TAREA 02

DISEÑO DE PLANES DE SECURIZACIÓN

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información

ACTIVIDAD PRÁCTICA

El alumno debe identificar qué elementos/decisiones/acciones no cuadran con unas prácticas correctas de los planes de securización que pueden provocar problemas.

Escenario:

La empresa "Venus SA", dedicada a la cirugía estética y con sede en Ibiza. El grado de dependencia tecnológica es bajo ya que la mayor parte de la información que gestionan como los historiales de los pacientes se encuentran en formato físico. La empresa cuenta con 10 empleados distribuidos de la siguiente manera:

- Un CEO.
- Un empleado del departamento de RR.HH.
- 5 doctores en cirugía estética.
- 2 empleados encargados de la limpieza y saneamiento de la clínica.
- Un recepcionista.

El CEO de la empresa ha decidido modernizar la clínica para ello se han marcado los siguientes hitos:

- Desarrollar una herramienta informática que gestione:
  - Historiales de los pacientes.
  - Nóminas.
  - Relaciones con proveedores.
- Informatizar todos los historiales.
- Adquirir nuevos equipos con los que poder utilizar la herramienta.
- Crear una página web corporativa de carácter informativo.
- Adquirir un nuevo servidor para alojar la herramienta.
- Reducir al máximo posible los costes y plazos de entrega.

Debido a que el presupuesto es reducido varias empresas con las que se han puesto en contacto se han negado a realizar el desarrollo pero finalmente una empresa local acepta los términos además garantizar costes y plazos.

Transcurrido no más de un mes la empresa desarrolladora ha terminado y deciden presentar al CEO de Venus SA. los resultados de su trabajo. Para ello pactan una reunión en la que los principales puntos tratados fueron:

- Con el fin de reducir costes tanto el programa gestor como la página web corporativa se ubican en el mismo servidor.
- La herramienta que gestiona informes, nóminas y proveedores ha sido desarrollada ex profeso para Venus SA.
- Para la página web corporativa se ha utilizado un gestor de contenidos o CMS de código abierto.
- El servidor se alojará en el cuarto destinado a guardar los productos y herramientas de limpieza.
- Como personal de mantenimiento de la herramienta y la página web se dará una formación al recepcionista de clínica.
- Todos los equipos serán configurados para que los usuarios puedan ser administrados por los propios usuarios.
- Le recomiendan que la informatización de los historiales antiguos la haga el personal interno, como el recepcionista, ya que el proceso es bastante sencillo y principalmente lo que hay que hacer es escanear documentos.

El CEO decide dar luz verde, para que la actualización sea lo menos traumática posible. Esta se realizará durante el fin de semana así como la formación de los empleados. Llegado el lunes, el recepcionista comienza a digitalizar todos los informes, el personal de recursos humanos hace lo propio con las nóminas y el CEO con los proveedores.

Después de una semana de arduo trabajo, sobre todo del recepcionista, el sistema está listo para ser utilizado por los doctores.

A los pocos días de uso de la herramienta esta deja de funcionar correctamente y constantemente se producen caídas del servicio pese a los intentos del recepcionista-técnico de sistemas por solucionarlo. Tanto los doctores, como el personal de RR.HH. y el CEO deben volver a hacer su trabajo como lo habían estado haciendo hasta antes de la informatización de la clínica.

Información sobre la empresa

Riesgos

Apartado 1: Tarea de investigación
Una vez que conoces los diferentes modelos para aplicar ciberseguridad en una organización, en base al supuesto planteado deberás:

- **Identificar qué elementos/decisiones/acciones no cuadran con unas prácticas correctas de los planes de securización.**
- **Ofrecer las mejores soluciones a los problemas previos.**

Identificar qué elementos/decisiones/acciones no cuadran con unas prácticas correctas de los planes de securización.

La modernización de la clínica Venus SA presenta una serie de errores en su proceso de implementación de tecnología, que afectan tanto a la infraestructura como a la seguridad, la formación del personal y la elección de proveedores. Los errores identificados no solo han expuesto a la empresa a vulnerabilidades tecnológicas, sino que también han impactado directamente en el funcionamiento diario, con constantes caídas del sistema y la incapacidad de resolver los problemas de manera eficiente. Los elementos que no cumplen con una buena práctica son los siguientes:

- Análisis y planificación previos

La modernización de la clínica se inició sin un análisis de riesgos ni un plan estratégico que evaluará las necesidades y los recursos. No se llegaron a identificar los requerimientos técnicos, las normativas de protección de datos, ni se definieron los roles para el personal encargado. Esto derivó en decisiones erróneas y apresuradas que pudieron convertirse en vulnerabilidades para la infraestructura.

- Un único servidor

Al tener bajo presupuesto se comprometió la calidad de la infraestructura. Alojar la herramienta de gestión, que maneja historiales clínicos y nóminas, junto con la página web en el mismo servidor puede suponer un riesgo de seguridad y de rendimiento. Además el servidor se alojó en el cuarto junto con los productos de limpieza, lo que puede suponer un daño físico por la posible suciedad, humedad, accidentes…

- Personal no cualificado

El recepcionista fue elegido como técnico de sistemas y encargado de la digitalización, una tarea que requiere cualificación técnica y comprensión de la sensibilidad de los datos manipulados. Esta decisión infravaloró la complejidad de las funciones y sobre cargó al empleado en el desempeño de sus funciones y el correcto manejo de la informatización.

- Medidas de seguridad

La configuración de los equipos permitió que los usuarios tuvieran privilegios de administrador, lo cual es una mala práctica que facilita errores humanos y posibles ataques. Además, no se implementaron controles de acceso ni cifrado para proteger los datos sensibles. Esto pudo suponer una vulnerabilización de la confidencialidad de los datos, exponiéndolos a accesos no autorizados y pérdida de información.

- Proveedor no especializado

La empresa contratada cumplió plazos irreales, priorizando la rapidez a la calidad. Esto resultó en un software mal diseñado y con fallos, que después ocasionaron caídas del servicio.

- Soporte técnico

No se planificó un servicio de mantenimiento técnico, auditorías, ni la contratación de personal especializado para gestionar el sistema. Se hizo un intento de formar al recepcionista como técnico, lo que demuestra una falta de previsión a largo plazo. Adicionalmente el resto de personal tampoco recibió formación para garantizar el uso eficiente y seguro de las herramientas.

En resumen, los problemas principales surgen de una combinación de decisiones apresuradas, falta de preparación y la subestimación de la complejidad que implica digitalizar datos sensibles. Sin un enfoque adecuado en seguridad, formación y mantenimiento, los esfuerzos de informatización no solo han fallado en alcanzar los objetivos planteados, sino que han dejado a la empresa vulnerable a fallos tecnológicos y riesgos de seguridad.

Ofrecer las mejores soluciones a los problemas previos.

Las soluciones planteadas abordan los problemas identificados, con el objetivo de garantizar una transición tecnológica exitosa y segura para Venus SA. La clave para corregir los errores radica en una planificación sólida, una mejora en la infraestructura tecnológica y la adopción de medidas de seguridad adecuadas. Además, es esencial contar con personal cualificado y proveedores de confianza que garanticen la calidad y estabilidad del sistema en un largo plazo. Las propuestas también incluyen un soporte técnico adecuado y una formación continua para el personal.

1. Planificación y análisis inicial

Realizar un análisis de riesgos y necesidades antes de la implementación del proyecto, que incluya: la identificación de los recursos tecnológicos necesarios (servidores, equipos…), la evaluación de la formación requerida de los empleados, definiendo los roles y el análisis del cumplimiento de normativas de protección de datos.

2. Servidores

Utilizar servidores dedicados y separados para las diferentes funciones, uno para la herramienta de gestión y otro para la página web corporativa. Debemos asegurar que ambos estén ubicados en un espacio adecuado con condiciones controladas como temperatura, humedad…

3. Proveedor cualificado

Elegir una empresa de desarrollo con experiencia que ofrezca un diseño seguro y fiable, respetando plazos y presupuestos realistas que implante estándares de calidad y la seguridad adecuada. Asegurar que la empresa proporcione soporte técnico continuo y actualizaciones periódicas del sistema.

4. Personal especializado

Contratar un técnico de TI especializado para la instalación, configuración y mantenimiento de los sistemas. Además se debe proveer formación especifica al personal que usará las nuevas tecnologías, garantizando que el personal esté cualificado para realizar su trabajo sin comprometer la seguridad.

5. Seguridad de los sistemas

Se debe implementar controles de acceso, asegurando que cada usuario tenga privilegios mínimos según su rol, también cifrar los datos sensibles tanto en tránsito como el almacenamiento para proteger la información de accesos no autorizados. Además, implementar políticas para realizar copias de seguridad automáticas para garantizar la recuperación si se produce algún fallo.

En conclusión, las soluciones propuestas ofrecen un enfoque estructurado y estratégico para corregir las deficiencias actuales, mejorar la seguridad y garantizar el buen funcionamiento de la clínica en el futuro. Al aplicar estas medidas la empresa podrá resolver los problemas inmediatos de caídas del sistema y establecer una base sólida para el manejo seguro y eficiente de la información crítica, mejorando tanto su operatividad como la confianza de sus pacientes.