UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

NOVIEMBRE 2023 - MARZO 2024

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE LA INCIDENCIA DE LAS POLÍTICAS Y PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN LA ARQUITECTURA FÍSICA EXISTENTE EN LA DIRECCIÓN DE TECNOLOGÍAS Y SISTEMAS INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO.

ESTUDIANTE:

HERRERA MORA ANA ZOBEYDA

TUTOR:

ING. OMAR RODRIGO MONTECE MORENO

AÑO 2024

Resumen

Este estudio de caso se basa en un análisis del impacto de las políticas y prácticas de seguridad informática en la arquitectura física existente de la Dirección de Sistemas y Tecnologías de la Información de la Universidad Tecnológica de Babahoyo, ya que la Educación Superior (IES) enfrenta actualmente algunos desafíos relacionados con seguridad de software y hardware. Por lo anterior, se revisaron las políticas actualmente desarrolladas y se hicieron recomendaciones para la implementación y actualización de una nueva política de seguridad basada en la arquitectura física de la Dirección de Tecnologías y Sistemas de Información.

Palabras claves: incidencias, seguridad, políticas, tecnología, hardware.

Abstract

This case study is based on an analysis of the impact of information security policies and practices on the existing physical architecture of the Information Systems and Technologies Directorate of the Technological University of Babahoyo, since Higher Education (HEI) is currently facing some challenges related to software and hardware security. Therefore, the currently developed policies were reviewed and recommendations were made for the implementation and updating of a new security policy based on the physical architecture of the Directorate of Information Systems and Technologies.

Keys words: incidents, security, policies, technology, hardware.

Contenido

Planteamiento del Problema

La Dirección de Tecnologías y Sistemas de Información de la Universidad Técnica de Babahoyo se encarga de las tecnologías utilizadas en la institución, como los sistemas de registro, gestión y administración de la misma, pero también del apoyo a los estudiantes y profesores, además de esto, la Dirección de Tecnologías y Sistemas de Información también se encarga de la gestión y apoyo de las redes de computadoras, de la seguridad informática y de la protección de datos y de la infraestructura tecnológica del lugar.

La Dirección de Tecnologías y Sistemas de Información tiene como función de vital importancia salvaguardar la infraestructura tecnológica, dado a que la dependencia tecnológica es crucial nace la necesidad de un estudio de las incidencias de las políticas y prácticas de seguridad en la arquitectura física de esta dirección.

Actualmente la infraestructura tecnológica de esta dirección cuenta con sistemas de firewall y seguridad informática que abordan la detección de amenazas, identificando y respondiendo a incidentes cuyo propósito es vulnerar los equipos informáticos de la institución.

Un análisis crítico que permita determinar con que políticas se cuenta y que procedimientos de seguridad están establecidos permite comprender en qué manera se realiza la distribución y disposición de los recursos tecnológicos de tipo hardware, así también este tipo de análisis ayudar a determinar brechas de seguridad no identificadas que podrían poner en riesgo la integridad y confidencialidad de la información de la institución.

Por ello la pregunta crucial que motiva el desarrollo de este estudio es:

¿De qué manera las políticas y prácticas de seguridad informática inciden en la arquitectura física de la dirección de tecnologías y sistemas información (DTSI) de la universidad técnica de Babahoyo (UTB)?

Este problema da lugar a la realización de un análisis detallado de las prácticas y políticas que se aplican dentro de la institución para proteger, mejorar y fortalecer la resiliencia ante posibles amenazas hacia los equipos tecnológicos con los que se cuenta, para así robustecer la seguridad informática y salvaguardar el entorno tecnológico de manera óptima y efectiva.

Justificación

En la actualidad, las instituciones de educación superior (IES) tienen que enfrentar algunos desafíos en cuanto a la seguridad del software y hardware, ya que con el significativo avance tecnológico que se ha dado están siendo propensas a daños que afectan la integridad y disponibilidad de toda la entidad. La Dirección de Tecnologías y Sistemas de Información de la Universidad Técnica de Babahoyo es un área que cuenta con un entorno tecnológico muy importante donde las políticas de seguridad informática son las que deben proteger en todo momento la arquitectura física existente.

El presente trabajo se justifica en la necesidad de establecer cómo la aplicación de políticas y prácticas de seguridad informática afectan a la infraestructura física de la Dirección de Tecnología y Sistemas de Información. Por otra parte, es importante aplicar estrategias de ciberseguridad que ayuden a reducir el acceso de personal no autorizado a computadores, redes, servidores y otros equipos que permiten el tratamiento de la información de los diferentes procesos que se realizan en la Universidad, evitando que posibles atacantes afecten de forma grave a estudiantes, docentes y personal administrativo que se ven involucrados en la formación de profesionales.

Además, una infraestructura tecnológica robusta genera beneficios como mayor resistencia ante amenazas y ataques, independencia operativa en relación a una administración de red más eficiente, escalabilidad y flexibilidad mejoradas con respecto a la evolución de la infraestructura tecnológica.

Objetivos del Estudio

Analizar las incidencias de políticas y prácticas de seguridad informática implementadas en la arquitectura física en la Dirección de Tecnologías y Sistemas de Información para mejorar y salvaguardar el entorno tecnológico de manera óptima y efectiva.

Examinar las políticas y prácticas de seguridad informática actuales en la dirección de tecnologías y sistemas de información.

Documentar el impacto de la aplicación de políticas de seguridad informática en la arquitectura tecnológica física de la universidad.

Recomendar mejoras a las políticas y prácticas de seguridad informática relacionadas con la infraestructura tecnológica.

Líneas de Investigación

Sistemas de información y comunicación, emprendimiento e innovación.

Redes y tecnologías inteligentes de software y hardware.

El presente trabajo se relaciona con la línea y Sublínea de investigación a través de análisis de prácticas actuales sobre la seguridad de los equipos informáticos y como estas se implementan sobre los dispositivos hardware de la institución, involucrados en la gestión de redes y sistemas disponibles.

Además, se involucra con la innovación tecnológica a la hora de buscar la forma adecuada de recomendar el fortalecimiento y abordar los desafíos de la seguridad en la arquitectura física de la Dirección de Tecnologías y Sistemas Información, de esta manera se busca poner en práctica lo aprendido en las diferentes cátedras a lo largo de los semestres anteriores.

Por otra parte, el tema en cuestión se encuentra directamente relacionado con la ejecución de tecnologías avanzadas para lograr distinguir vulnerabilidades y así poner en marcha la vigilancia de seguridad para dar seguimiento a la arquitectura física de la Universidad Técnica de Babahoyo logrando así mantener altas expectativas en el desarrollo y crecimiento tecnológico de la institución.

Marco Conceptual

Definición y Conceptos Fundamentales de Seguridad Informática

La seguridad informática es un conjunto de tecnologías, procesos y prácticas diseñadas para proteger redes, dispositivos, programas y datos de ataques cibernéticos, piratería informática, corrupción o acceso no autorizado. Esto es algo que puede representar el área de TI de tu empresa o tener un departamento propio. Independientemente de su funcionamiento y existencia, es muy importante garantizar que toda la información y los procesos críticos de la organización estén protegidos contra ataques como DDoS, robo u otras actividades maliciosas de terceros. (Coppola, 2023)

Según Burin (2022) “la seguridad informática está diseñada para proteger los sistemas informáticos personales y comerciales. Hoy en día, la protección de sistemas se ha convertido en una necesidad específica que ha creado una enorme demanda de personas especializadas en este campo”.

Implementación de Políticas y Procedimientos de Seguridad

Fomentar políticas, procedimientos y pautas de seguridad completos para abordar diversos problemas de seguridad puede ser muy ventajoso. Estas medidas son fundamentales en el entorno actual para garantizar la protección de la información confidencial. Los beneficios incluyen:

- Mitigación de riesgos: Una política de seguridad bien definida ayuda a identificar, evaluar y reducir riesgos potenciales, violaciones de seguridad y acceso no autorizado.
- Eficiencia en la respuesta de incidentes: Los procedimientos establecidos facilitan una respuesta veloz y reducen el tiempo de inactividad. Además, permiten una recuperación de datos más rápida.

- Conciencia del Empleado: Esta política encamina a los trabajadores sobre las mejores prácticas de seguridad y promueve una cultura de vigilancia y responsabilidad.
- Seguridad Adaptativa: Las instituciones de educación pueden adaptarse a las amenazas cambiando sus medidas de seguridad revisando y actualizando las políticas (Linkedin, 2023).

Principios de Seguridad de la Información

Confidencialidad de la Información

También conocido como privacidad, esto significa que solo aquellos que necesitan conocer la información y tienen permiso para hacerlo pueden conocer la información. Este principio garantiza que la información no se filtre accidental o intencionalmente.

Integridad de la Información

Esto significa que la información almacenada en el dispositivo o transmitida a través de cualquier canal de comunicación no ha sido manipulada por un tercero. Esto garantiza que la información no pueda ser modificada por personas no autorizadas.

Disponibilidad de la Información

Esto significa que la información debe estar disponible para quienes están autorizados a acceder a ella y procesarla, y que debe ser recuperable en caso de un incidente de seguridad que resulte en pérdida o daño. Es decir, se puede proporcionar información cuando sea necesario. (UNIR México, 2022)

Importancia de la Seguridad Informática en Entornos Educativos

La seguridad informática es fundamental para proteger la información en la educación digital y garantizar su integridad, confidencialidad y disponibilidad. Sobre este tema se han realizado diversos estudios, enfatizando la aplicación de estándares internacionales como ISO/IEC 27002:2013 en las instituciones educativas.

El énfasis en las buenas prácticas para las amenazas a la seguridad informática, especialmente entre los usuarios, se considera una vulnerabilidad clave. Los recursos de educación digital están diseñados para abordar el ciberacoso y utilizar tecnología para analizar los riesgos en la educación superior.

En la gestión formativa, la seguridad informática es una competitividad de educación digital importante que debe abordarse de manera integral. Se ha enfatizado la importancia del programa de educación digital en América Latina para abordar los desafíos actuales de la educación superior. Estos estudios se centran en auditorías de seguridad informática y soluciones holísticas para mejorar la gestión tecnológica y las comunicaciones en la educación. Proponer un plan de gestión de la seguridad basado en estándares reconocidos como la ISO 27001. (Guaña, 2023)

De acuerdo con (Linkedin, 2023) la educación ha experimentado una transformación radical en cuanto a las tecnologías, pues se ha pasado de las aulas tradicionales a entornos en línea. Esto ha traído consigo muchos beneficios, pero a su vez ha aumentado la preocupación con la ciberseguridad en el ámbito educacional.

La evolución tecnológica ha abierto nuevas puertas en la educación, las plataformas de aprendizaje digital y videoconferencias han hecho posible que los estudiantes logren acceder a todo tipo de información de cualquier parte del mundo para prepararse. Sin embargo, este campo

también ha dado paso a que exista ingeniería social para obtener información confidencial de estudiantes y profesores logrando interrumpir las operaciones normales en la institución educativa. De esta forma, la reputación de las mismas puede verse gravemente dañada si se convierte en víctima de un ataque cibernético.

Tecnologías Emergentes en la Ciberseguridad

La inteligencia artificial se ha convertido en una poderosa herramienta en la lucha contra las ciberamenazas. Mediante el aprendizaje automático se puede detectar y prevenir ciberataques antes de que ocurran. Además, se puede emplear esta herramienta para generar contraseñas y autenticar usuarios. (Linkedin, 2023)

¿Qué es una vulnerabilidad?

Es un error en el código de un software. Una vez implementado, puede poner en riesgo a las organizaciones al comprometer los principios de la información que están almacenados, el acceso no autorizado, la escalada de privilegios o la denegación de servicio. (Zapata, 2023)

Análisis de Vulnerabilidades

Según Pachón (2023) “el análisis de vulnerabilidades escanea e identifica vulnerabilidades de seguridad descubiertas en la red y en los dispositivos conectados a Internet o que reciben direcciones IP, ya sean servidores, firewalls, conmutadores, puntos de acceso, computadoras, equipos, impresoras, etc”.

¿Qué es un Data Center?

Es un espacio diseñado para albergar, procesar y distribuir datos o información de la empresa, optimizando las conexiones y recursos necesarios para su funcionamiento. Estos espacios pueden tener el tamaño de una oficina, cubrir un edificio completo de cientos o incluso

miles de metros cuadrados y contener grandes cantidades de equipos electrónicos, informáticos como servidores, racks, equipos de ventilación, redes de fibra óptica, etc. (Win Empresas, 2023)

La Importancia

Para Tiepolo (2023) el centro de datos proporciona conexiones rápidas y confiables para un acceso eficiente a los servicios en línea. Esto es fundamental para garantizar la satisfacción del usuario y una buena experiencia, así como la eficiencia empresarial. Con la creciente cantidad de datos y la demanda de servicios en línea, los centros de datos se han convertido en la parte fundamental para la infraestructura tecnológica que existe en la actualidad. Además, son considerados como un almacenamiento seguro y confiable que brinda la conectividad necesaria para resguardar la evolución digital de una entidad.

¿Qué es un Tier?

Este término define el tipo o clasificación utilizada en la fabricación de centros de datos, independientemente de la propia infraestructura. Nos hemos familiarizado con todas las normativas y permisos necesarios para ello. El nivel refleja la calidad y confiabilidad del centro de datos ya que tenemos diferentes tipos desde el nivel I hasta el nivel IV. No hay que confundir que el nivel más bajo I es el nivel bajo de confiabilidad, pues hasta el día de hoy estos cuatro niveles están definidos por tiempos de disponibilidad entre 99,761% y 99,999% (el nivel I es 99,671%). (Moya, 2023)

Elementos de la Infraestructura de TI

Hardware

El hardware incluye servidores, centros de datos, PC, enrutadores, conmutadores y otros equipos. El equipo que alberga y enfría el centro de datos y el equipo que lo mantiene en funcionamiento también pueden considerarse parte de la infraestructura.

Software

El software se refiere a las aplicaciones utilizadas por las empresas, como servidores web, sistemas de gestión de contenidos y sistemas operativos (como Linux). Un sistema operativo es responsable de administrar los recursos del sistema y de establecer conexiones con los recursos físicos que realizan tareas.

Redes

Los elementos interconectados proporcionan comunicación, control y operaciones de red entre sistemas internos y externos. Esta red consta de cableado de Internet, soporte de red, firewalls y seguridad, y componentes de hardware como enrutadores, conmutadores y cables.

Tipos de Infraestructuras de Tecnología de la Información

Tradicional

En la infraestructura tradicional, la empresa es propietaria de todos los elementos (como centros de datos, sistemas de almacenamiento de datos, etc.) y los gestiona en sus propias instalaciones. Esta infraestructura generalmente se considera costosa de operar y requiere extensos sistemas de hardware (como servidores), así como energía y espacio físico. (Redhat, 2023)

En la Nube

De acuerdo a lo establecido por Vásquez (2023) “se basa en servicios y el proveedor de estos es responsable administrar y gestionar la infraestructura”.

La seguridad de la Infraestructura

La seguridad de la infraestructura en línea es un concepto central de la seguridad de la red que se centra en proteger los elementos físicos de la infraestructura técnica y garantizar la seguridad de los activos digitales contra amenazas anti físicas. Si bien a menudo se habla de ciberseguridad como la protección virtual de datos y sistemas, la seguridad física es tan importante ya que puede afectar directamente a todo. (Linkedin, 2023)

Crear Políticas Estrictas de Control de Acceso

Un punto importante a considerar al mejorar los protocolos de seguridad de una organización es controlar estrictamente las políticas de autenticación y gestión de identidad. De esta manera, puede asegurarse de que cierta información esté disponible para los empleados autorizados en el momento adecuado. (Santos, 2023)

¿Qué son las Políticas de Seguridad Informática?

De acuerdo a lo encontrado en DocuSign (2023) son un compuesto de prácticas establecidos por una institución para salvaguardar los datos y los sistemas de posibles amenazas. Las mismas definen estrategias de seguridad digital a ejecutar, el rol de los empleados, procedimientos de gestión de incidentes y respuestas a amenazas de la seguridad.

Son esenciales para promover la cultura de seguridad de una organización y crear un sistema que garantice los 3 pilares de la información. Además, ayudan en el desempeño de las exigencias legales relacionadas con la seguridad informática.

Políticas de Buenas Prácticas Informáticas

Promueve el uso seguro, ético y responsable de los recursos informáticos dentro de una entidad. Además, de proteger la información confidencial, garantiza la integridad del sistema y promueva un ambiente de trabajo productivo. Dentro de esta categoría se encuentran las siguientes políticas:

- Seguridad de contraseña.
- Acceso y privilegios.
- Política de uso aceptable.
- Respaldo de datos.
- Seguridad de la red.
- Educación y concienciación.
- Actualización de software.

Políticas de Riesgos Informáticos

Son las directrices y medidas que están diseñadas para distinguir, calcular y administrar los riesgos que están vinculados con la seguridad de la información y el software de una institución. Estos son establecidos para disminuir debilidades y preservar los activos de información de cualquier ofensa.

Algunas políticas de la gestión de riesgos son:

- Evaluación de riesgos.
- Clasificación de la información.
- Gestión de accesos.
- Parches y actualizaciones.
- Administración de contraseñas.

- Control de incidentes.
- Seguridad en la red.

Es importante que las políticas de seguridad informática se comuniquen claramente a todos los socios comerciales y que existan mecanismos para garantizar y monitorear el cumplimiento de estas políticas. (DocuSign, 2023)

El Control de Acceso

Es un elemento esencial de la seguridad de cualquier institución, esto a ayuda a determinar quién tiene acceso a la información y bajo qué circunstancias. En otras palabras, es la tecnología que permite o niega a los empleados el acceso a determinados datos, plataformas o espacios físicos dentro de una entidad. (Santos, 2024)

Gestión de Incidentes de Seguridad

La Escuela Iberoamericana de Postgrado (2024) define que es un proceso integral y estructurado cuyo objetivo es determinar y responder a posibles ofensas hacia la seguridad cibernética, así como aprender de hechos desfavorables y potencialmente peligrosos para proteger al software y hardware.

¿Qué son las Amenazas de la Seguridad Informática?

Según lo estipulado por Hernandez (2022) “cuando hablamos de amenazas a la seguridad, hablamos de explotar vulnerabilidades o errores para afectar el funcionamiento de un sistema con la intención de explotar esas vulnerabilidades o fallos”. Las amenazas informáticas se pueden dividir en dos categorías según su origen:

Amenazas Informáticas Externas

Estas provienen de afuera de la organización y no están controladas por el departamento de Tecnologías de la Información. Esto incluye virus, gusanos, troyanos, etc.

Amenazas Informáticas Internas

Son las que se originan dentro de la organización y que pueden ser controladas hasta cierto punto por la Dirección de Tecnologías. Estas intimidaciones incluyen acceso no autorizado a sistemas informáticos, robo de datos, etc.

Las ciberamenazas pueden afectar significativamente la actividad económica de una organización. Pueden causar pérdida de datos, tiempo de inactividad del sistema crítico, pérdidas financieras y más. Por lo tanto, es importante desarrollar una estrategia de ciberseguridad eficaz para protegerse de estas amenazas. (Hernandez, 2022)

Como Protegerse Contra Ataques

(Ready.gov, 2023) establece que existe una serie de formas con las que se puede evitar riesgos, por lo cual las entidades están obligadas a poner en práctica todas las medidas requeridas para salvaguardar cada bien perteneciente a la misma. Cabe recalcar que cada organización en base a su funcionabilidad dispone de manera diferente de las reglas, mientras más grande es, mayor es su responsabilidad.

Sin embargo, por el hecho de ser entidades pequeñas no deben descuidarse ya que con el tiempo van creciendo y el estar preparadas desde el día cero les dará ventaja frente a las ofensas cibernéticas. Dentro de las medidas que se deben tomar con antelación se encuentran: poner límites de datos personales en la privacidad de contraseñas, mantener actualizados los sistemas operativos, todo estos solo es el inicio de las posibles directrices a tener en cuenta.

Además, se puede poner en marcha:

- Estar atento a las actividades sospechosas.
- Mantener una conexión a internet y red inalámbrica segura.
- Utilizar dispositivos con escaneo biométrico.
- No se puede compartir información comprometedora con el personal de la entidad.
- Usar soluciones contra software malicioso.
- Hacer copias de respaldo de los archivos.
- Verificar bien los remitentes de correos electrónicos, ya que a veces puede tratarse de estafadores que quieren aplicar phishing.

Evaluaciones Periódicas en la Arquitectura Física

A través de evaluaciones periódicas, las instalaciones pueden identificar cualquier brecha en sus medidas de invulnerabilidad y de esta manera abordarlas para dar paso a una mejora. Y así logar mitigar las ofensas de violaciones de seguridad y mantener un ambiente inmune para sus colaboradores y la propiedad.

En general, se recomienda realizar una lista de verificación exhaustiva de la seguridad física del edificio cada año. Si bien un profesional debe realizar una evaluación exhaustiva de los riesgos de seguridad física, es útil realizarla usted mismo como parte de una estrategia de seguridad proactiva. Siga la lista de verificación de seguridad del edificio a continuación para evaluar la preparación de sus instalaciones ante posibles amenazas. (Avigilon, 2021)

Marco Metodológico

De acuerdo a la naturaleza que presentan los objetivos detallados para este estudio de caso se puede considerar que esta investigación presentara un enfoque descriptivo, a fin de poder analizar y comprender la situación actual de la aplicación de políticas y prácticas de seguridad informática en la dirección de tecnologías y sistemas de información de la universidad.

Enfoque Descriptivo

En base al objetivo de examinar políticas y prácticas de seguridad informática actuales se considera necesario ofrecer una descripción detallada de las políticas y prácticas encontradas en nuestra investigación, por lo cual se considerará el enfoque descriptivo. Por otra parte, de acuerdo a como avance nuestra investigación se podrá considerar un enfoque metodológico que permita dar paso a una fase exploratoria que ayude a comprender el panorama general y nos guía a una fase descriptiva orientada a la detección de posibles brechas de seguridad.

Desde este punto para poder realizar la identificación de estas posibles brechas en la infraestructura tecnológica institucional es recomendable la utilización de una metodología de auditoría de seguridad que implique estrategias como la revisión de la infraestructura, la verificación de los procesos logs, la identificación de vulnerabilidades a través de pruebas de penetración, entre otros mecanismos que permitan dar una mejor seguridad a la infraestructura tecnológica.

Se utilizará el método cualitativo para la recopilación de información, mediante la técnica de la entrevista que puede ayudar a entender que tipos de políticas y prácticas de seguridad se aplican por parte de la dirección de tecnologías.

Recopilación de Datos

Para la realización de este estudio de caso se considerarán como fuente principal de datos a los mecanismos de Entrevistas y observación debido a limitación del tiempo que actualmente es bastante reducido, y ya que estas herramientas nos proporcionaran la información necesaria para evidenciar la importancia de la aplicación de políticas y prácticas de seguridad sobre la infraestructura tecnológica de la dirección de tecnologías y sistemas de información

Entrevista

Como técnica se hará uso de la entrevista, la misma que se realizará al personal de la Dirección de Tecnología y Sistemas de Información y contribuirá a comprender desde diversas perspectivas como aplican las políticas y prácticas de seguridad informática.

Observaciones

El proceso de observación ayudara a corroborar la información obtenida del tema en cuestión, así como determinar cómo se aplican las políticas de seguridad en las iteraciones diarios sobre los diferentes equipos tecnológicos.

Análisis de Datos

Para este estudio de caso dada la naturaleza se considera un enfoque cualitativo ya que el problema planteado puede involucrar métodos cualitativos, la aplicación del método lo establece el enfoque que tome la investigación. Como enfoque cualitativo se considera la realización de entrevistas con el personal clave de la Dirección de Tecnología y Sistemas de Información para conocer su percepción, opinión y experiencia respecto a la aplicación de políticas y prácticas de seguridad informática y como esta afecta a la arquitectura física y tecnológica bajo su gestión.

Resultados

Se ha realizado una entrevista a 2 personas que integran la Dirección de Tecnologías y Sistemas de Información.

Tabla 1

Detalles de la entrevista aplicada a la Dirección de Tecnologías y Sistemas de Información

Preguntas	Entrevistado 1: Ing. Alex Jiménez García	Entrevistado 2: Ing. Alexis Cedeño Hernández
1. ¿En la DTSI cuentan con políticas de seguridad Informática?	Si existen	Si existen políticas de seguridad informática.
2. ¿Podría usted, describir las políticas de seguridad informática actualmente implementadas en la DTSI?	Nosotros actualmente tenemos firewall dedicado en el cual tenemos implementadas políticas de seguridad para las conexiones externas e internas con las cuales bloqueamos acciones maliciosas como virus, malware, phishing, ataques DOS, entre otros y tenemos creadas políticas de seguridad para protección de nuestros servidores evitando al máximo las conexiones externas que no tengan que ver con nuestro servicio.	Establecimiento de requisitos mínimos de longitud, complejidad y caducidad de contraseñas, configuración de firewalls y filtros de paquetes para controlar el tráfico de red. Programación de mantenimientos preventivos y actualizaciones de software. Realizar copias de seguridad regulares de datos críticos y almacenarlas de forma segura. Mejorar continuamente los procedimientos de gestión de incidentes basándose en lecciones aprendidas.
3. ¿Cuáles de estas políticas se aplican a la infraestructura tecnológica física de la DTSI?	Ninguna.	Programar mantenimientos preventivos y actualizaciones de software.
4. ¿Cómo se gestiona el acceso físico a los equipos y servidores en la DTSI?	De ninguna manera.	No existe una adecuada gestión del acceso a los dispositivos físicos de la institución.
5. ¿Cuál es la percepción del personal sobre la efectividad de las	No	Funcionan, pero deberían mejorar ya que existen muchas vulnerabilidades.

	políticas de seguridad informática en la protección de la infraestructura física?		
6.	¿Existen procedimientos específicos para la gestión de incidentes de seguridad que afectan la arquitectura física en la DTSI, podría describirme alguno?	La única gestión de incidentes que tenemos es para problemas eléctricos mediante la implementación de un UPS el cual tiene gestión de almacenamiento energético de 8 horas la cual nos permite tener una ventana de energización de equipos cuando tengamos inconvenientes eléctricos.	Considero que no existen procedimientos de gestión de incidentes para la infraestructura tecnológica.
7.	¿Se lleva a cabo alguna evaluación periódica de la seguridad física en la DTSI, cada que tiempo?	No se realiza ninguna evaluación periódica de los equipos de infraestructura.	No se lleva a cabo ningún tipo de evaluación a la infraestructura.
8.	¿Existen estrategias para mitigar los riesgos de perdida de información por inconvenientes con la infraestructura tecnológica física de la DTSI?	Realmente no contamos con ninguna estrategia deberíamos tener servidores de manera redundante en otros sitios, pero lamentablemente no contamos con alta disponibilidad.	Considero que realizar copias de seguridad regulares contribuye a mitigar los riesgos en caso de pérdida de información.

Nota. *Información que fue recolectada.*

Discusión de Resultados

Los entrevistados dieron a conocer diferentes puntos de comprensión de las políticas y prácticas de seguridad informática que se aplican en la dirección de tecnologías y sistemas de información de la Universidad Técnica de Babahoyo, lo cual demuestra la utilización de las políticas desde diversos escenarios basados en las tareas que realizan en su labor diaria.

Analizando el punto de vista de ambos entrevistados se da a conocer la existencia de firewall dedicado y políticas de protección en las conexiones tanto internas como externas y también se da a conocer la aplicación práctica para fortalecer las contraseñas, así como la realización de tareas de mantenimiento y actualización de equipos.

De acuerdo a lo respondido en la entrevista, se da a conocer que actualmente no se mantiene políticas aplicadas a la infraestructura física y que lo único que se realiza es mantenimientos preventivos.

Se considera que existe un gran problema con respecto a la gestión del acceso físico a los servidores y equipos de gestión de la red, lo cual parece un tema que genera mucha preocupación ya que esto puede dar paso a una gran variedad de mecanismos de robo de datos o de manipulación de los equipos para sacar algún tipo de beneficio de ello.

Existe una percepción variada de cuan efectiva son las políticas de seguridad ya que al ser contrastada desde diferente perspectiva no se puede concluir en una respuesta unánime, ya que uno opina que, si funcionan, y el otro no considera tal cosa, lo cual es una clara muestra que existe una falta de consenso o entendimiento de las políticas y prácticas de seguridad utilizadas en las diferentes áreas de la dirección de tecnologías y sistemas de información.

Se destaca como una fuerte debilidad la falta de procedimientos en casos de incidentes sobre la infraestructura tecnológica física ya que esta práctica es un pilar fundamental al momento de reducir los efectos de la penetración a través de una posible brecha de seguridad o introducción no debida en los servidores de la universidad, cabe recalcar que solo existe un Sistema de Alimentación Ininterrumpida (UPS por su siglas en ingles) que contribuye con los inconvenientes de electricidad lo que en cuanto a infraestructura permite mantener disponibilidad de servicios si llegase a suceder algún fallo de energía eléctrica.

Los entrevistados dan a conocer que no se aplican evaluaciones periódicas sobre la seguridad física por lo cual no se puede establecer la existencia de integridad de la infraestructura tecnológica en la Dirección de Tecnologías y Sistemas de Información, las evaluaciones son un punto crítico que permite detectar y solventar la aparición de vulnerabilidades en la seguridad física de los sistemas y recursos tecnológicos de la institución, entonces, lo más idóneo es que si se realicen dichas evaluaciones.

La respuesta que dieron los entrevistados es que no se cuenta con estrategias y que solo realizan copias de seguridad regulares, por lo que esta actividad no es una estrategia del todo efectivas y con la falta de las mismas para reducir la de perdida de información a causa de una situación de riesgo en la infraestructura tecnológica física de la Dirección de Tecnologías y Sistemas de Información de la Universidad Técnica de Babahoyo se crearan inconvenientes que dificultarían la continuidad de los procesos automatizados por esta dirección y lentitud al aplicar procesos de recuperación de datos, esto conlleva a que la adecuada aplicación de políticas y prácticas de seguridad informática se vuelvan muy efectivas ya que ayudara a contar con procesos que agilicen tareas que pueden resultar complejas en situaciones extremas.

No es necesario estar apegados a una normativa estándar para prevenir riesgos, teniendo en consideración que actualmente la información es un activo muy valioso para instituciones tanto públicas como privadas, se vuelve necesario resaltar que es igual de importante salvaguardar y reemplazar de forma oportuna cada uno de los equipos hardware que permiten la generación, almacenamiento, respaldo y gestión de este activo, las políticas de seguridad informática a pesar de enfocarse mayormente en la información, cuentan con indicadores que dan importancia a la infraestructura física, aunque en este tema más que políticas se encuentran prácticas que ayudaran a que el entorno tecnológico sea el óptimo para sacar el máximo provecho de los sistemas y servicios informáticos.

Además, se debe tener en cuenta que una Institución de Educación Superior (IES) manipula grandes volúmenes de datos relevantes para el estudiantado, docentes, etc. y es más que necesario que la arquitectura que aloja dicha información se mantenga integra para evitar pérdidas.

Conclusiones

Las entrevistas revelaron una variedad de puntos de vista sobre las políticas y prácticas de seguridad informática en la Universidad Técnica de Babahoyo (UTB). Por una parte, se destaca la existencia de medidas como firewalls dedicados y políticas de protección en las conexiones, por la otra parte se enfocan en las deficiencias en la gestión del acceso físico a los servidores y equipos de red.

Se identificaron áreas de mejora en la seguridad física de la infraestructura tecnológica de la Dirección de Tecnología y Sistemas de Información en la Universidad Técnica de Babahoyo. La falta de procedimientos claros para casos de incidentes, la ausencia de evaluaciones periódicas de seguridad física, y la carencia de estrategias para reducir la pérdida de información en situaciones de riesgo son algunas de las debilidades identificadas.

La Dirección de Tecnología y Sistemas de Información en la actualidad cuenta con políticas no muy claras y poco específicas para la gestión del acceso físico a los equipos informáticos, así como la elaboración de procedimientos detallados para casos de incidentes de seguridad.

Recomendaciones

Se recomienda llevar a cabo estrategias que permitan un consenso para involucrar al personal de la Ddirección de Tecnologías y Sistemas de Información en la comprensión de las políticas y prácticas de seguridad informática que se llevan a cabo para salvaguardar la infraestructura tecnológica de la misma, así como de las características y beneficios del equipo firewall dedicado con el que se cuenta y como se llevan a cabo los procesos de protección de las conexiones.

Establecer a través de una documentación la aplicación de políticas de seguridad informática más detalladas y los procedimientos claros para los casos de incidentes. Además, ayuden a mejorar la seguridad física de la infraestructura tecnológica de la dirección de tecnologías y sistemas de información para dar continuidad a los procesos automatizados.

Implementar políticas claras y específicas para gestión el acceso físico a los equipos informáticos, así como la elaboración de procedimientos detallados para casos de incidencias de seguridad, se recomienda tener en cuenta la norma ISO/IEC 27002 que tienen en consideración aspectos relevantes en cuanto a la seguridad física de la institución:

Esta norma se toma en consideración el control de acceso que se debe dar a las áreas donde se procesa y almacenan los activos críticos de la institución, la seguridad física de los equipos de tecnología de la información, la protección de las instalaciones y áreas seguras donde se procesan o almacenan los activos de información crítico, normas para la gestión de equipos móviles, mecanismos de seguridad para medios extraíbles entre otras características que permitirán contribuir a la seguridad física de la IES.

Bibliografía

Avigilon. (2021). Obtenido de https://www.avigilon.com/es/blog/office-security-safety-audit

Burin, A. (4 de Mayo de 2022). Obtenido de https://www.teclab.edu.ar/que-es-la-seguridad-informatica/

Coppola, M. (28 de Mayo de 2023). Obtenido de https://blog.hubspot.es/website/que-es-seguridad-informatica

DocuSign. (21 de Agosto de 2023). Obtenido de https://www.docusign.com/es-mx/blog/politicas-de-seguridad-informatica

Escuela Iberoamericana de Postgrado. (2024). Obtenido de https://www.escuelaiberoamericana.com/blog/gestion-de-incidentes-de-seguridad-informatica

Guaña, J. (30 de Mayo de 2023). Obtenido de https://recimundo.com/index.php/es/article/view/1998

Hernandez, Y. (18 de Abril de 2022). *Dongee*. Obtenido de https://www.dongee.com/tutoriales/que-es-una-amenaza-en-seguridad/

Linkedin. (21 de Septiembre de 2023). Obtenido de https://es.linkedin.com/pulse/qu%C3%A9-es-la-seguridad-de-infraestructura-all-in-software

Linkedin. (10 de Julio de 2023). Obtenido de https://es.linkedin.com/pulse/tecnolog%C3%ADas-emergentes-en-la-ciberseguridad-y-aspectos-psicol%C3%B3gicos

Linkedin. (31 de Agosto de 2023). Obtenido de https://es.linkedin.com/pulse/pol%C3%ADticas-y-procedimientos-de-seguridad-implementaci%C3%B3n

Linkedin. (19 de Septiembre de 2023). Obtenido de https://es.linkedin.com/pulse/ciberseguridad-en-los-entornos-educativos-protegiendo-el-futuro

Moya, J. (11 de Febrero de 2023). Obtenido de https://www.elgrupoinformatico.com/pro/que-es-tier/

Pachón, C. (10 de Julio de 2023). *Nsit*. Obtenido de https://www.nsit.com.co/que-es-y-como-funciona-el-analisis-de-vulnerabilidades/

Ready.gov. (2023). Obtenido de https://www.ready.gov/es/ataque-cibernetico

Redhat. (04 de Agosto de 2023). Obtenido de https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure

Santos, J. (30 de Noviembre de 2023). Obtenido de https://www.deltaprotect.com/blog/protocolos-seguridad-informatica

Santos, J. (13 de Febrero de 2024). Obtenido de https://www.deltaprotect.com/blog/controles-de-acceso-que-son-y-por-que-son-importantes-para-proteger-tu-empresa

Tiepolo, E. (16 de Agosto de 2023). *Cirion*. Obtenido de https://blog.ciriontechnologies.com/es/importancia-data-centers-era-digital/

UNIR México. (19 de Octubre de 2022). Obtenido de https://mexico.unir.net/ingenieria/noticias/principios-seguridad-informatica/

Vásquez, F. (26 de Abril de 2023). *Icorp.* Obtenido de https://icorp.com.mx/blog/infraestructura-de-ti-componentes/

Win Empresas. (15 de Agosto de 2023). Obtenido de https://winempresas.pe/blog/que-es-un-data-center-y-cual-es-su-importancia#strong-stylebackground-color-transparent-color-rgb0-0-0que-es-un-data-centerstrong

Zapata, D. (23 de Enero de 2023). *ManageEngine Blog*. Obtenido de https://blogs.manageengine.com/espanol/2023/01/23/analisis-vulnerabilidad.html

Anexos

Anexo 1

Entrevista 1

Fecha: 21/02/2024

Entrevistado: Ing. Alex Jiménez García

Objetivo de la Entrevista: conocer a fondo cómo se lleva a cabo la gestión de acceso a los equipos informáticos.

1. **¿En la Dirección de Tecnologías y Sistemas de Información cuentan con políticas de seguridad Informática?**

   Si existen

2. **¿Podría usted, describir las políticas de seguridad informática actualmente implementadas en la Dirección de Tecnologías y Sistemas de Información?**

   Nosotros actualmente tenemos firewall dedicado en el cual tenemos implementadas políticas de seguridad para las conexiones externas e internas con las cuales bloqueamos acciones maliciosas como virus, malware, phishing, ataques DOS, entre otros y tenemos creadas políticas de seguridad para protección de nuestros servidores evitando al máximo las conexiones externas que no tengan que ver con nuestro servicio.

3. **¿Cuáles de estas políticas se aplican a la infraestructura tecnológica física de la Dirección de Tecnologías y Sistemas de Información?**

   Ninguna.

4. **¿Cómo se gestiona el acceso físico a los equipos y servidores en la Dirección de Tecnologías y Sistemas de Información?**

De ninguna manera

5. **¿Cuál es la percepción del personal sobre la efectividad de las políticas de seguridad informática en la protección de la infraestructura física?**

No

6. **¿Existen procedimientos específicos para la gestión de incidentes de seguridad que afectan la arquitectura física en la Dirección de Tecnologías y Sistemas de Información, podría describirme alguno?**

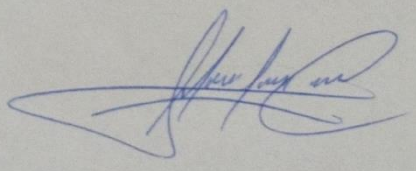
La única gestión de incidentes que tenemos es para problemas eléctricos mediante la implementación de un UPS el cual tiene gestión de almacenamiento energético de 8 horas la cual nos permite tener una ventana de energización de equipos cuando tengamos inconvenientes eléctricos.

7. **¿Se lleva a cabo alguna evaluación periódica de la seguridad física en la Dirección de Tecnologías y Sistemas de Información, cada que tiempo?**

No se realiza ninguna evaluación periódica de los equipos de infraestructura.

8. **¿Existen estrategias para mitigar los riesgos de perdida de información por inconvenientes con la infraestructura tecnológica física de la Dirección de Tecnologías y Sistemas de Información?**

Realmente no contamos con ninguna estrategia deberíamos tener servidores de manera redundante en otros sitios, pero lamentablemente no contamos con alta disponibilidad.



Anexo 2

Entrevista 2

Fecha: 21/02/2024

Entrevistado: Ing. Alexis Cedeño Hernández

Objetivo de la Entrevista: conocer a fondo cómo se lleva a cabo la gestión de acceso a los equipos informáticos.

1. **¿En la Dirección de Tecnologías y Sistemas de Información cuentan con políticas de seguridad Informática?**

   Si existen políticas de seguridad informática.

2. **¿Podría usted, describir las políticas de seguridad informática actualmente implementadas en la Dirección de Tecnologías y Sistemas de Información?**

   Establecimiento de requisitos mínimos de longitud, complejidad y caducidad de contraseñas, configuración de firewalls y filtros de paquetes para controlar el tráfico de red. Programación de mantenimientos preventivos y actualizaciones de software. Realizar copias de seguridad regulares de datos críticos y almacenarlas de forma segura. Mejorar continuamente los procedimientos de gestión de incidentes basándose en lecciones aprendidas.

3. **¿Cuáles de estas políticas se aplican a la infraestructura tecnológica física de la Dirección de Tecnologías y Sistemas de Información?**

   Programar mantenimientos preventivos y actualizaciones de software.

4. **¿Cómo se gestiona el acceso físico a los equipos y servidores en la Dirección de Tecnologías y Sistemas de Información?**

No existe una adecuada gestión del acceso a los dispositivos físicos de la institución.

5. **¿Cuál es la percepción del personal sobre la efectividad de las políticas de seguridad informática en la protección de la infraestructura física?**

Funcionan, pero deberían mejorar ya que existen muchas vulnerabilidades.

6. **¿Existen procedimientos específicos para la gestión de incidentes de seguridad que afectan la arquitectura física en la Dirección de Tecnologías y Sistemas de Información, podría describirme alguno?**

Considero que no existen procedimientos de gestión de incidentes para la infraestructura tecnológica.

7. **¿Se lleva a cabo alguna evaluación periódica de la seguridad física en la Dirección de Tecnologías y Sistemas de Información, cada que tiempo?**

No se lleva a cabo ningún tipo de evaluación a la infraestructura.

8. **¿Existen estrategias para mitigar los riesgos de perdida de información por inconvenientes con la infraestructura tecnológica física de la Dirección de Tecnologías y Sistemas de Información?**

Considero que realizar copias de seguridad regulares contribuye a mitigar los riesgos en caso de pérdida de información.

Anexo 3

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD ADMINISTRACION FINANZAS E INFÓRMATICA
DECANATO

Babahoyo, 16 de febrero de 2024
D-FAFI-UTB-0183-2024

Archivar

Director de tic
Sírvase proceder con el trámite de ley que corresponde
Ing. Marcos Oviedo Ph. D.
RECTOR UTB
19/02/2024

Ingeniero.
Marcos Oviedo Rodríguez, Ph.D.
RECTOR DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO
En su despacho. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

La señorita **ANA ZOBEYDA HERRERA MORA,** con cédula de identidad No. **125003784-1** estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculada en el proceso de titulación en el periodo NOVIEMBRE 2023 – ABRIL 2024, trabajo de titulación modalidad examen de carácter complexivo, previo a la obtención del grado académico profesional universitario de tercer nivel como INGENIERA EN SISTEMAS DE INFORMACIÓN, solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar su Estudio de Caso, en el Departamento de Dirección de Tecnológicas y Sistemas de Información de la Universidad Técnica de Babahoyo, en el cual su tema es: **"ANÁLISIS DE LA INCIDENCIA DE LAS POLITICAS Y PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN LA ARQUITECTURA FISICA EXISTENTE EN LA DIRECCIÓN DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO".**

RECIBIDO

Atentamente,

Lcdo. Eduardo Galeas Guijarro MAE.
DECANO
cc: Archivo

Recibido 19-02-2024 12:35

Anexo 4

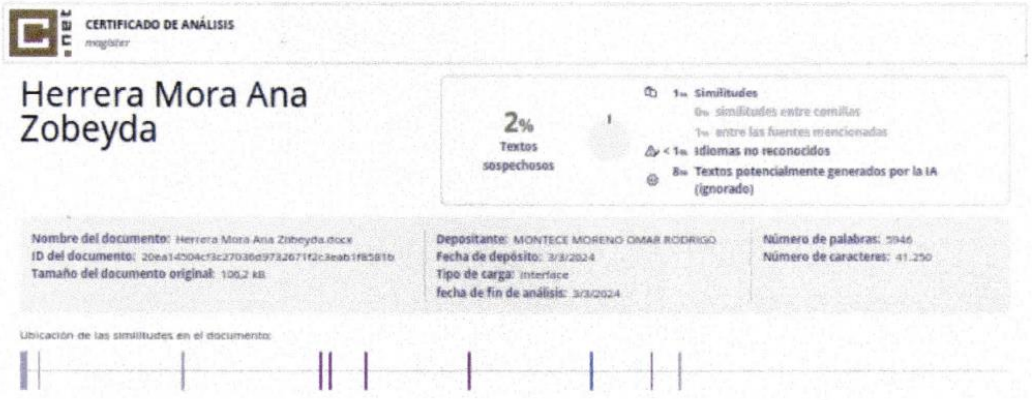
UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

Babahoyo 1 de Marzo del 2024

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación de: la Señorita: **HERRERA MORA ANA ZOBEYDA,** cuyo tema es: **ANÁLISIS DE LA INCIDENCIA DE LAS POLÍTICAS Y PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN LA ARQUITECTURA FÍSICA EXISTENTE EN LA DIRECCIÓN DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO**, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de **[2 %]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

Ing. Omar Montecé Moreno, MDTI
Docente Tutor de Titulacion
de FAFI