Ciberseguridad avanzada

BlasAST

May 2025

Índice

1. Introducción

La ciberseguridad es una disciplina fundamental en esta era digital, las amenazas cibernéticas crecen en complejidad y frecuencia a la vez que las organizaciones se vuelven cada vez más dependientes de la tecnología para sus tareas diarias. Proteger la información y los sistemas se convierte en una prioridad importantisima. Para entender la ciberseguridad se necesita un conocimiento sólido de los fundamentos que la conforman, incluyendo modelos organizativos, conceptos básicos y tecnológicos al igual que el rol que desempeñan las personas en este ámbito.

1. Los modelos organizativos en ciberseguridad proporcionan una estructura para implementar gestionar y superviar las estrategias de protección de la información de una organización.
2. Los conceptos basicos y tecnológicos son sobre los que se construye todo el sistema de protección incluyendo los conocimientos de los tipos de amenazas que hay.
3. El rol de las personas es importante dado que son una parte vital de la defensa dado que son el eslabon más debil y más fuerte de la cadena. Hay que concienciar a todos los empleados para que no comprometan información de la organización.

Las amenazas cibernéticas evolucionan constantemente por lo que los conocimientos y habilidades deben de actualizarse continuamente. TODO debe funcionar en armonía con los demás componentes de para proteger lo máximo posible.

2. Modelos organizativos

Estructuras que estratégicas que determinan cómo una organización gestiona, aborda y protege sus activos digitales frente a amenazas cibernéticas. Es imprescindible para garantizar la seguridad y la resiliencia frente a posibles ataques. Para que un modelo organizativo sea robusto debe de comenzar con una clara definición de roles y responsabilidades en la organización dejando claro quien es el responsable de la seguridad en distintos niveles y que entienda que sus miembros entiendan su papel.
Debe de haber políticas claras y procedimientos estandares que guíen las acciones de la organización en diversas situaciones. Desde política de contraseñas, manejo de datos sensibles, respuestas a incidentes de seguridad y formación continua de los empleados. Frente a un incidente cibernético debe de darse una respuesta rapida coherente y efectiva, minimizando así el impacto en la organización.
Estos modelos organizativos deben de ser también lo suficientemente flexibles para adaptarse a las necesidades de la organización y a las distintas amenazas en evolución. Por ello, las organizaciones debe de estar dispuestas a revisar y ajustar sus modelos a medida que sugen nuevas tecnologías y amenazas.

Con un modelo organizativo bien diseñado conseguimos una defensa solida.

Tipos de modelos:

- Centralizado: (todas las decisiones y funciones de seguridad se concentran en un solo equipo o departamento, normalmente ÇISO - Chief Information Security Officer") manejando politicas, procedimientos y controles de seguridad.

Ventajas:

1. Consistencia en la aplicación de las políticas de seguridad.
2. Mejor coordinación y control centralizado de los recursos de seguridad.
3. Facilidad de implementar estándares uniformes en toda la organización.

Desventajas:

1. Puede ser menos ágil al responder a incidentes locales o específicos
2. Riesgo de sobrecargar el equipo central con todas las responsabilidades
3. La falta de autonomía en las unidades locales puede limitar la adaptabilidad

- Descentralizado: (Las responsabilidadesse distribuyen en diferentes departamentos o unidades de negocio cada una con su equipo y toman decisiones de manera independiente bajo las directrices generales de la organización)

Ventajas:

1. Mayor flexibilidad y rapidez para responder a amenazas locales o específicas
2. Adaptación de las políticas de seguridad a las necesidades de cada unidad
3. Fomenta la autonomíay la responsabilidad en distintas áreas de la organización

Desventajas:

1. Riesgo de inconsistencias al aplicar las políticas de seguridad
2. Posible generación de duplicación de esfuerzos y recursos
3. Dificultad en la coordinación y comunicación entre equipos de seguridad

3. Conveptos básicos y tecnológicos

La ciberseguridad abarca una amplia gama de conceptos básicos y tecnológicos para proteger la integridad, confidencialidad y disponibilidad de la información en un entorno digital.
Con el aumento de las amenazas cibernéticas conocer sobre esto es fundamental para organizaciones de todos los tamaños y sectores.
A continuación