Actividad 04. Bastionado, Defensa en Profundidad, Ciber Resiliencia y Zero Trust

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

BASTIONADO DE SISTEMAS:

Es un proceso de endurecimiento y configuración de sistemas informáticos para minimizar la superficie de ataque. Implica deshabilitar servicios y puertos innecesarios, aplicar parches de seguridad, configurar adecuadamente los permisos y accesos, y eliminar el software no esencial. El **objetivo** es reducir al mínimo las vulnerabilidades que pueden ser explotadas por atacantes.

Sus **características clave** son:

- ***Reducción de Superficie de Ataque***: Si se limita la cantidad de servicios y funcionalidades activas en el sistema, se disminuyen las posibles vías de acceso para los atacantes.
- ***Configuración Segura***: Se deben establecer configuraciones de seguridad que limiten los privilegios y accesos, impidiendo que los usuarios y/o aplicaciones no autorizadas realicen acciones potencialmente peligrosas.
- ***Actualización continua***: Se debe implicar la aplicación regular de actualizaciones y parches de seguridad para proteger los sistemas contra vulnerabilidades conocidas.

DEFENSA EN PROFUNDIDAD:

Es una estrategia de seguridad que emplea múltiples capas de protección para salvaguardar los activos de una organización. En lugar de confiar en una barrera de seguridad única, se implementan diversas medidas de seguridad en capas, de modo que si se falla una capa, las demás continúan proporcionando protección.

Sus **componentes de la Defensa en Profundidad** son:

- ***Perímetro de Red***: Firewalls y sistemas de detección de intrusos (IDS/IPS) que controlan el tráfico de entrada y salida.
- ***Seguridad de Red Interna***: Segmentación de la red y control de accesos para limitar la capacidad de un atacante de moverse lateralmente dentro de la red.
- ***Protección en los Dispositivos Finales***: Antivirus, antimalware, cifrado de datos para proteger los dispositivos de usuario.
- ***Capas Adicionales***: Autenticación multifactor (MFA), políticas de gestión de contraseñas, auditorías regulares.

CIBER RESILIENCIA:

Es la capacidad de una organización para prepararse, responder y recuperarse de incidentes cibernéticos. No sólo es enfocarse en la prevención de ataques, sino también en la continuidad del negocio y la rápida recuperación ante cualquier eventualidad. Consiste en un enfoque integral que combina la seguridad cibernética con la gestión de riesgos y la planificación de la continuidad del negocio.

Sus **elementos** son:

- ***Prevención***: Implementación de controles de seguridad para evitar incidentes.
- ***Detección***: Habilidad para identificar rápidamente cuando un incidente ha ocurrido.
- ***Respuesta***: Capacidad para mitigar el impacto de un incidente en curso.
- ***Recuperación***: Estrategias para restaurar operaciones normales lo más rápido posible tras un incidente.

ZERO TRUST:

Se basa en el principio de que ninguna entidad (interna o externa), debe ser automáticamente confiable. Todo acceso debe ser verificado y autenticado antes de permitir la conexión a recursos o datos. Este enfoque asume que las amenazas pueden venir desde dentro y fuera de la

organización, y que cada solicitud de acceso debe ser tratada con escepticismo.

Sus **principios del modelo de Confianza Cero (Zero Trust)** son:

- ***Verificación Continua***: Cada solicitud de acceso se verifica, independientemente de dónde provenga.
- ***Mínimos Privilegios***: Los usuarios y aplicaciones sólo reciben los permisos estrictamente necesarios para realizar sus funciones.
- ***Segmentación***: La red y los recursos están segmentados para contener posibles ataques y limitar el movimiento lateral.