Actividad 04. Bastionado, defensa en profundidad, ciber resiliencia y Zero Trust

Existen varias técnicas que ayudan a mejorar la seguridad de los sistemas de información:

Hardening o bastionado de sistemas

Consiste en el endurecimiento del sistema, con el fin de reducir y evitar las amenazas y los peligros de este.

Defensa en profundidad

Es un concepto que implica el uso de múltiples capas de seguridad para mantener la información segura.

Ciber resiliencia

Basado en la premisa de que no se confía ciegamente en nadie y se le permite acceder a los activos de la empresa hasta que hayan sido validados como legítimos y autorizados.

Zero Trust o confianza cero

Describe la capacidad de un sistema u organización para resistir y/o recuperarse ante ataques o incidentes cibernéticos.

En los siguientes artículos se habla sobre bastionado, defensa en profundidad, ciber resiliencia y Zero Trust:

- ¿Qué es el Hardening en Ciberseguridad?
- ¿Qué es el hardening de sistemas en informática?
- ¿Qué es la defensa en profundidad?
- ¿Qué es la defensa en profundidad? | Seguridad en capas
- ¿Qué es la ciber resiliencia?
- Ciber resiliencia: la clave para sobreponerse a los incidentes
- ¿Qué es el modelo Zero Trust en ciberseguridad?
- ¿Qué es el modelo Zero Trust?

En los siguientes vídeos se habla sobre el uso de Firewall:

- Bastionado de Sistemas | Minimiza el riesgo de tu negocio
- Defensa en profundidad
- ¿Qué es ciber resiliencia?
- ¿Qué es ZERO TRUST?

Se pide:

- Realiza un documento explicando los conceptos de Bastionado de sistemas, Defensa en profundidad Ciber resiliencia y Confianza cero.