Manual de seguridad del UIT-T – 4.ª edición

- Requisitos y arquitecturas de seguridad
- Aspectos de la gestión de seguridad
- Directorio, autenticación y gestión de identidad
- Seguridad de la infraestructura de red
- Planteamientos específicos a la seguridad de la red
- Seguridad de aplicación
- Contrarrestar amenazas comunes en las redes
- El futuro de la normalización de seguridad de las TIC/ telecomunicaciones

La hoja de ruta de las normas de seguridad de las TIC

Parte 1: Organizaciones de desarrollo de normas TIC y sus trabajos

Parte 2: Normas de seguridad TIC aprobadas (base de datos con enlaces directos)

Parte 3: Normas de seguridad en desarrollo

Parte 4: Futuras necesidades y nuevas normas de seguridad propuestas

Parte 5: Mejores prácticas de seguridad

Parte 6: Panorama de la gestión de identidades (IdM).

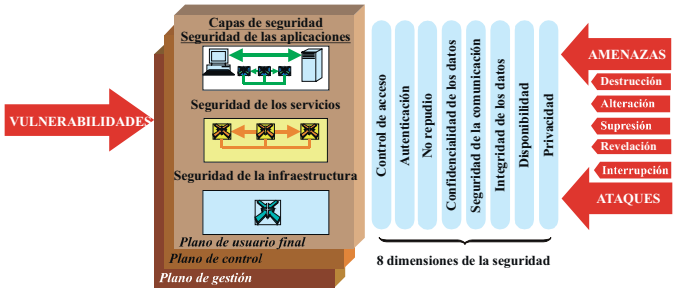
Compendios de seguridad

- Catálogo de las Recomendaciones aprobadas relacionadas con la seguridad de las telecomunicaciones
- Lista de las definiciones de seguridad extraída de las Recomendaciones UIT-T aprobadas
- Resumen de las Comisiones de Estudio del UIT-T con actividades relacionadas con la seguridad
- Resumen de las Recomendaciones que se están revisando para incluir consideraciones sobre seguridad
- Resumen de otras actividades de seguridad de la UIT.

Arquitecturas de seguridad

La Recomendación UIT-T X.805 "Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo", así como algunas arquitecturas específicas de la aplicación, fueron elaboradas para abordar temas como la gestión de red, las comunicaciones entre pares y los servidores móviles de la web.

La arquitectura de la X.805 que se describe más abajo se define en tres conceptos principales para una red de extremo a extremo: las capas de seguridad, los planos de seguridad y las dimensiones de seguridad. Se adopta un criterio jerárquico al dividir los requisitos de seguridad entre las capas y los planos, garantizando que se logra la seguridad de extremo a extremo.



Esta arquitectura puede utilizarse como base para una evaluación de la seguridad o para orientar el desarrollo de una política de seguridad, una respuesta en caso de incidente y planes de recuperación, así como la elaboración de arquitecturas de tecnología, teniendo en cuenta la dimensión de seguridad aplicable en cada capa y plano de seguridad durante la fase de definición y planificación.

www.itu.int/itu-t/studygroups

Unión Internacional de Telecomunicaciones

Seguridad

Desarrollar la confianza y la seguridad en la utilización de las TIC (CMSI – Línea de acción C.5)

01.2012 tsbpromo@itu.int

UIT-T

Seguridad de las TIC/ telecomunicaciones

Los trabajos del UIT-T sobre seguridad de las TIC/telecomunicaciones están en curso desde hace más de dos décadas. Varias Comisiones de Estudio han elaborado Recomendaciones y directrices en algunos ámbitos fundamentales. La Comisión de Estudio 17 asume actualmente la responsabilidad principal para los trabajos del UIT-T en materia de seguridad y ha sido designada como la Comisión de Estudio rectora para las cuestiones de seguridad.

Protección de activos

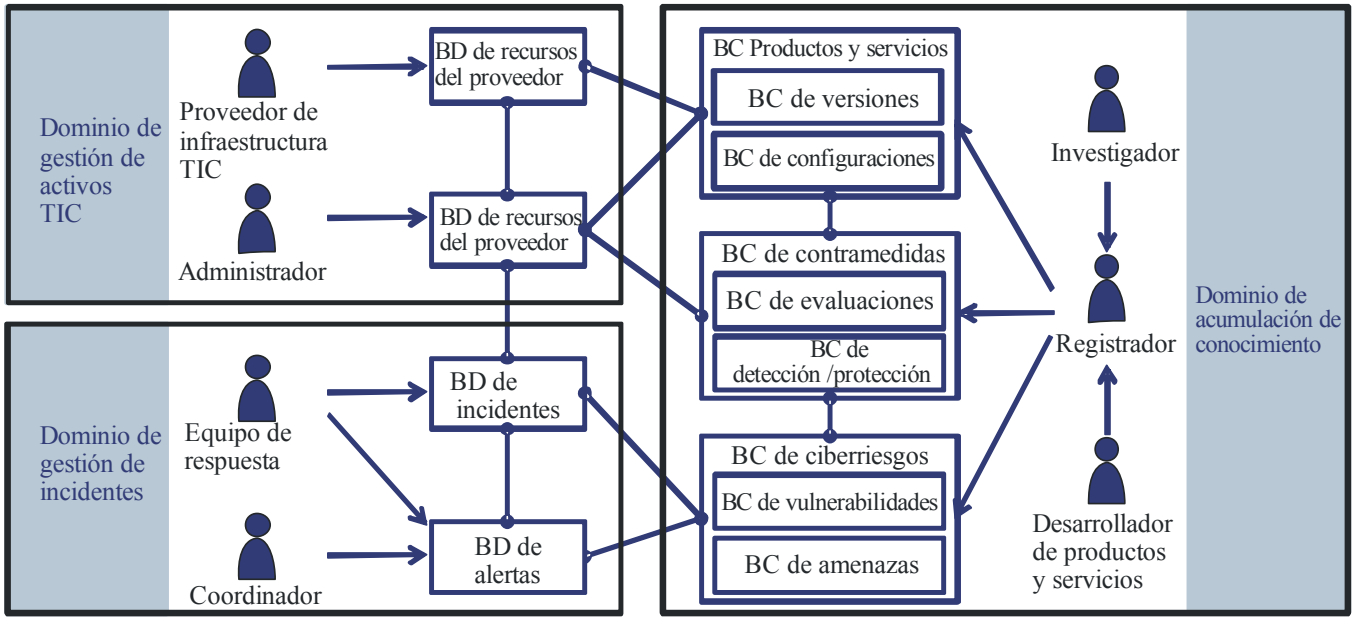
En lo que respecta a la seguridad de las TIC, en términos generales habrá que proteger los dispositivos de las siguientes partes interesadas:

- clientes/abonados que necesitan confiar en la red y en los servicios que se ofrecen, incluida la disponibilidad de los servicios (en particular de los servicios de emergencia);
- comunidad/autoridades públicas que demandan seguridad mediante directrices y/o leyes, con el fin de garantizar la disponibilidad de los servicios, la libre competencia y la protección privada;
- los propios operadores de red/proveedores de servicio que precisan seguridad para salvaguardar su explotación y sus intereses económicos y para cumplir sus obligaciones con los clientes y el público, en el ámbito nacional e internacional.

Rec. UIT-T de la serie X.1500 – Intercambio de información de ciberseguridad

La serie CYBEX presenta técnicas para el intercambio de información de ciberseguridad, a través de las siguientes funciones básicas, que pueden utilizarse por separado o conjuntamente, según corresponda:

- estructurar la información de seguridad para la realización de intercambios;
- identificar y descubrir información y entidades de ciberseguridad;
- establecer confianza y acuerdos sobre la política entre entidades que realicen intercambios;
- realizar peticiones y respuestas con información de ciberseguridad;
- garantizar la integridad del intercambio de información de ciberseguridad.



BD= Base de datos, BC= Base de conocimiento

La figura anterior ilustra en qué consiste el CYBEX, presentado en forma de un contexto operativo. Las operaciones de ciberseguridad se desarrollan principalmente en tres ámbitos: la gestión de incidentes, la gestión de activos de TIC y la acumulación de los conocimientos.