Conceptos Fundamentales

Ámbito Ciberseguridad

Contribuye a las necesidades básicas de la seguridad, seguridad, fiabilidad y disponibilidad de la infraestructura

Se basa en la seguridad de la información, seguridad de aplicaciones, seguridad de red y segurisas de Internet

Términos que se basan en Ciberespacio

Se dividen en tres categorías.
Tangibles
Intangibles
Relacionados con la red

- Ciberterrorismo
- Cibercrimen
- Ciberguerra
- Ciberseguridad

El ciberespacio incluye elementos tangibles pero tambien es virtual, también todas las definiciones incluyen información, esta información son datos, señalización entre procesos y dispositivos.

Naturaleza del ciberespacio

Capa de información son: la creación, captura, almacenamiento y procesado de datos
La capa de personas son: los usuarios activos

Capa física son : Ordenadores, Servidores, Cables entre otros

Capa lógica son : servicios de nivel más bajo, aplicaciones, servicios mas complejos

Existen 4 capas que son las siguientes:
- Personas
- Información
- Bloques lógicos
- Fisica

Servicios de nivel más bajo

-Entornos de ejecución de programas
- Los mecanismos de transporte de datos

- los estándares para el formato de datos

NORMAS ISO

Para mejorar el estado de ciberseguridad, los implicados en el ciberespacio tienen que jugar un papel activo en su respectivo uso y en el desarrollo de Internet.

Norma ISO 27032

- **Las redes públicamente visibles son las redes expuestas a Internet.**

GUÍAS DE USUARIO

Usuarios

-Usuario de una aplicación del ciberespacio

-Comprador/vendedor

-Blogger

-Miembro de una organización

Consumidores

Proporcionan Información de un cierto tema dentro de un espacio de una APP en el ciberespacio.

Medidas preventivas

- - Gestión adecuada de la seguridad de la información mediante la operación de un sistema de gestión. ISO 27001 proporciona requisitos para un SGSI
- - Incorporación de seguridad como parte del ciclo de vida del desarrollo de software SDLC.
- - Adecuada monitorización de la seguridad

Como soporte a esta norma

1. El estándar ISO/IEC 29147 proporcionará guías para la revelación de vulnerabilidades.
2. ISO/IEC proporciona guías de preparación de continuidad en el negocio
3. ISO/IEC 27035 gestión de incidentes de seguridad.
4. ISO/IEC 27034-1 proporciona guías de seguridad en aplicaciones

PRINCIPIOS DE SEGURIDAD

ISO 27032

1. La Seguridad de las Aplicaciones
2. La Seguridad en la Redes
3. Seguridad en Internet

- Una introducción a la evaluación y gestión de riesgos
- Directrices para los consumidores
- Directrices para las organizaciones, incluyendo proveedores de servicio
  - Gestión de riesgos de la información de seguridad en la empresa
  - Requisitos de seguridad para los servicios de alojamiento y otros servicios de aplicaciones

EVALUACIÓN Y GESTIÓN DE RIESGOS

ISO 31000
- Gestión de riesgos
- Principios y directrices

ISO/IEC 27005
- Tecnología de la información
- Técnicas de seguridad
- Gestión de riesgos de la seguridad de la información

Aspectos han de tenerse en cuenta al definir el enfoque para la gestión de riesgos:
- Identificación de activos críticos
- Identificación de riesgos
- Responsabilidad
  - Reconocimiento
  - Retirada del sistema o servicio
  - Consistencia

GUÍA DE SEGURIDAD PARA CLIENTES

Los proveedores de servicios deben orientar a los consumidores sobre cómo mantenerse seguros en línea

El proveedor de servicio nunca le pedirán:
- Información personal
- Nombres de usuarios
- Contraseñas
- Nunca incluirán enlaces relacionados con la seguridad para que el lector haga clic.

GUÍAS PARA CONSUMIDORES

1. **Conocer y comprender la política de seguridad y privacidad del sitio o la aplicación**
2. **Conocer y comprender los riesgos de seguridad y privacidad involucrados y determinar los controles aplicables.**
3. **Establecer y poner en práctica una política de privacidad para proteger la identidad personal**
4. **Reducir al mínimo el intercambio de información personal**
5. **Informar sobre eventos o encuentros sospechosos**
6. **Asegurarse de que la privacidad de los interesados no se dan a conocer**
7. **Proporcionar documentación de seguridad del código y las políticas**
8. **Asegurarse de que la privacidad de los interesados y la información sensible no se dan a conocer**
9. **Aprender y entender la política corporativa de seguridad de la información de la organización**
10. **Cuando un consumidor visita un sitio que requiere autorización y consigue acceder de forma no intencionada, el usuario puede ser etiquetado como un intruso**

GUÍAS PARA ORGANIZACIONES

Gestionar los riesgos de seguridad de información en la empresa

Requisitos de seguridad para alojamiento de webs y otros servicios de aplicaciones

Proporcionar una guía de seguridad para los consumidores