Nombre de alumno:

Teresa Méndez Pérez

Nombre del profesor:

Icel Bernardo Lepe Arriaga

Nombre del trabajo:

Ensayo unidad I

Materia:

Seguridad en la información

Grado: 9 cuatrimestre

Comitán de Domínguez Chiapas a 25 de mayo del 2022

INTRODUCCION

En este ensayo se verá el tema “introducción a la seguridad de la información” como su nombre lo dice seguridad, nos dice que veremos temas relacionados a cómo proteger nuestra información tanto físicamente como digitalmente, te preguntaras ¿Digitalmente? Si digitalmente nosotros cuando estamos en una computadora agregamos información personal/privada la cual nosotros protegemos dependiendo la privacidad de la información, ejemplo, cuando tenemos documentos como un escaneo de acta (cualquier tipo) lo guardamos y lo convertimos en un documento zip, otro ejemplo cuando ingresamos a nuestra cuenta de Facebook lo primero que nos pide es nuestra contraseña para poder ingresar y de esa manera evitar que otra persona ajena acceda a ella.

Hablando en el término informático la seguridad es muy valiosa hablemos de un sistema de banco, imagínate cuanta seguridad tiene y cuantos protocolos se deben pasar para ingresar a lo que se desea saber, pero sobre todo su base de datos debe estar muy bien protegida para evitar de hacker u otros virus puedan acceder a esa información para su conveniencia, si esto falla habría un completo caos.

En algunos casos la misma computadora se encripta, así diseñada para guardar toda la información que ahí se almacena, ¿se puede recuperar? Si pero depende que tipo de encriptado sea por lo regular lleva mucho tiempo y algunas partes de la información no se recupera.

Esto es una pequeña introducción, pasaremos a la investigación esperando cumplir con las expectativas pero sobre todo que los temas queden claros pasaremos a la investigación y dejare las fuentes que consulte hasta el final del trabajo.

INTRODUCCIÓN A LA SEGURIDAD INFORMACIÓN

1.1 EL VALOR DE LA INFORMACIÓN.

La información tiene un gran impacto en la toma de decisiones. Aunque no tiene valor absoluto, su valor está relacionado con quién la usa y en la situación de uso.

• El valor normativo de la información: Se refiere al conocimiento a priori o preliminar que tenemos acerca de la ocurrencia de los eventos los cuales son relevantes para nuestras decisiones (probabilístico).

• El valor realístico de la información: Es el de reconocer que la información apoya las decisiones. Las acciones tomadas afectan a los logros de desempeño.

• El valor subjetivo de la información: Refleja la impresión comprendida de la gente para la información.

• Beneficios tangibles: Reducción en los niveles de inventario, en la línea de crédito, en horas-hombre, incremento de ventas y reducción en los costos de mantenimiento.

• Beneficios intangibles: Mejora de los procesos de toma de decisiones; amplía los horizontes de planeación; extiende las bases de información para la toma de decisiones; facilita la integración de datos.

Sistemas de información y tecnología

• Datos: son descripciones básicas de cosas, acontecimientos, actividades y transacciones que se registran, clasifican y almacenan. Pueden ser datos numéricos, alfanuméricos, figuras, sonidos e imágenes.

• Información: representa datos organizados que han adquirido valor y significado para el receptor.

• Conocimiento: se constituye de datos o información que se ha organizado y procesado de tal forma que sea entendible.

1.2 DEFINICIÓN Y TIPOS DE SEGURIDAD INFORMACIÓN.

Las medidas de seguridad que abarca pueden ser: antivirus, firewalls u otras medidas que dependen del usuario como, por ejemplo, la activación o desactivación de algunas de las funciones del software como el Java, ActiveX, para asegurar el uso de la computadora, los recursos de red o del Internet.

La seguridad informática busca la preservación de la confidencialidad, integridad y disponibilidad de la información. Debido a que la información corporativa es uno de los activos más importantes que maneja toda empresa, se encargan de invertir en un sistema de gestión que busque garantizar su protección.

>Amenazas lógicas

Existen dos tipos de *softwares* que pueden dañar un sistema informático:

- **Vulnerabilidades del software:** Son posibles errores en el sistema operativo que ponen en riesgo la seguridad del dispositivo si llega a ser encontrado por un atacante.
- ***Software* malicioso**: Existen programas con objetivos malignos, como, por ejemplo, los virus, gusanos o troyanos.

>Amenazas físicas

Se originan por 3 causas principales:

- **Fallo del dispositivo:** Ante un agente externo como una caída del sistema eléctrico o por un desperfecto físico del dispositivo.
- **Accidentes:** Que pueden ocurrir por un sinnúmero de razones.
- **Catástrofes naturales:** Como terremotos, tormentas, etcétera.

1.3 OBJETIVOS DE LA SEGURIDAD INFORMACIÓN.

Las áreas principales de la información que cubren son 4:

1. **Integridad:** Se trata de la autorización de algunos usuarios en particular para el manejo y modificación de datos cuando se considere necesario.

2. **Confidencialidad:** Únicamente los usuarios autorizados tienen acceso a los distintos tipos de recursos, datos e información, logrando filtrar y robustecer el sistema de seguridad informática.
3. **Disponibilidad:** Los datos deben estar disponibles para el momento en que sean necesitados. Es la capacidad de permanecer accesible en el sitio, momento y en la forma que los usuarios autorizados lo necesiten.
4. **Autenticación**: Se basa en la certeza de la información que manejamos.

1.3 POSIBLES RIESGOS EN LA INFORMACIÓN.

Riesgos de la seguridad de la información

*Permiso de administrador en el ordenador

* Correo malicioso o no deseado

* No realizar copias de seguridad

* Buen uso de las contraseñas

* Uso de aplicaciones de almacenamiento on-line

Como evitar riesgos innecesarios

• Podríamos empezar por formar a los trabajadores en la cultura de la ciberseguridad, que sean cuidadosos y precavidos a la hora de abrir un determinado correo electrónico sospechoso, o de instalar un programa de dudosa procedencia. También insistir en el buen uso de las contraseñas.

• Limitar el uso de los trabajadores en los ordenadores de la empresa para usos particulares. Puede ser que se den simplemente instrucciones de que los recursos de la empresa sean de uso meramente laboral, y por tanto esté prohibido el uso del ordenador para fines particulares (correos personales tipo Gmail, uso de redes sociales, etc), o bien que se limite tecnológicamente el acceso vía internet a páginas relacionadas con el negocio de la empresa.

• Si no se está haciendo ya, aunque su empresa tan solo trabaje con la información de su cartera de clientes, haga copias de seguridad de está.

• No permita el intercambio de información crítica de la empresa a través de almacenamiento on-line, pendrives sin encriptar, etc.

1.4 TÉCNICAS DE ASEGURAMIENTO DEL SISTEMA

Consideraciones con el software: Existe software que es conocido por la cantidad de agujeros de seguridad que introduce. Se pueden buscar alternativas que proporcionen iguales funcionalidades, pero permitiendo una seguridad extra.

Consideraciones de una red: Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles. Mantener al máximo el número de recursos de red sólo en modo lectura, impide que ordenadores infectados propaguen virus.

En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo. Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

1.5 CRIPTOLOGIA, DEFINICION YTIPOS

El arte y la técnica de crear mensajes codificados con procedimientos o claves secretas con el objeto de que no pueda ser descifrado salvo por la persona a quien está dirigido o que detenta la clave.

El objetivo de la criptografía es, pues, proteger la información enviada, de modo que solamente el destinatario o las personas que posean la clave, puedan leer el mensaje de manera correcta**.**

Criptografía simétrica
Método en el cual se emplea la misma clave para encriptar y descifrar mensajes, por lo cual ambas partes, tanto el emisor como el receptor, han de tener la misma clave. Por ejemplo: la autenticación de un celular de tecnología GSM.

Criptografía asimétrica
Es un método en el cual son empleadas dos claves, una pública y otra privada. A la clave pública cualquier persona puede acceder, mientras que a la privada solo tiene acceso su propietario.

1.12 EJEMPLOS DE LA ESTADÍSTICA DEL LENGUAJE.

1. Lo primero, un «conjunto de datos».

2. En dicho conjunto el requisito es tener mínimo dos «variables» (éste es el nombre técnico), según unas técnicas u otras se han denominado «dominios», «campos» de una base de datos y similares.

3. Conocer las bases matemáticas y estadísticas del análisis de datos, en concreto

Un ejemplo práctico de lo que no es una correlación en seguridad: es contar el número de direcciones IP bloqueadas por un determinado filtro dentro de una base de datos o log de sistemas, cuando el número de conexiones hacia una «network destination
 address» concreta sobrepasa un umbral máximo establecido desde una determinada localización («source address» o geográfica).

CONCLUSION

En esta unidad se vio lo que es la seguridad de la información, como debemos protegerla tanto físicamente como virtualmente, pero sobre todo que debemos evitar para pasar sobre estos casos.

En lo personal el punto más importe para mi es sobre la criptografía, se me hace un tema muy interesante sobre como antes en la antigüedad tenían esa genialidad de entender los mensajes para que no todos lograran descubrir lo que contenía y en la actualidad como también la encriptación funciona la complejidad de cada diferente tipo de encriptación, la dificultad de descifrar la información.

En lo personal adquiero nuevo s conocimientos y eso es de lo que se trata conocer más sobre temas distintos temas que tal vez al principio nos parece aburrido pero con forme vamos investigando y viendo de lo que trata nos llama más y más la atención.

Esperando que este trabajo haya quedado comprendido y bien explícito doy por terminado este ensayo, agrego fuentes de información con la que complemente el ensayo apoyándome también de la antología.

https://blog.posgrados.ibero.mx/seguridad-informatica/