Contenido

1.- RESUMEN DE LA UNIDAD

1.1.- ¿Qué es la ciberseguridad?

La ciberseguridad comprende el conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica así como los servicios y la información que presta.

1.2.- Triada de seguridad (CIA)

1.2.1.- Confidencialidad

Consiste en proteger la información sensible para que solo quienes estén autorizados puedan acceder.

1.2.2.- Integridad

Consiste en asegurar que la información no sea alterada sin permiso.

1.2.3.- Disponibilidad

Consiste en garantizar que los sistemas estén operativos cuando los usuarios los necesiten.

1.3.- Otros principios

1.3.1.- Fiabilidad

Consiste en garantizar que el sistema funcione de manera correcta y predecible, de acuerdo con lo que se espera de él, sin errores o fallos inesperados.

1.3.2.- Autenticidad

Consiste en asegurar que la información o el usuario es quien dice ser, y que la información no ha sido manipulada por nadie más durante su transmisión o almacenamiento.

1.3.3.- No repudio

Consiste en asegurar que ninguna de las partes involucradas en una comunicación o transacción puede negar que esa acción ocurrió.

1.4.- Decálogo de la ciberseguridad

a) **Cultura de la ciberseguridad y concienciación del empleado**

b) **No abrir enlaces ni descargar archivos sospechosos**

c) **Usar software de seguridad**

d) **Limitar la superficie de exposición a amenazas**

e) **Cifrar la información sensible**

f) **Utilizar contraseñas adaptadas a la funcionalidad**

g) **Borrado seguro de información**

h) **Realizar copias de seguridad periódicas**

i) **Mantener actualizados los sistemas y aplicaciones**

j) **Revisar regularmente la configuración de seguridad**

1.5.- Activos, amenazas, vulnerabilidades y riesgos

1.5.1.- Activo

Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste.

1.5.2.- Vulnerabilidad

Debilidad o fallo que existe en nuestro sistema y que puede ser explotado por una amenaza.

1.5.3.- Amenaza

Toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

1.5.4.- Riesgo

Probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad y produciendo consecuentemente un daño o impacto.

Podemos eliminar el riesgo, mitigar su impacto, compartir o transferir el riesgo con terceros o bien aceptarlo.

Para evaluar la magnitud y la gravedad de las consecuencias del riesgo realizaremos un

1.5.5.- Análisis de riesgos

Los pasos para llevarlo a cabo son:

a) **Definición del alcance del análisis**

b) **Identificación de activos**

c) **Identificación de medidas de seguridad existentes**

d) **Descubrir las vulnerabilidades que afectan a los activos**

e) **Valorar las posibles amenazas que pueden afectar a los activos**

f) **Obtener el riesgo para cada activo/amenaza**

g) **Establecer los objetivos de seguridad de la organización**

h) **Seleccionar las medidas de protección posibles**

1.6.- Plan director de seguridad

1.6.1.- ¿En qué consiste?

Consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables.

1.6.2.- Fases

1.6.2.1.- Estudio de la situación actual de la empresa

Para hacer esto deberemos

a) **Analizar el contexto de la empresa y la estrategia de negocio**

b) **Acotar y establecer el área a analizar**

c) **Identificar a los responsables de la gestión de los activos**

d) **Realizar un análisis de riesgos**

e) **Establecer unos objetivos basados en los activos críticos**

1.6.2.2.- Estudio de la estrategia de la organización

En esta fase deberemos considerar las estrategias de seguridad, TIC y de negocio de la empresa. Este apartado es fundamental para implantar medidas de seguridad acordes a la naturaleza de la organización.

1.6.2.3.- Definición de proyectos e iniciativas

A partir de la información obtenida hasta el momento deberemos definir las acciones e iniciativas a llevar a cabo.

1.6.2.4.- Clasificación y priorización

En esta fase deberemos clasificar y ordenar por prioridad cada una de las iniciativas propuestas, ya que no todas tendrán el mismo peso e importancia, ni tampoco el mismo coste.

1.6.2.5.- Aprobación por la dirección

Una vez se tenga un borrador del plan, este debe ser revisado y aprobado por la dirección, para posteriormente ser trasladado a todos los empleados.

1.6.2.6.- Puesta en marcha

En esta última fase se implementará la metodología de proyectos para llevar a cabo el plan.

1.7.- Protección del puesto de trabajo

1.7.1.- Definición y elementos de un puesto de trabajo

El puesto de trabajo es el lugar desde el cual un empleado común realiza su trabajo diario, accediendo a sistemas, aplicaciones y datos que necesita para cumplir con sus tareas.

En el entorno de seguridad informática, el puesto de trabajo es mucho más que el lugar físico donde una persona se sienta a trabajar. Representa el **conjunto de elementos que un empleado utiliza para realizar sus tareas**. Algunos

son: dispositivos, software, acceso a redes, instalaciones físicas, acceso a datos y el propio empleado.

Para cada uno de esos elementos existirán unos escenarios de riesgo asociados.

1.7.2.- Normativa de protección del puesto de trabajo

Una normativa en lo referente al puesto de trabajo, es un conjunto de reglas y requisitos específicos que deben cumplirse para garantizar un ambiente de trabajo seguro.

Algunos ejemplos de medidas que pueden incluirse en una normativa de protección del puesto de trabajo son restricciones de acceso, medidas de seguridad física y digital, procedimientos de actualización y parches y buenas prácticas de uso diario.

Las medidas de seguridad aplicadas se clasificarán según su nivel de complejidad (Básico o Avanzado) y su alcance (Procesos, Tecnología o Personas).

1.7.3.- Políticas, normativas y procedimientos

1.7.3.1.- Política

Declaración general que define la intención y los principios de una organización respecto a un tema específico. En seguridad, una política marca el rumbo y establece el **marco de referencia** que guía las acciones para proteger los activos.

1.7.3.2.- Normativa

Traduce la política en **reglas y requisitos más concretos** que deben cumplirse para seguir esa política. Es decir, establece **qué** se debe hacer o cumplir para mantener la seguridad, y a veces **quién** es responsable de llevarlo a cabo.

1.7.3.3.- Procedimiento

Detalla los **pasos específicos** que deben seguirse para cumplir con la normativa y, por ende, con la política.

1.7.4.- Estándares a aplicar

a) **ISO/IEC 27001: Estandarización en la Seguridad del Puesto de Trabajo**

b) **GDPR (General Data Protection Regulation): Protección de Datos Personales en el Puesto de Trabajo**

c) **LOPDGDD (Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales): Cumplimiento en España para el Puesto de Trabajo**

2.- REFLEXIÓN CRÍTICA

2.1.- ¿Qué te han parecido los temas tratados?

Pienso que la mayor parte de los temas tratados me serán de gran ayuda para mi futuro profesional ya que se hace hincapié en varios aspectos clave de la ciberseguridad como son los principios generales o las medidas de seguridad, los cuales siempre hay que tener en cuenta a la hora de desempeñar cualquier función dentro del sector puesto que nos muestran cómo debemos actuar ante cualquier problemática que nos encontremos.

2.2.- ¿Qué te ha parecido más útil para tu futuro puesto de trabajo en un equipo de seguridad?

Lo que me ha resultado de mayor utilidad son los apartados en los que se hace referencia a las vulnerabilidades y amenazas que nos pueden afectar, ya que para mí es de gran importancia conocer todos los inconvenientes a los que me podría enfrentar en mi futuro laboral y saber cómo solventarlos.

2.3.- ¿Conocías todos los puntos tratados en la unidad? ¿Cuáles no?

Confieso que desconocía por completo la existencia de los planes directores de seguridad. Es el único apartado que me ha pillado de sorpresa.

2.4.- ¿Alguno te ha llamado especialmente la atención? ¿Por qué?

Pues me ha sorprendido gratamente el apartado de los planes directores de seguridad que he mencionado antes, ya que con ellos se analizan al milímetro todas las deficiencias de seguridad que existen en una organización y se

proponen proyectos e iniciativas con el fin de gestionarlas, lo cual, a mi parecer, es indispensable en cualquier empresa.

2.5.- ¿Descartarías algún punto de la unidad? ¿Cuál y por qué?

Se ha hecho mención al principio de la unidad a la diferencia entre sistema informático y sistema de información, y en mi opinión este punto no tiene tanta relevancia como otros presentes en la unidad, así que yo lo omitiría.

2.6.- ¿Has echado en falta algún tema?

Como dije antes a lo largo de la unidad se hace referencia a bastantes puntos clave de la seguridad informática, los cuales, para mí, son los más adecuados para nuestro aprendizaje, luego no echo nada en falta.