Universidad Gerardo Barrios San miguel

Facultad de ciencia y tecnología

Carrera:

Ingeniería de software y redes informáticas

Materia:

Administración de Base de Datos II

Catedrático:

Gisela Espinoza

Estudiantes:

Villatoro Pérez Ángel Armando código SMIS924020

Chávez Herrera Cesar André código SMIS033320

Quintanilla Chávez Manfredy José código SMIS021120

Jiménez Guzmán William Rene código SMIS031920.

Benítez Turcios Jhonatan Josué código SMIS024420

Ciclo: 2022/I

Índice:

1. capítulo I

1.1. Introducción

1.2. Objetivos

1.3. Planificación del trabajo (Cronograma)

2. capítulo II

2.1. Situación actual

2.1.1. Descripción de la organización

2.1.2. Actividad y entorno

2.1.3. Tamaño y estructura organizacional

2.2. Análisis de riesgos

2.2.1. Identificación de activos (un activo es algo que tiene valor o utilidad en la organización para la realización de sus operaciones)

2.2.2. Identificación de amenazas y vulnerabilidades

2.2.3. Cálculo de la probabilidad

2.2.4. Evaluación del riesgo

2.2.5. Cálculo del riesgo residual

2.3. Propuesta

2.3.1. Plan de acción – controles sugeridos

3. capitulo III

3.1. Conclusiones

3.2. Recomendaciones

4. capitulo IV

4.1. Glosario

4.2. Bibliografía

5. Entrega final y defensa

Capítulo 1

Introducción:

En el siguiente trabajo, nosotros como grupo realizaremos una investigación a la base de datos del Hospital San Juan de Dios, hablando con el personal administrativo para solventar dudas y obtener información de como ellos manejan las ISO o cualquier método de seguridad virtual con los que ellos cuentan, de no ser el caso, indagar como manejan la seguridad en general. También realizaremos una evaluación y cálculos de los riesgos y proponer ideas o planes de acción para la resolución de los riesgos. Para los planes de seguridad entraría las normas ISO, nos enfocaremos en el reglamento de protección de datos, Normas ISO 27001 y 27002, donde estudiaremos la base de datos de la empresa, para saber si la empresa trabajo con este reglamento de seguridad de datos, como la maneja dentro de la base de datos, como se adaptarían los usuarios a este reglamento, comprender la estructura de la base de datos con las normas ISO y estudiarla para saber cómo sería el análisis de riegos y utilizar un plan de control.

Objetivos:

Objetivo General:

• Identificar el tipo de Seguridad con la que Cuenta el hospital San Juan de Dios, Si trabajan con la ISO 27001 o cualquier tipo de seguridad con la que ellos cuenten, a su vez determinar las ventajas y desventajas junto a sus riesgos.

Objetivos Específicos:

* Analizar el sistema de seguridad hacia la base de datos y cómo implementar el reglamento ISO 27001 para detectar las posibles vulnerabilidades y riesgos a los que podrían estar expuestos los datos
* Estudiar y comprender la idea de la creación del plan de seguridad para la empresa usando la Norma ISO 27001 insistiendo en la importancia y aplicación de este dentro de la organización.
* Indicar los pasos a seguir para lograr cumplir con la ejecución del plan de seguridad a todo el personal que manipula la entrada o que tiene privilegios sobre el ingreso de datos.

Planificación del trabajo (Cronograma).

Gráfico

Descripción generada automáticamente con confianza media

Capítulo 2.

2.1 SITUACION ACTUAL

El Hospital San Juan de Dios en el departamento de San Miguel, al área de tecnología específicamente para poder obtener información acerca de cómo ellos manejan la seguridad base de datos y como se protegen de cualquier tipo de amenazas, después de recibir una entrevista con la ingeniera Nathalia, jefe en el área de tecnología, pudimos concluir que: el área laboral es el correcto, la infraestructura es la adecuada para poder albergar las bases de datos, Adquieren licencias de distintos proveedores para poder manejar la enorme cantidad de datos que maneja un hospital de las distintas áreas.

La seguridad de los datos es la adecuada puesto que los diferentes servicios que necesita el hospital san juan de Dios son gestionados de manera priva por diferentes empresas que se dedican específicamente al desarrollo de software para el país, haciendo que el hospital san juan de dios solo gestione los datos de entrada y salida de la base de datos y las copias locales que tiene el mismo para gestionar son equipo ensamblado por las empresas que dan los diferentes servicios.

2.1.1 Descripción de la organización

La institución que hemos elegido es El hospital San Juan de Dios, lo que significa que es un servicio público, capaz de ayudar a cualquier salvadoreño en una emergencia, pero nosotros nos enfocamos en el área de tecnología, como el Hospital funciona sin ningún tipo de atraso, como la información es manejada internamente, desde los registros de pacientes hasta el registro de todo el personal de salud, hasta como la información es enviada al exterior y viceversa. El área de tecnología se encuentra en un edificio aparte del Hospital, donde se encuentra el personal administrativo junto a todos los equipos que permiten el dicho paso o retención de información.

2.1.2 Actividad y entorno

Se realizan actualización y registros de datos al día ya que nuevos pacientes son registrados y a los antiguos se les actualiza su expediente, cabe recalcar que son alrededor de trecientos recién nacidos por mes en la cual cada uno de los recién nacido es un registro nuevo que alberga la base de datos de la institución. De igual forma se mantienen registros a mano, los cuales se realizarán con ayuda de digitadores o pasantes que se emplearán a digitar cada uno de los registros que se mantienen, la meta hoy en día es de trescientos registros diarios ya que hace un tiempo era de cincuenta.

2.1.3 Tamaño y estructura organizacional

El área administrativa es un edificio de 30x50 metros cuadrados, la cual cuenta con la tecnología necesaria para su correcto funcionamiento, la estructura organizacional es en cascada, el jefe de área como la cabeza del área de tecnología, el encargado en el área de mantenimiento preventivo y correctivo. El encargado del área de redes, el encargado de sistemas, el encargado de base de datos, las secretarias, los digitadores, los pasantes. Y por último los ordenanzas.

2.2 ANÁLISIS DE RIESGOS

Identificación de activos (un activo es algo que tiene valor o utilidad en la organización para la realización de sus operaciones)

Activos de la institución:

|  |  |
| --- | --- |
| Hardware | |
| Computadoras. | Computadoras usadas por el personal. |
| Ups. | Batería para salvar computadoras en un apagón. |
| Servidores. | Cajón físico de la base de datos. |
| Routers. | Hacen llegar el internet al edificio. |
| Repetidores. | Permite expandir el área del router. |
| Generador alterno de energía. | En cualquier apagón este protegerá todo |

|  |  |
| --- | --- |
| Software. | |
| Ofimática. | Toda la paquetería office. |
| Cassandra. | Gestor de base de datos del hospital. |
| Sistemas operativos. | Windows y Linux. |
| Aplicaciones del gobierno | Al ser una institución pública necesita un registro con el gobierno. |

|  |  |
| --- | --- |
| Persona. | |
| Jefe | El que se encarga de dirigir el área de tecnología. |
| Encargado de mantenimiento | Hace mantenimientos correctivos y preventivos. |
| Encargado de redes | Es el que mantiene las redes funcionando. |
| Encargado de base de datos | Mantiene las bases de dato funcionando. |
| Secretaria | Mantiene todo tipo de registros. |

|  |  |
| --- | --- |
| Datos. | |
| Registros de pacientes. | Se recopila toda la información del paciente. |
| Registro de medicamentos. | Que medicamentos han sido enviados. |
| Registros de muertes. | Registro de gente fallecida. |
| Información de los trabajadores. | Información personal de cada trabajador de todo el hospital. |

|  |  |
| --- | --- |
| Infraestructura | |
| Edificio administrativo | Lugar en donde se encuentra todo lo relacionado a la tecnología. |
| Edificio hospital. | El hospital donde se atienden a los pacientes. |
| Estacionamiento. | Lugar para que los trabajadores dejen sus carros. |
| Bodegas. | Lugar donde se guardan todo tipo de cosas. |

2.2.2 Identificación de amenazas y vulnerabilidades

Los activos están sujetos a diferentes amenazas y vulnerabilidades las cuales pueden ocasionar pérdidas significativas.

|  |
| --- |
| **Listado de amenazas.** |
| * Autorización accidental a personal no capacitado. |
| * Mala gestión de mantenimiento en los equipos. |
| * Espionaje/hurto de información de los equipos. |
| * Circulación ilegal de la información recopilada en la institución. |
| * Robo de identidad. |
| * Infección por virus |
| * Mala gestión técnica. |
| * Ataque DDOS |

**Identificación de amenazas y vulnerabilidades por activo**

**Activo: Software**

|  |  |  |
| --- | --- | --- |
| **Activos** | **Amenazas** | **Vulnerabilidades** |
| **Ofimática.** | Circulación ilegal de la información recopilada en la institución | Descargas de sitios web no autorizados u oficiales. |
| Empleado molesto |
| **Cassandra.** | * Autorización accidental a personal no autorizado. * Ataques externos(Vulnerabilidad: Falta de restricción de los equipos de red, límites de conexión no definidos.) | Personal no autorizado adecuadamente al manejo de gestión de datos. |
| Ejecución remota de código (capacidad de acceder y cambiar la propiedad de un servidor o base de datos) |
| **Sistemas Operativos.** | Código malicioso | Falta de protección contra virus. |
| Falta de actualizaciones. |
| **Aplicaciones de Gobierno.** | Robo de identidad. (Contraseñas débiles, asignación deficiente de permisos)   * Código malicioso. | Inyección. |
| Fallos de identificación y autenticación. |

**Activo: Hardware**

|  |  |  |
| --- | --- | --- |
| **Activos** | **Amenazas** | **Vulnerabilidades** |
| **Computadoras.** | Mala gestión de mantenimiento en los equipos.   * Desastres naturales * Usos no autorizados. (falta de políticas de acceso, espacios de trabajos abierto, empleados molestos) | Protección deficiente contra virus. |
| Gestionar mal las particiones de los discos duros. |
| **UPS/Generador alterno de energía.** | Mala gestión técnica.  Desastres naturales | Problemas eléctricos como corto circuitos o perjudicar componentes de los equipos. |
| Fallos y probabilidad de perdida de datos. |
| **Servidores.** | Circulación ilegal de la información recopilada en la institución.  Desastres naturales | Personal no capacitado adecuadamente al manejo de gestión de datos. |
| Fallos y probabilidad de perdida de datos. |
| **Routers/Repetidores** | Ataque DDOS  Desastres naturales | Inyección. |
| Ejecución remota de código (capacidad de un atacante de acceder y cambiar la propiedad de un servidor o base de datos) |

**Activo: Personas (Recursos humanos)**

|  |  |  |
| --- | --- | --- |
| **Activos** | **Amenazas** | **Vulnerabilidades** |
| **Jefe.** | Corrupción de los datos | Falta de conocimientos en el área asignada. |
| Actualización de datos confidenciales. |
| **En cargado de mantenimiento.** | Mala gestión de mantenimiento en los equipos. | Falta de conocimientos en el área asignada. |
| Robo de información. |
| **Encargado de redes.** | Mala gestión técnica. | Mantener la conexión de red abierta. |
| Robo de información. |
| **Encargado de base de datos.** | Espionaje/hurto de información de los equipos.  (Mal diseño de base de datos, mala asignación de los permisos, no aplicar las políticas de seguridad). | Personal no capacitado adecuadamente al manejo de gestión de datos. |
| Fallos y probabilidad de perdida de datos. |
| **Secretaria.** | Errores humanos. (Vulnerabilidad, prestar equipo de la empresa a terceros.) | Descargas de sitios web no autorizados u oficiales. |
| Falta de capacitación con nuevas tecnologías. |

**Activo: Datos**

|  |  |  |
| --- | --- | --- |
| **Activos** | **Amenazas** | **Vulnerabilidades** |
| **Datos e información** | Corrupción de datos. | Datos duplicados. |
| Respaldos no actualizados. |
|  |  |
|  |
| Destrucción de copias de seguridad. | Autorización ilegal a copias de seguridad. |
| Error humano. |
| Divulgación ilegal de la información. | Falta de políticas de restricción uso de la información. |
| Falta de controles para la movilización de los datos. |

2.2.3 Valoración de impacto.

**Activo: Software.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| **Ofimatica.** | 2 | 3 | 2 | 2 |
| **Casandra.** | 2 | 2 | 3 | 2 |
| **Sistemas operativos.** | 2 | 1 | 1 | 1 |

**Activo: Hardware.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| **Computadoras.** | 3 | 3 | 3 | 3 |
| **UPS/Generador alterno de energía.** | 1 | 2 | 2 | 2 |
| **Servidores.** | 3 | 3 | 3 | 3 |
| **Routers/Repetidores** | 2 | 1 | 3 | 2 |

**Activo: Persona.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| **Jefe.** | 3 | 3 | 3 | 3 |
| **En cargado de mantenimiento** | 2 | 2 | 2 | 2 |
| **Encargado de redes.** | 2 | 3 | 3 | 3 |
| **Encargado de base de datos.** | 2 | 3 | 3 | 3 |
| **Secretaria.** | 1 | 1 | 2 | 1 |

**Activo: Datos.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| **Registro de pacientes.** | 3 | 3 | 3 | 3 |
| **Registro de medicamentos.** | 3 | 2 | 2 | 2 |
| **Registro de muertes.** | 2 | 1 | 1 | 1 |
| **Información de trabajadores.** | 2 | 2 | 2 | 2 |

**Activo: Infraestructura.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Integridad** | **Disponibilidad** | **Confidencialidad** | **Impacto** |
| **Edificio Administrativo.** | 3 | 2 | 2 | 2 |
| **Edificio Hospital.** | 3 | 3 | 3 | 3 |
| **Estacionamiento.** | 2 | 1 | 1 | 1 |
| **Bodegas.** | 2 | 2 | 2 | 2 |

2.2.4 Evaluación del riesgo