Trabajo realizado por:
Álvaro Caro Fernández

ÍNDICE

¿Qué te ha parecido los temas tratados?

Me parecieron muy interesantes y útiles, sobre todo porque tocan aspectos claves de la ciberseguridad que se aplican en el día a día. Algunos conceptos, como el análisis de riesgos y la importancia de proteger el puesto de trabajo, me hicieron pensar sobre cómo se pueden prevenir problemas antes de que ocurran. Además, me gustó cómo se relacionan todos los temas para ofrecer una visión completa y más detallada, con todos los temas en conjunto se entiende mucho mejor todo.

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

El análisis de riesgos y la protección del puesto de trabajo son aspectos clave. El primero posibilita la priorización de esfuerzos en función de los riesgos más relevantes para la organización, mientras que el segundo define acciones específicas para salvaguardar los puntos de acceso más vulnerables, como los dispositivos de los trabajadores.

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

Tenía conocimientos previos sobre la triada CIA (Confidencialidad, Integridad y Disponibilidad) y sobre las medidas de protección del puesto de trabajo.

Sin embargo, no había visto nada sobre la estructura detallada de normativas y procedimientos para proteger el puesto de trabajo, ni en las fases específicas del análisis de riesgos. Me ha sorprendido la importancia de clasificar activos y vincular amenazas con salvaguardas ya que nunca había leído ni estudiado nada relacionado con este tema.

¿Alguno te ha llamado especialmente la atención? ¿Por qué?

El tema de la normativa de protección del puesto de trabajo me llamó la atención porque detalla cómo una política general puede traducirse en normativas específicas y procedimientos prácticos. Esto muestra lo importante que es tener un enfoque completo en seguridad, desde establecer reglas generales hasta definir pasos claros que los empleados puedan seguir.

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

No descartaría ninguno de los puntos porque todos tienen una utilidad evidente para construir una estrategia sólida de ciberseguridad. Sin embargo, algunos apartados, como las explicaciones básicas de ciberseguridad pienso que podrían reducirse o enfocarse más en ejemplos prácticos.

¿Has echado en falta algún tema?

No, con lo que hay creo que es bastante completo el temario pero me parece que podría ser interesante incluir algunos puntos como por ejemplo:

- Gestión de incidentes en tiempo real, para entender cómo actuar frente a ataques cibernéticos en el momento de que ocurran.
- Casos prácticos de análisis de riesgos aplicados a incidentes reales.
- Más ejemplos sobre cómo implementar sistemas de seguridad avanzados en entornos empresariales modernos, como por ejemplo oficinas remotas (desde casa) porque pienso que puede ser uno de los casos en los que podríamos acabar trabajando, en remoto.

Resumen de la unidad

1.1. Principios Generales

La ciberseguridad es la práctica de proteger sistemas, redes y datos de accesos no autorizados, daños o robos. Cada sistema informático es una fortaleza digital que resguarda información valiosa. Para mantenerla segura, la Triada CIA es fundamental:

- **Confidencialidad**: Solo las personas autorizadas deben poder acceder a la información.
- **Integridad**: La información debe ser precisa y no alterada sin permiso.
- **Disponibilidad**: Los sistemas deben estar disponibles para quienes los necesiten.

Además de estos tres pilares, conceptos como fiabilidad, autenticidad y no repudio añaden capas adicionales de protección, garantizando que los sistemas sean no solo seguros, sino también confiables y verificables.

1.2. Análisis de Riesgos

El análisis de riesgos es el proceso de identificar, evaluar y priorizar los riesgos que afectan a una organización. Este análisis es crucial para comprender qué activos son más valiosos y qué amenazas pueden comprometerlos. A través de este proceso, las organizaciones pueden tomar decisiones informadas sobre cómo proteger sus sistemas y datos.

El proceso incluye varias fases:

- **Definir el alcance:** Determinar qué áreas de la organización serán evaluadas.
- **Identificar activos**: Determinar qué elementos son críticos, como datos, sistemas y hardware.
- **Identificar amenazas:** Analizar qué amenazas pueden poner en peligro esos activos.
- **Evaluar el riesgo:** Analizar la probabilidad e impacto de las amenazas.
- **Mitigar el riesgo:** Establecer medidas preventivas, como transferir, eliminar, asumir o mitigar los riesgos.

Este análisis ayuda a priorizar esfuerzos de seguridad y recursos, permitiendo a las organizaciones estar mejor preparadas para posibles incidentes.

1.3. Puesto de Trabajo

El puesto de trabajo es uno de los puntos más vulnerables en ciberseguridad, ya que es donde los empleados interactúan directamente con los sistemas de la organización. La protección de estos puestos es esencial para reducir los riesgos de seguridad.

Es necesario implementar normativas de protección que incluyan medidas como:

- **Restricciones de acceso:** Definir quién puede acceder a qué información.
- **Cifrado de datos:** Asegurar que la información esté protegida incluso si se accede sin permiso.
- **Bloqueo de pantalla:** Evitar que personas no autorizadas tengan acceso a los sistemas cuando los empleados se alejan de sus estaciones de trabajo.

Además, las actualizaciones regulares y el mantenimiento de los dispositivos son cruciales para garantizar que el software y hardware sean seguros y estén al día con las últimas medidas de protección.

1.4. Concienciación y Formación

El componente humano es, muchas veces, el eslabón más débil en la cadena de ciberseguridad. Por eso, concienciar y formar a los empleados es fundamental para proteger los sistemas de la organización. Un programa de concienciación y formación en ciberseguridad debe incluir:

- **Reconocimiento de amenazas:** Enseñar a los empleados a identificar correos electrónicos sospechosos, enlaces maliciosos o archivos adjuntos peligrosos.
- **Buenas prácticas:** Promover el uso de contraseñas seguras, la autenticación multifactor y el cifrado de datos.
- **Simulacros de seguridad:** Realizar ejercicios prácticos para entrenar a los empleados en cómo actuar en caso de un incidente de seguridad.

La formación continua también ayuda a reducir los errores humanos, que son una de las principales causas de brechas de seguridad. Al tener empleados bien preparados, la organización fortalece su defensa contra los ataques cibernéticos.