHAN ENRIQUE
GAIBOR JIMENEZ

GAIBOR JIMÉNEZ, JONATHAN ENRIQUE
1719106989

GAIBOR JIMÉNEZ, JONATHAN ENRIQUE en calidad de autor y titular del trabajo de titulación “Propuesta De Implementación - Plan De Mejoras En Ciberseguridad A Un Hospital De La Red Integral De Salud” 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.

Firmado electrónicamente por:
JONATHAN ENRIQUE
GAIBOR JIMENEZ

GAIBOR JIMÉNEZ, JONATHAN ENRIQUE
1719106989

PROPUESTA DE IMPLEMENTACIÓN - PLAN DE MEJORAS EN CIBERSEGURIDAD A UN HOSPITAL DE LA RED INTEGRAL DE SALUD.

INTRODUCCIÓN.

La ciberseguridad es un ámbito esencial que engloba la protección de sistemas informáticos, redes y datos frente a amenazas digitales. Su relevancia radica en la creciente dependencia de la sociedad en la tecnología y la información digital, lo que hace imperativo salvaguardar contra accesos no autorizados, ataques cibernéticos y otros riesgos que pueden comprometer la integridad, confidencialidad y disponibilidad de los recursos informáticos. (Arroyo Guardeño, Gayoso Martínez, & Hernández Encenas, 2020)

En el ámbito sanitario, la Seguridad de la Información es crucial para proteger los datos de los pacientes. Las instituciones médicas deben considerarla como un pilar fundamental en la gestión de la información. La filtración, alteración o robo de datos es un riesgo latente que puede afectar los sistemas de información en estos entornos. La ciberseguridad en hospitales públicos debe seguir políticas claras para defenderse de amenazas cada vez más avanzadas. En Ecuador, se estudia la seguridad de la información en hospitales públicos tipo II, analizando normativas como la Ley HIPAA, el Reglamento 2016/679 y la ISO 27799. A pesar de los esfuerzos, se identifican falencias en el aseguramiento de datos de los pacientes, lo que requiere un proceso de mejora continua. (Quimiz, 2019)

En la trama de la atención médica, la ciberseguridad juega un papel fundamental en la protección de la información de los pacientes, la integridad de los datos clínicos y el funcionamiento ininterrumpido de los Sistemas de Atención Médica. Los hospitales y las instituciones de salud están adoptando rápidamente tecnologías digitales para mejorar la eficiencia y la calidad del cuidado, pero esta digitalización también introduce nuevos riesgos

y desafíos en términos de seguridad de la información. En este sentido, es crucial comprender la importancia de implementar medidas de seguridad cibernética robustas para proteger la confidencialidad, la disponibilidad y la integridad de los datos médicos sensibles, así como para garantizar la continuidad de las operaciones clínicas. En este documento, exploraremos las amenazas específicas que enfrentan los hospitales en el entorno digital actual y analizaremos las mejores prácticas y soluciones para mitigar estos riesgos y fortalecer la ciberseguridad en el sector de la salud.

A lo largo de esta maestría se han aplicado los conocimientos adquiridos y los módulos que mejor se adecuaron a mi realidad laboral fueron: Gerencia, Operación y Planificación de la Ciberseguridad; Tecnología, Modelos y Técnicas de Ciberseguridad; Estrategias y Políticas Multilaterales para la Ciberseguridad; Marco Legal y Análisis Forense; Hacking Ético y Análisis del Ciberataque. Estos módulos no solo se ajustaron de manera destacada a mi contexto laboral, sino que también me permitieron diseñar un plan a futuro para la implementación de lo aprendido, con la capacidad de llevar a cabo acciones a corto plazo**.**

DESARROLLO.

El módulo de Gerencia, Operación y Planificación de la Ciberseguridad, fue primordial en el proceso de aprendizaje de esta maestría, ya que me proporcionó las bases para poder dar inicio a una implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una institución de salud “DHG”. Durante este módulo, se exploraron las herramientas necesarias para establecer políticas de seguridad de la información, abarcando desde el control interno hasta los parámetros que deben regir en la organización. Esta formación es esencial para garantizar la protección de los datos y la continuidad de los servicios médicos.

En este módulo, se adquirió conocimientos fundamentales relacionados con los controles internos y los procesos necesarios para administrar, dirigir y diseñar un plan estratégico de Ciberseguridad en la casa de salud anteriormente mencionada. A grandes rasgos, se abordó el diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) a corto, mediano y largo plazo. Esto incluyó la definición de parámetros esenciales como la planificación, identificación, medición, control/mitigación, monitoreo/revisión y comunicación/consulta, de esta manera, se proyectó la implementación de un sólido plan de ciberseguridad.

En la actualidad, se ha elaborado un plan de acción para implementaciones tecnológicas en la casa de salud, por ende, este plan proyecta mejoras en ciberseguridad a mediano plazo, incluyendo la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para el próximo año 2025. La razón detrás de esta planificación es que durante el periodo 2024 se llevarán a cabo implementaciones de suma importancia en el nosocomio. Estas implementaciones permitirán establecer la planificación, identificación, medición, control/mitigación, monitoreo/revisión y comunicación/consulta siendo estos, factores cruciales para una exitosa implementación del SGSI ya que sin estas implementaciones no se podría realizar a cabalidad la implementación del SGSI lo que alargaría más su proceso. (EGSI, 2020)

El módulo de Tecnología, Modelos y Técnicas de Ciberseguridad, es fundamental en el proceso de aprendizaje sobre ciberseguridad. No se trata solo de proteger la información almacenada en los repositorios digitales, sino también de comprender las redes y sus protocolos de comunicación, para garantizar una comunicación eficiente en las redes alámbricas e inalámbricas. Es crucial reducir la interferencia y garantizar una conexión segura y fiable, la calidad de los conectores y paneles de control, así como las

configuraciones de los switches y routers, son pasos fundamentales para fortalecer la ciberseguridad y proteger la integridad de la infraestructura de red.

En este módulo se profundiza el funcionamiento de los protocolos UTP y UDP, así como en su vulnerabilidad ante ataques como el sniffing, el vandalismo, la inserción de HUBS y el envenenamiento ARP. Estos ataques pueden llegar a surgir si no se toman las precauciones adecuadas al configurar los switches, por lo tanto, es importante cerrar los puertos de estos equipos, de manera apropiada para evitar intrusiones en la red por parte de personas externas que buscan sustraer información confidencial.

En la actualidad, se puede mencionar que se realizó un levantamiento de información relacionado con las direcciones IP y el cableado estructurado en el hospital con la finalidad de mejorar el estado de la red. Durante este proceso, se llegó a la conclusión de que era necesario actualizar todas las direcciones IP asignadas a los equipos electrónicos que se conectan a la red.

Durante el levantamiento de información, se observó direcciones IP duplicadas, lo que generaba conflictos en la conectividad. Además, se notó que el cableado estructurado, implementado en el año 2017, ya no cuenta con puertos disponibles para conexiones alámbricas. Algunos puntos de red presentan mal estado, y ciertos racks no tienen una distribución adecuada de cables lo que perjudica la excelencia de la conectividad.

En respuesta a estas observaciones, se ha documentado las necesidades y términos de referencia para la implementación de una nueva red interna. Esta red proporcionará conectividad alámbrica a los equipos electrónicos que lo requieran. Dicha implementación está programada para el año en curso, como parte del Plan de Acciones a mediano plazo para mejorar la infraestructura de red, al igual que la instalación de un Sistema de Porteros y Videoporteros IP, la cual ayudará con la seguridad interna en las diferentes áreas de trabajo.

El módulo de Estrategias y Políticas Multilaterales para la Ciberseguridad, esencial el aprendizaje en Ciberseguridad, ya que permitió revisar bases sobre las Políticas Nacionales en Ciberseguridad, como ha ido evolucionando en el medio y el alcance que en la actualidad tiene la seguridad de la información. Adicionalmente se revisaron las políticas creadas por el Ministerio de telecomunicaciones en el manejo de la seguridad de la información, profundizando también sobre el Sistema de Gestión de Seguridad de la Información (SGSI), y por qué este debe ser implementado en las diferentes empresas para salvaguardar la seguridad de la información y sobre todo lo más relevante que es Alcanzar una Certificación ISO 27001. Esta certificación ayuda a respetar las leyes y normativas vigentes como la Ley Orgánica de Protección de Datos y su reglamento que busca proteger a los datos e información de los ciudadanos contra el abuso, Código Orgánico Integral Penal (COIP).

El aprendizaje de este módulo permitió la elaboración de un Plan Estratégico de Seguridad Informática (PESI). Este plan, abarca las responsabilidades y políticas necesarias para garantizar la seguridad cibernética en la organización protegiendo la seguridad de la información estableciendo restricciones, ya que en la actualidad no existen. Por otro lado, cabe mencionar que la realización de charlas en ciberseguridad permite hacer hincapié sobre el Fishing y lo que abarca este.

Con la elaboración del Plan de Acción, el cual está proyectado en el año 2025 se realizará la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), complementando con la ayuda del Plan Estratégico de Seguridad Informática (PESI), se podrá realizar análisis de riesgo, estableciendo normas, políticas y procedimientos, seguridad a los activos físicos y lógicos, evaluación de riesgos, controles de seguridad, y sobre todo auditorías y revisiones. Todo esto para la implementación de los respectivos

controles para alcanzar una certificación ISO 27001 para la unidad hospitalaria donde se está implementando dicho proyecto.

El módulo de Marco Legal y Análisis Forense. Permite hacer una revisión de las leyes, reglamentos y tratados relacionados con los ciberdelitos, además, aprueba la exploración de cómo se regulan los delitos informáticos en Europa, comparándolos con la legislación ecuatoriana, aunque en la actualidad existe una reforma en el COIP (Código Orgánico Integral Penal) que aborda parte de los delitos informáticos. Por lo tanto, es fundamental conocer a fondo las leyes y reglamentos pertinentes para evitar cometer infracciones en el ámbito laboral como agentes de ciberseguridad, debido que este es un campo dinámico que se encuentra en constante evolución, de esta manera se podrá proteger a las organizaciones y la sociedad en general.

En la ley Orgánica de Protección de Datos (LOPD), en su artículo 30.- hace mención a los datos relativos a la salud, tanto las instituciones que conforman el sistema de salud y profesionales en dicha área pueden recolectar y tratar datos sensibles de sus pacientes (Asamblea, 2021).

Como indica la LOPD (2021), "Autoridad de Protección de Datos Personales en coordinación con la autoridad sanitaria nacional. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad", acorde a la elaboración del Plan Estratégico de Seguridad de la Información (PESI). Este plan está alineado con la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos y su Reglamento, el Código Orgánico Integral Penal y el Acuerdo No. 006-2021 sobre Políticas de Ciberseguridad, Seguridad de la Información, mismo que es necesario por no contar con un reglamento interno ya que en la actualidad para algún tipo de proceso para el tratado de la información se

usa un Acuerdo Ministerial, el cual es muy generalizado y da muchos espacio para justificar alguna inobservancia si por algún motivo se llegara a perder o mal utilizar la información. (Secetaría Nacional de la Administración Pública, 2013)

Cabe recalcar que, mediante las investigaciones y la puesta en práctica de este proyecto se destacado que el phishing es la técnica más utilizada por los ciberdelincuentes para suplantar identidades y robar datos personales, esta práctica consiste en enviar correos electrónicos fraudulentos que aparentan ser de entidades legítimas para engañar a las víctimas y obtener información confidencial.

En el Plan de Acción que se ha desarrollado, se proyecta la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para el próximo año 2025. El objetivo principal es preservar la confidencialidad, la integridad y disponibilidad de la información. Para ello se aplicará un Proceso de Gestión de Riesgos de Seguridad de la Información y se seleccionará controles adecuados para mitigar los riesgos identificados. Este enfoque también se alinea con la Ley Orgánica de Protección de Datos, que garantiza el ejercicio del derecho a la protección de datos personales y establece principios, derechos, obligaciones y mecanismos de tutela relacionados con la privacidad y la seguridad de la información personal. De esta manera para el año 2026 se pondrá en marcha y se logrará una certificación ISO 27001.

En el módulo de Hacking Ético y Análisis del Ciberataque, permite conocer sobre las técnicas de hacking aplicadas a las redes, direccionando la exploración de la vulnerabilidad inherente de las redes si no se cuenta con un buen firewall. Sin duda, lo más fascinante es la realización de pruebas de penetración utilizando Kali Linux en una red determinada. Estas pruebas permiten identificar posibles intrusos, como sucedió al momento de explorar una red determinada se encontró un intruso en dicha red, optando como medida

de seguridad, el cambio de la contraseña de esta red, Cabe recalcar la importancia de los fundamentos del escaneo de dispositivos conectados a la red e ingreso a esta sin permiso esta catalogada como una infracción por las leyes y reglamentos vigentes en la legislación.

Para el levantamiento de información de las IP en la institución en estudio, se aplicó técnicas de escaneo, encontrado direcciones IP repetidas por lo que se realizó una reasignación de estas para evitar posibles brechas de inseguridad en la red. Cabe destacar que, durante el proceso de escaneo, se identificaron puertos abiertos en la infraestructura. Sin embargo, una ventaja significativa en el sistema hospitalario, no se cuenta con una página web enlazada con dicho sistema, de tal manera se evita la vulneración por este medio. En el plan de acción actual, existe la propuesta de implementar medidas para mejorar la ciberseguridad en esta institución de salud. Estas acciones incluyen fortalecer la configuración de seguridad, monitorear constantemente la red y garantizar que los sistemas estén actualizados y protegidos. La seguridad de la información es fundamental para preservar la confidencialidad, integridad y disponibilidad de los datos médicos y garantizar la continuidad de los servicios asistenciales.

El plan de acción está proyectado para el segundo semestre de 2024, se contempla la adquisición de un Firewall físico. Este componente es esencial para garantizar la seguridad de la red, permitiendo detallar los aspectos clave relacionados con esta decisión:

1. Seguridad de la red: El firewall físico actúa como una barrera de seguridad entre las redes internas protegidas y las redes externas no confiables, como Internet. Su función principal es controlar el tráfico entrante y saliente, permitiendo o bloqueando según las reglas de seguridad establecidas.

2. Prevención de intrusiones: Los firewalls físicos tienen la capacidad de bloquear intentos no autorizados de acceso a la red. Esto ayuda a prevenir ataques maliciosos y protege contra intrusiones no deseadas.

3. Control de aplicaciones: Estos dispositivos pueden reconocer y bloquear aplicaciones riesgosas o no autorizadas. Es fundamental para mantener la seguridad y la productividad en la red.

4. Protección contra amenazas modernas: Los firewalls de próxima generación (NGFW) ofrecen capacidades avanzadas, como la detección de amenazas en la capa de aplicación y la prevención de malware. Están diseñados para enfrentar las amenazas en constante evolución.

En relación con la infraestructura actual, se está trabajando en la creación de una red interna y la adquisición de nuevos switches, especificando una nueva reconfiguración de estos equipos, bloqueando todos los puertos y solo se deberá habilitar lo necesario en la configuración. La documentación detallada, incluyendo la definición de necesidades y los términos de referencia para el Firewall Físico, su elaboración se llevará a cabo a partir del próximo mes (marzo), según el cronograma establecido, es fundamental seguir estos pasos para fortalecer la ciberseguridad y garantizar un entorno protegido para los usuarios y trabajadores de dicha institución de salud.

CONCLUSIÓN.

En la actualidad conocer sobre la Ciberseguridad es algo indispensable para poder proteger nuestra información digital y/o física. Es por ello que en la casa hospitalaria donde laboro se logró poner en práctica los conocimientos adquiridos, con la finalidad de proteger y salvaguardar datos sensibles de miles de personas usuarias de dicha institución. Por cuanto se

ha dado uso a las diferentes herramientas claves que aconseja la ciberseguridad. Es por ello que viendo la necesidad de tener un buen manejo de la información y a la vez prevenir la substracción de esta, se ha realizado el proceso de cambio de computadoras de sistema operativo w95 a w7 las mismas que se puede decir que por la falta de soporte ya se encuentran obsoletas. Dando un cambio radical a la adquisición de nuevos equipos con un sistema operativo actual como w10 y w11 los mismos que si tienen un soporte técnico por parte del fabricante y poseen mejores defensas contra vulneraciones. En la actualidad queda un 33% de computadoras por ser actualizadas, es por ello que se realizó una implementación de antivirus a estas computadoras para prevenir que sean vulneradas y a su vez se realizó la reestructuración de las IP's de todos los equipos electrónicos que utilizan acceso a internet tanto computadoras como equipos médicos IoT.

Para concluir puedo mencionar que, con toda esta reestructuración de equipos y programas, establecidos a corto, mediano y largo plazo se ha podido proporcionar las bases necesarias para iniciar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Institución de Salud. A todo esto, debo mencionar que estos aprendizajes sientan las bases para la implementación de un robusto plan de ciberseguridad, crucial en la protección y resiliencia de la infraestructura informática. Es por eso que considero que mi preparación en la Maestría en Ciberseguridad ha sido una pieza clave para contribuir de manera efectiva a la seguridad de la información, brindando un servicio informático más eficiente y competitivo.

Bibliografía

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encenas, L. (2020). *CIBERSEGURIDAD.*

Asamblea, N. (21 de Mayo de 2021). *telecomunicaciones.gob.ec*. Recuperado el 02 de 2024, de

https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

EGSI. (10 de Enero de 2020). *gobiernoelectronico*. Recuperado el Febrero de 2024, de https://www.gobiernoelectronico.gob.ec/egsi-v2/

Quimiz, M. (13 de Febreo de 2019). *repositorio.uees.edu.ec*. Recuperado el Febrero de 2024, de http://repositorio.uees.edu.ec/browse?type=author&value=Quimiz+Moreira%2C+Mauricio+Alexander.

Secetaría Nacional de la Administración Pública,. (09 de 2013). *gobiernoelectronico.gob.ec*. Recuperado el 02 de 2024, de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/10/Acuerdo-Nro-166-Seguridad-de-la-Informaci%C3%B3n.pdf

ANEXO I

Enlace a Evidencias de Aprendizaje

https://curious-chestnut-1fc.notion.site/EVIDENCIAS-DEL-APRENDEZAJE-0ca8acbdaaef44a3bb1f84dd359da13b

ANEXO II

Enlace a Propuesta de Implementación

https://curious-chestnut-1fc.notion.site/660aeef55fe84bea98bfd2100f56aa3f?v=25f4ddf2a0744ceeb0d4bd9f4400ef44