REPÚBLICA DE PANAMÁ UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

SISTEMA DE SEGURIDAD TECNOLÓGICA PARA SERVIDOR SAGE 50 Y RECURSOS COLABORATIVOS DE LA EMPRESA ALTA TECNOLOGÍA MÉDICA EN LA CIUDAD DE PANAMÁ

PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD

Tutor : **Prof. José Rivera**

Autor: **Jiménez, Irving**

Ciudad de Panamá, junio de 2021

REPÚBLICA DE PANAMÁ UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

SISTEMA DE SEGURIDAD TECNOLÓGICA PARA SERVIDOR SAGE 50 Y RECURSOS COLABORATIVOS DE LA EMPRESA ALTA TECNOLOGÍA MÉDICA EN LA CIUDAD DE PANAMÁ

PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD

Autor: Jiménez, Irving

Ciudad de Panamá, junio de 2021

Ciudad de Panamá, 1 de junio de 2020

Profesor (a)

Nagib Yassir

Coordinador Comité de Titulación de Estudios de Licenciatura.

Presente.

En mi carácter de Tutor del Trabajo de Grado presentado por el Bachiller Irving Jiménez, documento de identidad Nro. xxxxxxxx, para optar al grado de: LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD, considero que el trabajo: reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado examinador que se designe.

Atentamente,

_____

Prof. José Rivera

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE ACTIVIDADES DE TUTORÍA OPCIÓN DE TITULACIÓN II

Estudiante: Irving Jiménez

Tutor: Prof. José Rivera

Título tentativo del trabajo de grado (TG): SISTEMA DE SEGURIDAD TECNOLÓGICA PARA SERVIDOR SAGE 50 Y RECURSOS COLABORATIVOS DE LA EMPRESA ALTA TECNOLOGÍA MÉDICA EN LA CIUDAD DE PANAMÁ.

SESIÓN	FECHA	HORA REUNIÓN.	ASPECTO TRATADO	OBSERVACIÓN
1	21/01/2021	2:30pm	Revisión del anteproyecto	Determinación de objetivo.
2	04/02/2021	7:30pm	Revisión y validación del instrumento	Dudas de por qué usar un Checklist
3	28/06/2021	7:00pm	Revisión Final	Agregar contenido en Marco Teórico y en análisis de resultados
4	/05/2021		Firma de aprobación	

Título definitivo: SISTEMA DE SEGURIDAD TECNOLÓGICA PARA SERVIDOR SAGE 50 Y RECURSOS COLABORATIVOS DE LA EMPRESA ALTA TECNOLOGÍA MÉDICA EN LA CIUDAD DE PANAMÁ.

Comentarios finales acerca de la investigación: Declaramos que las especificaciones anteriores representan el proceso de dirección del trabajo de grado arriba mencionado.

AGRADECIMIENTOS

En primer lugar, agradezco a Dios por permitirme llegar hasta esta etapa. A mi tutor, profesores, así como a la **Universidad Internacional de Ciencia y Tecnología (UNICyT**), por facilitarme todos los recursos que necesité para lograr llevar este proceso de aprendizaje de la mejor manera.

Por último, pero no menos importante quiero agradecer a mi familia y amistades por apoyarme, en todo este proceso, por cada palabra de ánimo para que lograra este objetivo, el cual plasmo y presento ante su evaluación

Muchas gracias a todos.

ÍNDICE GENERAL

REPÚBLICA DE PANAMÁ UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

SISTEMA DE SEGURIDAD TECNOLÓGICA PARA SERVIDOR SAGE 50 Y RECURSOS COLABORATIVOS DE LA EMPRESA ALTA TECNOLOGÍA MÉDICA EN LA CIUDAD DE PANAMÁ

Autor: **Irvin Jiménez**

Tutor: **Prof. José Rivera**

Año: **2021**

RESUMEN

Mediante lo aprendido estos años en los temas de análisis de seguridad de la información y basándonos en los pilares de Disponibilidad, Integridad y Confidencialidad, el presente trabajo tiene como propósito, detectar las vulnerabilidades a la que la empresa en estudio está expuesta por la falta de controles de seguridad tanto físicos y lógicos. A través de reuniones, observación y de la herramienta de checklist se pudo determinar que la empresa no cumple con los requisitos mínimos necesarios para considerar que la información alojada en su servidor sea considerada segura. También se pudo constatar que la empresa es incapaz de reaccionar de manera exitosa ante un evento. Por todo esto al final de este trabajo se sugiere todos los cambios necesarios para empezar el camino y dar el primer salto importante en la seguridad de sus datos

Descriptores: Servidor de Archivos, Seguridad Física, Seguridad Lógica, Confidencialidad, Integridad, Disponibilidad.

REPUBLIC OF PANAMA
INTERNATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY FACULTY OF COMPUTER SCIENCES AND TECHNOLOGY

TECHNOLOGICAL SECURITY SYSTEM FOR SAGE 50 AND SERVER COLLABORATIVE RESOURCES OF THE HIGH MEDICAL TECHNOLOGY COMPANY IN PANAMA CITY

Author : Irving Jiménez
Tutor : Prof. José Rivera
Year : 2021

Through what has been learned these years in the topics of information security analysis and based on the pillars of Availability, Integrity and Confidentiality, the purpose of this work is to detect the vulnerabilities to which the company under study is exposed due to the lack of both physical and logical security controls. Through meetings, observation and the checklist tool it was determined that the company does not meet the minimum requirements necessary to consider that the information hosted on its server is considered safe. It was also found that the company is unable to react successfully to an event. For all this, at the end of this work all the necessary changes are suggested to start the journey and take the first important leap in the security of your data.

Descriptors: File Server, Physical Security, Logical Security, Confidentiality, Integrity, Availability.

INTRODUCCIÓN

El trabajo que presentamos se centra en una empresa del sector salud, exactamente tecnología médica. Sus primeros pasos dados en el 2005 fueron dentro de una cochera. En década y media han experimentado un crecimiento exponencial, y aunque sus dueños fueron siempre conscientes que la seguridad de la información es importante, no es sino hasta ahora que se plantean el tema con prioridad. Realizando inspección en campo y mediante la aplicación del instrumento para la recolección de los datos, Se pudo conocer las deficiencias que poseía la misma, y aprovechando una reestructuración de la oficina principal, basada en nuestras recomendaciones, surge por parte de la empresa el deseo de invertir y aplicar métodos que los protejan de cualquier riesgo físico y lógico. La empresa no cuenta con un espacio seguro para los equipos de red, ni con el dispositivo adecuado para ejercer funciones de servidor y se hace necesario que esta empresa del sector salud adecue su servidor principal y la infraestructura.

Hoy en día manejamos la información de que todas las empresas del mundo disponen grandes cantidades de sus datos en la Internet, dejándolos vulnerables a un ataque cibernético, actos que demandan tener una infraestructura fortificada que resguarde la seguridad de la información.

Entre los elementos que determinan la infraestructura de red de una empresa y que concentran y gestionan sus datos, están los servidores. Equipos capaces de soportar sistemas de información y que deben ser tratados bajo procesos eficientes, adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información.

Mediante recomendaciones deseamos mostrar a la empresa lo importante que es contar con herramientas, equipos, sistemas que le permitan, mejorar sus estándares de calidad.

CAPÍTULO I

ASPECTOS GENERALES DEL PROYECTO

1.1 Planteamiento y Formulación del Problema.

La tecnología es una tendencia que está en constante desarrollo. Las redes de comunicaciones han dado paso a la interconexión global que, si bien es cierto desencadena grandes beneficios, no es menos cierto que conlleva enormes riesgos.

Hoy en día es bien sabido que todas las empresas del mundo disponen grandes cantidades de sus datos en la Internet, dejándolos vulnerables a un ataque cibernético, actos que demandan tener una infraestructura fortificada que resguarde la seguridad de la información.

Entre los elementos que determinan la infraestructura de red de una empresa y que concentran y gestionan sus datos, están los servidores. Equipos capaces de soportar sistemas de información y que deben ser tratados bajo procesos eficientes, adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información.

Bajo este contexto, exponemos el caso de una pequeña empresa como la de nuestro estudio. Una empresa del sector salud, exactamente tecnología médica sus primeros pasos dados en el 2005, fueron dentro de una cochera, en década y media han experimentado un crecimiento exponencial y aunque sus dueños fueron siempre conscientes que la seguridad de la información es importante. No obstante, es hasta ahora aprovechando una reestructuración de la oficina principal, que nace el deseo de invertir y aplicar métodos que los protejan de cualquier riesgo físico y lógico.

En estos momentos la empresa no cuenta con un espacio seguro para los equipos de red, ni con el dispositivo adecuado para ejercer funciones de servidor. (ver Anexo A)

¿Es necesario que esta empresa del sector salud adecue su servidor principal y la infraestructura?

1.2 Objetivos

1.2.1 Objetivo General.

Analizar los sistemas de seguridad tecnológica para servidor de Sage 50 y recursos colaborativos de la empresa Alta Tecnología Médica en la ciudad de Panamá.

1.2.2 Objetivos Específicos.

- Identificar las oportunidades de mejorar el sistema de seguridad física y lógica del servidor de la empresa.
- Determinar los elementos necesarios para lograr este fin.
- Diseñar un esquema de seguridad que permita tener disponibilidad, integridad y confidencialidad del servidor de la empresa.

1.3 Justificación del Problema.

La confidencialidad, integridad y disponibilidad de la información, son los principios base para definir un servicio de red como un sistema seguro. La caída del servicio de un servidor ocasiona en primer lugar pérdidas económicas, algo de lo que es claramente consciente para la mayor parte de las empresas. Al ver la necesidad de la empresa Alta Tecnología Médica que por largos años ha tenido una computadora con toda la base de datos que manejan y quienes se encuentran en constante crecimiento, vemos la imperante necesidad de crear un espacio que se adecue a la demanda actual.

Alta Tecnología Médica, se encuentra creciendo y con el objetivo de tener una estructura de red robusta y con altos estándares de seguridad, se ha elaborado este proyecto que les permitiría contar con un sistema seguro, que garantice que la información estará siempre disponible, sin interrupción y al alcance de sus necesidades.

Se ofrece la seguridad que este proyecto contribuirá enormemente en un mejor desarrollo y almacenamiento de datos, en aras de estar a la vanguardia de la tecnología y sus mínimos estándares de seguridad.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes.

En el año 2013, Flores, J. y Puppi, G., en su evaluación pudo determinar que los niveles de seguridad del centro de datos de su estudio salieron con un puntaje inferior al deseado. Al mismo tiempo, en cada aspecto evaluado se encontró por lo menos una característica no atendida.

Flores y Puppi concluyeron también que el estándar TIA 942 y las recomendaciones brindadas por el Orange Book son muy ambiciosas para el centro de datos analizado, motivo por el cual, se crearon checklist (físico/lógico) para alcanzar un nivel mínimo recomendable. Si se establece que el estado óptimo es el recomendado por estas fuentes se incurriría en un costo superior al millón de dólares.

Tal cual se demostró en evaluación de seguridad lógica, no existe documentación sobre ninguna de las responsabilidades de los encargados del centro de datos. No existe una clara segregación de funciones entre el personal encargado del centro de datos y área de sistemas de la universidad.

Como quedó demostrado al revisar las mejores prácticas de gestión de la seguridad, es necesario definir los procesos que se encargan de manejar la seguridad a nivel físico y lógico con las directrices de seguridad.

Al revisar toda la documentación que ha sido utilizada para la construcción de este proyecto, se puede concluir que no existe un único estándar que asegure una gestión adecuada de la seguridad. Sin embargo, de cada uno de estos se puede rescatar cada requisito y formar un estándar que conlleve a una gestión global de la seguridad en un centro de datos.

Medina López, J. (2014), concluye que uno de los aspectos más relevantes en seguridad informática son las vulnerabilidades de software, las mismas que al no ser actualizadas se convierten en una clara invitación para vulnerar la

seguridad de una empresa. Un altísimo porcentaje de ataques a la información de las empresas se conocen como ataques directos, son producidos por los empleados de la misma empresa, clientes insatisfechos o competidores. No existen alternativas para proteger los servicios de un ataque de denegación de servicios.

Las redes inalámbricas wifi de las empresas motivo del presente estudio, no contemplan medidas de seguridad adicionales a las definidas por defecto de parte del proveedor de servicio de Internet. La gran mayoría de sistemas informáticos se encuentran vulnerables a un ataque de fuerza bruta para violentar las claves de usuario.

Macias, X. y Dueñas, J. (2015) en su tesis concluyen que la recopilación de los valores de los activos, aunque no eran precisos, permitió completar el análisis y extraer los resultados donde se evidenciaron los riesgos de seguridad que podrían estar afectando el desempeño del área.

El desarrollo de una política de Seguridad en cualquier organización cubre la gran parte de los aspectos que componen un Sistema de Gestión de la Seguridad de la Información. El análisis de riesgos permitió tener una noción real del estado actual de la empresa a nivel de seguridad en el entorno relacionado con el Data Center. El análisis realizado a partir de la norma ISO/IEC 27001:2013 permitió identificar la necesidad de implementar un plan y una política de seguridad, con el fin de mitigar los riesgos o vulnerabilidades a los que pueda estar expuesta la empresa.

Con la implementación de la herramienta de monitoreo, aplicando los controles de seguridad pertinentes y haciendo uso de la zonificación de red establecida se logró evidenciar que es posible mitigar vulnerabilidades de los sistemas, haciendo de estos unos equipos con alto nivel de seguridad.

2.2 Bases Teóricas.

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información. Salamanca y Rozo (2021)

2.2.1 Servidor de Archivos.

Según Onyx Systems (2016) un servidor es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

En nuestra empresa de estudio se quiere implementar un servidor dedicado, que es aquel que dedica todos sus recursos a atender solicitudes de los equipos cliente.

Si hablamos de tipo de servidores en nuestro caso de estudio estamos hablando de un Servidor de Archivos.

Digital Guide (2020) nos dice:

Servidor de archivos: un servidor de archivos se encarga de almacenar los datos a los que acceden los diferentes clientes a través de una red. Las empresas apuestan por dicha gestión de archivos para que sea mayor el número de grupos de trabajo que tengan acceso a los mismos datos. Un servidor de archivos contrarresta los conflictos originados por las diferentes versiones de archivos locales y hace posible tanto la creación automática de las diferentes versiones de datos como la realización de una copia de seguridad central de la totalidad de datos de la empresa.

2.2.2 Seguridad Física.

Si un intruso tiene la posibilidad de acceder físicamente a los equipos e infraestructura de red y servidores podría dañar o robar los dispositivos junto con la información que contienen. La seguridad física de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema. Las principales amenazas que se prevén son:

- Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
- Amenazas ocasionadas por el hombre como robos o sabotajes.
- Disturbios internos y externos deliberados.
- Evaluar y controlar permanentemente la seguridad física del sistema es la base para comenzar a integrar la seguridad como función primordial del mismo.

2.2.3 Seguridad Lógica.

La seguridad lógica de un sistema informático consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y a la información contenida en él.

El activo más importante de un sistema informático es la información y, por tanto, la seguridad lógica se plantea como uno de los objetivos más importantes. Una brecha de seguridad lógica informática afecta a los datos y el software sin afectar físicamente el hardware. El daño muchas veces es invisible hasta que alguien intenta procesar o visualizar los datos.

El perímetro lógico se protege instalando cortafuegos, redes privadas virtuales, routers bien configurados y redes inalámbricas debidamente protegidas. Todo esto apoyado con la creación de perfiles de usuarios que utilicen contraseñas, utilizando algoritmos de encriptación para la trasmisión de información y utilizando sistemas de monitoreo para llevar un control

2.2.4 Seguridad Informática.

La seguridad informática pretende minimizar la vulnerabilidad en los sistemas de información, además se puede decir, que es el conjunto de procedimientos y recursos utilizados con el fin de guardar la integridad, confidencialidad, y

disponibilidad de la información. De ahí que las medidas de seguridad que se implanten deberán ser proporcionales al bien que se intenta proteger.

2.2.5 Confidencialidad de la Información.

Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

2.2.6 Integridad de la Información.

La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

2.2.7 Disponibilidad de la Información.

Se refiere a que la información debe encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos, aplicaciones, el acceso a ésta debe darse por personas autorizadas en el momento requerido.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Tipo de Investigación.

La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. Fidias G. Arias (2012).

El presente trabajo de investigación tiene como principal objetivo reemplazar el servidor actual, que en la actualidad no cuenta con la seguridad física y lógica para un funcionamiento óptimo, el cual permita realizar todos los procesos de control y administración.

Ser ente de solución a las distintas carencias detectadas en la empresa, brindando las soluciones posibles, de manera que se vean las factibilidades de implementarlas o no dentro de la misma., mostrando a quien lo requiera y este autorizado de hay que tener en cuenta que para que la información de la empresa este salvaguardada conlleva un engranaje entre sistema de seguridad física y lógica.

Por ende, podemos definir que, bajo este proceso de investigación, el trabajo que se plantea podrá dar como resultado la optimización del servidor, apoyada de la investigación de campo, toda vez que se tiene libre acceso al lugar, proceso que nos facilita el detectar donde se encuentra el problema; obteniendo así información de primera y darle solución a la problemática que es el objetivo de nuestra investigación.

3.2 Enfoque de la Investigación.

Por sus características de medir fenómenos, prueba de hipótesis y teoría además su proceso de analizar la realidad junto a sus bondades de precisión y predicción se va a utilizar un enfoque de investigación tipo cualitativa.

3.3 Diseño de la Investigación.

Nuestro Diseño de la investigación es de Campo debido a que los datos se obtienen directamente de la realidad que vive la empresa motivo de este estudio; y Transeccional porque se capturan las evidencias en un tiempo concreto, preciso del problema que se está tratando.

3.4 Población y Muestra

Para esta investigación, la población objetivo es definida, finita y se tiene acceso directo a ella, enfocándonos en un usuario de cada área. Usando estos usuarios como muestra intencional, sería suficiente para obtener la información necesaria, que nos complemente la ya obtenida de la infraestructura y las limitaciones que posee en el aspecto físico y adicionado el lógico.

3.5 Técnica e Instrumento de Recolección de Datos.

Para la recolección y análisis de los datos necesarios para la investigación, se utilizará la técnica de la Observación. Mientras que el instrumento para obtener los datos consiste en un cheklist definido por un conjunto de preguntas con 2 únicas opciones, afirmativa o negativa.

Con la intención de capturar el escenario real que experimenta la empresa en sus actividades diarias. Además de evaluar el estado físico que resguarda la infraestructura de red. Se realizará una visita para observar, a través del instrumento, la interacción que tienen los usuarios de distintas áreas con sus sistemas.

La evaluación de estos aspectos, permitirá determinar el nivel de seguridad que respalda la confidencialidad, disponibilidad e integridad de la información del servidor de la empresa.

CAPÍTULO IV

RESULTADOS DE LA INVESTIGACIÓN

4.1 Presentación de los Resultados.

Se ha elaborado un CHECKLIST, Sysadmin (2019) (ver Anexo B), herramienta que está diseñada o creada para las personas que dan mantenimiento y administran sistemas en una organización.

Con dicho instrumento se podrá saber qué mejorar y por dónde iniciar o atacar el problema, fomentar hábitos de seguridad digital que cuiden la información y equipos administrados.

También puede ser útil como documento de guía y revisión periódica de las actividades como administrador de sistemas.

El objetivo específico de esta herramienta, la cual se decidió implementar para la investigación motivo de este trabajo, es recopilar la información que nos indicará las carencias, debilidades en los aspectos físicos - lógicos de la empresa.

Desde un punto de vista más detallado, se busca observar el escenario; el comportamiento de los usuarios y su interacción con los sistemas; el acondicionamiento de los equipos de trabajo y el servidor; los estándares que manejan para el control de acceso, entre otros elementos que determinan la situación actual.

En este checklist se ha concentrado factores de manera tangible que influyen en la seguridad lógica del servidor, su seguridad física y perimetral, además en los usuarios en acciones que podrían impactar la seguridad del servidor.

4.2 Análisis de los Resultados.

Después de ser más que evidente, gracias a la herramienta del checklist, que la empresa no cuenta con una buena organización en cuanto a los factores

físicos – lógicos, se procedió a mostrar a la empresa cuán importante es la protección de la información de la misma, los vacíos que debe llenar en materia de infraestructura y seguridad lógica, informática para mantener la integridad de la empresa, por ende que debe tomar acciones que le permitan mejorar y adecuar de manera integrada todos los aspectos que en su momento pueden ser causantes de confrontar problemas que fácilmente pudiesen haber sido detectados y acatados para el funcionamiento completo de la misma.

En cuanto a las oportunidades de mejora que presenta el sistema de seguridad física y lógica del servidor de la empresa, la condición física del servidor, que está bajo la responsabilidad de la empresa, no cumple con los requisitos mínimo ni el tratamiento apropiado que se requiere para alcanzar un alto nivel de seguridad.

Además, el estudio reflejó un comportamiento bajo un contexto inseguro en todos los aspectos: políticas de seguridad inexistentes, nivel deficiente en el sistema de seguridad perimetral física y lógica del servidor, uso inadecuado de las contraseñas y el acceso a los sistemas para tratar los datos y dispositivos de la empresa.

Con relación a los elementos necesarios para lograr mejorar el sistema de seguridad del servidor, se determinó que la empresa requiere de un espacio exclusivo para el servidor, acondicionado adecuadamente con un plan de mantenimiento preventivo

Se logra que la empresa sea consciente de que es hora de hacer una buena inversión en el servidor que aloja el programa Sage 50 y el cual a su vez utilizan para datos colaborativos, comprenden que el mismo es vulnerable, que fácilmente pueden perder disponibilidad e integridad de su información.

La empresa está dispuesta a invertir en la integridad de su servidor, hacer lo posible para que la información este siempre disponible y estar confiados de que esa información es integra y que a su vez la misma debe contar con un espacio físico en donde se ubique todo el equipo y sistemas que le ayudaran a poseer una empresa que cuente con tecnología de punta en un área adecuada y segura

4.3 Propuesta.

Después de ser más que evidente gracias a la herramienta del checklist y la empresa estar consciente de que es hora de hacer una buena inversión en el servidor que aloja el programa Sage 50 y también usan para datos colaborativos, comprenden que fácilmente pueden perder disponibilidad e integridad de su información.

La empresa está dispuesta a empezar a invertir en la integridad de su servidor, hacer lo posible para que la información este siempre disponible y estar tranquilos de que esa información es integra.

Se propone lo siguiente en varias áreas:

SEGURIDAD FISICA

Ni los equipos de redes y comunicaciones ni el mismo servidor se encuentran en un área adecuada para su seguridad física.

Se pudo conseguir que la empresa aprovechando unas remodelaciones en su oficina otorgara un espacio para que los equipos y servidor fueran ubicados. (Ver Anexo D)

Este espacio contara con controles biométricos de acceso y cámaras de seguridad cuidando tanto el perímetro externo como interno, con esto se busca el objetivo de cumplir con las 3Ds…. Detener, Detectar y Demorar.

Se tendrá control del ambiente fresco para los equipos mediante dos equipos de aire acondicionado, alternándolos mes con mes para asegurarnos de que uno este siempre disponible.

El nuevo servidor será ubicado en un gabinete rack y este a su vez en un piso de doble altura. El gabinete contara con su bandeja de ventiladores para rack. (Ver Anexo E)

SERVIDOR

Se propone un servidor Marca Dell modelo PowerEdge R640. (Ver Anexo F)

Es un servidor de rack de 1U, ideal para esta empresa que quiere empezar con un equipo que cumpla las necesidades actuales pero que también tenga la capacidad de escalabilidad para optimizar el rendimiento.

Tiene la capacidad de proteger la configuración del servidor y el firmware ante modificaciones malintencionadas gracias a su característica de bloqueo de configuración.

Contará con un Procesador Intel Xeon de 2.2Ghz, Memoria de 32GB escalable hasta 768GB.

Control de energía con dos fuentes de alimentación redundantes. Con respecto al almacenamiento contara con 6 discos de 1TB cada uno, con arreglo de disco RAID.

Se propone contar con un sistema de backup automático y externo.

SISTEMA OPERATIVO

Se propone instalar un Sistema operativo Windows Server 2019, es el más reciente producido por Microsoft para servidores.

Con este Sistema operativo se podrá gestionar a los usuarios, esta es la tarea más importante en la administración del servidor ya que permite la conexión de los usuarios a los recursos de este.

El principio de “Menor privilegio” establece que, para garantizar la seguridad, los usuarios deben tener los privilegios y permisos estrictamente necesarios para su trabajo (carpetas compartidas, impresoras, conexiones por Escritorio Remoto, etc.).

Recomendaciones Generales En La Gestión De Usuarios

El principio de “Menor privilegio” establece que, para garantizar la seguridad, los usuarios deben tener los privilegios y permisos estrictamente necesarios

para su trabajo (carpetas compartidas, impresoras, conexiones por Escritorio Remoto, etc.).

La cuenta Administrador debe usarse sólo para tareas administrativas del servidor tales como inicio y parada de servicios, instalación de software, actualizaciones, reinicios, etc. Para todo lo demás se deben usar cuentas convencionales.

Los usuarios conectados al servidor que necesiten realizar alguna labor administrativa puntual deberán usar la función “Ejecutar como” para elevar sus privilegios de forma temporal.

Las políticas de cambio de contraseñas deben ser observadas de forma estricta, especialmente en cuentas administrativas, para mantener la seguridad en todo momento.

Se debe mantener un registro de las cuentas de usuario con un listado de a qué usuario real pertenece cada cuenta, cuál es su rol/función, fecha de alta, y fecha de baja.

Establecer políticas de contraseñas que no es más que un documento que establece una serie de parámetros que deberán ser de obligado cumplimiento para todas las contraseñas de las cuentas de usuario de una empresa. Cuanto más fuertes sean estas políticas mayor seguridad se agregarán a las cuentas de usuario y por tanto al servidor.

Otras seguridades lógicas y perimetral de red

FIREWALL

El firewall está diseñado para tratar de bloquear el acceso no autorizado a la red privada conectada a internet. El firewall se centra en examinar cada uno de los mensajes que entran y salen de la red para obstruir la llegada de aquellos que no cumplen con unos criterios de seguridad, al tiempo que da vía libre a las comunicaciones que sí están reglamentadas.

En nuestro caso de estudio usaremos un firewall físico Aruba 9004 (ver Anexo G) el cual es perfecto para implementaciones grandes o pequeñas es decir que a medida que nuestro cliente de estudio crezca el seguirá con la capacidad de

protegerla. Este firewall se configura y gestiona a través de Aruba Central, una plataforma de garantía y seguridad de operaciones de red basadas en la nube que es muy fácil de usar. Una aplicación móvil opcional también para que lo IT tengan control y monitoreo

SWITCH DE ACCESO.

También en la marca Aruba con la serie de Switch cx6100 (ver Anexo H) diseñada para la pequeña empresa. Este switch de capa 2 viene lista para una implementación sencilla y con los modelos con características PoE ideal para los AP conectados y también para el sistema de CCTV, que en nuestro caso los tendremos separados de la red de usuarios.

PUNTOS DE ACCESO

En cuanto a los puntos de acceso inalámbrico se recomienda el uso de los Aruba 500 (ver Anexo I), muy seguros con tecnología Wi-Fi 6 para entornos de interior como es el caso de la oficina del cliente de estudio.

Con la tecnología Wi-Fi 6 se puede manejar múltiples clientes en cada canal sin importar el dispositivo o el tipo de tráfico usando IA para eliminar los problemas de los clientes

Un equipo muy flexible y escalable aplica automáticamente políticas de seguridad y podemos habilitar la red de invitados lo cual es una de nuestras recomendaciones en este caso.

Toda esta infraestructura estará determinada bajo una topología de red sencilla (ver Anexo J), la cual describe el alcance esperado para la empresa.

CONCLUSIONES

Después de haber analizado toda la información recaba sobre la empresa motivo del presente trabajo podemos concluir lo siguiente.

En muchas ocasiones, las empresas cualesquiera fuese el campo que abarque o a que se dedique debe siempre tener presente la seguridad Físico – Lógico de la misma.

En el caso de la empresa de sector salud que hemos investigado, debido a sus deficiencias era punto vulnerable, de alto riesgo, en que su información podría ser víctima de amenazas, a las cuales no podría brindar, ni garantizar en su momento las medidas necesarias para salvaguardar la integridad de dicha información.

Que contar con un sistema que le permita bloquear el acceso no autorizado a la red privada conectada a internet, que es sumamente importante saber que a medida la misma crezca, su prioridad debe ser seguir con la capacidad de protegerla, teniendo de la mano una plataforma que le garantice seguridad y buen equilibrio en sus operaciones.

Que las tomas de decisiones bien justificadas y en donde las mismas fueron basadas en pruebas tangibles que te obligan a realizar correctivos, no solo por obligación, sino porque siempre el objetivo primordial debe ser el buen funcionamiento de la empresa en todos los aspectos.

RECOMENDACIONES

Al realizar esta investigación, hemos observado la necesidad imperante que tiene la empresa de invertir en el tema de seguridad de la información, el cual es un trabajo que requiere ajustes constantes; y su éxito se basa en el seguimiento, revisión y monitoreo continuo de todos los controles que se implementen.

El compromiso de la gerencia y la concienciación de los colaboradores es vital, ya que ellos son el engranaje que maneja y modifica la información de manera continua por lo cual todos deben hablar el mismo idioma y hacer uso adecuado de está y la tecnología.

Se debe considerad la implementación de una estrategia que se base en pequeños proyectos de acuerdo necesidades prioritarias de la empresa, para que al final con la suma de ellos se pueda llegar los más cerca posible a considerar esta empresa 100% segura a lo que información se refiere.

Todo esto no puede estar sobre los hombros del gerente general, ni del jefe de personal. Ya que el departamento de cómputo o de sistema no existe, se bebe considerar la creación del puesto y que entre sus responsabilidades este la tarea de asegurarse de que la información de la empresa siempre esté disponible se mantenga confidencial e integra

LISTA DE FUENTES DE INFORMACIÓN

- **Documentos Digitales:**

Flores, E. Jack, S. Puppi, B. y Gino A. (2013). ***Gestión de la seguridad física y lógica para un centro de datos***. Recuperado de: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/301540/flores_ej-pub- delfos.pdf?sequence=2&isAllowed=y [consulta enero de 2021]

Medina, J. (2014). ***Guía de seguridad informática para las pymes de la ciudad de Pelileo (Bachelor's thesis)***. Recuperado de: http://dspace.uniandes.edu.ec/bitstream/123456789/4448/1/TUASIS005-2013.pdf [consulta enero de 2021]

Macias, X. y Dueñas, J. (2015) ***Implementación de un modelo de seguridad informática en un sistema de monitoreo para los canales de comunicaciones y data center en la empresa Atento SA.*** Recuperado de: https://repository.udistrital.edu.co/bitstream/handle/11349/4258/MaciasMendezX iomaraMayerli2015.pdf;jsessionid=3653429B8E6D9BB8C65076EC12EDFDCA?sequence=9 [consulta enero de 2021]

Salamanca Rojas, D. M., & Rozo Bolívar, J. A. (2021). ***Esquema de seguridad de la información, basado en la Norma ISO27001: 2013, en entornos virtualizados sobre la herramienta HYPER-V la eps en liquidación.*** https://repository.ucatolica.edu.co/handle/10983/2574325743 [consulta junio de 2021]

Publicaciones Digitales:

ONYX System. (2016) ***Artículo: ¿Que es un servidor?*** Recuperado de: https://www.onyxsystems.es/que-es-un-servidor.html#:~:text=Un%20servidor%20es%20un%20equipo,solicitudes%20de %20los%20equipos%20cliente.&text=Servidor%20de%20archivos%3A%20es%20aquel,a%20equipos%20de%20una%20red [consulta febrero de 2021] Digital Guide

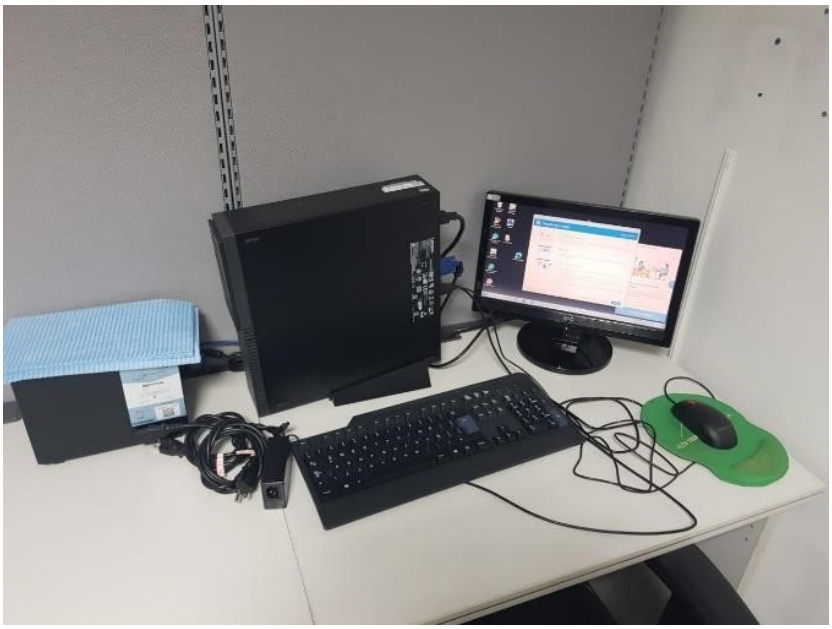
Ionos. (2020) ***Cliente Servidor*** https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-unconcepto-dos- definiciones/ [consulta marzo de 2021]

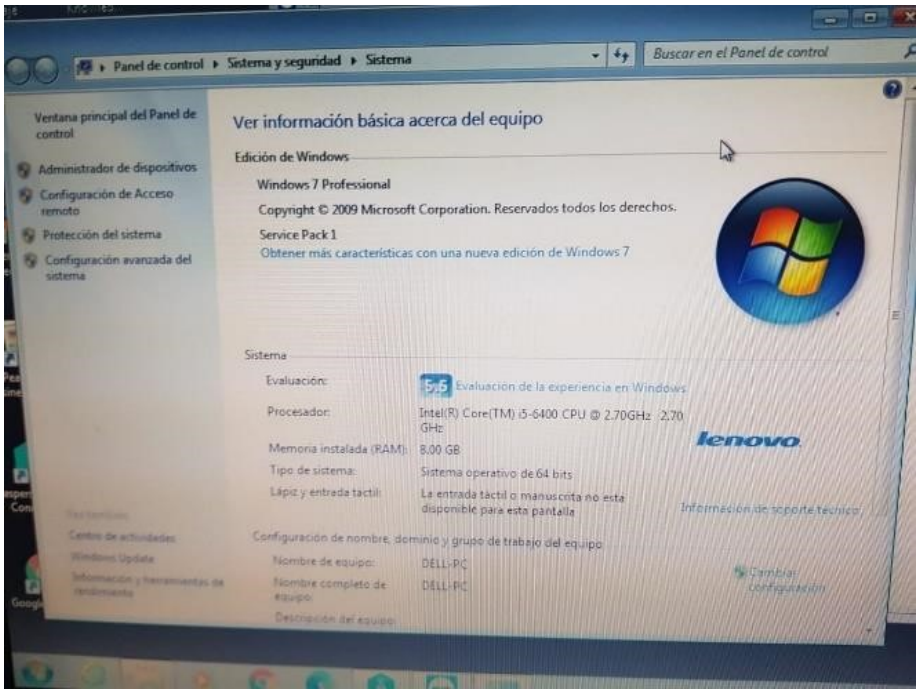
Arismendi E. (2013) ***Planificación de proyectos, Tipos y diseño de la investigación***. Recuperado de: http://planificaciondeproyectosemirarismendi.blogspot.com/2013/04/tipos-ydiseno-de-la-investigacion_21.html#:~:text=Arias%20(2012))%2C%20define%3A,informaci% C3%B3n%20pero%20n o%20altera%20las [consulta marzo de 2021]

ANEXOS

A. FOTOS QUE ILUSTRAN EL PROBLEMA

Esta es la evidencia del estado en que se encuentra el espacio designado Para alojar los equipos de comunicación y servidor de la empresa Alta Tecnología Medica





B. CHECKLIST.

1. **Cuando se procesan grandes cantidades de datos, ¿parece que la operación tarda mucho tiempo?**

☒ Sí.

☐ No.

2. **¿Se tiene la seguridad de que el servidor es capaz de almacenar, recuperar y proporcionar de forma fiable los datos que la empresa utiliza?**

   ☐ Sí.

   ☒ No.

3. **¿El servidor cuenta con arreglo de disco o redundancia?**

   ☐ Sí.

   ☒ No.

4. **¿El servidor se encuentra aislado en un área destinada?**

   ☐ Sí.

   ☒ No.

5. **¿Se tiene control para el acceso al área donde se encuentra el servidor?**

   ☐ Sí.

   ☒ No.

6. **¿Tiene el área de servidor un control de ambiente adecuado?**

   ☐ Sí.

   ☒ No.

7. **¿Tiene el servidor una fuente de alimentación alterna de fluido eléctrico?**

   ☐ Sí.

   ☒ No.

8. **¿El servidor cuenta con un SO de servidor?**

   ☐ Sí.

   ☒ No.

9. **¿Se mantiene actualizado el sistema operativo (SO) y aplicaciones de los equipos de usuarios?**

   ☒ Sí.

   ☐ No.

10. **¿Los equipos usan SO y programas originales? (es decir, no usan programas piratas o "crackeados")** ☐ Sí.

    ☒ No.

11. **¿Se han formateado los equipos hace menos de un año?**

    ☒ Sí.

    ☒ No.

12. **¿Tienen un antivirus instalado y configurado?**

    ☒ Sí.

    ☐ No.

13. **¿Tienen un antimalware instalado y configurado?**

    ☐ Sí.

    ☒ No.

14. **¿Tienen un firewall de pc instalado y configurado?**

    ☐ Sí.

    ☒ No.

15. **¿Mantienes la gestión y los permisos de las cuentas actualizadas y de acuerdo a tareas? Es decir: cuentas de usuarias con contraseña, separadas por accesos correspondientes.**

    ☐ Sí.

    ☒ No.

16. **¿Qué sucede con los computadores que incorporan de la empresa? En equipos y carpetas ¿está configurada la opción de visibilidad y acceso en red?**

    ☒ Sí.

    ☐ No.

17. **¿Los equipos tienen activada contraseña de bloqueo?**

    ☐ Sí.

    ☒ No.

18. **¿Los equipos cuentan con el bloqueo automático cuando no están en uso?**

    ☐ Sí.

    ☒ No.

19. **¿Se cuenta con programas de respaldos de la información de manera periódica y automática?**

    ☐ Sí.

    ☒ No.

20. **¿Se guardan los respaldos en algún lugar externo?**

    ☐ Sí.

    ☒ No.

21. ¿Has activado en los equipos un sistema de cifrado de archivos?

☐ Sí.

☒ No.

22. ¿Los equipos tienen instalados y configurados complementos (plugins o add-on) en el navegador que protegen la privacidad y seguridad de usuarios?

☐ Sí.

☒ No.

23. ¿Se ha configurado una VPN (Virtual Private Network, en español Red Privada Virtual)?

☐ Sí.

☒ No.

24. ¿Se ha cambiado los valores de fábrica de routers, switch y otros equipos de comunicaciones? Por ejemplo, el nombre de la red, clave de WiFi, frecuencia en la que trabaja, etc.

☒ Sí.

☐ No.

25. ¿Está activada una red de invitados a parte de la red que usan personas de la empresa?

☐ Sí.

☒ No.

26. ¿Se cambia las contraseñas de red periódicamente?

☐ Sí.

☒ No.

27. ¿Se encuentra desactivado el uso compartido de archivos y dispositivos?

☐ Sí.

☒ No.

28. ¿Utilizan redes alámbricas (es decir cableadas) para los equipos de cómputo?

☒ Sí.

☐ No.

29. ¿Cuentan con un diagrama de red actualizado? (Que indique qué equipos son parte de la red y su ubicación) ☐ Sí.

☒ No.

30. ¿Se mantiene un monitoreo del uso de red y del tráfico de información con el fin de observar patrones inusuales?

☐ Sí.

☒ No.

31. ¿Se utilizan firewall o equipos similares para seguridad del perímetro?

☐ Sí.

☒ No.

32. ¿Se monitorea regularmente el tráfico de red o uso de ancho de banda?

☒ No.

C. VALIDEZ DEL INSTRUMENTO.

El instrumento a aplicar, se define con un extracto del checklist usado por SYSADMIN (2019) **https://protege.la/wp-content/uploads/2019/05/ChecklistSysAdmin-2019..pdf** Creada para personas que administran sistemas en una organización, con el objetivo de mejorar o comenzar hábitos de seguridad digital.

Adicionalmente, este checklist es apoyado por grupos como

Protege.la **https://protege.la/**

Socialtic.org **https://socialtic.org/**

Estas son organizaciones sin fines de lucro dedicada a la investigación, formación, acompañamiento y promoción de la tecnología digital e información compartiendo recursos de seguridad y privacidad digital.

Por otro lado, para validar el instrumento, se consultó la opinión de un experto, para conocer si cumple con las características mínimas que permitan aplicarlo, para obtener la información necesaria que facilite el desarrollo de la investigación.

Identificación del experto

Nombre: José

Apellido: Rivera

Titulo o Profesión: Ingeniero en Sistemas

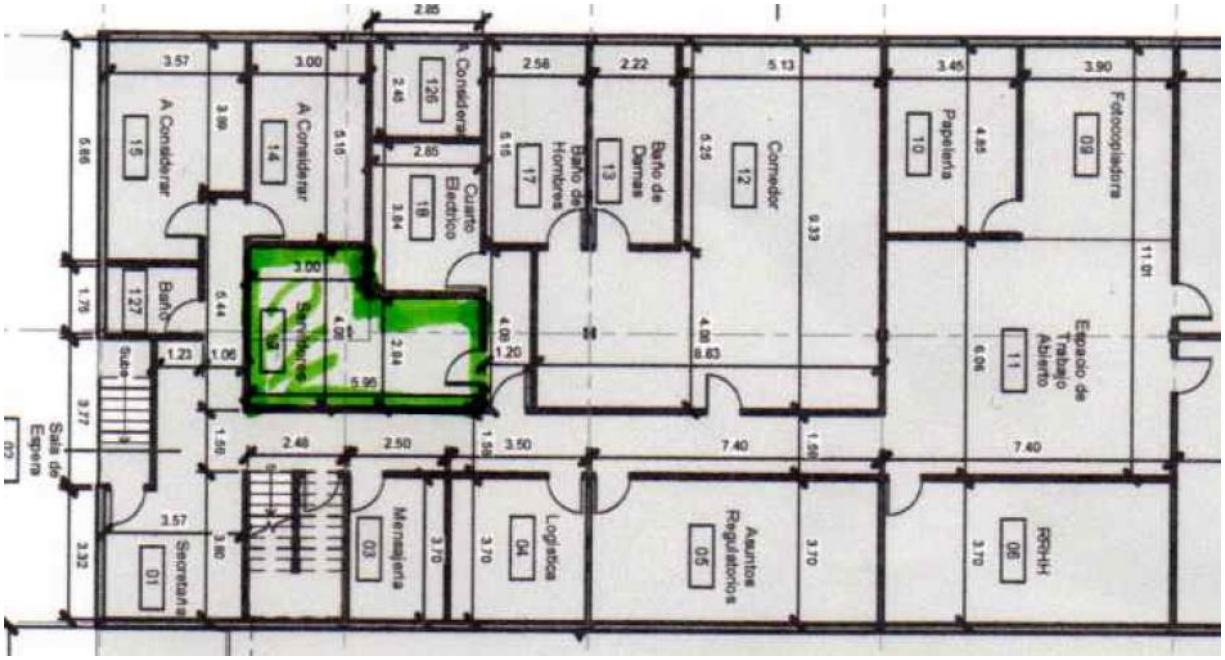
Institución donde trabaja: TeamOne Tech

Cargo: Gerente de ingeniería Opinión

o comentarios:

Cumple con los elementos necesarios para validar la información a nivel de Seguridad Lógica y Física.

D. NUEVA HUBICACION DE CUARTO DE COMPUTO.



E. SEGURIDAD FÍSICA.

F. SERVIDOR.

G. FIREWALL.

H. SWITCH.

I. PUNTO DE ACCESO.

J. TOPOLOGÍA DE RED.