Servicios de nivel más bajo

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

datos

- los estándares para el formato de datos

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

Términos que se basan en

Ciberespacio

Contribuye a las necesidades básicas de la seguridad. seguridad, fiabilidad y

Ámbito

Cibersegur — Conceptos
idad Fundamentales

señalización entre procesos y dispositivos.

Ciberterrorismo

Cibercrimen

Ciberguerra

Ciberseguridad

información, seguridad de aplicaciones, seguridad de red y El ciberespacio incluye elementos tangibles pero segurisas de Internet tambien es virtual, también todas las definiciones incluyen información, esta información son datos,

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

Naturaleza del ciberespacio Existen 4 capas que son las siguientes:

- Personas
- Información
- Bloques lógicos
- Fisica

Capa física son: Ordenadores.

Capa lógica son: servicios de nivel más Servidores, Cables bajo, aplicaciones,

entre otros servicios mas complejos

REDACTEUR.COM

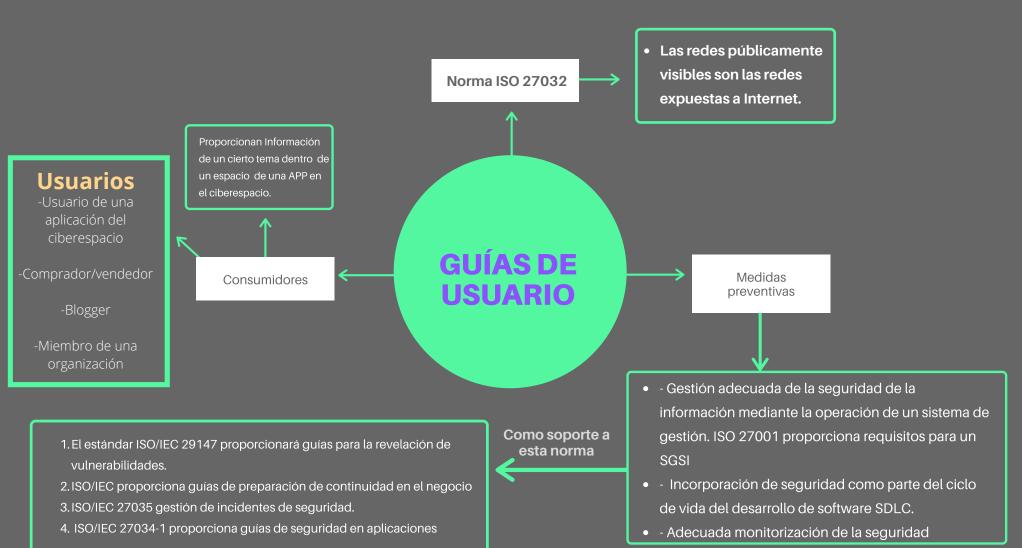
Se basa en la seguridad de la

disponibilidad de la infraestructura

usuarios activos

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.



- 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

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
 - o Retirada del sistema o servicio
 - Consistencia

ISO 27032

PRINCIPIOS DE SEGURIDAD

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 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

GUÍAS PARA CONSUMIDORES

EVALUACIÓN Y GESTIÓN DE RIESGOS

- Conocer y
 comprender la
 política de seguridad
 y privacidad del sitio
 o la aplicación
- 4. Reducir al mínimo el intercambio de información personal
- 7. Proporcionar documentación de seguridad del código y las políticas
- 2. Conocer y comprender los riesgos de seguridad y privacidad involucrados y determinar los controles aplicables.
 - 5. Informar sobre eventos o encuentros sospechosos
- 8. Asegurarse de que la privacidad de los interesados y la información sensible no se dan a conocer

- 3. Establecer y poner en práctica una política de privacidad para proteger la identidad personal
- 6. Asegurarse de que la privacidad de los interesados 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