SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL

TALLER No. 3 – SISTEMAS DE INFORMACION.

ACTIVIDADES DE APROPIACION DEL CONOCIMIENTO (Conceptualización):

Instrucciones:

1.- Trabajo en grupo .
2.-Con base en lo visto en clase, y mediante la lectura entregada sobre "La Seguridad de la Información y Seguridad de la Informática" .
3.- Conceptualice los siguientes términos:

Descripción Actividad 1

1.- Que diferencia entre la "La Seguridad de la Información y Seguridad de la Informática"

2.- En que consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. Que otras bases propone desde la investigación?

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la informacion?.

Recuerde que estoy atenta a sus inquietudes.

Éxitos en su aprendizaje.

Elaboro:
Lenny Kelly Hurtado R.
Instructora de Gestion Documental
Centro de Comercio y Servicios
SENA Regional Cauca
Lkhurtado0@misena.edu.co

Descripción Actividad 1

1.- Que diferencia entre la “La Seguridad de la Información y Seguridad de la Informática”

Respuesta:

Se ha convertido en una moda hablar de Seguridad de la Información y Seguridad Informática como si estuviésemos hablando de lo mismo, como si estas palabras no tuvieran diferencias, pero en realidad son dos mundos en un mismo plano. Les contare lo que significa cada uno de estos conceptos, y cuáles son sus diferencias.

En palabras simples podemos decir que la Seguridad Informática protege el Sistema Informático, es decir son medidas técnicas que preservan las infraestructuras tecnológicas y de comunicación que soporta una organización, en otras palabras, los Software y hardware. Acá escuchamos los conceptos de Virus, antivirus, malware, ransomware, firewall, dns, dlp, entre otros.

La Seguridad de la Información va mucho más allá, además de preservar y proteger la Información, en todos sus medios de soporte no solo informáticos, mejora los procesos del negocio donde a través de metodologías adoptados por la alta dirección, que incluye medidas organizativas, legales y técnicas, con esto se asegurara la confidencialidad, integridad y disponibilidad de la Información, y por sobre todo protegerá contra los riesgos de los activos, amenazas, vulnerabilidades e impactos que pueden atentar contra la Continuidad del negocio.

*En la Seguridad de la Información protegemos personas, procesos y tecnología, en la Seguridad Informática protegemos los Hardware y los Software.

2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

Respuesta:



PLANIFICAR (Plan): consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Actuar lleva de nuevo a la fase de Planificar para iniciar un nuevo ciclo de las cuatro fases, tomando en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, por ejemplo, puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? ¿Cree usted que son suficientes? Que otras bases propone desde la investigación.

Respuesta:

En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- Confidencialidad: Prevenir la divulgación no autorizada de la información.
- Integridad: Prevenir modificaciones no autorizadas de la información.
- Disponibilidad: Prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

Las interpretaciones de estos tres aspectos varían, según los contextos en que se desenvuelven. La interpretación de un aspecto en un ambiente dado dependerá de las necesidades de las personas, costumbres y/o normas de la organización particular.



Me parecen suficientes tienen tres pautas esenciales que protegen nuestra información, no propongo bases porque estas que están estipuladas me parecen correctas.

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos.

Respuesta:

Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña)
2. Por lo que uno tiene (una tarjeta magnética)
3. Por lo que uno es (las huellas digitales)

Autorización: Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

Administración: Define, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.

Auditoría: Continua vigilancia de los servicios en producción y para ello se recaba información y se analiza.

Registro: Mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo.

Mantenimiento de la integridad de la información: Procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada.

5.- Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

Respuesta:

Una **vulnerabilidad** (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos agujeros pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

Hay una serie de vulnerabilidades de seguridad, pero algunos ejemplos comunes son:

Autenticación rota
Cuando las credenciales de autenticación se ven comprometidas, las sesiones de usuario y las identidades pueden ser secuestradas por actores maliciosos para hacerse pasar por el usuario original.

Inyección de SQL
Como una de las vulnerabilidades de seguridad más frecuentes, las inyecciones de SQL intentan obtener acceso al contenido de la base de datos a través de la inyección de código malicioso. Una inyección SQL exitosa puede permitir a los atacantes robar datos confidenciales, identidades falsas y participar en una colección de otras actividades dañinas.

Secuencias de comandos entre sitios
Al igual que una inyección SQL, un ataque de secuencias de comandos entre sitios (XSS) también inyecta código malicioso en un sitio web. Sin embargo, un ataque de secuencias de comandos entre sitios se dirige a los usuarios del sitio web, en lugar del sitio web en sí, lo que pone en riesgo la información confidencial del usuario.

Falsificación de solicitudes entre sitios
Un ataque de falsificación de solicitudes entre sitios (CSRF) tiene como objetivo engañar a un usuario autenticado para que realice una acción que no tiene la intención de hacer. Esto, junto con la ingeniería social, puede engañar a los usuarios para que accidentalmente proporcionen datos personales a un actor malicioso.

Configuración incorrecta de seguridad
Cualquier componente de un sistema de seguridad que los atacantes puedan aprovechar debido a un error de configuración puede considerarse una “Configuración incorrecta de seguridad”.

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

Respuesta:

Podemos clasificar las personas 'atacantes' en dos grupos:

- Activos: su objetivo es hacer daño de alguna forma. Eliminar información, modificar o sustraerla para su provecho.

- Pasivos: su objetivo es curiosear en el sistema.

Tipos de personas que pueden constituir una amenaza para el sistema informático:

-Personal de la propia organización. - Exempleados. - Curiosos. -Crackers.

-Terroristas. -Intrusos remunerados.

Podemos tener otros criterios de agrupación de las amenazas, como son:

Origen de las amenazas

Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc...

Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc...

Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc...

Intencionalidad de las amenazas

Accidentes: averías del hardware y fallos del software, incendio, inundación, etc...

Errores: errores de utilización, de explotación, de ejecución de procedimientos, etc...

Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc...

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información?

Respuesta:

La implementación de un sistema de seguridad debe estar complementado con las políticas de seguridad.

La política de seguridad requiere no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino también establecer el origen de las mismas, que pueden ser internas o externas a la organización.

De nada valdría proteger la empresa de los usuarios del exterior si también existen amenazas internas. Por ejemplo, si un usuario utiliza un disquete que contiene un virus podría expandirlo a toda la intranet.

Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos". Los documentos de una política de seguridad deben ser dinámicos es decir, ajustarse y mejorarse continuamente según los cambios que se presentan en los ambientes donde se crearon.

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una Empresa, y garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización.

Las políticas de seguridad deben ser conocidos por todo el personal de una organización.

En el contenido de los documentos deben estar claramente establecidos: El objetivo, los responsables del cumplimiento, las medidas que se aplicarán en caso de incumplimiento.

Entre los documentos pueden citarse los siguientes:

Administración de usuarios que reglamentará el acceso a los recursos por el personal de la organización.

Copias de respaldo: Describirá los pasos a seguir para asegurar una adecuada recuperación de la información, a través de las copias de respaldo.

Tratamiento de la información: Definirá claramente los tipos de información que es manejada por las personas autorizadas dentro de la organización.

Software legal: Definirá claramente el uso de software en la Empresa con licencias de uso legal.

Uso del servicio de Internet y del correo electrónico: Describirá la protección de la información mediante el uso de correo electrónico y del servicio de Internet.

Ambientes de Procesamiento: Define el uso de los ambientes de procesamiento de información.

Seguridad en las comunicaciones: Describirá la protección de la información durante los procesos de transmisión y recepción de datos en las redes internas y externas.

Auditorías de los sistemas: Que permitirá hacer un control de los eventos de seguridad de los sistemas.

Continuidad del procesamiento: Se definirán y reglamentarán las actividades relativas a la recuperación de la información en casos críticos mediante una metodología adecuada.

Protección física: Definirá la protección física de los equipos, de procesamiento, almacenamiento y transmisión de la información.

Sanciones por incumplimientos: Este documento contemplará las medidas que se aplicarán por incumplimiento de las reglas definidas.



NOMBRE: ROBINSON ALEJANDRO MOLANO ARIAS

INSTRUCTORA: LENNY KELLY HURTADO R.

PROGRAMA: GESTION DEL TALENTO HUMANO

ACTIVIDAD No. 3: SISTEMAS DE INFORMACION

No DE FICHA:2254893

FECHA: 24/05/21

Descripción Actividad 1

1.- Qué diferencia hay entre la “La Seguridad de la Información y Seguridad de la Informática”

2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. Que otras bases propone desde la investigación?

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información?

-DESARROLLO –

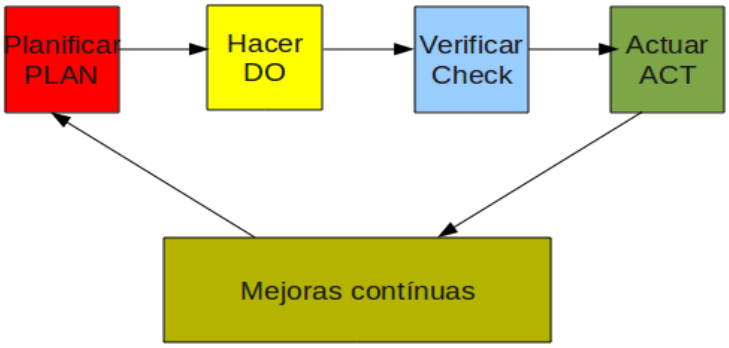
1) DIFERENCIA:

La seguridad de la información se define como conjunto de medidas técnicas, organizativas y legales, es decir, consiste en la preservación de la confidencialidad, la integridad(rectitud) y la disponibilidad de la información.

Mientras que la seguridad de la información permite digitalizar todo tipo de información y almacenarla en un menor espacio, facilitando su análisis y procesamiento.

2) modelo de seguridad (PDCA): Según la lectura para aplicar un modelo PDCA, debe aplicarse primero un sistema de gestión de la seguridad de la información (SGSI) que tiene como objetivo proteger la información, identificando los activos de información que deben ser protegidos y en qué grado.

Plan PDCA ('PLAN – DO – CHECK – ACT')



PLANIFICAR (Plan): consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

3) las bases planteadas en la lectura son:



Definimos la confiabilidad como la probabilidad de que un sistema se comporte tal y como se espera de él.

- Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

- Integridad: En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado. El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.

- Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

Desde el objetivo de la lectura creo que son suficientes una vez cumplidas legalmente.

Otras: misionalidad

4) MECANISMOS BÁSICOS DE LA SEGURIDAD DE LA INFORMACIÓN:

Autenticación: Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.
Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña. Pero, cada vez más se están utilizando otras técnicas más seguras.
Es posible autenticarse de tres maneras:
1. Por lo que uno sabe (una contraseña).
2. Por lo que uno tiene (una tarjeta magnética).
3. Por lo que uno es (las huellas digitales).

Autorización: Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.
El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.
Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente.
En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos.

Administración: establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.
Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema. La administración de la seguridad informática dentro de la organización es una tarea en continuo cambio y evolución ya que las tecnologías utilizadas cambian muy rápidamente y con ellas los riesgos.

Auditoría y registro: la Auditoría es continua vigilancia de los servicios en producción y para ello se recaba información y se analiza. Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización.
El Registro como el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo.
Pero auditar y registrar no tiene sentido sino van acompañados de un estudio posterior en el que se analice la información recabada.
Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo.

Mantenimiento de la integridad: conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la

información enviada desde un punto llegue al destino inalterada. Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos está: uso de antivirus, cifrado y funciones 'hash'.

5) Lo entiendo como debilidad o fragilidad del sistema informático donde hace referencia a la pregunta 1. Ya que al presentar el sistema informático facilidad de transportar la información como también facilitar el acceder a esta, implica posibilidades de que la información al ser transportada- desaparezca y al ser fácil acceder a ella también es más fácil modificar su contenido.

Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero

- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución “conocida”, pero se sabe cómo explotarla.

Vulnerabilidades conocidas

- Vulnerabilidad de condición de carrera (race condition).

Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.

6) De forma general podemos agrupar las amenazas en: amenazas físicas y amenazas lógicas.
Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por: las personas, programas específicos, catástrofes naturales.

Tipos de personas que pueden constituir una amenaza para el sistema informático:

- Personal de la propia organización.
- Ex-empleados.
- Curiosos.
- Crackers.
- Terroristas.

 Intrusos remunerados.

Podemos tener otros criterios de agrupación de las amenazas, como son:
Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc...
Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc...
Amenazas de agentes internos: Empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc.

7) Política de la Seguridad de la Información



La política de seguridad es la que establece las responsabilidades y reglas que se deben seguir para evitar las amenazas o minimizar los efectos por si se llegaran a producir. Esta se implementa mediante unos mecanismos seguridad que construyen las herramientas para la protección del sistema. Estos mecanismos se apoyan en normativas que cubren áreas más específicas.

Los mecanismos de seguridad se dividen en tres grupos:
Prevención: Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.
Detección: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema. Ejemplo: la herramienta DLP para la seguridad de los archivos.
Recuperación: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. Ejemplo: las copias de seguridad.

propósito en el manejo de la información: El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad

La empresa debe disponer de un documento formalmente elaborado sobre el tema y que debe ser divulgado entre todos los empleados.

No es necesario un gran nivel de detalle, pero tampoco ha de quedar como una declaración de intenciones. Lo más importante para que estas surtan efecto es lograr la concienciación, entendimiento y compromiso de todos los involucrados.

Cibergrafía

PDF, Universidad Piloto de Colombia. Calderón. Seguridad informática y seguridad de la información
Imagen, https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html

SEGURIDAD DE LA INFORMACION

INSTRUCTORA: KELLY HURTADO

APRENDICES:

DANIEL JARAMILLO ESPAÑA

KEVIN ALVARDO

ANGELA SILVA CAMPO

PROGRAMA: GESTION DE TALENTO HUMANO

POPAYAN-CAUCA

CONTENIDO

1.- Que diferencia entre la "La Seguridad de la Información y Seguridad de la Informática"

2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. ¿Qué otras bases proponen desde la investigación?

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información? Recuerde que estoy atenta a sus inquietudes. Éxitos en su aprendizaje.

1.- Que diferencia entre la "La Seguridad de la Información y Seguridad de la Informática"

¿QUE ES LA SEGURIDAD DE LA INFORMACION?

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos

Ejemplo: la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

¿QUE ES LA SEGURIDAD DE LA INFORMATICA?

Conjunto de métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que éstos almacenen.

Dentro de esta categoría, se puede mencionar la seguridad computacional, la cual se ciñe a la protección de los sistemas y equipos para el procesamiento de datos de una empresa

Ejemplo:

CIBERSEGURIDAD:

Conjunto de medidas de "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados

DIFERENCIAS

La **seguridad informática** atiende sólo a la protección de las instalaciones informáticas y de la información en medios digitales; mientras que la **seguridad de la información** integra toda la información independientemente del medio en el que esté.

Es decir la seguridad informática solo protege los que es la informática y todo lo relacionado con medios digitales; en cambio la seguridad de la información protege todo lo relacionado con la información sea digital o no.

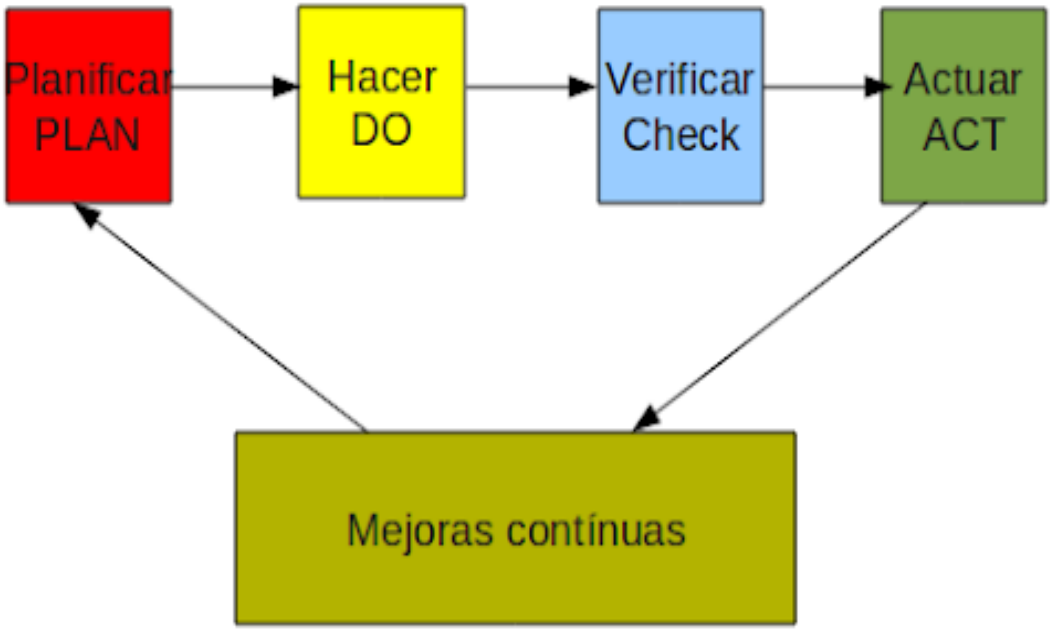
2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

La metodología PDCA tiene un carácter cíclico, que **garantiza la atención continua sobre la mejora de la calidad**. Después de la evaluación y aplicación de acciones correctivas, el proceso se reinicia. El modelo a menudo se usa a nivel organizacional, pero también se puede usar a nivel operativo.

El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.

Luego debe aplicarse el plan PDCA ('**PLAN – DO – CHECK – ACT'**) es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo. Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad.

Consiste en implementar el sistema de gestión de **seguridad** de la información, implementar el plan de riesgos e implementar los controles.


Planificar
PLAN
Hacer
DO
Verificar
Check
Actuar
ACT
Mejoras contínuas

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. ¿Qué otras bases proponen desde la investigación?



En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- **Confidencialidad**: Prevenir la divulgación no autorizada de la información.
- **Integridad**: Prevenir modificaciones no autorizadas de la información.
- **Disponibilidad**: Prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

La **seguridad informática**, también conocida como **ciberseguridad** o **seguridad de tecnología de la información**, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información.

La ciberseguridad comprende software (bases datos, metadatos, archivos), hardware, redes de computadoras, y todo lo que la organización entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas.

EJEMPLO:

Convirtiéndose así en información privilegiada.

restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores (confidencialidad, integridad y disponibilidad). No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador/root pueda acceder a él, ya que se está negando la disponibilidad.

¿QUE OTRAS BASES PROPONEN DESDE LA INVESTIGACION?

Desde la investigación aparte de las tres descritas anteriormente por la lectura estas también son importantes en una empresa. Las cuales son:

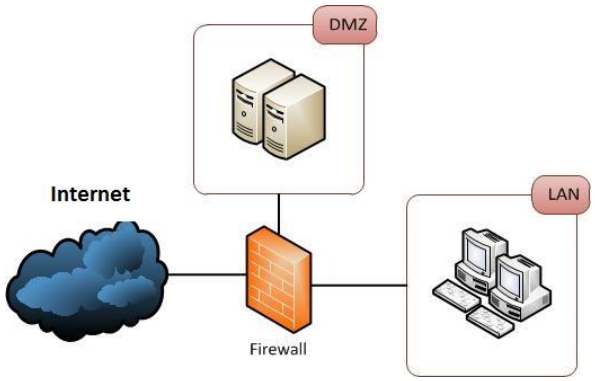
1. SOFTWARE ANTIVIRUS



En cualquier caso, todos los computadores conectados a la red -personales y corporativos- deben contar con un antivirus gratuito y confiable.

Este tipo de programas permite contar con medidas de protección efectivas ante la detección de malware u otros elementos maliciosos, por medio de ofrecer la posibilidad de eliminar las posibles amenazas o poner al dispositivo en estado de “cuarentena”.

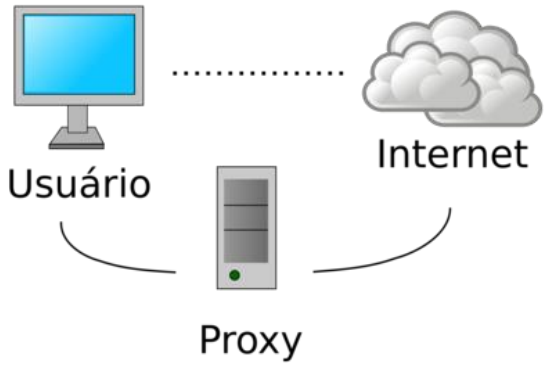
2. FIREWALL PERIMETRAL DE RED



Es una de las herramientas de ciberseguridad más recomendadas. Su funcionamiento es simple: escanea los paquetes de red, permitiéndolos o bloqueándolos según las reglas definidas por un administrador.

Si bien es cierto que su estructura es básica si se compara a la sofisticación de las amenazas, se pueden encontrar firewalls modernos que pueden clasificar los archivos utilizando varios parámetros. Así, se puede inspeccionar con eficiencia el tráfico web, identificar a usuarios, bloquear el acceso que no está autorizado, entre otras acciones.

3. SERVIDOR PROXY



Un proxy es un dispositivo o programa informático que actúa como intermediario entre las conexiones del navegador e Internet, filtrando todos los paquetes entre ambos.

Está catalogada como una de las buenas herramientas de seguridad informática debido a que, por medio de ella, se puede bloquear sitios web que se estimen como peligrosos o prohibidos dentro del ambiente laboral.

Por otro lado, permite establecer un sistema de autentificación, el cual limita el acceso a la red externa, permitiendo contar con registros sobre sitios, visitas, entre otros datos.

4. CIFRADO DE PUNTO FINAL



Es un proceso de codificación de datos para que no pueda ser leído o utilizado por nadie que no tenga la clave de descifrado correcta. En esencia, protege los

sistemas operativos de la instalación de archivos de arranque corruptos, bloqueando los archivos almacenados en computadores, servidores, entre otros puntos finales.

5. ESCÁNER DE VULNERABILIDADES



Es una de las herramientas de seguridad en sistemas informáticos fundamentales en las empresas de cualquier tamaño. Consiste en un software que se encarga de detectar, analizar y gestionar los puntos débiles del sistema.

Gracias a esta plataforma, se puede mantener controlada la exposición de los recursos empresariales a las amenazas de ciberseguridad y sus posibles consecuencias. Además, permite alertar en tiempo real, lo que ayuda a la solución de problemas de forma oportuna y sin comprometer la continuidad del negocio.

Es indispensable para cualquier empresa que no quiere arriesgar sus operaciones implementar las herramientas necesarias para fortalecer su infraestructura informática y así evitar riesgos que podrían involucrar la permanencia de la organización en el mercado.

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

RT/ Busca la integridad del usuario cuando quiere ingresar a la red la cual accede

A una base de datos.

Normalmente para ingresar al sistema informático se utiliza un usuario y una contraseña

También se pueden autenticar de tres maneras

- Por lo que uno sabe (una contraseña)
- Por lo que uno tiene (una tarjeta magnética)
- Por lo que uno es (las huellas digitales)

Dependiendo al nivel de conficialidad se puede aplicar las tres maneras mencionadas

Auditoria es continua vigilancia de los servicios en producción el cual recoge información para analizar este proceso permite a los administradores que validan los sistemas De verificación, cualquier tipo de ingreso fallido que violente el sistema de seguridad la almacenan en una base de datos.

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

RT/ Entendemos que vulnerabilidad como debilidad de cualquier tipo que ponga en peligro del sistema informático

puede haber varios tipos de vulnerabilidad.

Diseño

- Debilidad en el diseño de protocolos utilizando en las redes

- política de seguridad deficiente e inexistente

Implementación

-errores de programación

-existencia de "puerta trasera" en los sistemas informáticos

-descuido de los fabricantes

uso

-Mala configuración del sistema.

-Desconocimientos del usuario responsable del sistema.

vulnerabilidad de punto cero

-Son los que no tienen una solución conocida.

-Vulnerabilidad conocida: es el variable que cambia su estado y puede obtener un valor esperado

vulnerabilidad de Cross site scripting (xss)

-Son de la web que permite ingresar códigos vosript o javascript donde la victima cree que esta accediendo a URL

vulnerabilidad de denegación de servicio

-cuando un recurso no está disponible para algún usuario.

vulnerabilidad de ventana engañosa

-cuando te dicen que eres ganador de algo es falso.

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

RT/ En los sistemas de información tenemos dos tipos de amenazas físicas o lógicas

son provocadas por personas, programas específicos:

-Las personas atacantes pueden ser dos activos que el objetivo es hacer daño en el sistema y el pasivo solo curiosidad el sistema

- Lo pueden hacer empleados exempleados, curiosos, intrusos remunerados

- También tenemos las amenazas naturales como inundación incendio, explosiones además hay agentes externos sabotaje, terrorismo, intrusos en la red y robos

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información? Recuerde que estoy atenta a sus inquietudes. Éxitos en su aprendizaje

QUE ES:

Una política de seguridad en el ámbito de la criptografía de clave pública o PKI es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Pueden cubrir cualquier cosa desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio, hasta las directrices de seguridad de un país entero.

La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad.

Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos (véase referencias más adelante). Debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera.

PROPOSITO

El objetivo de las Políticas de Seguridad es fijar el marco de actuación necesario para proteger los resultados de las investigaciones de los Equipos de Trabajo, así como los recursos de información utilizados para su tratamiento y gestión, de amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

La eficacia y aplicación del Sistema de Gestión de la Seguridad de la Información es responsabilidad directa de la Gerencia, la cual es responsable de la aprobación, difusión y cumplimiento de la presente Política de Seguridad. En su nombre y representación se ha nombrado un responsable del Sistema de Gestión de la Seguridad de la Información, que posee la suficiente autoridad para desempeñar un papel activo en el Sistema de Gestión de la Seguridad de la Información, supervisando su implantación, desarrollo y mantenimiento.

La Gerencia procederá a desarrollar y aprobar la metodología de análisis de riesgos utilizada en el Sistema de Gestión de la Seguridad de la Información.

Toda persona cuya actividad pueda, directa o indirectamente, verse afectada por los requisitos del Sistema de Gestión de la Seguridad de la Información, está obligada al cumplimiento estricto de las Políticas de Seguridad.

En **FIDETIA** se implantarán todas las medidas necesarias para cumplir la legislación vigente, así como las normativas, licencias y cualquier otro condicionante en materia de seguridad de la información que resulten de aplicación.

La aplicación de controles, procedimientos y buenas prácticas en seguridad deberán permitir asegurar la confidencialidad, integridad, disponibilidad de la información, esenciales para:

Cumplir con la legislación vigente en materia de los sistemas de información.

Asegurar la confidencialidad de los datos gestionados por FIDETIA y sus equipos de trabajo incluidos en el alcance del SGSI.

Asegurar la disponibilidad de los sistemas de información, tanto en los servicios ofrecidos a los clientes como en la gestión interna.

Asegurar la capacidad de respuesta ante situaciones de emergencia, restableciendo el funcionamiento de los servicios críticos en el menor tiempo posible.

Evitar alteraciones indebidas en la información.

Promover la concienciación y formación en seguridad de la información.

SISTEMAS DE INFORMACIÒN

APRENDIZ

FLORALIA MORALES ORDOÑEZ

JORNADA: MIXTA

FICHA: 2254893

INSTRUCTORA

KELLY URTADO

CENTRO DE COMERCIO Y SERVICIO REGIONAL CAUCA

GESTIÒN DEL TALENTO HUMANO

POPAYAN CAUCA

2021

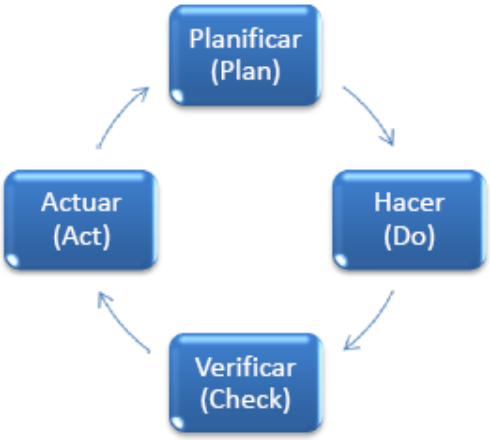
ACTIVIDAD

1.- Que diferencia entre la "La Seguridad de la Información y Seguridad de la Informática"

Seguridad de la información	Seguridad de la informática
conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de un sistema de información. • Ciberseguridad	conjunto de métodos, procesos y técnicas para la protección de los sistemas informáticos y la información en formato digital que estos almacenen. • Seguridad de hardware • Seguridad de software • Seguridad de red

2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

PDCA A ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo, también permite a las organizaciones controlar eficientemente sus procesos internos y externos, reduciendo así los errores y mejorando la toma de decisiones, esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua.



PLANIFICAR (Plan): consiste en establecer el contexto en el cual se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes

- **Confiabilidad:** Definimos la confiabilidad como la probabilidad de que un sistema se comporte tal y como se espera de él. En general, un sistema será seguro o confiable si podemos garantizar tres aspectos.



- **Disponibilidad:** En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.
  El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.



- **Confidencialidad**: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.
  El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.



- **Integridad**: la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado. El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.



¿Qué otras bases proponen desde la investigación?

- **Educar a los ciudadanos en ciberseguridad básica.** Podrían organizarse campañas de concienciación global para que los ciudadanos estén informados y ayuden a presionar a las entidades correspondientes para su implementación.

- **Reducir los costes globales del cibercrimen.** Que exista la posibilidad de iniciar procesos judiciales contra los cibercriminales para la recuperación de las pérdidas ocasionadas.

- **Concienciar al consumidor digital en seguridad.** Debería existir una 'ciber' entidad para educar a los ciudadanos a tomar precauciones frente a ciertas prácticas de riesgo

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

Autenticación: Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña).
2. Por lo que uno tiene (una tarjeta magnética).
3. Por lo que uno es (las huellas digitales).



Autorización: Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización. El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo.



Administración: establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema. Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema.



Mantenimiento de la integridad: conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no

autorizados y que la información enviada desde un punto llegue al destino inalterada.



5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero

- Cuando no exista una solución “conocida” para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como “vulnerabilidad 0 days”

Clasificación de Vulnerabilidades

Vulnerabilidades de desbordamiento de buffer.

Se produce cuando un programa no controla la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes.



Vulnerabilidades de condición de carrera (race condition).

La condición de carrera se da principalmente cuando varios procesos acceden al mismo tiempo a un recurso compartido.



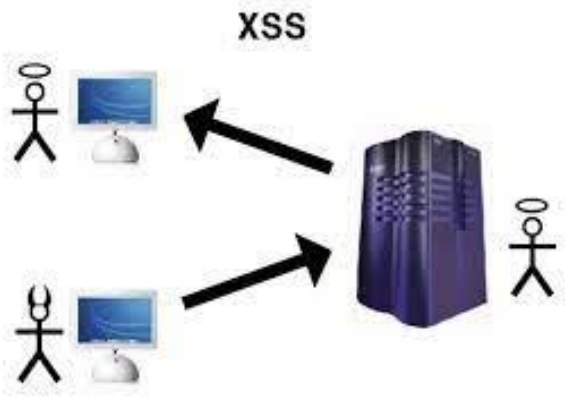
Vulnerabilidades de error de formato de cadena (format string bugs).

La principal causa de los errores de cadena de formato es aceptar sin validar la entrada de datos proporcionada por el usuario.



Vulnerabilidades de Cross Site Scripting (XSS).

Abarcaban cualquier ataque que permitiera ejecutar Estos errores se pueden encontrar en cualquier aplicación que tenga como objetivo final presentar la información en un navegador web.



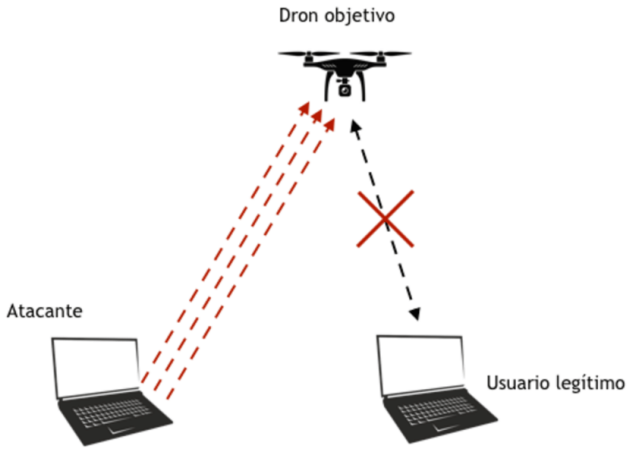
Vulnerabilidades de Inyección SQL.

se produce cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.ç



Vulnerabilidades de denegación del servicio.

La denegación de servicio provoca que un servicio o recurso sea inaccesible a los usuarios legítimos.



Vulnerabilidades de ventanas engañosas (Window Spoofing).

Las ventanas engañosas son aquellas que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que des información.



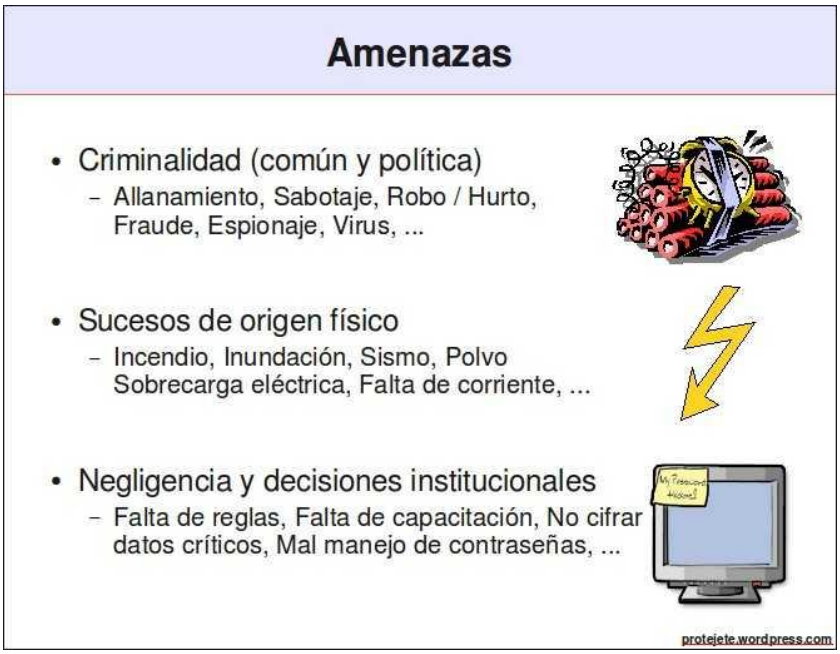
6.- Que tipo de amenazas se contemplan en los Sistema de Información?

De forma general podemos agrupar las amenazas en: amenazas físicas y amenazas lógicas, son materializadas básicamente por:

- Amenazas de personas, amenazas naturales, amenazas de agentes externos, amenazas de agentes internos

Amenazas físicas

Como su nombre indica que es la amenaza física afecta a la parte Física del ordenador es decir al Hardware.



Amenazas lógicas

Afecta a la parte lógica del sistema es decir a la parte que no se puede tocar del ordenador (software).



Personas

La mayor parte de los ataques a los sistemas informáticos son provocados, intencionadamente o no, por las personas.

Personal de la propia organización, Ex-empleados, Curiosos, Crackers, Terroristas, Intrusos remunerados.



Origen de las amenazas

Amenazas naturales

inundación, incendio, tormenta, fallo eléctrico, explosión, etc.



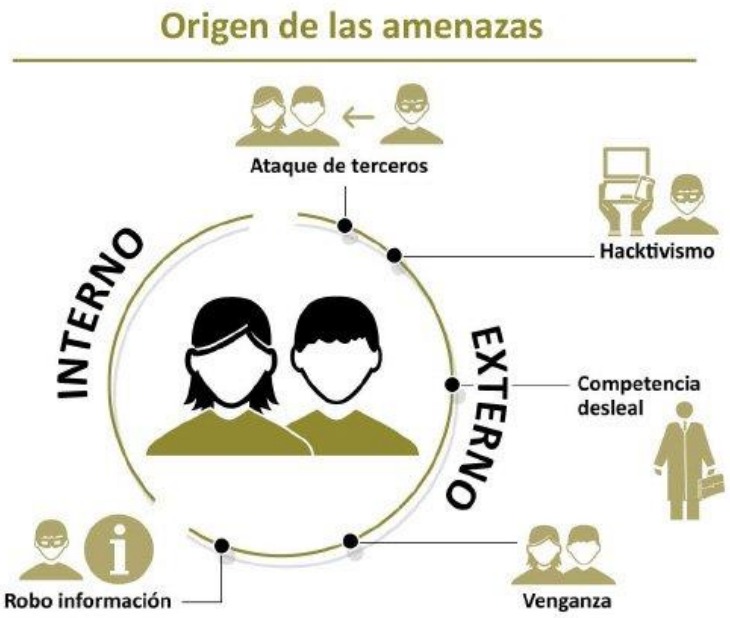
Amenazas de agentes externos

virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc.



Amenazas de agentes internos

empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc.



Intencionalidad de las amenazas

Accidentes: averías del hardware y fallos del software, incendio, inundación, etc.

Errores: errores de utilización, de explotación, de ejecución de procedimientos, etc.

Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc.

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información?

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y su propósito de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.

Los mecanismos de seguridad se dividen en tres grupos:

Prevención: Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

Detección: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema. Ejemplo: la herramienta DLP para la seguridad de los archivos.

Recuperación: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. Ejemplo: las copias de seguridad.

BIBLIOGRAFIA

https://www.esic.edu/rethink/tecnologia/tipos-de-seguridad-informatica-cuales-existen

https://virtual.itca.edu.sv/Mediadores/cms/u24_seguridad_de_la_informacin_modelo_pdca.html#:~:text=El%20nombre%20del%20Ciclo%20PDCA,Do%2C%20Check%2C%20Act%E2%80%9D.&text=HACER%20(Do)%3A%20consiste%20en,riesgos%20e%20implementar%20los%20controles

https://www.fundacionbankinter.org/blog/noticia/future-trends-forum/10-propuestas-para-mejorar-la-seguridad-informatica-

http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=5

SISTEMAS DE INFORMACION

TALLER No.3



INTEGRANTES:

CRISTHIAN CAMILO ARAQUE MITICANOY

SEBASTIAN SOLARTE DELGADO

MONICA ISABELLA QUIRA FERNANDEZ

ENTREGADO A:

KELLY HURTADO ROSAS

SENA CAUCA

GESTION DEL TALENTO HUMANO

FICHA: 2294893

POPAYAN

2021

1.-Que diferencia entre la "La Seguridad de la Información y Seguridad de la Informática"

Respuesta:

La seguridad de la información son las medidas y actividades que se colocan para proteger la información, que pueden ser conocimientos y datos que tienen valor para una organización, en diferentes formas y estados, reduciendo riesgos a un nivel aceptable, moderando las amenazas latentes.

A diferencia de la seguridad de la informática que es el conjunto de métodos, procesos o técnicas para la protección de los sistemas de información (redes e infraestructura) y la información en formato digital que se almacene.

Seguridad de la Información	Seguridad de la informática
• La información tiene una notable importancia para la empresa y por esta razón se debe proteger. • Conjunto de medidas técnicas, organizativas y legales que ayudan a la organización a asegurar la confidencialidad, integridad y disponibilidad de un sistema.	• La información importante de una organización que antes se almacenaba en papel. Gracias estos se puede digitalizar, reduciendo espacio y facilitando su análisis y procesamiento.

2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

Respuesta:

Es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras

Es un esquema para especificar y forzar políticas de seguridad, Un modelo de seguridad puede estar basado en un modelo formal de derechos de accesos, un modelo de computación, un modelo de computación distribuida o no estar basado en ninguna teoría particular.

3.-Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. ¿Qué otras bases proponen desde la investigación?

En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

Confidencialidad: hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos

- Objetivo de la confidencialidad: En general, cualquier empresa pública o privada y de cualquier ámbito de actuación, requiere que cierta información no sea accedida por diferentes motivos. Incluso en esta circunstancia existe un dato sensible que hay que proteger y es la clave de encriptación. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida.

-Integridad: Prevenir modificaciones no autorizadas de la información, En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado

-Objetivo de la integridad: Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

Confidencialidad: hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos

- Objetivo de la confidencialidad: En general, cualquier empresa pública o privada y de cualquier ámbito de actuación, requiere que cierta información no sea accedida por diferentes motivos. Incluso en esta circunstancia existe un dato sensible que hay que proteger y es la clave de encriptación. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida.

-Integridad: Prevenir modificaciones no autorizadas de la información, En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado

-Objetivo de la integridad: Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

4.-Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

Los mecanismos de seguridad se pueden clasificar en general en dos categorías:

a) Mecanismos de seguridad generalizados: se relacionan directamente con los niveles

de seguridad requeridos y algunos de estos mecanismos están relacionados al

manejo de la seguridad y permiten determinar el grado de seguridad del sistema ya

que se aplican a éste para cumplir la política general.

b) Mecanismos de seguridad específicos definen la implementación de servicios

concretos. Los más importantes son los siguientes: Confidencialidad, No repudio,

Integridad, Autenticación, Control de acceso y Disponibilidad

De manera particular, por las acciones que realizan se clasifican en:

a) Controles disuasivos: reducen la probabilidad de un ataque deliberado.

b) Controles preventivos: protegen vulnerabilidades y hacen que un ataque fracase o

reduzca su impacto.

c) Controles correctivos reducen el efecto de un ataque.

d) Controles detectores: descubren ataques y disparan controles preventivos o

correctivos.

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

Una vulnerabilidad de seguridad es una debilidad, falla o error que se encuentra dentro de un sistema de seguridad que tiene el potencial de ser aprovechado por un agente de amenaza para comprometer una red segura.

Hay una serie de vulnerabilidades de seguridad, pero algunos ejemplos comunes son:

Autenticación rota
Cuando las credenciales de autenticación se ven comprometidas, las sesiones de usuario y las identidades pueden ser secuestradas por actores maliciosos para hacerse pasar por el usuario original.

Inyección de SQL
Como una de las vulnerabilidades de seguridad más frecuentes, las inyecciones de SQL intentan obtener acceso al contenido de la base de datos a través de la inyección de código malicioso. Una inyección SQL exitosa puede permitir a los atacantes robar datos confidenciales, identidades falsas y participar en una colección de otras actividades dañinas.

Secuencias de comandos entre sitios
Al igual que una inyección SQL, un ataque de secuencias de comandos entre sitios (XSS) también inyecta código malicioso en un sitio web. Sin embargo, un ataque de secuencias de comandos entre sitios se dirige a los usuarios del sitio web, en lugar del sitio web en sí, lo que pone en riesgo la información confidencial del usuario.

Falsificación de solicitudes entre sitios
Un ataque de falsificación de solicitudes entre sitios (CSRF) tiene como objetivo engañar a un usuario autenticado para que realice una acción que no tiene la intención de hacer. Esto, junto con la ingeniería social, puede engañar a los usuarios para que accidentalmente proporcionen datos personales a un actor malicioso.

Configuración incorrecta de seguridad
Cualquier componente de un sistema de seguridad que los atacantes puedan aprovechar debido a un error de configuración puede considerarse una “Configuración incorrecta de seguridad”.

6.-Que tipo de amenazas se contemplan en los Sistema de Información?

Respuesta:

Se encuentran amenazas físicas y amenazas lógicas y son materializadas por las personas, programas específicos, catástrofes naturales.

- Amenazas provocadas por personas: estos pueden ser intencionales o no. Y se pueden clasificar a las personas en:
- Activos: su objetivo es hacer daño de cualquier forma como eliminando información, modificarla o sustraerla para su provecho.

Amenazas informáticas
Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas).

- Virus. Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente).
- Gusanos. Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo.
- Troyanos. Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.
- Ransomware. El ransomware se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).
- Keyloggers. Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.

7.-Que es Política de la Seguridad de la Información y cuáles su propósito en el manejo de la Información?

El SGC protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

La importancia de la seguridad informática de las empresas radica esencialmente en que la utilización maliciosa de sus sistemas de información privados y de los recursos internos puede acarrear desastrosas consecuencias en todas las áreas de la organización, deviniendo en problemas tanto productivos como financieros.

SENA

TALLER #3

TALLER DE SEGURIDAD INFORMATICA Y SEGURIDAD DE LA INFORMACION

PRESENTATDO POR: Aprendiz. Jessyca Alejandra Arteaga Ledesma

PRESENTADO A: Instructora. Kelly Hurtado

1. ¿Qué diferencia hay entre “la seguridad de la información y seguridad de la informática”?

Diferencias

Seguridad de la información	Seguridad de la informática
-También llamada seguridad de tecnologías de la información -Proteger los activos de información, entendiéndose éstos como los conocimientos o datos que tienen valor para una organización -Abarca tanto a la seguridad informática, como la ciberseguridad -Sistema de información (material informático o programas) de una organización, sean utilizados de manera correcta". -Se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o	-Disciplina que se encarga de llevar a cabo las soluciones técnicas de protección de la información -Métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que éstos almacenen -Soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa -Protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos

totales, cuando la información es el activo que se encuentra en riesgo -La seguridad de la información es la disciplina que se encarga de garantizar la: la confidencialidad, integridad y disponibilidad de la información -La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas	

2. En que consiste el modelo de seguridad PDCA, propuesto en la lectura

El nombre del Ciclo PDCA viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés “Plan, Do, Check, Act”. También es conocido como Ciclo de mejora continua.

Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales).

PLANIFICAR (Plan): consiste en establecer el contexto en el cual se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.
HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.
VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías

internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

3. ¿Cuáles son las bases de la seguridad informática planteadas en la lectura? Cree usted que son suficientes. ¿Que otras bases proponen desde la investigación?

Las bases de seguridad informática presentes en la lectura son:

- La confidencialidad: Prevenir la divulgación no autorizada de la información.
- Integridad: Prevenir modificaciones no autorizadas de la información
- Disponibilidad de la información: Prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

Estas bases son adecuadas para que quienes utilicen las diferentes bases de datos sientan confianza en que sus datos van a estar seguros y no disponibles para terceros.

4. Cuáles son los mecanismos básicos de la seguridad de la información

Los mecanismos básicos de la seguridad informática son:

- Autenticación
- Autorización
- Administración

5. ¿Qué entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del sistema para su comprensión?

El sistema informático busca proteger la información suministrada por quienes utilicen los diferentes sistemas de información y se reúnen en: hardware, software, datos; por lo tanto la seguridad informática busca la protección o la debilidad que comprometa estos 3 factores, agrupándose en funciones tales como: diseño, implementación, uso, vulnerabilidad del día cero, vulnerabilidades conocida,

vulnerabilidad de Cross site scripting, vulnerabilidad de denegación del servicio, vulnerabilidad de ventanas engañosas (Windows spoofing)

6. Que tipos de amenazas se contemplan en los sistemas de información

Los tipos de amenazas de los sistemas de información se agrupan en 4 categorías, las cuales son:

- Factores Humanos (accidentales, errores)
- Fallas en los sistemas de procesamiento de información
- Desastres naturales
- Actos maliciosos o malintencionados.

Las otras amenazas presentes en los sistemas de información son:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje

7. ¿Que es política de la seguridad de la información y cuál es su propósito en el manejo de la información?

Es en la que se establece las responsabilidades y reglas a seguir para evitar las amenazas o minimizar los efectos si se llegan a producir.

La política de seguridad se implementa mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema.

-Los mecanismos de seguridad se dividen en tres grupos: Prevención, Detección, Recuperación

- Dentro del grupo de mecanismos de prevención tenemos: Mecanismos de identificación e autenticación, Mecanismos de control de acceso, Mecanismos de separación, Mecanismos de seguridad en las comunicaciones,

Las políticas deben: Definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización.

-Definir la filosofía respecto al acceso a los datos.

-Establecer la base para poder diseñar normas y procedimientos referidos

Bibliografía

Grupo Atlas de Seguridad Integral. (ND de ND de ND). *Blog grupo atlas*. Obtenido de Diferencias entre seguridad informatica y seguridadd de la informacion: https://blog.atlas.com.co/seguridad-informatica-y-seguridad-informacion

Informatica, S. (ND de ND de ND). *Bases de la seguridad informatica*. Obtenido de Aula mentor: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/bases_de_la_seguridad_informtica.html#:~:text=Confidencialidad%3A%20Prevenir%20la%20divulgaci%C3%B3n%20no,controladas%20de%20los%20recursos%20inform%C3%A1ticos.

Lorena, C. A. (ND). *Seguridad informática y seguridad de la información.* Bogota: Universidad piloto de Colombia.

VIRTUAL ITCA. (ND de ND de ND). *U2.4 Seguridad de la Información Modelo PDCA*. Obtenido de VIRTUAL ITCA: https://virtual.itca.edu.sv/Mediadores/cms/u24_seguridad_de_la_informacin_modelo_pdca.html#:~:text=El%20nombre%20del%20Ciclo%20PDCA,Do%

2C%20Check%2C%20Act%E2%80%9D.&text=HACER%20(Do)%3A%20consiste%20en,riesgos%20e%20implementar%20los%20controles.

ACTIVIDADES EN CLASE

La Seguridad de la Información y Seguridad de la Informática

Nicole Gabriela Hoyos Arango
Anyi Vanesa Muñoz
Johana Andrea Damián González
Centro de Comercio y Servicios, SENA Popayán
2254893: Gestión del Talento Humano - Mañana
Kelly Hurtado

24 de Mayo de 2021

1.- Que diferencia entre la “La Seguridad de la Información y Seguridad de la Informática

La seguridad en su significado refiere a ausencia de peligro, de daño o de cualquier tipo de riesgo. Siendo realistas, deberían saber que esto no existe en un sentido total.

No existe el riesgo 0 en ningún aspecto de la vida en general. No por ello tenemos que tirarnos de los pelos, porque siempre se pueden tomar medidas de prevención para estar más seguros. Y ahí está la clave, en ser conscientes de que podemos estar más seguros, pero no seguros completamente. Como diría Helen Keller, «La vida es una aventura desafiante o nada en absoluto» y es así como tenemos que afrontarlo. Sin la posibilidad al fallo, no existe el logro. Igual que sin los riesgos no existe la seguridad.

Esto se acentúa en el medio on line, donde la evolución en sí pone en peligro. El ciberespacio supone una evolución, un paso más allá en el riesgo. La conectividad, el volcar toda la información y las tareas en él lo hace imprescindible, a la vez que, frágil. No solo lo hacen peligrar los ataques informáticos, sino, al ser un mundo virtual, cualquier hecho físico que amenace sistemas o datos.

Ahora bien, existen muchos tipos, o, mejor dicho, muchos ámbitos en los que estar seguros. En esta lectura, queremos centrarnos en dos: Seguridad informática y seguridad de la información.

Seguridad informática:

En la seguridad informática o ciberseguridad, su ámbito de actuación es toda la infraestructura de computación, es decir, sistemas de información interconectados como redes o dispositivos. Trata de proteger de ataques informáticos estas infraestructuras para así poder proteger la información. Pero hablamos en todo momento de un entorno digital.

Este entorno es muy complejo, ya que a cada segundo que pasa, se dan miles de ataques y amenazas. Es una lucha continua que no hay que descuidar por la seguridad de la información y de la empresa. Virus, malwares, phishing, spoofing, entre muchos otros son los métodos de ataque hace que se tenga especial interés en el tema.

Los motivos de estos ataques son miles, desde espionaje hasta suplantaciones de identidad, pero si destacara alguno de ellos sería el económico, sin duda alguna. Estos ataques comenzaron siendo meras bromas para los usuarios informáticos. Los hackers en un comienzo llamaban la atención una vez accedían a un ordenador con imágenes o pantallas emergentes que interrumpían la actividad. Querían que los afectados supieran que estaban ahí. Los primeros hackers eran gente curiosa que indagaba en la programación y querían que se viera lo que iban logrando. Esto evolucionó a un modo más incógnito en el que se accede o cifra la información de una empresa para poder

así reclamar un pago a cambio, por extorsión o por cualquier otro fin con un interés, al fin y al cabo. Es decir, se pasó de un mero «juego» a tener un objetivo beneficioso de algún modo u otro para el hacker.

¿Cómo se puede evitar un ataque? Con contraseñas con un fuerte nivel de seguridad, codificación de la información, herramientas y tecnologías protectoras, actualizar los equipos siempre en la última versión, permisos… También ayuda a mejorar la ciberseguridad de una empresa el Código de Derecho de la Ciberseguridad, recoge las principales normativas reguladoras del ciberespacio en España.

Seguridad de la información:

Este término incluye un campo más amplio. De tal forma que supone una protección para la información y datos de una empresa en cuanto **confidencialidad, integridad, autenticación y disponibilidad**. No es que ambos términos estén relacionados o tengan algo en común. Es que la ciberseguridad está englobada dentro del marco de la seguridad de información. Es decir, es una parte de ella. Una de las medidas que se adoptan para tener una seguridad de datos o información lo más completa posible.

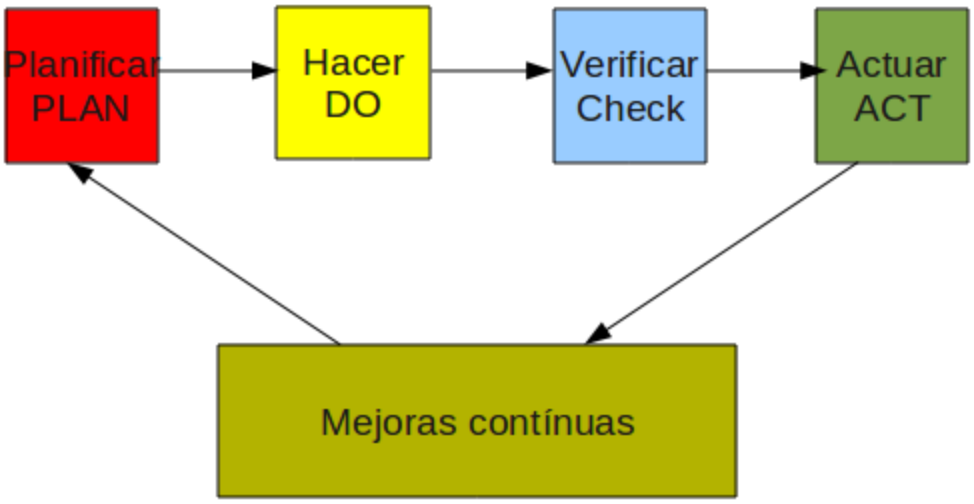
Mientras la seguridad informática se centra en los ataques de forma digital, la seguridad de la información abarca todos los riesgos posibles que puedan peligrar la información de forma digital o no. Desde pérdida de datos a sustracciones físicas de la información.

¿Cómo se puede evitar el riesgo en la información? Con VPN (Una conexión **VPN** (en inglés **Virtual Private Network**) es una tecnología de red que **sirve para** conectar una o más computadoras a una red privada utilizando como medio una red pública como internet, es decir, la Red Privada Virtual permite que estos dispositivos estén conectados entre sí a través de internet de una forma segura), copias de seguridad, firewall, planes de continuidad de negocios, cloud computing (El nuevo concepto de negocio en Internet también conocido como "computación en la nube"), protecciones de seguridad informática.

Mientras la preocupación se centra más en una protección ofensiva de su información, es decir, en la seguridad informática, descuidan otros aspectos de la seguridad de la información con el mismo peso y que pueden salvar de robos y pérdidas de datos. Es una forma global de defender la información para que pueda siempre estar disponible.

Fuente: https://gwc.global/seguridad-informatica-seguridad-informacion/

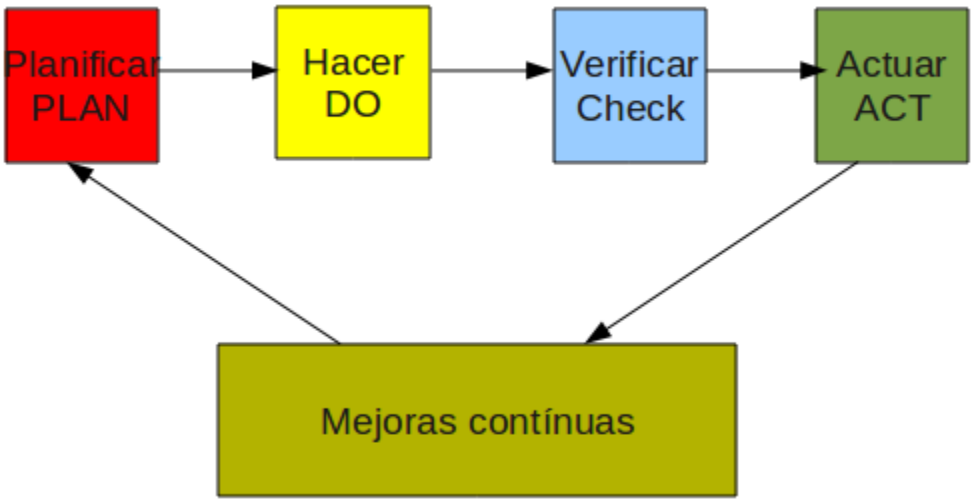
la seguridad de la información se basa en implementar S.G.S.I. es decir un SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION.





La seguridad informática: atiende sólo a la protección de las instalaciones informáticas y de la información en medios digitales mientras que la seguridad de la información integra toda la información independientemente del medio en el que esté.

2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?



En el área de calidad, el ciclo PDCA para la mejora continua, que ya cumple 81 años, ha demostrado ser una herramienta eficaz y aún actual, en el objetivo de alcanzar la conformidad con el requisito de mejora continua, no solo en Sistemas de Gestión de la Calidad, sino en otros basados en normas ISO.

La eficiencia del ciclo PDCA para la mejora continua, en la Gestión de la Calidad, en otros Sistemas ISO, o en la Gestión de Proyectos, han hecho de esta metodología la más popular para los profesionales en diferentes áreas.

Sin embargo, a pesar de formar parte de las tareas cotidianas en millones de organizaciones, y tal vez por su uso mecánico, aún existe un cierto grado de desconocimiento sobre los que es y cómo opera el ciclo PDCA para la mejora continua. Hoy hablaremos de ello: porqué se llama así, cuál es su origen, en que consiste y cómo funciona el ciclo PDCA para la mejora continua.

Ciclo PDCA para la mejora continua – Su origen

El ciclo PDCA, conocido también conocido como rueda de Deming, curiosamente no fue creado por el profesor William Edwards Deming, sino por el físico norteamericano Walter Andrew Shewhart en 1939.

Aunque el ciclo PDCA fue bautizado y popularizado apenas en la década del 50 del siglo pasado, por el profesor Deming, razón por la que esta metodología suele ser reconocida con el apellido de este gurú de la Gestión de la Calidad.

El clico PDCA es un acrónimo de cada uno de los pasos que comprende, por sus iniciales en inglés así: P (Plan), D (Do), C (Check), A (Action). En español, Planear, Hacer, Comprobar y Actuar (Ciclo PHVA).

¿En qué consiste el ciclo PDCA para la mejora continua?

La metodología PDCA tiene un carácter cíclico, que garantiza la atención continua sobre la mejora de la calidad. Después de la evaluación y aplicación de

acciones correctivas, el proceso se reinicia. El modelo a menudo se usa a nivel organizacional, pero también se puede usar a nivel operativo.

El ciclo PDCA permite a los profesionales evaluar su propio método de trabajo y mejorarlo cuando sea necesario. Debido a que el trabajo de un empleado forma parte de un proceso integral, los resultados del ciclo PDCA impactan positivamente a toda la organización.

El modelo, como ya lo advertimos, se **desarrolla** en cuatro etapas:

Plan

En esta etapa se identifican los problemas específicos que se pueden enfrentar en la ejecución de un proyecto, los recursos que se utilizarán, que recursos están disponibles y cuales tendrán que ser solicitados, los requisitos de las partes interesadas, las condiciones de ejecución, y los objetivos finales del proyecto.

Hacer

Una vez se ha encontrado la solución a un problema, o una nueva forma para optimizar un proceso, inicia la etapa de implementación en la práctica. Durante esta etapa se registra información relevante, sobre todo sobre los eventuales problemas que se presenten. Recordemos que lo que planeamos sobre el papel, no siempre se reproduce con fidelidad en la realidad.

Usualmente, este paso se desarrolla en dos etapas. Una en la que todo se hace en una escala de prueba, y otra en la que, de acuerdo con los resultados, se procede a una ejecución en escala real.

Verificar

En esta fase de verificación se miden y evalúan los resultados y se comparan con la expectativa planteada. En caso de grandes diferencias, es importante responder con prontitud y rastrear la causa.

Verificar los resultados es probablemente la fase más importante del ciclo PDCA. Se debe prestar suficiente atención para que los errores recurrentes no se presenten nuevamente y se produzca así una mejora evidente. Esta fase se caracteriza por la verificación activa y la evaluación de la efectividad del plan original.

Además, durante esta fase, el equipo del proyecto identifica áreas problemáticas del proyecto y toma la decisión de eliminar los riesgos o tomar acciones para mitigar el impacto en aras de una mejora continua.

Actuar

Finalmente, es posible tomar acciones correctivas -por lo general-, pero también de mejora cuando se detectan oportunidades, que se podrán aplicar en toda la organización. Si todo fue de acuerdo con el plan y los resultados son satisfactorios, no es necesario desviarse del curso original.

Pocas veces sucede así. Con buenos o deficientes resultados, tras la implementación de las acciones de mejora, el ciclo debe reiniciarse. Es en la continuidad de la metodología donde se encuentra su mayor fortaleza.

Ciclo PDCA para la mejora continua – Un ejemplo

Para comprender mejor el funcionamiento del ciclo PDCA, reproducimos un **ejemplo típico y usual**: el proceso de desarrollo de un nuevo producto en una organización.

Plan: planificar el desarrollo de nuevos productos y el proceso de producción.

Hacer: crear un prototipo, probarlo y recopilar datos del cliente.

Verificar: analizar los datos recopilados para medir la satisfacción del cliente.

Actuar: implementar el nuevo diseño desarrollado con base en la información recolectada e iniciar nuevamente el ciclo.

Cada vez que el ciclo se reinicie, se pueden definir nuevos objetivos. El ciclo se cumple para un proceso. No conviene reunir varios procesos en un mismo ciclo. Lo adecuado sería iniciar un ciclo para cada uno de los procesos o proyectos que sea necesario.

Un Sistema de Gestión de la Calidad, funciona de acuerdo con un ciclo PDCA, en el que la etapa final es la auditoría. Es esta el final del ciclo y el inicio de uno nuevo. De ahí la importancia de esta metodología y de los programas de formación que aseguren a la organización contar con profesionales idóneos, capacitados y certificados en la práctica de auditorías internas.

El programa Experto en Auditoría Interna ISO 9001:2015 SGC + Método de Auditorías Remotas de Sistemas de Gestión, reúne dos componentes esenciales en estos momentos de nueva normalidad: el conocimiento y las competencias para auditar un SGC basado en la norma ISO 9001, y la capacidad para hacerlo en forma remota, adoptando las mejores prácticas para esta actividad en estas condiciones.

Este es el momento para asumir el liderazgo en el área de calidad de tu organización. No esperes más. Inicia tu formación ahora.

Fuente: https://www.escuelaeuropeaexcelencia.com/2020/07/en-que-consiste-el-ciclo-pdca-para-la-mejora-continua/

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. ¿Qué otras bases proponen desde la investigación?

Confiabilidad:
Definimos la confiabilidad como la probabilidad de que un sistema se comporte tal y como se espera de él.
En general, un sistema será seguro o confiable si podemos garantizar tres aspectos, como se ve en la siguiente gráfica:



Figura No. 2 Seguridad de la información. Tomado de: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.
El objetivo: de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos más típicos es el de la inteligencia de un país. Además, es sabido que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Integridad: En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.
El objetivo: de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.
La integridad hace referencia a:
La integridad de los datos (el volumen de la información).
La integridad del origen (la fuente de los datos, llamada autenticación).

Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.
A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos.

Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.
En términos de seguridad informática “un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados”. Es decir, un sistema es disponible si permite no estar disponible.
Y un sistema 'no disponible' es tan malo como no tener sistema. No sirve.
Podemos decir que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.

OTRAS BASES DE SEGURIDAD INFORMATICA:

Llevamos ya casi un mes de 2019 y no parece que el panorama de la ciber seguridad sea muy halagüeño(Que da muestras o indicios de que una cosa tendrá éxito o causará satisfacción). En tan solo 3 semanas que llevamos de año se ha producido la filtración de datos más grande de la historia y una multa, también histórica, para Google por incumplimiento del Reglamento General de Protección de Datos.

Si quieres que tu empresa se mantenga a salvo de este 2019, no te pierdas los **10 principios** fundamentales de la seguridad informática que te contamos a continuación y que deben tenerse en cuenta cuando se quiere asegurar un negocio, ya que forman los pilares básicos de la ciberseguridad.

Aunque son difíciles de implementar en cualquier lugar y en cualquier momento, lo cierto es que deben tenerse en cuenta, ya que pueden ser de gran ayuda a lo hora de proteger los sistemas más preciados de una organización.

El privilegio mínimo:

Para hacer bien su trabajo, los seres humanos necesitan estar formados y entrenados, pero no necesita acceder a toda la información de la empresa. Son muchas las compañías que dan acceso a sus empleados a mucha más información de la que van a utilizar en su día a día. Esta práctica pone en peligro la información de la empresa de forma directa ya que, a mayor número de personas con acceso a los activos, mayor superficie de ataque (más empleados pueden hacer click en un mail infectado o acceder a una web indeseada y dar involuntariamente acceso a los cibercriminales a la información de la compañía).

En este sentido, este principio consiste en dar solo la información relevante y útil para que un usuario haga su trabajo. O lo que es lo mismo, evitar dar acceso a cualquier información inútil que pueda abrumar al usuario y causar un problema en la seguridad de los datos de la empresa.

Cerrado por defecto:

Esta norma está estrechamente ligada a la anterior. **Consiste en cerrar todos los accesos por defecto y abrirlos (para un usuario) solo cuando sea**

necesario. De manera que será el día a día de la empresa quien determine si hay que abrir una determinada puerta a X empleado o grupo de empleados. Se basa entonces en determinar lo que se necesita para abrir y así hacer un análisis de riesgo de forma que la empresa abre "sus puertas" a sabiendas.

Segregación de deberes:

La ética y deontología (Parte de la ética que trata de los deberes y principios que afectan a una profesión) debe ser clara en la seguridad de las empresas. Si se implementa correctamente, ayuda a reducir los conflictos de intereses. De hecho, es el pilar de la seguridad de una compañía: **todo el mundo debe saber qué hacer en caso de verse atacados y a quién se ha de acudir / quien ha de tomar las decisiones en ese supuesto.**

Defensa en profundidad:

Llevamos años diciendo que la superficie de ataque ha aumentado debido a la proliferación de objetos conectados y las nuevas formas de trabajo. Por ello, este principio hace hincapié en la **necesidad de colocar varias capas o niveles de seguridad de acuerdo con los riesgos asociados con los activos de la compañía**.

De esta manera el acceso a los bienes más sensibles requiere cruzar varios filtros de seguridad, mientras que los bienes "públicos" pueden ser gratuitos y, por tanto, el acceso a los datos clave de la compañía es más difícil ya que requiere superar otras capas de seguridad sin ser visto.

Lo diversificado y lo coherente:

La dependencia de una empresa de otras es una pérdida de poder. De hecho, es muy peligroso depender de un solo cliente o proveedor para asegurar su supervivencia, ya que el descontento de este último puede causar mucho daño. Del mismo modo, uno no debe atar su defensa completa a un solo producto.

No solo será más costoso, sino que, además, facilita el trabajo a un ciberatacante interesado en tomar el control de la empresa. Este principio va estrechamente ligado al anterior, cuantas más capas y más diversa sea la forma de secularizar los sistemas, más difícil será acceder a los activos de la empresa**. Por lo tanto, es necesario diversificar las defensas de manera coherente.**

Seguridad con sistemas simples y unitarios:

Todo lo que es complejo está perjudicando al negocio y por lo tanto a la seguridad de la empresa. De hecho, un mecanismo simple es puro, claro y quizás fácilmente seguro. Sin embargo, el negocio de hoy es cada vez más complejo, al igual que los servicios públicos. Por ello, **es necesario evitar la complejidad lo máximo posible para poder asegurar cada servicio correctamente**.

Transparencia con un sistema abierto:

La experiencia muestra que la seguridad es a menudo caótica. Por eso, cuando uno se basa en normas y estándares conocidos como ISO 2700x, OWASP, SOX, RGPD, etc., y tiene unos límites establecidos para cada rango o estamento en a la empresa, la seguridad es más sencilla y el acceso de una cibercriminal a los sistemas más complejo.

¿El eslabón más débil?:

Si de algo se habla en ciberseguridad es de cómo proteger los activos de una empresa de su eslabón más débil: **el empleado**. Pero ¿son los empleados realmente el eslabón más débil? si la respuesta es afirmativa, es la empresa la que debe sentirse culpable. Y es que, recordemos, los mayores errores que se comenten en ciber seguridad se basan en el desconocimiento o la falta de atención.

Si se forma adecuadamente a los empleados sobre qué hacer o qué no hacer en una determinada situación, no serán el eslabón más débil sino, quizás, el más fuerte ya que podrán dar la alarma en caso de ver algún comportamiento anómalo en sus dispositivos.

Auditoria regular:

¿Cómo asegurar que las medidas de defensa sean efectivas y eficientes? **Encontrando las fallas (y corregirlas) antes de que los malvados las conozcan y las aprovechen**. ¿Cómo podemos hacer esto? Sencillo: realizando estudio periódicos con los que podamos ser conscientes de los posibles peligros a los que se enfrentan los activos de nuestra compañía y cómo debemos protegerlos.

Estrategia clara:

Los ciberataques se han convertido ya en la principal amenaza para la supervivencia de las empresas y es por eso por lo que, para evitar entrar a formar parte de la lista de empresas que han cesado su actividad a causa de un ciberataque, **es vital contar con una estrategia clara a llevar a cabo ante un ataque de este tipo.**

Fuente: https://globbsecurity.com/estos-son-los-10-principios-fundamentales-de-la-seguridad-informatica-43955/

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos:

Es posible autenticarse de tres maneras:

1.Por lo que uno sabe, ejemplo: una contraseña
2. por lo que uno tiene: ejemplo una tarjeta magnética
3.por lo que uno es: ejemplo las huellas digitales

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Para la decisión de adoptar más de un método de autenticación por parte de las empresas debe estar en relación en valor a la información a proteger.

Autorización: el mecanismo o grado de autorización puede variar dependiendo de que sea lo que se está protegiendo, no toda la información de la organización es igual DE CRITICA, los recursos en general y los datos en particular se organizan en niveles y cada nivel de tener una autorización.

Administración: la administración de la seguridad informática dentro de la organización es una tarea en continuo cambio y evolución, ya que las tecnologías utilizadas cambian muy rápidamente y con ellas los riesgos

Auditoria y registro: este proceso permite a los administradores verificar que las técnicas de autorización y autenticación utilizadas se realicen según lo establecido y se cumplan los objetivos fijados por la organización.

Registro: auditar y registrar si no tiene sentido si no van acompañados de un estudio posterior monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos y como una periodicidad que dependerá de los critico que sea la información protegida y el nivel de riesgo.

Mantenimiento de la integridad: dentro de las técnicas mas utilizadas para mantener o controlar la integridad de los datos están: usos de antivirus, encriptación y funciones.

5. ¿Qué se entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema de compresión?

Vulnerabilidad

Debilidad de cualquier tipo que compromete la seguridad del sistema informático. Las vulnerabilidades de los sistemas informáticos (SI) las podemos agrupar en función de:

Diseño

1. Debilidad en el diseño de protocolos utilizados en las redes.
2. Políticas de seguridad deficientes e inexistentes.

Implementación:

1. Errores de programación.
2. Existencia de “puertas traseras” en los sistemas informáticos.
3. Descuido de los fabricantes.

Uso

1. Configuración inadecuada de los sistemas informáticos.

2. Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.

3. Disponibilidad de herramientas que facilitan los ataques.
4. Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero:

Cuando no exista una solución “conocida” para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como “vulnerabilidad 0 days”.

Globalmente clasificamos las vulnerabilidades en:

Vulnerabilidades de desbordamiento de buffer:

Se produce cuando un programa no controla la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Se puede aprovechar para ejecutar código que nos de privilegios de administrador.

Vulnerabilidades de condición de carrera (race condition):

La condición de carrera se da principalmente cuando varios procesos acceden al mismo tiempo a un recurso compartido, por ejemplo, una variable, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma.

Vulnerabilidades de error de formato de cadena (format string bugs).:

La principal causa de los errores de cadena de formato es aceptar sin validar la entrada de datos proporcionada por el usuario.
Es un error de programación y el lenguaje más afectado es C/C++. Un ataque puede conducir de manera inmediata a la ejecución de código arbitrario y a revelación de información.

Vulnerabilidades de Cross Site Scripting (XSS):

Abarcaban cualquier ataque que permitiera ejecutar scripts como VBScript o JavaScript, en el contexto de otro sitio web. Estos errores se pueden encontrar en cualquier aplicación que tenga como objetivo final presentar la información en un navegador web.

Un uso de esta vulnerabilidad es hacer phishing. La víctima ve en la barra de direcciones un sitio, pero realmente está en otro. La víctima introduce su contraseña y se la envía al atacante.

Vulnerabilidades de Inyección SQL.:

Una inyección SQL se produce cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el

funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.

Vulnerabilidades de denegación del servicio:

La denegación de servicio provoca que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

Vulnerabilidades de ventanas engañosas (Window Spoofing):

Las ventanas engañosas son aquellas que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que des información. Hay otro tipo de ventanas que, si las sigues, obtienen datos del ordenador para luego realizar un ataque.

Fuente:
http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

6. Que tipo de Amenazas se contemplan en los sistemas de información:

Amenazas de Malware:

Los programas maliciosos son una de las mayores ciberamenazas a la que se exponen las empresas. Dentro del malware existen distintos tipos de amenazas, siendo las principales.

Virus: Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente).

Gusanos:
Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo.

Troyanos: Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.

Ransomware: se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).

Keylogger:
Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.

Otras amenazas informáticas:

Existen muchas otras amenazas informáticas que afectan a las empresas como los ataques por Inyección SQL que afectan a servidores de bases de datos empresariales, red de equipos zombies (utilizando recursos de la empresa para actividades ilícitas), ataques MITM (man in the middle), etc.

Los ciberdelincuentes no descansan y siempre buscan nuevas formas de atacar, infectar y robar información de las empresas, por lo que la ciberseguridad debe ser una actividad flexible y dinámica que se adapte a las nuevas amenazas.

Las vulnerabilidades hacen susceptibles a las empresas de las amenazas informáticas. Eliminar vulnerabilidades será por lo tanto una de las principales acciones de la ciberseguridad para reducir las amenazas informáticas.

Existen muchos tipos de vulnerabilidades y amenazas informáticas, muchas de ellas provenientes del exterior como el malware o los ataques DDoS, y otras internas causadas por los propios usuarios o colaboradores de la empresa, como robos, accesos con privilegios incorrectos, o simplemente errores humanos.

Fuente: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Una metodología de implementar un sistema de seguridad está expuesta en la figura siguiente:



Fuente:
http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

7. ¿Qué es política de la seguridad de la información? ¿Y cuál es el propósito en el manejo de la información?

La implementación de un sistema de seguridad debe estar complementado con las políticas de seguridad.

La política de seguridad requiere no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino también establecer el origen de estas, que pueden ser internas o externas a la organización.

De nada valdría proteger la empresa de los usuarios del exterior si también existen amenazas internas. Por ejemplo, si un usuario utiliza un disquete que contiene un virus podría expandirlo a toda la intranet.

Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos". Los documentos de una política de seguridad deben ser dinámicos, es decir, ajustarse y mejorarse continuamente según los cambios que se presentan en los ambientes donde se crearon.

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una Empresa, y garantizando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización.

Las políticas de seguridad deben ser conocidos por todo el personal de una organización.

En el contenido de los documentos deben estar claramente establecidos: El objetivo, los responsables del cumplimiento, las medidas que se aplicarán en caso de incumplimiento.

Entre los documentos pueden citarse los siguientes:

Administración de usuarios que reglamentará el acceso a los recursos por el personal de la organización.

Copias de respaldo: Describirá los pasos a seguir para asegurar una adecuada recuperación de la información, a través de las copias de respaldo.

Tratamiento de la información: Definirá claramente los tipos de información que es manejada por las personas autorizadas dentro de la organización.

Software legal: Definirá claramente el uso de software en la Empresa con licencias de uso legal.

Uso del servicio de Internet y del correo electrónico: Describirá la protección de la información mediante el uso de correo electrónico y del servicio de Internet.

Ambientes de Procesamiento: Define el uso de los ambientes de procesamiento de información.

Seguridad en las comunicaciones: Describirá la protección de la información durante los procesos de transmisión y recepción de datos en las redes internas y externas.

Auditorías de los sistemas: Que permitirá hacer un control de los eventos de seguridad de los sistemas.

Continuidad del procesamiento: Se definirán y reglamentarán las actividades relativas a la recuperación de la información en casos críticos mediante una metodología adecuada.

Protección física: Definirá la protección física de los equipos, de procesamiento, almacenamiento y transmisión de la información.

Sanciones por incumplimientos: Este documento contemplará las medidas que se aplicarán por incumplimiento de las reglas definidas.

Manejo de Información (IM por su sigla en inglés) es la recolección y el manejo de la información de uno o más fuentes y la distribución de esa información a uno o más audiencias. Esto en algunos casos involucra a ellos quienes tienen un papel en la producción o un derecho sobre la información. Gerenciar significa la organización de y el control sobre la estructura, el procesamiento y el envío de la información.

Durante los años 70, este proceso fue enfocado principalmente a archivos físicos, el mantenimiento de estos archivos, y la Gerencia del Ciclo de Vida de la Información de archivos físicos, otros medios y registros. Con la difusión de la tecnología de la información empezando en los años 70, el trabajo del manejo de la información tomó un nuevo rumbo, empezando con el área de mantenimiento de datos. Ya no fue un trabajo sencillo que cualquier podría llevar a cabo. Un entender de la tecnología fue necesario, además de la teoría atrás. El almacenamiento de la información se reenfocó a medios electrónicos, volviendo el trabajo más técnico.

A finales de los años 90, cuando la información ya empezó a mover por redes de computadores, los gerentes de redes volvieron manejadores de la información. Estos individuos ya empezaron ser encargados de tareas de mayor complejidad, incluyendo manejos de equipos y software. Con las últimas herramientas disponibles, el manejo de la información ha vuelto un recurso poderoso y un gasto grande para muchas organizaciones.

En resumen, el manejo de la información involucra a la organización, recogida, adquisición y mantenimiento de la información. Está cercana a y cruce con la práctica de Manejo de Datos.

Fuente:
https://wiki.salahumanitaria.co/wiki/Manejo_de_Informaci%C3%B3n#:~:text=Manejo%20de%20Informaci%C3%B3n%20(IM%20por,a%20uno%20o%20m%C3%A1s%20audiencias.&text=Gerenciar%20significa%20la%20organizaci%C3%B3n%20de,el%20env%C3%ADo%20de%20la%20informaci%C3%B3n.

TALLER

Integrantes: Anyi Vanessa Chito Anacona

Andrés Felipe Gaviria Obando

Johana Marcela Velarde Meneses

Programa: Gestión de Talento Humano

Instructora: Leny Kelly

Ficha: 2254893

1. **Qué diferencia entre la “La Seguridad de la Información y Seguridad de la Informática”.**

Seguridad de la información

Esta requiere dedicarle tiempo y recursos. La organización debe plantearse un Sistema de Gestión de la seguridad de la Información (SGSI).

Esta seguridad de la información, tiene como objetivo aplicar tres áreas las cuales son ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo a repetir el ciclo para con esto lograr mejorar la seguridad.

Esta seguridad de la información integra toda la información independientemente del estado en el que se encuentre.

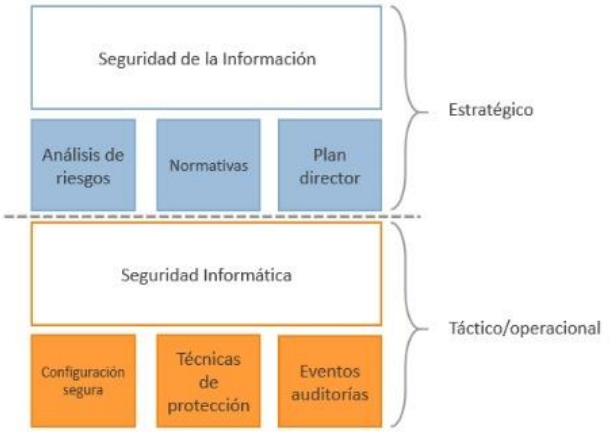
La seguridad de la información es la línea estratégica de la seguridad.

Seguridad de la informática

Esta seguridad en la informática se enfoca en tres aspectos; Confidencialidad, integridad y disponibilidad.

Estos tres aspectos tienen como objetivo proteger y prevenir la divulgación no autorizada de la información y esta seguridad informática se enfoca en la protección de infraestructura (redes, sistemas operativos, ordenadores.

La seguridad informática se describe como la distinción táctica y operacional de la seguridad



2. ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

El modelo PDCA consiste en tres aspectos para mejorar la seguridad de la información, estos aspectos son; ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

a este se le conoce como el proceso que nunca termina ya que los riesgos nunca se eliminan o al menos no en su totalidad.

Cada uno de estos aspectos tiene una función las cuales son:

Planificar (Plan): Consiste en establecer en contexto en el que se crean las políticas de seguridad, se hace el análisis de riesgos, la selección de controles y el análisis de aplicabilidad

Hacer (Do): Consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos y controles.

Verificar (Check): consiste en monitorear las actividades y hacer auditorías internas.

Actuar (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

3. ¿Cuáles son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que es suficiente. ¿Qué otras bases proponen desde la investigación?



Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

Integridad: En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

4. Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos.

Es posible autenticarse de tres maneras:

Disponibilidad: Aseso a la información de acuerdo con la privacidad

Confidencialidad: Solo es para personas autorizadas

Integridad: Se protege frente a los errores humanos

1. Por los que uno sabe (contraseña)
2. Por lo que uno tiene (Tarjeras magnética)
3. Por lo que uno es (huellas dactilares)

Debemos estar actualizando porque esto nos puede proteger la información de nuestros registros, aunque eso depende de cada empresa ya cual sea los documentos o información a proteger.

Se dice que la contraseña es un método bueno de proteger la información pero debe ser larga puesto que así será difícil de adivinarla, además debe ser combinada con mayúsculas o números.

5. Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del ¿Sistema para su comprensión?

Yo entiendo que la vulnerabilidad del sistema informático es más un riegos que tomamos en el momento que usamos para guardar documentos importantes ya que pueden ser vulnerables si no se tiene un buen respaldo de protección.

Se consideran características propias de los sistemas

Los podemos agrupar de la siguiente manera:

Diseño

- Debilidad en los protocolos de utilización en las redes.

- Políticas de seguridad deficiente e inexistente.

Implementación

- Errores de programación.

- Existencia de puertas traseras en los sistemas de informáticos.

- Descuido de fabricantes.

USO

- configuración inadecuada de los sistemas informáticos.

Desconocimientos y falta de sensibilización de los usuarios y de los responsables de informática.

- Falta de disponibilidad de herramientas que facilitan los ataques.

- Limitación gubernamental de tecnologías de seguridad.

6. Qué tipo de amenazas se contemplan en los Sistema de Información?

Una amenaza se refiere a circunstancias o eventos de seguridad cibernética que le pueden causar daños a una organización. Unas amenas.

Virus: Los virus son programas que tienen las características de replicarse y programarse por si mismo. Toma el control o modifica programas pero es casi siempre ejecutable.

Gusanos: Los gusanos pueden colapsar los ordenadores, los servidores y la red, acaparando recursos , consumiendo ancho de banda y provocando serios problemas de rendimiento

Troyanos: habitualmente entra en el equipo o dispositivo aprovechando la descarga de soflware legitimo.(ojo a la descarga de programas) siempre debes tener mucho cuidado con la palabra GRATIS casi siempre lleva algo escondido.

Adwere: El adwere se puede ver aparentemente inofensivo, pero es el encargado de bajarle el rendimiento de los trabajadores que necesitan navegar

por internet para realizar sus tareas.(son las ventanas o anuncios que aparecen en un lado de la pantalla)

7. Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información.

Su propósito es proteger el sistema informático.

La política de seguridad es la que establece las responsabilidades y reglas que se deben seguir para evitar las amenazas o minimizar los efectos por si se llegaran a producir.

Esta se implementa mediante unos mecanismos de seguridad que construyen las herramientas para la protección del sistema. Estos mecanismos se apoyan en normativas que cubren áreas más específicas.

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL

TALLER No. 3 – SISTEMAS DE INFORMACION.

PRESENTADO POR:
SARA CASTRO
LAURA GUZMAN

Tecnólogo Gestión del talento humano
Ficha 2254893

POPAYAN
SENA
2021

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL

ACTIVIDADES DE APROPIACION DEL CONOCIMIENTO (Conceptualización):

Instrucciones:

1.- Trabajo en grupo.
2.-Con base en lo visto en clase, y mediante la lectura entregada sobre “La Seguridad de la Información y Seguridad de la Informática” .
3.- Conceptualice los siguientes

Actividad 1

1.- Que diferencia entre la “La Seguridad de la Información y Seguridad de la Informática”

Primero que todo hay que definir los dos siguientes términos.

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 un sistema de información.
Y la **seguridad informática** es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema **informático**.
Dos diferencias son las siguientes:

- La seguridad informática atiende sólo a la protección de las instalaciones informáticas y de la información en medios digitales mientras que la seguridad de la información integra toda la información independientemente del medio en el que esté.
- La diferencia más significativa entre estos dos términos se da en que la seguridad informática se refiere a la forma tradicional de asegurar activos relacionados con la infraestructura y tecnología que administra o gestiona la información de una organización, básicamente este tipo de seguridad hace referencia al área de IT de una compañía la cuales es encargada de perseverar equipos de cómputo, manteniendo el software y hardware actualizados con el fin de cumplir con los pilares de la información, y la seguridad de información se refiere en la actualidad a un concepto mucho más amplio , ya que no solo tiene en cuenta la parte técnica, sino que compromete a toda la organización desde las altas gerencias , hasta el personal que realiza la operativa.

2.- En que consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

PLANIFICAR (Plan): consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.
HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.
VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.
ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de

mejora, acciones preventivas y acciones correctivas.

Al aplicarse el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo. Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad

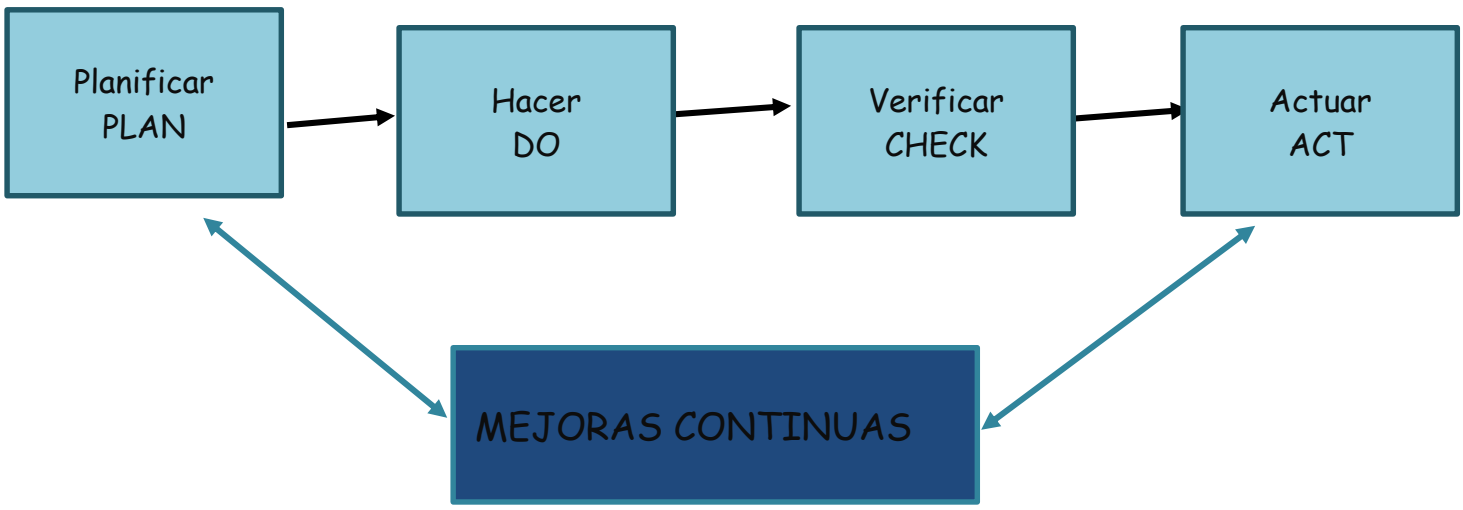
3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura?

Cree usted que son suficientes. Que otras bases propone desde la investigación?

Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. Prevenir la divulgación no autorizada de la información

Integridad: En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado. Prevenir modificaciones no autorizadas de la información.

Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. Prevenir interrupciones no autorizadas/controladas de los recursos informáticos



También pudimos averiguar otras bases o mecanismos de la seguridad

Informática que son las siguientes;

- **Prevención**:

Evitan desviaciones respecto a la política de seguridad.

Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

- **Detección**:

Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.

Ejemplo: la herramienta Snort para la detección de intrusiones de red.

- **Recuperación**:

Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

Ejemplo: las copias de seguridad.

Dentro de este grupo de mecanismos hay un subgrupo llamado **mecanismos de análisis forense** cuyo objetivo es, no solo devolver el sistema a su situación normal, sino averiguar también el alcance de la violación, lo que ha hecho el intruso en el sistema y qué puerta ha utilizado para entrar en el sistema. De esta forma se previenen posibles ataques posteriores.

De estos tres grupos de mecanismos es importante enfocarnos en los de prevención y detección. Siempre será mucho menos lesivo y comprometedor para el sistema informático evitar un ataque o detectar un intento de violación que no aplicar medidas de recuperación por muy buenas y seguras que sean.

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos.

En primer lugar Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña)
2. Por lo que uno tiene (una tarjeta magnética)
3. Por lo que uno es (las huellas digitales)

Y los mecanismos de seguridad se dividen en tres grupos.

- Autorización.

Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.
El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.
Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente.
En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos.
Por otra parte, solo se dará la autorización a acceder a un recurso a aquellos usuarios que lo requieran para la realización de su trabajo, y si no se le negará.

- Administración

Establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema. Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema

- Mecanismos de control de acceso.

Los objetos del sistema deben estar protegidos mediante mecanismos de acceso que establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema.
El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización. Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

Según lo que entendemos, es que la vulnerabilidad del sistema informático es aquel que se ve en riesgo en múltiples ocasiones o Una vulnerabilidad de seguridad es una debilidad, falla o error que se encuentra dentro de un sistema de seguridad que tiene el potencial de ser aprovechado por un agente de amenaza para comprometer una red segura. Un gran ejemplo sería; donde se despliegan ventanas engañosas, o mensajes de texto falsos que dicen que eres el ganador de

un carro o de mil millones de pesos y lo cual todo es falso, una mentira, además piden datos personales, los cuales no debemos dar, y esto es un estado del vulnerabilidad que se compromete con la seguridad.

Y en un sistema informático, se busca proteger los recursos que forman parte del sistema, entre ellos están Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

• Debilidad en el diseño de protocolos utilizados en las redes. • Políticas de seguridad deficiente e inexistente. Implementación • Errores de programación. • Existencia de “puertas traseras” en los sistemas informáticos. • Descuido de los fabricantes. Uso • Mala configuración de los sistemas informáticos. • Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.

• Disponibilidad de herramientas que facilitan los ataques.

• Limitación gubernamental de tecnologías de seguridad.

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

Se encuentran amenazas, tanto físicas como lógicas, son materializadas básicamente por: las personas, programas específicos, catástrofes naturales.
En general lo que se busca es conseguir un nivel de privilegio
en el sistema que les permita realizar acciones sobre el sistema no autorizadas.
Podemos clasificar las personas 'atacantes' en dos grupos:
Activos: su objetivo es hacer daño de alguna forma.
Eliminar información, modificar o sustraerla para su provecho.
Pasivos: su objetivo es curiosear en el sistema.

Tipos de personas que pueden constituir una amenaza para el sistema informático:
Personal de la propia organización.
Ex-empleados.
Curiosos.
Crackers.

Terroristas.
Intrusos remunerados

- **Amenazas informáticas**

Se entiende como amenaza informática toda aquella acción que aprovecha una

vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas).

- Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión.
- Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas.
- Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc.Intencionalidad de las amenazas
- Accidentes: averías del hardware y fallos del software, incendio, inundación,
- Errores: errores de utilización, de explotación, de ejecución de procedimientos.
- Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión.

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de lainformación?

Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan.

Y su propósito en el manejo de la informática es la recolección y el manejo de la información de uno o más fuentes y la distribución de esa información a uno o más audiencias. El almacenimiento de la información se reenfocó a medios electrónicos, volviendo el trabajo más técnico

Recuerde que estoy atenta a sus

inquietudes. Éxitos en su aprendizaje.

Elaboro: Lenny Kelly Hurtado R
Instructora de Gestion Documental Centro de Comercio y Servicios SENA Regional Cauca Lkhurtado0@misena

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL

TALLER No. 3 – SISTEMAS DE INFORMACION.

ANGIE TATIANA FLOREZ SANCHEZ.

PRESENTADO A:

NELLY KELLY HURTADO

FICHA:

2254893

SENA.

GESTIÓN DEL TALENTO HUMANO.

POPAYÁN.

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL
TALLER No. 3 – SISTEMAS DE INFORMACION.

ACTIVIDADES DE APROPIACION DEL CONOCIMIENTO (Conceptualización):

Instrucciones:

1.- Trabajo en grupo .

2.-Con base en lo visto en clase, y mediante la lectura entregada sobre "La Seguridad de la Información y Seguridad de la Informática" .

3.- Conceptualice los siguientes términos:

Descripción Actividad 1

1.- Que diferencia entre la "La Seguridad de la Información y Seguridad de la Informática"

2.- En que consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. Que otras bases propone desde la investigación?

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la informacion?.

Recuerde que estoy atenta a sus inquietudes.

Éxitos en su aprendizaje.

Elaboro:
Lenny Kelly Hurtado R.
Instructora de Gestion Documental
Centro de Comercio y Servicios
SENA Regional Cauca
Lkhurtado0@misena.edu.co

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL

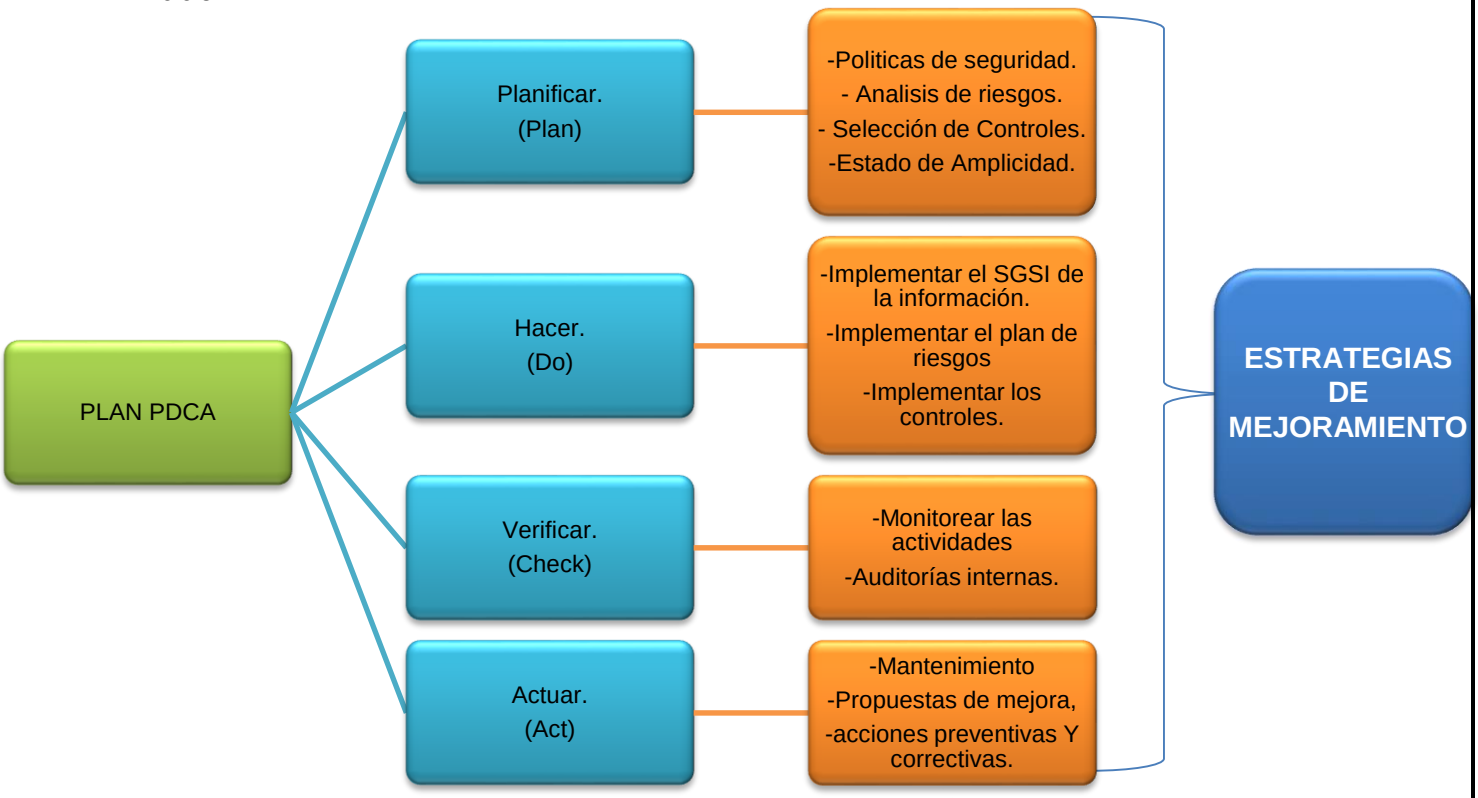
DESARROLLO.

1. **DIFERENCIAS.**

SEGURIDAD DE LA INFORMACIÓN.	SEGURIDAD DE LA INFORMATICA.
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 un sistema de información.	La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene.
Pueden estar involucradas otras propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio.	Área de la informática que consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización, sean utilizados de manera correcta.
Es habitual que la seguridad de la información se apoye en la política de seguridad que se desarrolla mediante la elaboración de un plan director de seguridad.	Implementa técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que-articulados con prácticas de gobierno de tecnología de información-establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.
Las medidas técnicas serán llevadas a cabo por el equipo de seguridad informática, administradores de sistemas y seguridad, los roles de seguridad.	Con el fin de establecer una evaluación de riesgos, se necesita realizar una evaluación a los activos, además de identificar cualquier amenaza que pueda aprovechar y explotar las vulnerabilidades de estos activos.
No solo al cuidado de la información, también a la mejora de los procesos de la empresa, agregando más medidas de seguridad como es la organización y las cuestiones legales.	

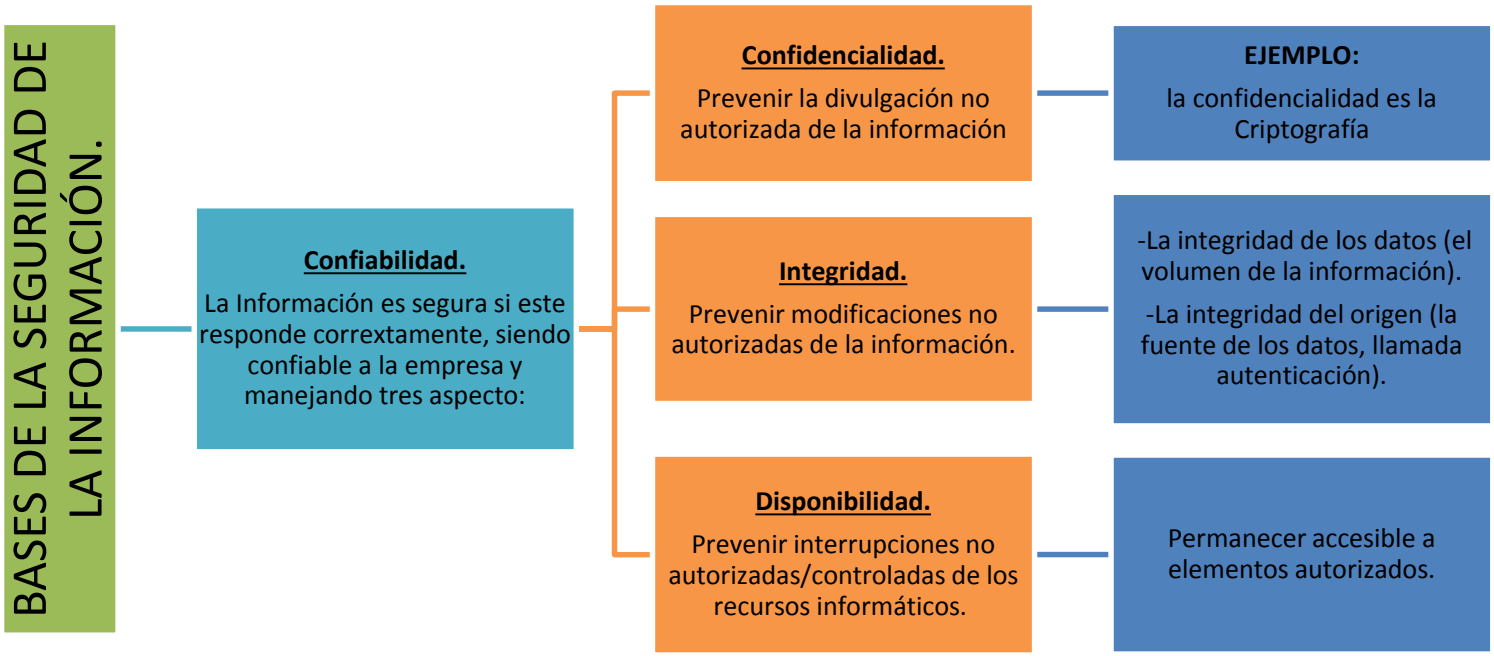
2. **Modelo de Seguridad PDCA.**

Debido a que la seguridad se entiende como un proceso que no tiene un final, puesto que se presentan riesgos que no se eliminan fácilmente o simplemente no llegan a ser eliminados. Frente a esta situación desde el Sistema de la Gestión la Seguridad de la Información se *aplica* el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.



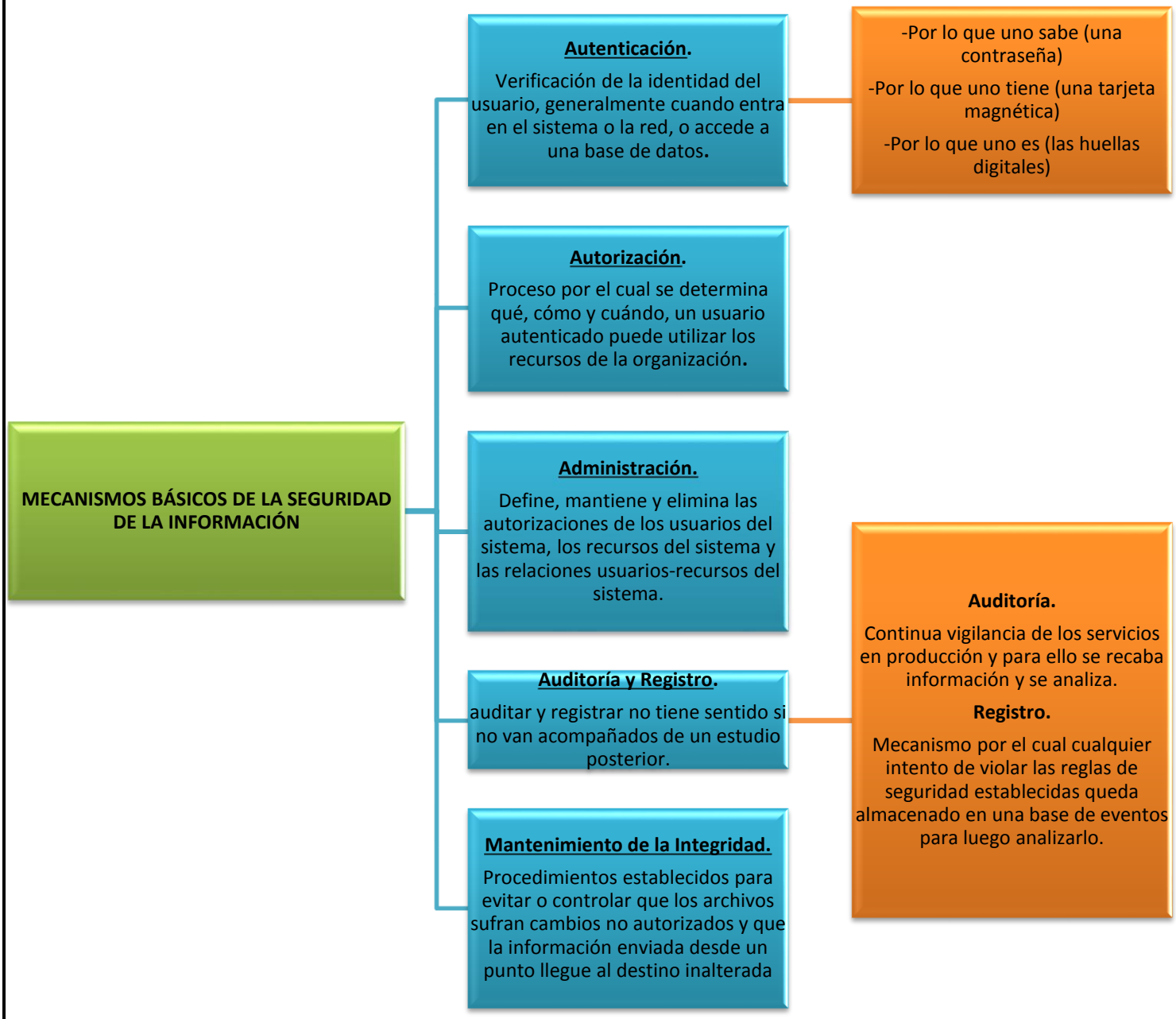
SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL

3. BASES DE LA SEGURIDAD DE LA INFORMACION.



SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL

4. MECANISMOS BÁSICOS DE LA SEGURIDAD DE LA INFORMACIÓN.



5. VULNERABILIDAD DEL SISTEMA INFORMÁTICO Y DE CÓMO SE AGRUPA

La vulnerabilidad de un sistema informático se presenta cuando se genera una debilidad en los "SI", es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software. De esta manera, cuando a un sistema informático se le detecta una vulnerabilidad y existe una amenaza asociada a la misma, puede ocurrir que el suceso o evento se produzca y el sistema estará en riesgo.

Agrupación de Vulnerabilidades.



Diseño.

Debilidad en el diseño de protocolos utilizados en las redes y políticas de seguridad deficiente e inexistente



Implementación.

Errores de programación, existencia de "puertas traseras" en los sistemas informáticos y descuido de los fabricantes.



Uso.

Mala configuración de los sistemas informáticos. Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática. Disponibilidad de herramientas que facilitan los ataques. Limitación gubernamental de tecnologías de seguridad.



Vulnerabilidad del día cero.

Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución "conocida", pero se sabe cómo explotarla.



Vulnerabilidades conocidas.

Vulnerabilidad de condición de carrera , es decir, que tiene una condición.



Vulnerabilidad de Cross Site Scripting (XSS)

Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBScript o JavaScript en páginas web vistas por el usuario.



Vulnerabilidad de denegación del servicio.

La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios.



***Vulnerabilidad de ventanas engañosas (Windows* Spoofing).**

Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, esto resulta ser un engaño para obtener información.

6. AMENAZAS

Las amenazas pueden ser físicas y lógicas, dependiendo de la causa que las active en el sistema de información, como son las personas, cuya clasificación se divide en ***activos*** (hace daño directamente eliminando, modificando o sustrayendo) y ***pasivos*** (cuyo propósito es curiosear en los datos), programas específicos, catástrofes naturales. Por otro lado, las amenazas también pueden agruparse en:

- Origen de las amenazas
    - **Amenazas naturales**: catástrofes creadas por la naturaleza, ejemplo: inundación, incendio.
    - **Amenazas de agentes externos**: ataques contra la organización o hackeo de seguridad, ejemplo, virus informáticos o disturbios y conflictos sociales,
    - **Amenazas de agentes internos**: personal inexperto haciendo una mala utilización de las herramientas de la información.
- Intencionalidad de las amenazas
    - **Accidentes**: averías del hardware y fallos del software.
    - **Errores**: errores de utilización y de ejecución de procedimientos.
    - **Actuaciones malintencionadas**: robos, fraudes, sabotajes, intentos de intrusión.

7. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.

Desde un análisis de prevención a las amenazas que puedan surgir, se establece una política de seguridad en la que se establezcan las responsabilidades y reglas, para evitar que estas mismas amenazas crezcan o se disminuyan. Por lo tanto, estas políticas deben definir qué es seguridad de la información y cuáles son sus objetivos principales, de la misma manera que su importancia dentro de la organización. También debe mostrar el compromiso de sus altos cargos con la misma entidad llegando a obtener la filosofía respecto al acceso a los datos. Así mismo se establecen las dichas responsabilidades inherentes al tema en discusión y la base para poder diseñar normas o procedimientos referidos a Organización de la seguridad. Se llega una clasificación y control de los datos, permitiendo la seguridad de las personas, seguridad física y ambiental. Para finalmente se obtenga un plan de contingencia que lleve a prevenir y detectar virus perjudiciales para el sistema de información.

Siguiendo en esta línea de creación e implementación de una política de seguridad, se disponen unos mecanismos de seguridad que se dividen en tres grupos:

- Prevención: Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.
- Detección: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.
- Recuperación: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
GESTION DOCUMENTAL

CYBERGRAFIA.

- Bases de la seguridad informática. Tomado de: **http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/bases_de_la_seguridad_informtica.html#:~:text=Fiabilidad%20se%20define%20como%20la,no%20autorizada%20de%20la%20informaci%C3%B3n**



SERVICIO NACIONAL DE APRENDIZAJE SENA

INSTRUCTORA: **KELLY HURTADO R.**

TALLER NO.3 SISTEMAS DE INFORMACION

APRENDIZES:

LUNA VALENTINA
DANIELA GONZALEZ
DAYANA REALPE

Ficha: 2254893

1.-Que diferencia entre “la seguridad de la información y seguridad de la informática”

cuando hablamos de seguridad de la información estamos indicando que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger. Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés de una organización se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores. Datos de los clientes o proveedores de la organización, o de los empleados quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesamiento.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesamiento.

Pero aparecen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca. Si es más fácil acceder a ella también es más fácil modificar su contenido, etc. Desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos.

Aumenta la sofisticación en el ataque y ello aumenta la complejidad de la solución, pero la esencia es la misma. 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 un sistema de información. Existen también diferentes definiciones del término Seguridad de la Información.

“La seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden estar involucradas otras propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio.”

2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

El objetivo es proteger la información y para ello lo primero que debe hacer es identificar los activos de la información que deben ser protegidos con un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica y por ese motivo nunca se eliminan de su totalidad la seguridad de la información siempre cumple cuatro niveles repetitivos que comienzan a planificar y terminan en actuar, consiguiendo así mejorar la seguridad como se identifica en la siguiente:

PLANIFICAR (Plan): consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

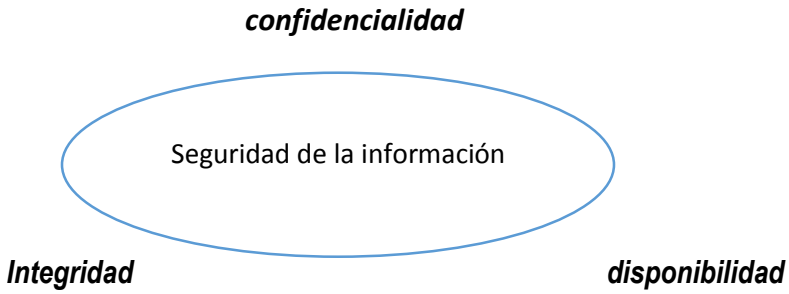
HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. ¿Qué otras bases propone desde la investigación?

Confiabilidad como la probalidad de que un sistema se comporte tal y como se espera en general que un sistema sea seguro o confiable si podemos garantizar tres aspectos



Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos más típicos es el de la inteligencia de un país. Además, es sabido que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.

La integridad: es importante del origen de la integridad ya que puede afectar su exactitud de crebilidad y confianza que las personas ponen en la información, a menudo ocurre que al hablar de la integridad de la información se da en estos dos aspectos

Un periodo difunde una información cuya fuente no es correcta podemos decir que no se mantiene la integridad de la información ya que se difunde por medio impreso, pero, sin embargo, al ser fuente de esa información errónea no se está manteniendo la integridad del origen ya que la fuente no es correcta

Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos. En términos de seguridad informática "un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados".

Es decir, un sistema es disponible si permite no estar disponible. Y un sistema 'no disponible' es tan malo como no tener sistema. No sirve. Podemos decir que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

Autenticación: Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos. Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña. Pero, cada vez más se están utilizando otras técnicas más seguras. Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña).

2. Por lo que uno tiene (una tarjeta magnética).

3. Por lo que uno es (las huellas digitales).

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger las técnica más usual de la autenticación es la contraseña entre sea mas grande y compleja para ser adivinada más difícil será burlar esta técnica adema la contraseña debe ser confidencial y debe ser difícil de adivinar por otro usuario variado de con minúsculas, mayúsculas, números, símbolos;

Autorización: en el cual se determina que como y cundo un usuario autenticando puede utilizar los recurso s de la organización dependiendo del recurso la autorización pueden variar de que se está protegiendo. no toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.

Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante de una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente, en el caso de los datos la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura

Por otra parte, solo debe dar autorización a aquellos usuarios que lo necesiten para hacer su trabajo; aunque también es posible dar autorizaciones transitorias o modificarlas a medida que las necesidades del usuario varíen

Administración: establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema. Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema. La administración de la seguridad informática dentro de la organización es una tarea en continuo cambio y evolución ya que las tecnologías utilizadas cambian muy rápidamente y con ellas los riesgos

Auditoria de registro: es continua vigilancia de los servicios en producción y para ello se recaba información y se analiza. El registro es el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo. Pero auditar y registrar no tiene sentido sino van acompañados de un estudio posterior en el que se analice la información recabada

Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos y con una periodicidad que dependerá de lo critica que sea la información protegida y de nivel de riesgo

Mantenimiento de integridad: conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada. Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos está: uso de antivirus, cifrado y funciones 'hash'.

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

Una vulnerabilidad en términos de informática es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

Por su parte, una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

Hardware: elementos físicos del sistema informático, tales como procesadores, cableado de red, medios de almacenamiento (cabinas, discos, cintas, USB, DVD,...).

Software: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones. Datos: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.

De ellos los más críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

Definimos Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático. Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

• Debilidad en el diseño de protocolos utilizados en las redes. • Políticas de seguridad deficiente e inexistente.

Implementación

• Errores de programación. • Existencia de “puertas traseras” en los sistemas informáticos. • Descuido de los fabricantes.

Uso

• Mala configuración de los sistemas informáticos. • Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática. • Disponibilidad de herramientas que facilitan los ataques. • Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero

- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución “conocida”, pero se sabe cómo explotarla.

Vulnerabilidades conocidas

- Vulnerabilidad de condición de carrera (rase condition).

Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.

- Vulnerabilidad de Cross Site Scripting (XSS).

Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBScript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.

- Vulnerabilidad de denegación del servicio. La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

- Vulnerabilidad de ventanas engañosas (Windows Spoofing).

Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

Amenazas físicas y Amenazas lógicas

Estas amenazas tanto físicas como lógicas son materializadas básicamente por la persona, programas específicos catástrofes naturales

Amenazas provocadas por personas: su objetivo es hacer daño de alguna forma. Eliminar información, modificar o sustraerla para su provecho su objetivo es curiosear en el sistema. Lo que busca es el privilegio que permita realizar acciones sobre el sistema no autorizados

Podemos clasificar las personas 'atacantes' en dos grupos:

- Activos: su objetivo es hacer daño de alguna forma. Eliminar información, modificar o sustraerla para su provecho.

- Pasivos: su objetivo es curiosear en el sistema.

Tipos de personas que pueden constituir una amenaza para el sistema informático:

- Personal de la propia organización.
- Exempleados.
- Curiosos.
- Crackers.
- Terroristas
- Intrusos remunerados.

Podemos tener otros criterios de agrupación de las amenazas, como son:

Origen de las amenazas Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc...

Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc...

Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc...

Intencionalidad de las amenazas Accidentes:

averías del hardware y fallos del software, incendio, inundación, etc...

Errores: errores de utilización, de explotación, de ejecución de procedimientos, etc...

Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc...

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información?

Lo primero que debemos de hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran. A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y La empresa debe disponer de un documento formalmente elaborado sobre el tema y que debe ser divulgado entre todos los empleados.

No es necesario un gran nivel de detalle, pero tampoco ha de quedar como una declaración de intenciones. Lo más importante para que estas surtan efecto es lograr la concienciación, entendimiento y compromiso de todos los involucrados.

Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Las políticas deben:

- Definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización.
- Mostrar el compromiso de sus altos cargos con la misma.
- Definir la filosofía respecto al acceso a los datos.
- Establecer responsabilidades inherentes al tema.
- Establecer la base para poder diseñar normas y procedimientos referidos a Organización de la seguridad.
- Clasificación y control de los datos.
- Seguridad de las personas.
- Seguridad física y ambiental.
- Plan de contingencia.
- Prevención y detección de virus.
- Administración de los computadores

a partir de las políticas se podrá comenzar a desarrollar primero las normas y luego los procedimientos de seguridad que serán la guía para la realización de las actividades. La política comprende todas las reglas de la seguridad que sigue organización, Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados.
- Un procedimiento para administrar las actualizaciones.
- Una estrategia de realización de copias de seguridad planificada adecuadamente.
- Un plan de recuperación luego de un incidente.
- Un sistema documentado actualizado

Por lo tanto, la política de seguridad es el documento de referencia que define los objetos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos

SERVICIO NACIONAL DE APRENDIZAJE SENA

CENTRO DE COMERCIO Y SERVICIOS

GESTION DOCUMENTAL

Aprendiz:

ESPERANZA SARRIA CONEJO

YULIETH VALENTINA PARRA RUIZ

LEIDY YEXUNY MOSQUERA GARCIA

JULIANA TARINE URREA SANCHEZ

INSTRUCTORA:
LENNY KELLY HURTADO

PROGRAMA GESTION DEL TALENTO HUMANO 2254893

POPAYAN - CAUCA

2021

TALLER No. 3 – SISTEMAS DE INFORMACION.

ACTIVIDADES DE APROPIACION DEL CONOCIMIENTO (Conceptualización):

Instrucciones:

1. Trabajo en grupo.
2. Con base en lo visto en clase, y mediante la lectura entregada sobre "La Seguridad de la Información y Seguridad de la Informática".
3. Conceptualice los siguientes términos:

Descripción Actividad 1

1. ¿Qué diferencia entre la "La Seguridad de la Información y Seguridad de la Informática"
2. ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?
3. ¿Cuáles son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. ¿Qué otras bases proponen desde la investigación?
4. ¿Cuáles son los mecanismos básicos de la Seguridad de la Información? Descríbalos
5. ¿Qué entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?
6. ¿Qué tipo de amenazas se contemplan en los Sistema de Información?
7. ¿Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información?

Desarrollo de actividad.

1.- ¿Qué diferencia entre la “La Seguridad de la Información y Seguridad de la Informática”?

- La diferencia más significativa entre estos dos términos se da en que la seguridad informática se refiere a la forma tradicional de asegurar activos relacionados con la infraestructura y tecnología que administra o gestiona la información de una organización. Básicamente este tipo de seguridad hace referencia al área de IT de una compañía la cuales la encargada de preservar equipos de cómputo, manteniendo el software y hardware actualizados con el fin de cumplir con los pilares de la información.

- La seguridad de información se refiere en la actualidad a un concepto mucho más amplio, ya que no solo tiene en cuenta la parte técnica, sino que compromete a toda la organización desde las altas gerencias, hasta el personal que realiza la parte operativa.

Seguridad de la información: Medidas y actividades que procuran proteger los activos de información, entendiéndose éstos como los conocimientos o datos que tienen valor para una organización, en sus diferentes formas y estados, a través de la reducción de riesgos a un nivel aceptable, mitigando las amenazas latentes.

Seguridad de la informática se refiere a la forma tradicional de asegurar activos relacionados con la infraestructura y tecnología que administra o gestiona la información de una organización. Básicamente este tipo de seguridad hace referencia al área de IT de una compañía la cuales la encargada de preservar equipos de cómputo, manteniendo el software y hardware actualizados con el fin de cumplir con los pilares de la información

2.- ¿En qué consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

Es un capítulo muy importante que requiere dedicarle tiempo y recursos. La organización debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI).

SGSI protege la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.

Al aplicar el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad. Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad.

PLANIFICAR (Plan): consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas. ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

3.- ¿Cuáles son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. ¿Qué otras bases proponen desde la investigación?

Las bases de la seguridad de información según la lectura son:

- **Integridad:** En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado su objetivo es, entonces, prevenir modificaciones no autorizadas de la información.

  La integridad hace referencia a:

  - La integridad de los datos (el volumen de la información).
  - La integridad del origen (la fuente de los datos, llamada autenticación).

La integridad del origen puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

- **Disponibilidad:** En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados su objetivo es prevenir interrupciones no autorizadas/controladas de los recursos informáticos. En términos de seguridad informática "un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados". Es decir, un sistema es disponible si permite no estar disponible.

  un sistema 'no disponible' es tan malo como no tener sistema. No sirve. Podemos decir que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.
- **Confidencialidad:** En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos su objetivo es prevenir la divulgación no autorizada de la información.

¿Qué otras bases proponen desde la investigación?:

Proponen algunos mecanismos básicos de seguridad los cuales son:

- **Autenticación:** Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos. Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña. Pero, cada vez más se están utilizando otras técnicas más seguras. Es posible autenticarse de tres maneras:
  1. Por lo que uno sabe (una contraseña).
  2. Por lo que uno tiene (una tarjeta magnética).
  3. Por lo que uno es (las huellas digitales).
- **Auditoría y registro:** la Auditoría es continua vigilancia de los servicios en producción y para ello se recaba información y se analiza. Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización.
- **Mantenimiento de la integridad:** conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada. Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos está: uso de antivirus, cifrado y funciones 'hash'.

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

Los mecanismos de seguridad se dividen en tres grupos:

Prevención: Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

Detección: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema. Ejemplo: la herramienta DLP para la seguridad de los archivos.

Recuperación: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. Ejemplo: las copias de seguridad.

Autorización: Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

Dentro del grupo de mecanismos de prevención tenemos:

Mecanismos de identificación e autenticación: Permiten identificar de forma única 'entidades' del sistema. El proceso siguiente es la autenticación, es decir, comprobar que la entidad es quien dice ser.

En concreto los sistemas de identificación y autenticación de los usuarios son los mecanismos más utilizados.

Mecanismos de control de acceso: Los objetos del sistema deben estar protegidos mediante mecanismos de control de acceso que establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema.

Mecanismos de separación: Si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos dentro de cada nivel.

Los mecanismos de separación, en función de cómo separan los objetos, se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación.

Mecanismos de seguridad en las comunicaciones: La protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante. Clásicamente se utilizan protocolos seguros, tipo SSH o Kerberos, que cifran el tráfico por la red.

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

Entiendo que la vulnerabilidad del sistema informativo es aquel que se ve en riesgo en múltiples ocasiones una de estas por ejemplo donde se despliegan ventanas engañosas como lo menciona en el texto, que son la que dicen que eres el ganador de tal o cual cosa, lo cual es una mentira y lo único que quieren que el usuario de su información , es algo grave por que piden demasiados datos personales ,por eso el estado de vulnerabilidad es aquella debilidad de cualquier tipo que compromete su seguridad.

En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en: Hardware: elementos físicos del sistema informático, tales como procesadores, cableado de red, medios de almacenamiento (cabinas, discos, cintas, usb, DVDs,...). Software: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones. Datos: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red. De ellos los más críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el

hardware y que son procesados por las aplicaciones software. Definimos Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

El sistema de información lo podemos agrupar en función de:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

Implementación

- Errores de programación.
- Existencia de "puertas traseras" en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad. Vulnerabilidad del día cero
- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución "conocida", pero se sabe cómo explotarla. Vulnerabilidades conocidas
- Vulnerabilidad de condición de carrera (race condition). Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.
- Vulnerabilidad de Cross Site Scripting (XSS). Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBSript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.
- Vulnerabilidad de denegación del servicio. La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda.

de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

- Vulnerabilidad de ventanas engañosas (Windows Spoofing). Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

Las amenazas la podemos definir en dos partes la cuales son: amenazas físicas y amenazas lógicas. Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por: las personas, o catástrofes naturales.

Podemos clasificar las personas 'atacantes' en dos grupos:

- Activos: su objetivo es hacer daño de alguna forma. Eliminar información, modificar o sustraerla para su provecho.
- Pasivos: su objetivo es curiosear en el sistema.

Tipos de personas que pueden constituir una amenaza:

- Personal de la propia organización.
- Ex-empleados.
- Curiosos.
- Terroristas.
- Intrusos remunerados.

También tenemos otras amenazas como la son las amenazas naturales, las cuales se pueden dar por: Inundación, incendio, tormenta, fallo eléctrico, explosión, etc.

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información?

Son las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran, su **propósito** es que la política de seguridad se implemente mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas más específicas.

Los mecanismos de seguridad se dividen en tres grupos:

Prevención: Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

Detección: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema. Ejemplo: la herramienta DLP para la seguridad de los archivos.

Recuperación: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. Ejemplo: las copias de seguridad. Dentro del grupo de mecanismos de prevención tenemos: Mecanismos de identificación e autenticación: Permiten identificar de forma única 'entidades' del sistema. El proceso siguiente es la autenticación, es decir, comprobar que la entidad es quien dice ser. En concreto los sistemas de identificación y autenticación de los usuarios son los mecanismos más utilizados.

Mecanismos de control de acceso: Los objetos del sistema deben estar protegidos mediante mecanismos de control de acceso que establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema. Mecanismos de separación: Si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos dentro de cada nivel. Los mecanismos de separación, en función de cómo separan los objetos, se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación. Mecanismos de seguridad en las comunicaciones: La protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante. Clásicamente se utilizan protocolos seguros, tipo SSH o Kerberos, que cifran el tráfico por la red.

Mecanismos de separación: Si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos dentro de cada nivel. Los mecanismos de separación, en función de cómo separan los objetos, se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación. Mecanismos de seguridad en las comunicaciones: La protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante. Clásicamente se utilizan protocolos seguros, tipo SSH o Kerberos, que cifran el tráfico por la red. El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.

El **objetivo** de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.

Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Las políticas deben:

- Definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización.
- Mostrar el compromiso de sus altos cargos con la misma.

- Definir la filosofía respecto al acceso a los datos.
- Establecer responsabilidades inherentes al tema.
- Establecer la base para poder diseñar normas y procedimientos referidos a Organización de la seguridad.
- Clasificación y control de los datos.
- Seguridad de las personas.
- Seguridad física y ambiental.
- Plan de contingencia.
- Prevención y detección de virus.
- Administración de los computadores.

A partir de las políticas se podrá comenzar a desarrollar, primero las normas, y luego los procedimientos de seguridad que serán la guía para la realización de las actividades. La política de seguridad comprende todas las reglas de seguridad que sigue una organización. Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema. La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concienciación. Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados.
- Un procedimiento para administrar las actualizaciones.
- Una estrategia de realización de copias de seguridad planificada adecuadamente.
- Un plan de recuperación luego de un incidente.
- Un sistema documentado actualizado.

La política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

Link de video complementario

https://www.youtube.com/watch?v=zV2sfyvfqik

Bibliografía.

http://polux.unipiloto.edu.co:8080/00002658.pdf.

TALLER No. 3 – SISTEMAS DE INFORMACION.

ACTIVIDADES DE APROPIACION DEL CONOCIMIENTO (Conceptualización):
Instrucciones:
1.- Trabajo en grupo.
2.-Con base en lo visto en clase, y mediante la lectura entregada sobre "La Seguridad de la
Información y Seguridad de la Informática" .
3.- Conceptualice los siguientes términos:
Descripción Actividad 1

1.- Que diferencia entre la "La Seguridad de la Información y Seguridad de la Informática"

La seguridad informática **protege el sistema informático**, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa.

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 un sistema de información.

La seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información

2.- En que consiste el Modelo de Seguridad PDCA, Propuesto en la lectura?

Es un proceso repetitivo el cual busca la mejora continua de la seguridad de la información; basada en el hacer, verificar y actuar y volver a repetir el ciclo, ya que los riesgos nunca terminan pero si se pueden gestionar.

3.- Cuales son las bases de la Seguridad Informática planteadas en la lectura? Cree usted que son suficientes. Que otras bases propone desde la investigación?

Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

Integridad: En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

4.- Cuales son los mecanismos básicos de la Seguridad de la Información. Descríbalos

Autenticación: Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

Autorización: Proceso por el cual se determina **qué, cómo y cuándo**, un usuario autenticado puede utilizar los recursos de la organización.

Administración: establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema. Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema.

5.-Que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del Sistema para su comprensión?

Definimos Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

AMENAZAS FÍSICAS

Como su nombre indica que es la amenaza física afecta a la parte Física del ordenador es decir al Hardware. Estas amenazas se pueden producir tanto de forma voluntaria e involuntaria, por ejemplo de ese tipo de amenazas sería como un cortocircuito, un incendio,un robo etc...

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos para proteger el hardware y medios de almacenamiento de datos. Cada sistema es único, por lo tanto la política de seguridad a implementar no sera única es por ello siempre se recomendara pautas de aplicación general y no procedimientos específicos.

AMENAZAS LÓGICAS

Afecta a la parte lógica del sistema es decir a la parte que no se puede tocar del ordenador (software).Este tipo de amenazas son más difíciles de prever y la mayoría no se pueden eliminar fácilmente hasta que no conozca la existencia del sistema.

Las amenazas Lógicas son más difíciles de reparar y causas mucho más daño que las amenazas Físicas y no influye sólo al funcionamiento del sistema informático si no que también se pueden perder fácilmente los datos del sistema.

Y las amenazas que considero más importante del tipo Lógicas son las siguiente:

- Virus
- Gusanos
- Troyanos
- Rootkits

https://sites.google.com/site/seguridadinformaticafpb/tipos-de-amenazas/11amenazasfisicasylogicas

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información?

Es un mecanismo de seguridad constituido por herramientas que brindan protección al sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas específicas.

Estos se dividen en tres grupos:

Prevención: Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

Detección: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema. Ejemplo: la herramienta DLP para la seguridad de los archivos.

Recuperación: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. Ejemplo: las copias de seguridad.

SEGURIDAD DE LA INFORMATICA Y SEGURIDAD DE LA INFORMACION

PRESENTADO POR:

DELIA MONTENEGRO

PRESENTADO A:

KELLY HURTADO

FICHA:

2254893

PROGRAMA:

GESTION DEL TALENTO HUMANO

POPAYAN: CAUCA/(2021)

SEGURIDA DE LA INFORMATICA Y SEGURIDAD DE LA INFORMACIÓN

1. Que diferencia hay entre la seguridad informática y la seguridad de información?
   Respuesta/ La seguridad informática atiende sólo a la protección de las instalaciones informáticas y de mucha información en medios digitales mientras que la seguridad de la informacion integra toda una
   información independientemente del medio en el que esté.

2. En que consiste el modelo PDCA propuesto en la lectura?
   Respuesta/es un punto muy importante que consiste en dedicarle tiempo El **ciclo PDCA** permite a las organizaciones controlar eficientemente sus procesos internos y externos, reduciendo así los errores y mejorando la toma de decisiones en cada una de las áreas. ... En español se le conoce como **ciclo** PHVA, que corresponde a sus respectivas traducciones: planificar, hacer, verificar y actuar.

3. Cuales son las bases de la seguridad informática planteadas en la lectura? Cree usted que son suficientes que otras bases propone desde la investigación?
   Respuesta/ son integridad confidencialidad y disponibilidad creo que si son suficiente por que estoa tres factores pueden mantener un buen equilibrio en la seguridad.

4. Cuales son los mecanismos basicos de la seguridad de la informacion describalos
   Respuesta/ Auditoría y registro: auditoría es continua vigilancia de los servicios en producción y Para ello se recaba información y se analizan. Este proceso permite a los

administradores verificar que las técnicas de autenticación y autorización utilizada se realicen según lo establecido y se cumplen los objetivos fijados.
Monitorear la información registrada auditiva se puede realizar mediante medios manuales o automáticos, y con una periodicidad que venderá de la crítica que sea la información protegida y del nivel de riesgo

Entendimiento de la integridad conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llega el destino inalterada. Seguido dentro de las técnicas más utilizadas para mantener o control controlar la integridad de los datos están: uso de antivirus, cifrado y funciones

5. Qué entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta estabilidad del sistema para comprensión?
   Respuesta/Una **vulnerabilidad** (en términos de **informática**) es una debilidad o fallo en un **sistema** de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, **por** lo que es necesario encontrarlas y eliminarlas.

6. Qué tipo de amenazas se en los sistemas de información?
   Respuesta/Podemos agrupar las amenazas en amenazas físicas y amenazas lógicas. Aparte esas amenazas tanto físicas como lógicas son materializadas básicamente por las personas programas específicos catástrofes naturales. Aparte amenazas provocadas por persona la mayor parte del ataque de los sistemas de información son provocados coma intencionalmente o no, por las personas reglas a seguir para evitar esas amenazas o minimizar los efectos se llegan a producir la política de seguridad se implementa mediante Una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Seguido esos mecanismos normalmente apoyan en normativas que cubren áreas más específicas.

7. Que es política de la seguridad de la información y cuál es su propósito en el manejo de la información?
   Respuesta/ La política de seguridad es donde se debe hacer un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran a partir de este análisis habrá que diseñar una política de seguridad en la que se establece las responsabilidades y la empresa debe disponer de un documento formalmente elaborado sobre el tema.

El propósito de políticas de seguridad fijar el marco de actuación necesario para proteger resultados de las investigaciones de los equipos de trabajo como así como los recursos de información utilizadas para su tratamiento y gestión, de amenazas internas o externas.

TALLER No.3

Fecha: lunes 10 de mayo

SISTEMAS DE INFORMACION

INSTRUCTURA:

Lenny Kelly Hurtado Rosas

APRENDICES:

Misshell Dayana Ávila torres

Carlos Daniel Guaca Vázquez

Junior Leandro Panesso Garzón

PROGRAMA:

Gestión De Talento Humano

FICHA

2254893

SISTEMAS DE INFORMACION

1. ¿Qué diferencia hay entre la "seguridad de la información y seguridad de la informática?

Es evidente la diferencia entre seguridad informática y seguridad de la información, pero también es indiscutible que ambos temas se encuentran muy ligados entre sí. A pesar de ser disciplinas diferentes, la una no puede ir sin la otra.

La seguridad **informática** atiendo solo a la protección de las instalaciones informáticas y de a información en medios digitales mientras que la seguridad de la **información** integra toda la información independientemente del medio en el que este.

La seguridad de la información para conseguir el objetivo se apoya de la seguridad informática, es decir la seguridad de la información será la encargada de regular y establecer las pautas a seguir para la protección de la información.

La seguridad de la información va más allá de la seguridad informática puesto que intenta proveer de medidas de seguridad a otros medios donde se localiza la información como:

- Impresos en papel
- Discos duros
- Medidas de seguridad respecto de las personas que las conocen

En conclusión, la seguridad informática se enfoca en la protección de (infraestructura, redes, sistemas operativos, ordenadores.)
L seguridad informática se encarga de la parte operativa de la seguridad, es decir, las medidas técnicas que aseguran la seguridad de la información.



2. ¿En qué consiste el modelo de seguridad PDCA, propuesto por la lectura??

El nombre del ciclo o modelo de seguridad **PDCA** proviene de las siglas en inglés (**P**=Plan, **D**=Do, **C**=Check, **A**=Act) que traducido al español significa (**Planificar, hacer, verificar, actuar**).

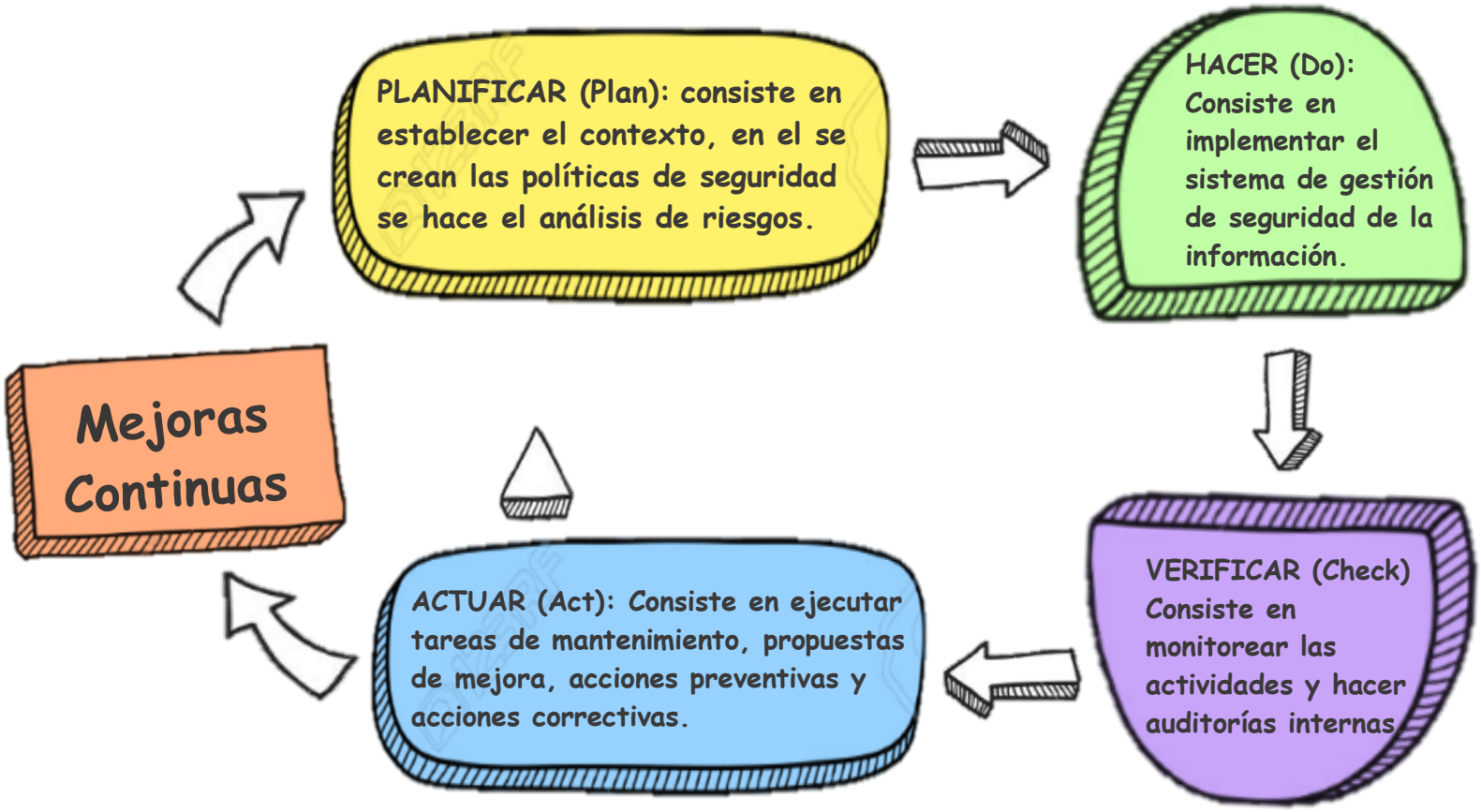
Esta metodología describe los cuatro pasos esenciales que se deben llevar en una forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuo de la calidad, (disminución de fallos, aumento de la eficacia y eficacia, solución de problemas, previsión y eliminación de riesgos potenciales…). El sistema de seguridad **PDCA** es un clico de vida continuo, lo cual quiere decir que la fase de Actuar lleva de nuevo a la fase de planifica para iniciar un nuevo ciclo de las **cuatro fases**, tomando en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, por ejemplo, puede haber actividades de implantación que ya se han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

Dentro de la organización el tema de la seguridad es un capítulo de la información muy importante que requiere dedicarle tiempo y recursos. La organización debe plantearse un Sistema de Gestión dela Seguridad de la Información.

El objetivo de un **SGSI** es protegerla información y para ello lo primero que debe hacer es identificar los “activos de información” que deben ser protegidos y en qué grado. Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar.

De los **riesgos** se desprende que los riesgos de seguridad no son únicamente de naturaleza tecnológica y por ese motivo nunca se eliminan en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por planificar y terminan en actuar como lo veremos en el siguiente gráfico.



"El único Sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de concreto, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él"

(Eugene Spafford)

3. ¿Cuáles son las bases de seguridad informática planteadas en la lectura? Cree usted que son suficientes.

En general, un sistema será seguro o fiable si podemos garantizar tres aspectos

Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

- **Objetivo:** *Prevenir la divulgación no autorizada de la información*

Integridad: En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, o normalmente se expresa a lo referente a prevenir el cambio impropio o desautorizado.

- **Objetivo:** Prevenir modificaciones no autorizadas de la información.

Disponibilidad: En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

- **Objetivo:** Prevenir las interrupciones no autorizadas/controladas de los recursos informáticos

¿Cree usted que son suficientes?

No, ya que el avance de la tecnología ha demostrado que todo esto ya no es suficiente y debemos protegernos de mucho más.

¿Qué otra base propone desde la investigación?

Seguridad de software: La seguridad se software se utiliza para proteger el software contra ataques malicioso de hackers y otros riesgos.

Seguridad de hardware: se puede relacionar con un dispositivo que se utiliza para escanear u sistema o controlar el tráfico de red.

4. ¿Cuáles son los mecanismos básicos de la seguridad de la información? Descríbelos

Autenticación: El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quien ellos dicen que ellos son – que el usuario que intenta realizar funciones en un sistema está autorizado para hacerlo.



Autorización: Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma. Podemos hablar de permisos en redes sociales como Instagram, Facebook, twitter, correos entre otro.



Administración: La administración lograr la exactitud, integridad y protección de todos los procesos y recursos de los sistemas de información. De este modo la administración de seguridad minimiza errores, fraudes y pérdidas en los sistemas de información que interconectan a las empresas actuales, así como a sus clientes, proveedores y otras partes interesadas.



Auditoría y registro: El propósito principal de la auditoría y control de recursos humanos es mostrar cómo está funcionado el programa, localizando prácticas y condiciones que son perjudiciales para la empresa o que no están justificando su costo, o prácticas y condiciones que deben incrementarse.



Mantenimiento de la integridad: Mantenimiento de la Integridad de los Sistemas de Información Es recomendable, por lo tanto, llevaron catálogo de peticiones de mantenimiento sobre los sistemas de información, en el que se registren una serie de datos que nos permitan disponer de la información antes mencionado, se debe mantener este orden claro al momento de cada procedimiento de actualización de algún dato que se vaya a realizar se debe mantener la integridad de los datos adquiridos que estos no vayan a ser difundidos.



5 .¿Qué entiende por vulnerabilidad del sistema informático?

las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones. Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene.

6. ¿Qué tipo de amenazas se contemplan en los sistemas de información?

La amenaza en un sistema de información puede abarcar la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. podemos agrupar las amenazas a la información en cuatro grandes categorías: Factores Humanos (accidentales, errores); Fallas en los sistemas de procesamiento de información; Desastres naturales y; Actos maliciosos o malintencionados; algunas de estas amenazas son:

❖ *Virus informático o código malicioso*



❖ *Uso no autorizado de sistemas informáticos*



❖ *Robo de información*



❖ *Suplantación de identidad*



❖ *Desastres naturales*



❖ *Espionaje*



❖ *Divulgación de información*



❖ *Denegación de Servicios (DoS)*



7. ¿Qué es política de la seguridad de la información? ¿cuál es el propósito en el manejo de información?

La protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones. Esta seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos todo enmarcado en el estricto cumplimiento de las leyes.

Taller: 3 Sistemas de información

Cristina Sotomayor

Talento humano

Instructora: Kelly hurtado.

Popayan: 24-Mayo 2021

① ¿Cual diferencia existe entre la seguridad de la información y seguridad informatica?

Rta

→ Seguridad de la información → Son aquellas medidas y actividades que prevean proteger las actividades de la información entendiendose estas como las de conocimientos o datos que tienen valor para una organización en sus diferentes formas y estados; atraves de la reducción de riesgos a un nivel aceptable, mitigando las amenazas latentes.

→ Seguridad informatica

- Conjunto de metodos, procesos, o técnicas para la protección de los sistemas informaticos (redes e infraestructura) y la información en formato digital que estos almacenan.
- Dentro de esta categoria se puede mencionar la seguridad Computacional, la cual se cine a la protección de los sistemas y de equipos para el procesamiento de datos de una empresa: por ejemplo:

CIBERSEGURIDAD → Conjunto de medidas de protección de activos de información, através del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

→ Algunas diferencias entre Seguridad de información y Seguridad informática.

• Seguridad de la información → Esta se orienta a proteger los activos de información sin importar su forma o estado, valiendose de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnologías y otras elementos, para la aplicación y gestión de las medidas de seguridad apropiadas en cada caso. Por tanto abarca tanto a la Seguridad informática como a Ciberseguridad.

• Seguridad de la informática → Esta se limita a proteger los activos de información en formato digital y los sistemas informáticos que los procesan y almacenan, indistintamente si estan interconectados o no.

• LA CIBERSEGURIDAD → Se orienta a proteger los activos de información en formato digital que circulan através de sistemas interconectados. A diferencia de la seguridad de la información, en la Ciberseguridad se aplican medidas ofensivas y no solo de defensa.

② En que consite el modelo de Seguridad PDCA propuesto en la lectura?

Rtar. Es una herramienta eficaz y a un actual, cuyo objetivo es la de alcanzar la conformidad con el requisito de mejora continua, no solo en sistemas de gestión de la calidad. Si no en otros basados en normas iso C

PDCA: Metodología que tiene un caracter ciclico, que garantiza la atención continua sobre la mejora de la calidad. Despues de la evaluación y aplicación de acciones correctivas, se reinicia. los procesos de mejora.

El modelo de PCDA se desarrolla en 4 etapas:

1 PLAN - Consitee en identificar los problemas especificos que se pueden presentar en la ejecusión de un proyecto, los recursos que se utilizarán, que recursos estan disponibles y cuales tendrán que ser solicitados a los requisitos de las partes interesadas.

② Hacer → En esta etapa una vez se ha encontrado la solución a un problema o una nueva forma para optimizar un proceso

③ Verificar → En esta etapa de verificación se miden y evaluan los resultados y se comparan con la expectativa plantada en caso de grandes

diferencias, es importante responder con prontitud y rastrear las causas del problema.

En esta fase de verificación de resultados es netamente importante el ciclo PDCA ya la cual debe estar suficiente atención para que los errores recurrentes no se presenten nuevamente y de esta manera se ejecuten mejoras evidentes para la organización.

④ Actuar – En esta etapa se toman acciones correctivas por lo general, pero también de esta misma manera detectando oportunidades que se podrían aplicar en toda la organización para su mejora de manera significativa.

→ El funcionamiento del ciclo PDCA se determina en 4 pasos.

- PLAN – Planificar el desarrollo de nuevos productos y el proceso de producción
- Hacer – Crear un prototipo, probarlo y recopilar datos del cliente.
- Verificar – Analizar los datos recopilados para medir la satisfacción del cliente.
- Actuar – Implementar un nuevo diseño desarrollado con base en la información recopilada y reiniciar nuevamente el ciclo.

(3) ¿ Cuales Son las bases de la Seguridad Informatica planteadas en la lectura ?

Rta La Seguridad de la Información Se basaen 4 pilares

- Disponibilidad → Acceso a la Información cuando Se requiere, teniendo encuenta la Privacidad. Evitando "caidas" en el Sistema que permitan Accesos ilegitimos, que limiten el acceso al Correo.

- Confidencialidad → Información accesible Solo para Personal autorizado. La Información No debe llegar a Personas o entidades que no esten autorizados.

- Integridad → Información Correcta Sin modificaciones no autorizadas por terceros. Se protege frente a vulnerabilidades externas o posibles errores humanos.

- Autenticación → La información procedente de un Usuario que es quien dice Ser. Se identifica y debe garantizar que el origen de los datos Sean correctos.

• Niveles de la seguridad informática

Rta: Nivel D
Nivel C2 Protección de acceso Controlado
Nivel C1 Protección discrecional
Nivel B3 Dominios de Seguridad
Nivel B2 Protección estructurada
Nivel B1 Seguridad etiquetada
Nivel A Protección Verificada.

④ ¿ Cuales son los mecanismos basicos de la Seguridad Informática

• Preventivos → Actuan antes de que un hecho ocurra y su función es de tener agentes no deseados.

• Detectivos → Actuan antes de que un hecho ocurra y su función es revelar la presentada de agentes no deseados en algún Componente del sistema. Se Caracterizan por emitir un aviso y registrar la incidencia

• Correctivos → Actuan luego del ocurrido el hecho, y su función es Corregir las consecuencias

⑥ ¿Que tipos de amenazas se contemplan en los sistemas de información?

Rta

Basicamente podemos agrupar las amenazas a la información en 4 grandes categorías.

- Factores humanos (accidentales, exprofesos) Fallas en los sistemas de procesamiento de información; Desastres naturales y/ otros maliciosos o malintencionados; algunas de estas amenazas son:

- Virus informáticos o código malicioso,
- Uso no autorizado de sistemas informáticos
- Robo de información
- Fraude basado en el uso de computadores
- Suplantación de identidad
- Denegación de servicios (DOS)
- Ataques de fuerza bruta;
- Alteración de la información
- Divulgación de información
- Desastres naturales
- Sabotaje, Vandalismo
- Espionaje.

⑦ ¿Que es política de la Seguridad? de la información?

Rta: Consiste en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan

- La definición de una política de seguridad debe estar basada en una identificación y análisis previos de los riesgos a los que esta expuesta la información

y debe incluir todos los procesos, Sistemas y Personal de la organización, teniendo encuenta dicha política debe haber sido aprobada por la dirección de la organización y Comunicada a todo el personal

-¿Cual es el proposito principal de la política de Infamación?

Rta Protcger el recurso Información de una amplia gama de amenazas, con el Fin de asegurar la continuidad del negocio, minimizando daños y cumplir mision y objetivos estrategicos de la organización.

-¿Caracteristicas de una politica de seguridad de la Información?

Rta:

- Deben de poder ser implementadas a través de determinados procedimientos administrativos y la publicacion de unas vias de uso.
- Debe definir Claramente las responsabilidades erigidas al personal Con acceso al Sistema (técnicos, analistas usuarios Finales..)
- Debe cumplir Con las exigencias de su entorno legal LOPD (Ley Organica de protección de datos.
- Se tiene que revisar de Forma Periodica para poder adaptarlos a las nuevas exigencias

Un plan de Seguridad nunca es estatico, es dinamico.

PRESENTADO POR: LAURA KATHERINE GAONA
DAYANA MARIANA HURTADO

PRESENTADO A: INSTRUCTORA KELLY HURTADO

GESTIÓN DE TALENTO HUMANO

TALLER.3 GESTION DOCUMENTAL

1 Que diferencia entre la "la seguridad de la información y seguridad de la informática"

Encontramos diferencias como: la seguridad de información se centra a la protección de los activos de información fundamentales para el éxito de cualquier organización y la seguridad informática: se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan nuestro negocio. En la seguridad de la información también busca proteger y mantener la confidencialidad, disponibilidad en la integridad de la misma. Otra diferencia es que la seguridad informática se observan leyes, protocolos y herramientas para minimizar los posibles riesgos de ella y del control de la información manejada por la computadora

2.- en que consiste el modelo de seguridad pdca, propuesto en la lectura?

La organización debe plantearse un sistema de gestión de la seguridad de la información. El objetivo de un (sgsi) es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.
Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan se podrían identificar de la siguiente manera:

Planificar (plan): consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.
Hacer (do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.
Verificar (check): consiste en monitorear las actividades y hacer auditorías internas.
Actuar (act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

3. Cuáles son las bases de la seguridad informática planteadas en la lectura? cree usted que son:

Confidencialidad: hacer referencia a la necesidad de ocultar a mantener secreto sobre determinada información o recursos y así prevenir la divulgación no autorizada de la información.
Integridad: se centra a la fidelidad de la información o recursos y así no permitir modificaciones no autorizadas de la información. Utilizando contraseñas la cual debe ser confidencial.
Autorización: proceso por el cual se determina que y que usuario puede utilizar los recursos de la organización
Administración: los administradores son responsable de transformar políticas de la organización y monitorear.
Disponibilidad: en términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.
Objetivo: de la disponibilidad, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.
En términos de seguridad informática un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados. Es decir, un sistema es disponible si permite no estar disponible.
Y un sistema 'no disponible' es tan malo como no tener sistema. No sirve.
Pensamos que cada uno de ellos van ligados cumpliendo una función muy importante para la seguridad. Aunque en casos dependiendo de la organización uno se implementa más que otro. Ofreciendo confianza para no causar problema tanto en los clientes como los que la componen.

4.- cuales son los mecanismos básicos de la seguridad de la información. Descríbalos

La seguridad de la información, como concepto, se basa en **cuatro pilares**: la disponibilidad, la integridad, la confidencialidad y la autenticación.

- **disponibilidad**: acceso a la información cuando se requiere, teniendo en cuenta la privacidad. evitar “caídas” del sistema que permitan accesos ilegítimos, que impidan el acceso al correo…
- **confidencialidad**: información accesible solo para personal autorizado. la información no debe llegar a personas o entidades que no estén autorizados.
- **integridad**: información correcta sin modificaciones no autorizadas ni errores. se protege frente a vulnerabilidades externas o posibles errores humanos.
- **autenticación**: información procedente de un usuario que es quien dice ser. se verifica y se debe garantizar que el origen de los datos es correcto.

5.-que entiende por vulnerabilidad del sistema informático y de cómo se agrupa esta debilidad del sistema para su comprensión?

Una vulnerabilidad, es una debilidad o fallo en un sistema información que pone en riesgo la seguridad de la información permitiendo que un atacante pueda comprometer la integridad de la misma

Se puede agrupar en:

Diseño: puede estar las políticas de la seguridad deficiente

Implementación: errores de programación, descuido de los fabricantes

Uso: mala configuración de los sistemas informáticos

Vulnerabilidad del día cero: son las cuales no existen una solución " conocido " pero se sabe cómo explotarla

Vulnerabilidades conocidas: son varios procesos que acceden al mismo tiempo y se produce este tipo de vulnerabilidad

6.- Que tipo de amenazas se contemplan en los Sistema de Información?

Se pueden agrupar las amenazas como: amenazas físicas y amenazas lógicas. Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por: las personas, programas específicos, catástrofes naturales. Amenazas provocadas por personas La mayor parte de los ataques a los sistemas informáticos son provocados, intencionadamente o no, por las personas.

Otras amenazas:

Amenazas: Para conseguir un sistema de información seguro y confiable se establecen una serie de estándares, protocolos, métodos, reglas y técnicas. Sin embargo, existen amenazas que deben tenerse en cuenta:

Usuarios: Se considera la causa del mayor problema ligado a la seguridad de un sistema informático. Es así porque con sus acciones podrían ocasionar graves consecuencias.

Programas maliciosos: Conocidos como malware son destinados a perjudicar un ordenador cuando se instala o hacer uso ilícito de datos. Suelen ser un virus informático, un troyano o un spyware.

Errores de programación: Más que un peligro, se trata de un mal desarrollo. Pero también se tiene que ver como un riesgo evitando que los sistemas operativos y aplicaciones estén sin actualizar.

Intrusos: Cuando personas que no están autorizadas acceden a programas o datos que no deberían, como es el caso de los hackers.

Siniestro: También se puede perder o deteriorar material informático por una mala manipulación o mala intención. Aquí entrarían situaciones como robo, incendio o inundación.

Fallos electrónicos: Un sistema informático en general puede verse afectado por problemas del suministro eléctrico o por errores lógicos como cualquier otro dispositivo que no es perfecto.

Catástrofes naturales: Rayos, terremotos, inundaciones…

Según el efecto que produce alguna de las anteriores amenazas se distingue entre:

- Robo de información.
- Destrucción de información.
- Anulación del funcionamiento de los sistemas.
- Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información…
- Robo de dinero o estafas.

Copias de seguridad

Una empresa debe proteger permanentemente su información ya que es el activo más importante que puede dañarse por gran cantidad de factores: robos, incendios, virus…Para proteger de forma eficiente los datos son imprescindibles las copias de seguridad o *backups*. En función del volumen de contenido generado y la cantidad de equipos se perfilará el mejor plan de protección.

7.- Que es Política de la Seguridad de la Información y cuál es su propósito en el manejo de la información?

La política de seguridad se implementa mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas más específicas. Los mecanismos de seguridad se dividen en tres grupos:

Prevención: Evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

Detección: Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema. Ejemplo: la herramienta DLP para la seguridad de los archivos.

Recuperación: Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. Ejemplo: las copias de seguridad.

La política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

https://www2.sgc.gov.co/AtencionAlCiudadano/Paginas/politica-seguridad-de-la-informacion.aspx

https://tecon.es/la-seguridad-de-la-informacion/#:~:text=La%20seguridad%20de%20la%20informaci%C3%B3n%2C%20como%20concepto%2C%20se%20basa%20en,teniendo%20en%20cuenta%20la%20privacidad.&text=Confidencialidad%3A%20Informaci%C3%B3n%20accesible%20solo%20para%20personal%20autorizado.

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
TECNICO EN ASISTENCIA EN ORGANIZACIÓN DE ARCHIVOS

TALLER No1.- DIGITALIZACION DE DOCUMENTOS

Actividad de Reflexión Inicial

Reconocer la necesidad de adquirir nuevas habilidades como la digitalización para su futuro inmediato en cuanto a su derecho al trabajo o iniciativas de emprendimiento.

Descripción actividad 1: • En forma individual lea la siguiente reflexión:

La gestión de la información se ha convertido en un reto para las organizaciones, pues a las exigencias normales de la actividad se suman ahora los retos tecnológicos, cada vez más variados. Como afirma Pérez (2010), le ha correspondido al archivista especializarse y convertirse, además de alguien que presta un servicio como ayudar a un usuario a encontrar lo que necesita, valerse de recursos y documentos electrónicos, buscar en bases de datos especializadas, dominar herramientas de colaboración, desarrollar la colección con recursos digitales y en línea, incursionar en redes sociales, entre otras actividades.

Igualmente, para quienes administran documentos de archivo en las organizaciones, el mapa documental es cada vez más variado y complejo, pues, además de los documentos en papel que se producen y llegan a la oficina cada día, hay un acervo enorme de ellos microfilmados (2500 páginas tamaño carta en un rollo estándar), en microfichas (207 páginas de un reporte de cómputo) y en Jackets (60 fotogramas en cada uno); aquellos que se producen todavía por medio del fax; los generados en CD, llamados también sistema COLD o generación de reportes en CD, con un incremento notorio en la cantidad de páginas almacenadas (en un CD se podían almacenar hasta 180000 páginas de un reporte de computador); hoy se deben sumar los documentos que llegan vía correo electrónico a los buzones de los funcionarios, de los cuales debería tener conocimiento el archivo; aquellos producidos por sistemas de mensajería instantánea; los soportes de transacciones electrónicas; los documentos digitalizados y aquellos que reflejan la evolución de la empresa, como su sitio web, que también hacen parte del acervo documental.

Esto significa que, si el archivista no cambia, lo cambian. la sociedad exige cada vez con mayor vehemencia personas con conocimientos y capacidades técnicas, tecnólogos y profesionales con nuevas habilidades, con el fin de satisfacer públicos mejor informados, de las más diversas tendencias, orientaciones, conocimientos e intereses. Sin embargo, y aunque casi todo es ahora diferente, su función principal

no, como lo recuerda Kane (2011), para quien, a pesar del surgimiento de nuevas formas para acceder a la información, la función del bibliotecario y el archivista sigue siendo la misma y así seguirá, la cual es conectar a la gente con la información. Por estar siguiendo las últimas tendencias tecnológicas se le está olvidando a muchos su función principal, el servicio.

Ahora, si el archivista no adquiere habilidades ni conocimientos, como los anteriormente vistos en el proceso formativo ¿cuáles serán las posibilidades de su empleabilidad o de emprendimiento?

- 1.- Responda la pregunta final de la lectura y socialice su respuesta con el grupo

Actividad Individual No. 2

- Consulte en la página del Archivo General de la Nación www. Archivogeneral.gov.co normativa en relación con la digitalización de algunas series documentales o requisitos para este procedimiento, entre otros: Acuerdo 005 de 2018, Decreto 1080 De 2015, Acuerdo 003 De 2015, Acuerdo 008 De 2014, Acuerdo 002 de 2014, Acuerdo 5 de 2013, Acuerdo 005 de 2013, Acuerdo 006 de 2011.

- Esquematice mediante una línea del tiempo los requerimientos normativos relacionados específicamente con la digitalización de documentos.

Siempre atenta a sus inquietudes!

Éxitos.

Elaboro:
Lenny Kelly Hurtado R.
Instructora de Gestion Documental
Centro de Comercio y Servicios
SENA Regional Cauca
Lkhurtado0@misena.edu.co

Digitalización de Documentos – Ejercicio en Clase

Silhi Dayana Muñoz Rave

Centro de Comercio y Servicios, Servicio Nacional de Aprendizaje – SENA

Técnico en Asistencia en Organización de Archivos – 2210879

Instructora Lenny Kelly Hurtado R.

Actividad 1

Conceptualizar sobre:

- ***Digitalización.***

La digitalización de documentos es uno de los procesos más importantes dentro del desarrollo de la gestión documental, en el cual se lleva a cabo la transformación de los formatos de todo lo concerniente a los documentos físicos que se manejan al interior de la empresa.

Después de la debida revisión, se seleccionan los documentos físicos (análogos) y se pasan a un formato binario (digital). La realización de este proceso ayuda a la empresa a mantener los archivos de importancia en las mejores condiciones a través del tiempo. De igual modo la digitalización ayuda a realizar la administración de una manera más eficiente, ya que se reducen los tiempos de búsqueda, clasificación y acceso.

La digitalización es un proceso en el que se captura la información por medio de procesos tecnológicos, a fin de conservar los documentos a través del tiempo.

- ***Digitalización certificada.***

La digitalización certificada es el proceso que valida ante los entes legales un documento digitalizado. Es decir, todo documento bajo digitalización certificada tiene una validez legal y jurídica, por lo que no todos los documentos digitalizados pueden tener este estatus. Por otro lado, este tipo de digitalización valida la información del documento por medio de una firma digital, la cual asegura la autenticidad de la información registrada.

- ***Clases de firmas electrónicas.***

  - ✓ **Firma electrónica simple**

Es la que cuenta con un menor nivel de seguridad. Son los datos anexos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el usuario para firmar. Produce efectos legales y es un elemento de prueba admisible ante un tribunal, aunque es posible que tenga que complementarse con otros elementos de prueba.

  - ✓ **Firma electrónica avanzada**

Es aquella que se encuentra vinculada al firmante de manera única y permite identificarlo. Ha sido creada utilizando datos que el firmante puede utilizar con un alto nivel de confianza, bajo su control exclusivo, y está vinculada con los datos firmados

por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable. Este tipo de firma asegura la identidad del firmante y la integridad de los datos, por lo que ofrece más garantías legales.

- ✓ **Firma electrónica cualificada**

Se crea mediante un dispositivo cualificado de creación de firmas electrónicas y se basa en un certificado cualificado. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una manuscrita.

- ***Documento.***

Un documento es un escrito en papel u otro tipo de soporte con que se prueba o acredita una cosa, como un título, una profesión, un contrato, entre otros.

- ***Valoración documental.***

A través de la Valoración Documental se obtienen los tiempos de retención, así como la disposición final de los documentos; este es un proceso que consiste en analizar la producción documental de una institución a fin de determinar, de una parte, su valor inmediato o primario, es decir, cuáles documentos son necesarios para que la administración pueda cumplir con su misión y las funciones que tiene asignadas, así mismo, sirven a sus destinatarios o beneficiarios. Por otra parte identificar los documentos que poseen valor mediato o secundario, es decir, que serán útiles a futuro para la construcción de la vida institucional de productor, como fuente para la historia o para fines científicos.

Valores Primarios

- ✓ **Valor administrativo**: cualidad que tienen los documentos para la entidad productora dado que son testimonio de sus procedimientos y actividades.
- ✓ **Valor jurídico o legal:** valor del que se derivan derechos y obligaciones legales, regulados por el derecho común y que sirven ante la ley como testimonio.
- ✓ **Valor fiscal:** utilidad de los documentos de archivo para el Tesoro o Hacienda Pública.
- ✓ **Valor contable:** cualidad de los documentos que soportan el conjunto de cuentas y de registros de los ingresos, egresos y los movimientos económicos de una entidad pública o privada.
- ✓ **Valor técnico:** atributo de los documentos producidos y recibidos por una institución en virtud de sus funciones misionales.

Valores Secundarios

- ✓ **Valor histórico:** cualidad atribuida a los documentos que por ser útiles para la reconstrucción de la historia o memoria de una comunidad deben conservarse.
- ✓ **Valor científico:** cualidad de los documentos que registran información relativa a la creación de conocimiento en cualquier área del saber.
- ✓ **Valor cultural:** cualidad de los documentos que por su contenido son testimonio de los hechos, vivencia, tradiciones, costumbres, hábitos, valores, modos de vida o desarrollos económicos, sociales, políticos, religiosos o estéticos propios de una comunidad y útiles para el conocimiento de su identidad.

- ***Protección personal para la digitalización.***

De acuerdo con la **GUÍA DE DIGITALIZACIÓN Y PRESERVACIÓN DIGITAL DE LA BIBLIOTECA NACIONAL DE COLOMBIA**, se establecen las siguientes medidas durante todo el proceso de digitalización;

Use elementos de protección personal:

1. Guantes de algodón y de nitrilo, tapabocas y bata.
2. La bata de trabajo se usa únicamente en las instalaciones del Centro de Conservación.

La manipulación debe regularse tanto en la presión que se hace en el escáner, como en el movimiento de cada hoja o volumen encuadernado.

El documento se manipula de acuerdo con las siguientes instrucciones:

1. Las hojas se pasan con cuidado y nunca mojando el dedo con saliva.
2. Se evita doblar las esquinas y hacer dobleces.
3. No forzar la apertura de los libros manualmente y controlar la presión cuando el libro está debajo del vidrio del escáner porque en este proceso es cuando más deterioro se produce sobre el documento.
4. Se toma el libro de manera correcta y nunca de las partes frágiles, como la cofia.
5. Los documentos frágiles se manipulan teniendo en cuenta las siguientes instrucciones:

- Cuando la hoja se encuentre en buen estado, la manipulación se realiza con cuidado, sin llevar la hoja bruscamente, ayudándose con la superficie del propio material.
- Cuando la hoja se encuentra en estado friable se manipula de manera más delicada y buscando un soporte con el otro brazo y mano.

6. Se almacena el libro correctamente durante el proceso: se ubica en posición vertical de acuerdo con su tamaño o en forma horizontal sin colocar pilas de más de tres volúmenes, no se pone peso sobre documentos con cubierta frágil.
7. Finalizada la digitalización de cada obra se almacena en su respectivo contenedor, asegurándola en la estantería.
8. El consumo de bebidas y comidas no es permitido durante el proceso de digitalización.
9. El puesto de trabajo, equipos y herramientas deben permanecer limpios y ordenados.

Para mantener la limpieza se realizan las siguientes acciones;

1. Se utiliza una bayetilla blanca y limpia para no contaminar o manchas los libros que se digitalizarán.
2. Se aplica alcohol antiséptico al 75% para limpiar y desinfectar el vidrio templado de la parte superior y el área plana del escáner. Está área se bebe limpiar de manera constante o cada vez que se termine de digitalizar un libro.

- ***Escáner y sus diferentes tipos. Resaltar las características.***

Escáner de mesa o escáner plano.



Es de los escáneres más conocidos y populares entre los usuarios, es el más recomendable para uso doméstico ya que está especializado para digitalizar objetos opacos planos como son las fotografías, documentos o ilustraciones, por su superficie plana de cristal. Son veloces, fáciles de manejar y produce imágenes digitalizadas de calidad aceptable. Dentro de estos tipos de escáner se agrupan los escáneres de libros y el escáner con alimentador de hojas. Se encuentran disponibles en el mercado a un precio económico en comparación con otros tipos de escáner.

Escáner de tambor.



Son los más recomendados cuando se quiere escanear con alta calidad y resolución, su funcionamiento es lento y requiere de un operador experimentado. Los materiales son fijados a una especie de tambor o rodillo, el cual gira para que se efectúe la digitalización, es generalmente usado para el trabajo de pre-prensa y en el diseño gráfico con materiales de uso corriente. Se pueden capturar materiales como transparencias o negativos de gran tamaño. El costo de su adquisición es alto.

Escáner para microfilm.



Son dispositivos que se utilizan para digitalizar microfichas, películas en rollo y tarjetas de apertura. Puede ser difícil obtener una calidad buena y consistente por lo que la calidad y condición de la película puede variar, suelen tener un funcionamiento complejo, son escáneres muy caros y existen pocas empresas que los fabriquen. La definición depende directamente del estado de la película.

Escáner para diapositivas.



Se emplea en la digitalización de diapositivas impresas, de materiales fotográficos tridimensionales y de determinados documentos aptos para el escaneo directo. En el mercado puedes encontrar varios modelos de escáneres, como escáneres comerciales, escáneres semi-profesionales, escáner de diapositivas y negativos, y escáneres profesionales, también los hay en modelos portátiles y, por supuesto, de precios muy variados.

Escáner de mano.

Es uno de los modelos más prácticos y económicos, puede conectarse directamente a las impresoras de un ordenador, es muy similar a un mouse pero con dimensiones mayores, puedes obtener imágenes de calidad regular, solo necesitas una superficie plana para el papel.



Escáner 3D



El escaneado 3D, también conocido como digitalizado 3D, es la técnica que sirve para la obtención digital de la forma de un objeto a partir de la captación de una nube de puntos. Un software conveniente reconstruye geométricamente la nube de puntos transformándola en una malla o modelo 3D que además de información geométrica, puede contener color. Estos dispositivos se usan mucho en la industria del entretenimiento para películas o video juegos; también se utilizan imágenes digitales de los objetos escaneados en 3D para diseño industrial, diseño de prótesis, invertir la ingeniería, control de calidad o para documentación de bienes culturales.

- ***Importancia de la confidencialidad, discreción, responsabilidad, ética en el desarrollo de los archivos.***

De acuerdo a la Ley 1409 de 2010, el cual reglamenta el ejercicio profesional de la archivística y dicta el código de ética y otras disposiciones; El archivista protegerá la integridad de los bienes documentales que custodian, para que constituyan fiel testimonio del pasado. El archivista valorará, seleccionará y conservará el material de archivo en su contexto histórico, legal, administrativo y documental, manteniendo el principio de procedencia de los documentos de archivo. El archivista evitará la realización de intervenciones que pueden afectar la autenticidad de los documentos. El archivista garantizará el continuo acceso y la legitimidad de los documentos. El archivista registrará y justificará plenamente las acciones realizadas sobre el material que tuviera a su cargo. El archivista promoverá el mayor acceso posible a los documentos y ofrecerá sus servicios a todos los usuarios de manera imparcial.

El archivista respetará tanto el acceso público como la privacidad de la documentación dentro del marco de la legislación vigente. El archivista no deberá de utilizar en beneficio propio o de terceros su posición especial y la confianza que la comunidad ha depositado en él. El archivista se esforzará por alcanzar la excelencia profesional mediante el enriquecimiento sistemático y continuo de sus conocimientos y la difusión de los resultados de sus investigaciones y experiencias. El archivista trabajará conjuntamente con sus colegas, así como con profesionales de otras disciplinas para promover la conservación y la utilización de la herencia documental del mundo.

Actividad 2

- Emita un concepto analítico desde lo archivístico sobre el proceso de Digitalización Documental, con base en su importancia, uso y beneficios para el manejo de la información.

La digitalización de documentos es una de las principales estrategias de la gestión documental, ya que por un medio de un análisis al detalle y del uso de las herramientas adecuadas, se conservan los documentos en un formato que puede ser consultado, revisado y utilizado al alcance de un clic. La digitalización de documentos surge como una necesidad debido a dos factores puntuales: el avance tecnológico y el acceso a nuevas tecnologías, y la optimización y automatización de procesos en pro de la eficiencia. De esta manera la digitalización se convierte en una forma confiable de cumplir con las nuevas maneras de acceder a la información y de facilitar su consulta, control y manejo desde diferentes lugares en tiempo real. La digitalización de documentos es muy importante para optimizar el uso de los recursos, permite un acceso rápido y simultaneo a multiples documentos. La digitalización de documentos nos brinda un espacio perdurable de por vida y más seguro, donde los documentos pueden contener límites de seguridad como contraseñas o acceso único a ciertos usuarios. Las principales ventajas de llevar a cabo de la digitalición de documentos son:

- **Económica:** ahorro en costos de almacenamiento, gestión y mejora de la eficiencia organizativa.
- **Informativas:** permite la búsqueda, el acceso y la recuperación de documentos por varios usuarios simultáneamente, es decir, que es de fácil trnsferencia por medio de la red.
- **Jurídicas:** garantiza la accesibilidad a la información y evita la pérdida de la misma.
- **Preservación:** conserva y preserva los originales evitando que se desgaste o deterioren, y almacena la información por mucho más tiempo.
- **Valor agregado:** usar las TICS nos da una ventaja competitiva y simplifica las tareas administrativas.

DIGITALIZACION DE DOCUMENTOS

INSTRUCTORA: NELLY KELLY HURTADO
APRENDIZ: BLANCA FABIOLA PISSO
FICHA: 2210879

SENA
CENTRO DE COMERCIO Y SERVICIOS
POPAYAN- CAUCA

DIGITALIZACION DE ARCHIVOS

DIGITALIZACION DE ARCHIVOS: Es un sistema tecnológico que permite, mediante la aplicación de técnicas foto electrónicos o de escáner, convertir la imagen contenida en una imagen digital.

Es una forma de capturar u almacenar imágenes utilizando la tecnología computacional.

Una cámara digital o un escáner sacan una fotografía electrónica, que convierten la imagen del documento en códigos numéricos para que sean tratados por el ordenador mediante un software de captura.

Archivo Digital: El Archivo Digital es un sistema de gestión de documentos electrónicos y sus meta datos, guardados con criterios de archivo, y gestionables mediante unos servicios web. El Archivo digital dará servicio a todos los Sistemas de Información que requieran funcionalidades de gestión documental, tanto si estos sistemas derivan de la tramitación como de otros procesos de gestión que no estén originados en un procedimiento administrativo

Digitalización certificada: se entiende por digitalización certificada el proceso tecnológico que permite, mediante la aplicación de técnicas fotoeléctricas o de escáner, convertir la imagen contenida en un documento en papel en una imagen digital codificada conforme a alguno de los formatos estándares de uso común y con un nivel de resolución que sean admitidos.

Es el proceso que valida entre los entes legales un documento digitalizado.

Todo documento bajo digitalización certificada tiene una validez legal y jurídica porque no todos los documentos digitalizados pueden tener este estatus.

Clases de firmas electrónicas Ley 527 de 1999

Mediante esta se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.

Esta ley tiene como fuente de inspiración la Ley Modelo de Comercio Electrónico, de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. Aquí se define el principio de equivalencia funcional de la firma electrónica, que debe cumplir los siguientes requisitos, destinados a que la firma electrónica tenga las mismas funciones atribuidas a su versión manuscrita:

- ***Identificar al iniciador de un mensaje de datos.***
- ***Indicar que el contenido cuenta con su aprobación.***
- ***Ser confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado.***

La firma digital debe presentar las siguientes características:

- ***Identificar de forma única a la persona firmante.***
- ***Puede ser verificada.***
- ***Su usuario debe tener su control exclusivo.***
- ***Cualquier modificación de la información que contiene supondrá su invalidación.***

- ***Cumple con todas las disposiciones legales impuestas por el Gobierno***
-

Clases de firmas electrónicas

- ***Simple: Se refiere únicamente a los datos electrónicos que utiliza la persona firmante para llevar a cabo la rúbrica. Aunque es perfectamente legal y puede presentarse en un juicio, es posible que necesite de pruebas complementarias debido a que es la opción con menor seguridad posible.***

- ***Avanzada: Se refiere a aquella que cumple las condiciones recogidas en la rúbrica debe estar vinculada al firmante de manera única, debe permitir identificarlo, debe tener bajo su control los datos utilizados para su creación y debe poder detectarse si ha habido alguna modificación posterior.***

- ***Cualificada: Se trata de una firma electrónica avanzada que ha sido creada mediante un dispositivo cualificado y con un certificado cualificado. Su valor jurídico es exactamente idéntico al de la firma manuscrita tradicional.***

Cabe destacar que todas ellas son perfectamente legales. Los requisitos del proceso o de documento en cuestión serán los que determinen la que se va a utilizar en cada uno de los casos.

Documento: conjunto de documentos producidos, recibidos o reunidos por una persona física o jurídica de modo involuntario, natural y espontáneo en el transcurso, y como apoyo, de su actividad de la que es testimonio, haciendo uso de la electrónica que se conservan y transmiten también mediante medios electrónicos en depósitos de conservación permanente, tras efectuar una selección a partir de la identificación y valoración de las series, con medidas de autentificación y de preservación adecuadas y con una organización respetuosa con su modo de producción, con el fin de garantizar su valor informativo, legal y cultural así como de permitir su acceso y uso también mediante las tecnologías la información.

***Valoración Documental*: De acuerdo al Diccionario de Terminología Archivística, la valoración documental se define como fase del tratamiento archivístico que consiste en analizar y determinar los valores primarios y secundarios de las series documentales, fijando los plazos de transferencia, acceso y conservación o eliminación total o parcial.**

Protección personal para la digitalización:

Gafas mono gafas contra radiaciones: Gafas en policarbonato, con antiempañante y protección para luz ultravioleta. Evita la proyección de partículas sólidas o líquidas a los ojos, tales como, manejo de sustancias corrosivas.

Guante plomado.





Mono gafas



PETO PLOMADO: Chaleco protector rayos x.

***ESCANER**: Periférico que permite convertir un texto o una imagen en un conjunto datos en formato electrónico,*



-Es un instrumento tecnológico.

-Fue creado en 1984.

- ***Se puede realizar una amplia gama de tareas tales como el reconocimiento de textos mediante el OCR, o la obtención de imágenes de elementos específicos, los que no se puede encontrar en Internet.***
- ***El dispositivo proyecta luz sobre la imagen que debe tomar.***
- ***Convierten los caracteres escritos o gráficos impresos en un formato digital.***
- ***Está compuesto por un lenguaje binario de 0 y 1.***
- ***Funciona mediante luz.***
- ***La luz recorre leyendo línea por línea lo que está impreso en ella mediante sensores del tipo CCD o CID.***
- ***Es compresible por la computadora.***
- ***Analiza cada pixel de la imagen y les asigna un valor.***
- ***Manda la información a la computadora para que sea procesada.***
- ***Se comunica con el ordenador mediante una interfaz.***
- ***Incluye la profundidad del color, la resolución y la densidad de la calidad de la imagen.***
- ***El funcionamiento es similar a la función de una fotocopiadora.***
- ***Dispone de una resolución que es expresada en puntos por pulgada denominados dpi que se encuentra dentro de un orden de magnitud alrededor de los 1.200 por 2.400 dpi.***
- ***La resolución define la calidad de escaneo.***
- ***Según el tamaño, los tipos de escáner pueden procesar documentos de distintos tamaños: por lo general A4 (21 x 29,7 cm), o con menor frecuencia A3 (29,7 x 42 cm).***
- ***La velocidad de captura es expresada en páginas por minuto (ppm).***
- ***Depende del formato del documento y de la resolución elegida para el escaneo.***

- ***La velocidad de captura representa la capacidad del escáner para procesar un gran número de páginas por minuto.***
- ***Cuenta con diversas interfaces como el Fire Wires; el USB 2.0, el SCSI y puerto paralelo.***
- ***Su consumo de energía eléctrica es expresado en Watts (W).***
- ***Puede producir bastante ruido dependiendo del tipo de escáner que se emplee.***
- ***Generalmente se suministran los drivers y el manual del usuario.***
- ***Se debe verificar que se incluyan los cables de conexión; de lo contrario deberán adquirirse por separado.***
- ***Los diversos tipos e escáner se mueven a lo largo del documento, línea por línea; cada línea se divide en "puntos básicos".***
- ***El color de cada píxel se divide en 3 componentes que son rojo, verde y azul.***

Existen diferentes clasificaciones



Escáner de mesa: o plano dispone de una superficie plana de vidrio sobre la que se sitúa el documento que se desea escanear y bajo la cual hay un brazo móvil con una fuente de luz y un foto sensor que se desplaza a lo largo del área de captura.

- ***escáner más conocido y popular entre los usuarios.***
- ***Tiene una fuente de luz.***
- ***Cuenta con un sensor de luz CCD que constituyen una parte del brazo móvil que pasa a través del documento que se encuentra sobre la plaza de vidrio.***
- ***Son los más recomendables para el uso doméstico.***
- ***Dentro de estos tipos de escáner se agrupan los: Escáner de libros con medidas específicas para distintos libros. Y los tipos de escáner con alimentador de hojas generalmente utilizados en empresas.***
- ***Este escáner está formado por una superficie plana de cristal, sobre la cual deben situarse los documentos que se desea escanear.***
- ***También está constituido por un lente de lectura que se encuentra debajo del cristal, incluyendo un brazo que se desplaza por toda la superficie del cristal y así escanea el documento.***
- ***Están indicados para digitalizar objetos opacos planos como son las fotografías, documentos o ilustraciones.***
- ***Incluye una carcasa que se puede abrir y cerrar con la finalidad de tapar los documentos que han sido puestos sobre el cristal.***
- ***Los documentos deben estar mirando hacia el lente.***

- ***Son veloces, fáciles de manejar, producen imágenes digitalizadas de calidad aceptable***
- ***Para un correcto enfoque se deben colocar los documentos según las coordenadas que suelen venir indicadas en el escáner.***
- ***Su sistema de exploración cuenta con principio de exploración en una sola pasada.***
- ***El dispositivo de captura que utiliza es CCD trilineal.***
- ***Se encuentra diversos tipos como los de transparencias y originales opacos, color, blanco y negro, originales de tonos grises y de líneas, positivos y negativos.***
- ***Los formatos máximos de originales son opacos 431, 8 x 304, 8 mm (DIN A3)y transparencias 297 x 210 mm.***
- ***El margen de escalas que cumple es de 10% a 600% en modo alta resolución y de 10% a 300% en modo resolución estándar.***
- ***La resolución de exploración que dispone es variada como el modo alta resolución que es una resolución óptica 1200 x 2400 ppp, resolución interpolada 9600 x 9600 ppp, modo resolución estándar que es resolución óptica 600 x 1200, resolución interpolada 6400 x 6400 ppp.***
- ***Se encuentran disponibles en el mercado a un precio económico en comparación con otros tipos de escáner.***
- ***Acepta una densidad máxima o un margen dinámico de 3.4 D.***
- ***Cuenta con una profundidad de color de 30 bits con 10 bits por píxel y color.***
- ***Ofrece diversos modos de escaneado como line art, escala de grises, color RGB y color CMYK.***
- ***La velocidad de exploración que otorga es de 128 segundos con una resolución a 300 ppp, un formato A4, con tamaño de archivo 24,8 Mb).***
- ***Brinda una interface de SCSI – II.***
- ***Características físicas (ancho, alto, fondo y peso): 750 x 210 x 560 mm, 25 Kg.***
- ***Exige unos requisitos del sistema como en Apple Macintosh donde el procesador es de G3 con 128 Mb de RAM y 1 Gb de espacio libre en disco duro, en las computadoras de un procesador Pentium II con 128 Mb de RAM y 1 Gb de espacio libre en disco duro. En ambos casos se requiere de una tarjeta gráfica de 24 bits e interface SCSI – II.***
- ***Admiten también adaptadores especiales para escanear transparencias.***

Escáner de tambor

- ***Es de los tipos de escáner más recomendado cuando se quiere escanear con alta calidad y resolución.***
- ***Su funcionamiento es lento.***
- ***Requiere de un operador experimentado.***



- ***Los materiales son fijados a una especie de tambor o rodillo, el cual gira para que se efectúe la digitalización.***
- ***Están descartados los materiales delicados para su captura en estos tipos de escáner.***
- ***Generalmente es utilizado en el trabajo de pre prensa y en el diseño gráfico con materiales de uso corriente.***
- ***También se recomienda para capturar materiales como transparencias o negativos de gran tamaño.***
- ***Se puede obtener una digitalización de gran precisión, alcanzando resoluciones superiores a los 3,000 dpi.***
- ***Requiere mayores conocimientos para su operación y mantenimiento.***
- ***El costo para su adquisición es alto.***
- ***Es un dispositivo de reproducción electrónica de imágenes y posteriormente de digitalización.***
- ***En la actualidad es el sistema de más calidad y resolución sobre todo para la realización de ampliaciones.***
- ***Otorga una resolución de hasta 4000 ppp.***
- ***Pueden reconocer originales opacos o transparentes.***
- ***Utilizan un cilindro de cristal donde se coloca el original.***
- ***Su sistema de transmisión fotomecánico recorre la imagen punto por punto, obteniendo así una gran resolución.***
- ***Produce y devuelve una imagen con colores primarios, pero ésta puede ser convertida en CMYK, mientras el lector recorre la imagen.***
- ***Los originales (opacos y transparentes) se colocan en la superficie del tambor de exploración.***
- ***Al tratarse de diapositivas, se puede añadir en la cara de contacto del original y el tambor un aceite, denominado anti – anillos de Newton que es un efecto óptico en la formación de anillos concéntricos de diferentes colores.***
- ***Es muy importante realizar una limpieza a fondo del cilindro de exploración.***

Escáner para microfilm



- ***Son dispositivos que se utilizan para digitalizar microfichas, películas en rollo y tarjetas de apertura.***
- ***Puede ser difícil obtener una calidad buena y consistente en estos tipos de escáner.***
- ***La calidad y condición de la película puede variar.***
- ***Ofrecen una capacidad de mejora mínima.***
- ***Suelen tener un funcionamiento complejo.***
- ***La resolución alcanza los 1200 dpi.***
- ***Son escáneres muy caros, existiendo pocas empresas que los fabriquen.***

- ***La definición de las imágenes depende directamente del estado en que se encuentre la película.***

Escáner para diapositivas



- ***Es una máquina que digitaliza imágenes de diapositivas.***
- ***Se emplea en la digitalización de diapositivas impresas, de materiales fotográficos tridimensionales y de determinados documentos aptos para el escaneo directo.***
- **Recomendado para quienes desean preservar intactas sus imágenes o retratos más preciados.**
- ***Ha ido ganando mucha fama con el paso del tiempo por su funcionamiento y por su uso.***
- ***Cuentan con su propia batería.***
- ***Su mecanismo permite transformar a formato digital tus diapositivas físicas.***
- ***Ha logrado que los fabricantes de diversos tipos de escáner se esfuercen por brindar productos variados que puedan. satisfacer al cien por ciento las necesidades de cada uno de los clientes.***
- ***Según su función, el escáner debe de contar con ciertas características que le permita lograr un trabajo de calidad.***
- ***En el mercado puedes encontrar varios modelos de escáneres, como escáneres comerciales, escáneres semi profesionales, escáner de diapositivas y negativos, y escáneres profesionales, también los hay en modelos portátiles y, por supuesto, de precios muy variados.***
- ***Algunos tipos pueden trabajar sin estar conectados con el ordenador.***
- ***También te permiten corregir y restaurar tus imágenes.***
- ***Cuentan con conexión USB 2.0***
- ***Se puede escanear diapositivas enmarcadas.***
- ***Dependiendo del tipo que se emplee cuentan con pantalla LCD.***
- ***Algunos modelos disponen de un consumo de energía es bastante bajo.***
- ***Considerado como un escáner bastante versátil***
- ***Los precios de los escáneres de diapositivas va a variar dependiendo de la marca, del modelo y sus prestaciones.***

Escáner de mano



- ***Cuenta con una tarjeta propia.***
- ***También puede conectarse directamente a las impresoras de un ordenador.***
- ***Es uno de los modelos más prácticos y económicos.***
- ***Ofrece una baja resolución hasta de 400 ppp.***
- ***Tiene similitud al de los ratones o mouse, pero son más grandes.***
- ***Se pone el papel sobre una superficie plana.***

Escáner 3D



- ***Es un dispositivo de adquisición de datos masivos que analiza un objeto o el ambiente físicos.***
- ***Reúne los datos en su forma y posiblemente color.***
- ***Está basado en la tecnología LIDAR.***
- ***Reporta una nube de puntos tridimensional que es una representación discreta de una superficie continua.***
- ***Se combina perfectamente con imagen.***
- ***Desarrollados inicialmente en aplicaciones industriales metrología, automóvil.***
- ***Analiza un objeto o una escena para reunir datos de su forma y ocasionalmente su color.***
- ***Su funcionamiento es a partir de la medición de distancias y ángulo, mediante un rayo de luz láser.***
- ***Permite documentar geométrica y visualmente una realidad física con gran detalle, rapidez y precisión.***
- ***Captura las coordenadas geográficas de todas las superficies que lo rodean en un radio limitado.***
- ***Su funcionamiento es en cuestión de minutos y sin contacto con los elementos medidos.***
- ***Se recoge la información del color en cada punto.***
- ***Permite determinar y reproducir el color de la superficie representada.***
- ***Disponen con la incorporación cámaras fotográficas.***
- ***Se basan en tres principios: triangulación, tiempo de vuelo mediante pulsos y tiempo de vuelo mediante diferencia de fase.***

- ***Ofrece una alta precisión, en torno a la décima o centésima de milímetro.***
- ***Cuenta con una frecuencia elevada en torno a 100 MHz o incluso superior.***
- ***Las precisiones oscilan entre los 6-30 mm.***
- ***Se tratan de equipos que están fijos.***
- ***Desarrollados inicialmente en aplicaciones industriales metrología, automóvil.***
- ***han encontrado un vasto campo de aplicación en actividades como la arqueología, arquitectura, ingeniería y entretenimiento en la producción de películas y videojuegos.***

IMPORTANCIA DE LA CONFIDENCIALIDAD DENTRO DE LOS PROCESOS ARCHIVISTICOS:

Todos los temas tratados dentro de una institución o empresa deben ser respetados sobre todo, la información que como archivistas podemos llegar a conocer o de alguna manera conocemos está en nuestras manos salvaguardar dicha información de forma consecuente con nuestro trabajo.

Discreción: saber guardar silencio respecto a información delicada que perjudique a la institución o área de trabajo manejar idóneamente información de uso exclusivo o confidencial.

Responsabilidad: saber hacer las tareas o actividades estipuladas además de ser responsable por las tareas asignadas.

Ética y valores: discernir los valores que como persona o funcionario de cualquier empresa haga que nuestro nivel laboral ayude al mejoramiento de las funciones institucionales.

IMPORTANCIA DEL PROCESO DE DIGITALIZACION DOCUMENTAL.

Digitalizar los documentos en una entidad es indispensable para el mejoramiento y buen desarrollo de la tecnología la cual permite guardar de manera correcta en los dispositivos de almacenamiento como son: memorias, discos duros, microfilm.

Todo esto con el fin de optimizar la búsqueda de la información y protegerla de posibles desastres naturales como son: inundaciones, terremotos etc...

También la información guardada aquí debe ser protegida de posibles ataques de cibernautas que busquen afectar los datos obtenidos en esta institución para ello usar claves o contraseñas que no sean fácil de descifrar.

EJERCICIO EN CLASE

¿DIGITALIZACION?

Cuando hablamos de digitalización nos referimos a:

- La transcripción de información pasando de ser física a ser digital
- La digitalización es un convertidor de información o con codificador de la misma
- Se transfiere in formación a los dispositivos de información productoras de este tipo de documento
- Como digitalización tiene varios formatos como pdf .dxo

DIGITALIZACION CERTIFICADA

La digitalización certificada es aquella que cuenta con respaldo de autentificación, legal, calidez y no todos los documentos cuentan con ella. o no tienen este estado

FIRMAS DIGITALES

Una firma digital es el mecanismo ortográfico que permite validar la legalidad del documento y permite que la in formación enviada sea rectificada y certificada en la institución donde se envía el documento además también permite que la información se recuperada y no cueste trabajo saber de que parte viene

- FERMAS SIMPLES :

DOCUMENTO

Un documento se le atribuye a un papel o formato digital que contenga algún tipo de valides legal, cultural o histórico a de este término podeos dividirlo en dos

- **DOCUMENTO DIGITAL:**
  El documento digital es aquel documento que tiene soporte en un formato ya sea pdf o cualquier otro o por medio de las digitalizadoras de la empresa

- **DOCUMENTO FISICO:**
  Documento físico esta diligenciado , autentificado ,y firmado en un papel que tiene valides jurídica legal

VALORACION DOCUMENTAL:

Se define como la face del trtamiento archivistico que consite en alnalizar y determinarlos valores primaros secundarion en la serien documentales

POTECCION PERSONAL PARA LA DIGITALIZACION

Las entidade so empresas deben de estar pendientes de estos parametros ya que tanta digitalizacion trae males cono la expocisin ala radiacion el sedentarismos el cansancio visul y todo este tipos de cosas que le puedan dar problemas a sus trabajadores y esto lleva a cartar sus vidas un estudio relizado 15 de mayo de 2015 a rojo resuldoso inpactantes para la conunida archivista y mas para llos encargados de la dijitalizacion

ESCANER Y SUS TIPOS

Los escaner son fundamentales para la digitalizacion ya que son bastabnte eficientes y son apratos electonicos que exportan imjenes o documentos

Su tipos son

1. Escaner planos
2. Escaner aliniador de hajas
3. Escaner con tambor
4. Escaner con micro fil
5. Escanber de diapocitivas

IMPORTANCIA

COMFIDELIZACION : es importante porque los documentos que se van atrtar son muy delicados y no se puden mostrar aalgin por simple prvacidad que es un dercho fundamental

DISCREPCION: en estas simples definiciones se ve reflejado noestra etica archivistica y la in formcion que se encuentra en estos documkentos no se pude ir hablando con otras person tenemos que ser humanistas en el sentiodo de que no podemos hablar de problemas ajenos anustra profecin o nuestra vida personal

ACTIVIDAD 2

Bueno el consecto de digitalizacion trajo consigo un monton de beneficios con la eficiencia O el practico manejo que se le da ya sea para los archivistas o para las personas naturles Segun la cademia española la diguitalizacion les abre muchas puertas no tansolo en las herramientas que esta tiene sino en que tosdos los dias lapersonas que se especielisan en esto sacan mas herramientas y se vuelve mas automatico todos los prosedimientos que vayan arelezar tambienpdes detacr la gran conpetitividad que esto conyeva emn esta 4 industrializacion mundial

Pero todo esta eficiencia y conectividad tambienlleva su partes malas donde seponen en reisgo la salud de el trabajor archivista no solo con el sedentarismos sino con la radiacon y la perdida de vicion que esto conyeva

A largo plaso son mas los obtaculos que los beneficion

Pero esto se estan tomando medidas a tiempo para no presentar al gun percance de este tipo

Gracias …

BIBLIOGRAFIA

https://debitoor.es/glosario/digitalizacion

https://www.dropbox.com/es/business/resources/what-is-digitization

https://www.archivo.com/es/archivo/

Conceptos

Técnico en organización de archivo

Ficha: 2210879

Entregado a : Lenny Kelly Hurtado

Entregado por : Roxana Rivera

Centro de comercio y servicio Sena regional cauca

Concepto sobre digitalización: proceso tecnológico que permite convertir un documento en soporte análogo (papel video casettes, cinta ,película, microfilm) en uno o varios archivos digitales que contienen una imagen codificada fiel e integra del documento. Para su posterior clasificación para una consulta rápida y precisa.

La digitalización de documentos ayuda a prevenir pérdidas documentales y a recuperarse fácilmente de una situación conflictiva etc.

también ayudamos al impacto del medio ambiente

Que es digitalización certificada: es el proceso que se válida ante los entes legales un documento digitalizado. Es decir todo documento bajó digitalización certificada tiene una validez legal y jurídica por lo que no todos los documentos digitalizados pueden tener este estatus tiene un mayor grado de seguridad procedimental y tecnológica que la digitalización simple

Clases de firmas electrónicas

Firma electrónica simple esta firma cuenta con menor nivel de seguridad son los datos anexos a otros datos electrónicos o asociados de manera lógica

¤ ***firma biométrica:*** es la firma manuscrita capturada a través de Tablets o pad de firma con capacidad para recoger datos biométricos

Firma electrónica con certificados digitales: firma con un certificado digital emitido por un organismo a través del cual se válida la propia firma y la identidad del firmante

Firma en la nube: firma mediante certificado digital alojado en un servidor seguro (HSM), con autenticación robusta.

Firma electrónica desatendida: firma con certificado electrónico que no requiere intervención del usuario

Codigo de un solo uso (OTP SMS Y OTP Email): firma asociada al envió de un código OTP (One time password) mediante SMS, al número de teléfono móvil del firmante

Firma con huella dactilar: firma electrónica en la que se recoge la biometría dactilar

Las principales leyes que rigen las firmas electrónicas en Colombia son:

ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones

Decreto 1747 de 2000: por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación los certificados y las firmas digitales

Se define la firma electrónica en el ***Decreto 2364 de 2012*** como códigos contraseñas datos biométricos o claves criptográficos privadas que permiten identificar a una persona en relación con un mensaje de datos, siempre que sea confiable y apropiado según los términos de la ley

Decreto 333 de 2014 : reglamento las características requerimientos infraestructura, deberes y responsabilidades de las entidades de certificación

Que es un documentos: un documento recoge un acto o hecho realizado por una

institución o por una persona ya sea física, jurídica, pública o privada. puede ser una carta un memorándum, un oficio e incluso algún texto histórico, una novela o una nota periodística ejemplo : **acta de nacimiento:** documento legal **película:** documento audio visual

Los documentos escritos son las fuentes de información mas tradicionales y las que mayor cantidad de datos directos pueden proporcionar acerca de los acontecimientos históricos estudiados

Que es valoración documental: se define como fase del tratamiento archivístico que consiste en analizar y determinar los valores primarios y secundarios de las series documentales, fijando los plazos de transferencias acceso y conservación o eliminación total

Las tablas de valoración documental son el listado de asuntos o series documentales A los cuales se les asigna el tiempo de permanecía así como su disposición final

En la valoración primaria se identifican los valores administrativos, legales, jurídicos y/o financieros de los documentos que son de interés y uso para el organismo que le dio origen

Valor administrativo es el valor que tiene un documento o una serie documental Para la entidad productora relacionado con el trámite o asunto que motivo su creación.

Valor jurídico este valor esta relacionado con derechos y obligaciones

Valor legal aquel que tienen los documentos y sirve de testimonio ante la ley

Valor fiscal es el que tienen aquellos documentos que expresan movimientos de dinero y esta dado por la utilidad para el tesoro o Hacienda pública

Valor contable esta representado con los documentos que soportan el conjunto de cuentas, como los registros de ingreso egresos y movimientos económicos de la institución

Valor técnico utilidad de la información especificada de una función

Valores secundarios cualidad atribuida a aquellos documentos que por su importancia histórica, científica y cultural deben conservarse en un archivo

Valores secundarios son aquellos que afloran una vez agotado el valor inmediato o primario aunque algunos documentos lo tienen desde el momento en que se producen.

Son la cualidad atribuida a aquellos documentos que por su importancia histórica científica y cultural, deben conservarse en un archivo

Valor histórico cualidad atribuida a aquellos documentos que deben conservarse permanente por ser fuentes primarias de información, útiles para la reconstrucción de la memoria de una entidad.

Valores cultural calidad del documento que por su contenido, testimonio, entre otras cosas, hechos, vivencias, tradiciones, costumbres hábitos, valores, modos

de vida, o desarrollo de económicos, social, político, religioso o estético, propio de una comodidad y útiles para el conocimiento de su entidad

Valor científico cualidad de los documentos que registran información relacionada con la creación de conocimiento en cualquier área del saber. Estos documentos científicos van ligados con la investigación

Valor investigación sirven como fuente de consulta para los investigadores y como testimonio de la memoria colectiva



Principios.

.No se puede valorar sino esta organizado y no cuenta con sus instrumentos de control

.No se valoran documentos o expedientes si no series documentales

.se realiza conjuntamente con el responsable de archivo.

Protección personal para la digitalización : la persona debe tener perfil técnico y usar elementos como guante de hilo o desechable de látex, tapabocas bata gorro mono gafas y calzado adecuado

Escáner :

Es un periférico de captura utilizado para escanear documentos; es decir, convertir un documento en papel en una imagen digital similar a una fotocopiadora ya sean libros diapositivas entre otros

los tipos de escáner que existen son :

Escáner de mesa o escáner plano: es el modelo más conocido y utilizado por disponibilidad versatilidad y facilidad de uso.

Tiene una fuente de luz y un sensor de luz CCD que conforman el brazo móvil que pasa sobre el documento situado sobre la plaza de vidrio dentro de esta tipología se engloban

. Escáner de libros con medidas específicas para distintos libros

. Escáner con alimentador de hojas similar a las fotocopiadoras muy utilizadas en empresas.



Escáner de tambor: este modelo es el más recomendado cuando se quiere escanear con alta calidad y resolución. Es de funcionamiento lento y requiere de un operador experimentado.



Escáner para microfilm: se utiliza para digitalizar microfichas, películas en rollo y tarjetas de apertura



Escáner para diapositivas: se emplea en la digitalización de diapositivas impresas, de materiales fotográficos tridimensionales y determinados documentos aptos para el escaneo directo.



Cámaras digitales: cuenta con una tarjeta propia, aunque también puede conectarse directamente a las impresoras de un ordenador. Es uno de los modelos más prácticos y económicos, pero ofrecen una baja resolución (400 ppp)



Escáner digitalizado de video: se usan para realizar documentos que tengan aplicaciones informáticas integran tarjetas que consiguen digitalizar imágenes a la vez que las convierten en imágenes electrónicas analógicas.



Escáner de transferencia: diseñado para capturar películas transparentes, ya sean a color, en blanco y negro, negativo o positivo

Escáner de mano: Su calidad o resolución de imagen no es como los tipos que presentamos anteriormente. Este contiene una calidad muy baja que está considerada entre unos 400 ppp. Una resolución muy baja en comparación a otros escáneres que sobrepasan los 1000 ppp.

Tienen un gran parecido a la forma de un mouse o ratón de un ordenador o computador. Solamente que estos tipos de escáner son más grandes que este periférico.

Para el uso del escáner de mano que es largo y delgado, se debe colocar el documento o el papel encima de una superficie. Después de haber hecho esto pasamos el escáner por encima del mismo muy lentamente. Así podemos ir viendo la información en el dispositivo. Quizá te preguntes ¿Cómo se puede ver la información del documento en el escáner?, sencillo.



Escáner 3D

.Básicamente este dispositivo es uno de los que más se usa actualmente en las industrias y empresa. Su función principal es llevar todo lo que esté en la vida real a la realidad virtual en 3 dimensiones.

Este dispositivo es muy usado en las ramas del diseño para cuando se quiere realizar un modelo igual de una forma real. Por otro lado, existen muchos drones que capturan toda la realidad física de las superficies para luego mostrarlas en la realidad virtual. Son muy prácticos para detallar lugares como casas, edificios, apartamentos, establecimientos, etc.

También podemos encontrar los tipos de escáner 3D encargados de tomar todos los movimientos de una persona. Estos se usan muy frecuentemente en los videojuegos actuales. Anteriormente se diseñaban los personajes de un juego de formas más compleja que ahora.

Hoy en día podemos ver como en los videojuegos se incluyen personajes importantes de la vida real. Estos escáneres pueden verse en forma de traje para las personas donde el mismo contiene sensores de captación de movimiento. Todo lo que la persona haga o realice, se notará en una pantalla haciendo la acción de escaneo.



El escáner 3D tiene la capacidad de adquisición de datos masivos que analiza un objeto o el ambiente físico. También puede reunir toda la información de en todas las formas posibles y tomando cualquier color.

La importancia de la confidencialidad, discreción, ética en el desarrollo de los archivos es muy importante aplicar la ética profecional ya que se debe actuar con responsabilidad y honestidad con nuestro trabajo, con nosotros mismos y con la sociedad realizar un trabajo transparente equitativo honesto leal para brindar un servicio satisfactorio sin incurrir en procesos legales ya que la Archivistica se maneja información muy confidencial e importante

Concepto de digitalización: la digitalización es de vital importancia ya que nos ayuda en el manejo de la información de una manera mas ordenada, precisa puntual y así poder brindar un servicio eficiente para su consulta. Es un factor importante a la hora de conservar la información también nos permite tener la información ordenada aunque debemos tomar precauciones para su protección que también es de vital importancia ya que está expuesta a ciertos riesgos como perdida o filtración.

Ficha número:

2210879

Presentado a:

Lenny Kelly Hurtado

Presentado por:

Luisa Fernanda Jurado Muñoz

Servicio Nacional de Aprendizaje SENA

Centro Comercio y Servicios

Regional Cauca

Actividad 1

Conceptualizar sobre:

- DIGITALIZACIÓN

Técnica que permite la reproducción de información que se encuentra guardada de manera analógica (soportes: papel, video, casetes, cinta, película, microfilm y otros) en una que solo puede leerse o interpretarse por computador.

- DIGITALIZACIÓN CERTIFICADA

La digitalización certificada es el proceso que valida ante los entes legales un documento digitalizado. Es decir, todo documento bajo digitalización certificada tiene una validez legal y jurídica, por lo que no todos los documentos digitalizados pueden tener este estatus. Por otro lado, este tipo de digitalización valida la información del documento por medio de una firma digital, la cual asegura la autenticidad de la información registrada.

- CLASES DE FIRMAS ELECTRÓNICAS

Todos los tipos de firmas electrónicas son consecuencia directa de la transformación digital y la incorporación de nuevos procesos inteligentes para optimizar los tiempos de gestión y hacerlos más seguros.

- Firma electrónica simple: Es la que cuenta con un menor nivel de seguridad. Son los datos anexos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el usuario para firmar. Produce efectos legales y es un elemento de prueba admisible ante un tribunal, aunque es posible que tenga que complementarse con otros elementos de prueba.
- Firma electrónica avanzada: Es aquella que se encuentra vinculada al firmante de manera única y permite identificarlo. Ha sido creada utilizando datos que el firmante puede utilizar con un alto nivel de confianza, bajo su control exclusivo, y está vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable. Este tipo de firma asegura la identidad del firmante y la integridad de los datos, por lo que ofrece más garantías legales.
- Firma electrónica cualificada: Se crea mediante un dispositivo cualificado de creación de firmas electrónicas y se basa en un certificado cualificado. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una manuscrita.

- DOCUMENTO

Información registrada, cualquiera que sea su forma o el medio utilizado. Registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones Documento misional: Documento producido o recibido por una institución en razón de su objeto social.

• Documento físico: Son aquellos archivos que están en formato de papel y por sus características ofrece: Guardar la información de manera íntegra. Los archivos no pueden ser modificados o alterados. Se pude realizar la consulta de documentos sin tener que recurrir a algún dispositivo tecnológico

• Documento digital: En términos generales los documentos digitales son archivos que proporcionan información y cuentan con la capacidad de ser registrados en un soporte de almacenamiento para su fácil identificación y recuperación. Sin importar el formato de la información: texto, imagen, sonido, audiovisuales.

• Documento electrónico: Es un documento cuyo soporte material es algún tipo de dispositivo electrónico y en el que el contenido está codificado mediante algún tipo de código digital que puede ser leído o reproducido mediante el auxilio de detectores de magnetización.

- VALORACIÓN DOCUMENTAL

Labor intelectual por la cual se determinan los valores primarios y secundarios de los documentos con el fin de establecer su permanencia en las diferentes fases del ciclo vital.

- PROTECCIÓN PERSONAL PARA LA DIGITALIZACIÓN

El personal que tiene acceso al depósito de archivo debe contar permanentemente con elementos de protección mínimos, tales como tapabocas o mascarillas, guantes, gorros, gafas y batas.

ESCANER Y SUS DIFERENTES TIPOS:

- **Escáneres planos (de mesa):** Son versátiles, fáciles de manejar, y con una amplia disponibilidad.
- **Escáneres con alimentador de hojas:** Los escáneres con alimentador de hojas utilizan la misma tecnología básica que los escáneres planos, pero maximizan el rendimiento, por lo general a expensas de la calidad. Diseñados generalmente para entornos de negocios de grandes volúmenes, típicamente escanean en blanco y negro o escala de grises con resoluciones relativamente bajas
- **Escáneres de tambor:** Los escáneres de tambor producen escaneados con la mayor resolución y calidad que cualquier otro tipo de escáner.
- **Escáneres para microfilm:** Los escáneres para microfilm son dispositivos altamente especializados para digitalizar películas en rollo, microfichas y tarjetas de apertura.
- **Escáneres para diapositivas**: Los escáneres para diapositivas se utilizan para digitalizar colecciones de diapositivas ya existentes como así también materiales fotográficos intermedios de objetos tridimensionales y documentos que no son adecuados para el escaneado directo
- **Cámaras digitales**: Las cámaras digitales combinan un escáner con óptica de cámara para formar una herramienta versátil que puede producir imágenes de calidad superior.

Importancia de un escáner

Un escáner es un periférico de captura utilizado para escanear documentos; es decir, convertir un documento en papel en una imagen digital. En general, se puede decir que existen tres tipos de escáner: Los escáneres planos permiten escanear un documento colocándolo de cara al panel de vidrio.

IMPORTANCIA DE LA CONFIDENCIALIDAD

- Es el rol que uno como archivista logra ejercer como el de recolectar informacion, gestionar, facilitar y garantizar un buen acceso a cada documento, incluyendo todos los soportes electrónicos desde un ordenamiento para así lograr facilitar la consulta

DISCRECIÓN

El archivista debe proteger la autenticidad de los documentos y asegurar que su valor no sea alterado durante el proceso archivístico, la conservación y el uso. *El archivista debe asegurar el acceso continuo y la inteligibilidad del material archivístico

RESPONSABILIDAD

El archivista protegerá la integridad de los bienes documenta- les que custodian, para que constituyan fiel testimonio del pasado. La primera misión del archivista consiste en proteger la integridad de los documentos, conservarlos y custodiarlos.

Actividad 2

- Emita un concepto analítico desde lo archivístico sobre el proceso de Digitalización Documental., con base en su importancia, uso y beneficios para el manejo de la información.
- La digitalización nos permite compartir y comunicar de una manera más eficiente, el día a día para obtener la búsqueda de datos e información, una medida para ir sustituyendo poco a poco lo análogo, es decir los soportes con documentación en físico, un proceso que toma más tiempo cuando de solicitar información se trata. No obstante, tener en cuenta que es importante que no solo la tecnología hace al archivista, sino también la forma de brindar un buen servicio para conectar a las personas con la información y mantener al público mejor informado.

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
TECNICO EN ASISTENCIA EN ORGANIZACIÓN DE ARCHIVOS

DIGITALIZACION DE DOCUMENTOSEJERCICIO EN CLASE

Vanessa María López Labado Técnico Asistente en Archivo
SENA, Ficha 2210879, Digitalización de Documentos.

Instructora Lenny Kelly Hurtado
Digitalización de Documentos
Mayo, Popayán**.**

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
TECNICO EN ASISTENCIA EN ORGANIZACIÓN DE ARCHIVOS

Desarrollo

Con base en la temática expuesta en clase, desarrolle la siguiente actividad de conceptualización y análisis sobre el Proceso de Digitalización de documentos.

Instrucciones:

1.- Trabajo individual.

2.- El ejercicio debe presentarlo en forma escrita y en formato PDF.

Actividad 1

Conceptualizar sobre:

Digitalización: Es el proceso de convertir documentos de papel en imágenes u otros como videos, cintas, película, microfilm a través de un escáner, cámaras digitales u otros medios, lo que obtiene de estas las imágenes serán integradas en un sistema de gestión que permita la consulta, la recuperación y distribución de las mismas.  	**Digitalización certificada** La digitalización certificada es el proceso por el cual un documento digitalizado pasa a tener validez legal ante cualquier organismo oficial. Para la digitalización certificada de facturas es necesario utilizar un software homologado por la Agencia Tributaria para poder autenticar la digitalización de este tipo de documentos. AGN: Es el proceso tecnológico que permite convertir un documento en soporte físico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento, con certificación tecnológica de integridad, disponibilidad, fiabilidad y autenticidad. 

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
TECNICO EN ASISTENCIA EN ORGANIZACIÓN DE ARCHIVOS

Clases de firmas digitalizadas
Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;

Firma electrónica simple: Es la que cuenta con un menor nivel de seguridad. Son los datos anexos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el usuario para firmar. Produce efectos legales y es un elemento de prueba admisible ante un tribunal, aunque es posible que tenga que complementarse con otros elementos de prueba.
Firma electrónica avanzada: Es aquella que se encuentra vinculada al firmante de manera única y permite identificarlo. Ha sido creada utilizando datos que el firmante puede utilizar con un alto nivel de confianza, bajo su control exclusivo, y está vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable. Este tipo de firma asegura la identidad del firmante y la integridad de los datos, por lo que ofrece más garantías legales.

Firma electrónica cualificada: Se crea mediante un dispositivo cualificado de creación de firmas electrónicas y se basa en un certificado cualificado. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una manuscrita.



Documento: Un documento es un testimonio material de un hecho o acto realizado en funciones por instituciones o personas físicas, jurídicas, públicas o privadas, registrado en una unidad de información en cualquier tipo de soporte en lengua natural o convencional.

Documento Electrónico: Documento electrónico es aquel contenido en un soporte electrónico (algún aparato electrónico auxiliar) que, para su visualización requiere una pantalla textual, una pantalla gráfica, y/o unos dispositivos de emisión de audio, vídeo, etc.; según el tipo de información que contenga.

Documento Digital:
Un documento digital es la representación en medio digital de un documento, contenido, textos, imágenes, sonidos, videos. Un documento digital tiene información codificada en bits y para leer, visualizar o grabar la información se precisa de un dispositivo que transmita o grabe información codificada en bits. Al representarse digitalmente, los datos de entrada son convertidos en dígitos (0,1) inteligibles para la máquina y no para los sentidos humanos. [2]



Valoración Documental: Labor intelectual por la cual se determinan los valores primarios y secundarios de los documentos con el fin de establecer su permanencia en las diferentes fases del ciclo vital.

Responsabilidad: proteger la información, manteniendo los controles definidos por el dueño de la información. - Obtener aprobación del propietario de la información antes de realizar la divulgación de la misma. - Realizar y aprobar las copias de respaldo de la información para garantizar su disponibilidad. - Realizar restauraciones de las copias de respaldo. - Implementar los controles de acceso definidos o aprobados

	por el propietario de la información. - Realizar las tareas administrativas propias de su cargo con la información bajo su custodia. - Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
Escáner y sus diferentes Tipos. El escáner es un dispositivo de entrada de información que tiene la función de capturar imágenes de cualquier tipo y luego la plasma en una hoja de papel en imagen digital.  **Escáner de libros**   Escáner de Mano **Escáner de tambor** Este tipo de escáner es muy usado para realizar trabajos masivos y además ofrecen resultados con alta calidad y resolución, a pesar de que su nivel de procesamiento es lento, para su manejo es importante que sea llevado a cabo por un experto. Cuenta con un sistema de transmisión fotomecánico que hace un recorrido pausadamente por cada punto, con lo que se consigue una buena resolución.	**Protección personal para la Digitalización** **Contra radiaciones** Para casos de radiación infrarroja deben usarse lentes o pantallas protectoras provistas de filtro.  

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
TECNICO EN ASISTENCIA EN ORGANIZACIÓN DE ARCHIVOS

Escáner para microfilm El escáner para microfilm se usa especialmente para digitalizar microfichas, films en rollo y tarjetas de apertura, tienen la particularidad que no ofrecen una buena calidad de la digitalización, sin embargo, todo va a depender de la calidad y condición de cómo se encuentre originalmente la película. **Escáner para diapositivas** Esta herramienta se utiliza para digitalizar diapositivas que han sido impresas, igual documentos fotográficos tridimensionales y otro tipo similar de documento, se le sugiere a los usuarios que por algún motivo deben mantener imágenes perfectas de fotografías realizarlo con este tipo de herramienta. **Escáner digitalizador de vídeo** Este tipo de escáner se utiliza para ejecutar documentos que cuentan con otras aplicaciones informáticas, se le pueden integrar tarjetas para lograr digitalizar imágenes al mismo tiempo que las transforma en imágenes electrónicas analógicas. **Escáner de transferencia.** Dentro de sus funciones cuenta con un diseño especial para capturar films transparentes, dejando de un lado el tono que tengan, si están en negativo, son ideales para este tipo de actividad. **Escáner de códigos de barras.** Son los dispositivos que se usan en los diferentes comercios dedicados a la venta de cualquier artículo que se pueden evidenciar que se les coloca un código digitalizado que se lee en una computadora, lo que permite controlar los precios e inventario de la mercancía.	
DISCRECIÓN: Reserva o cautela para guardar un secreto o para no contar lo que se sabe y no hay necesidad de que conozcan los demás.	**IMPORTANCIA DE LA CONFIDENCIALIDAD:** Propiedad de la información que determina que esté disponible a personas autorizadas. Guía para realizar la priorización de proteger los documentos según la AGN. **https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/3_Transparencia/3.3%20Procesos%20y%20Procedimientos/GIT-G-01_GUIA_PARA_LA_CALIFICACI%C3%93N_DE_LA_INFORMACI%C3%93N_AGN.pdf**

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
TECNICO EN ASISTENCIA EN ORGANIZACIÓN DE ARCHIVOS

https://normativa.archivogeneral.gov.co/ley-1409-de-2010/?pdf=1256	**ÉTICA EN ELDESARROLLO DE LOS ARCHIVISTICOS:** **Velar por su transparencia, protección y conservación documental desde el inicio hasta el final .** http://ccarchivistas.co/nosotros/codigo-etica/#toggle-id-1

Actividad 2

2.1.- Emita un concepto analítico desde lo archivístico sobre el proceso de Digitalización Documental., con base en su importancia, uso y beneficios para el manejo de la información.

Digitalización:
La digitalización permite y permitirá a medida que las entidades adopten esta estrategias una herramienta para brindar un servicio ágil preciso y en un tiempo más corto la información que reposa en sus archivos y la que ya tendrán en su parte de electrónica, es vital tener en cuenta todo lo que el requiere, las indicaciones que se deben tener en el trato de esta información las normas que lo rigen y su protección que es de grandes proporciones para que haya seguridad tanto para quien posee la información como para quien la solicita o suministra.



Webgrafia

Repositorio normativo del archivo general de la nación https://normativa.archivogeneral.gov.co/

SERVICIO NACIONAL DE APRENDIZAJE SENA
CENTRO DE COMERCIO Y SERVICIOS
TECNICO EN ASISTENCIA EN ORGANIZACIÓN DE ARCHIVOS

Elaboro:
Lenny Kelly Hurtado R.
Instructora de Gestion Documental
Centro de Comercio y Servicios
SENA Regional Cauca
Lkhurtado0@misena.edu.co