Vulnerabilidad en la seguridad de las redes eléctricas.

Las redes eléctricas se pueden considerar como sistemas con infraestructuras críticas, por lo que el control remoto y la supervisión de las redes eléctricas pueden ser vulnerables ante amenazas como:

- Ataques externos
- Ataques internos
- Desastres naturales
- Fallas de equipo
- Descuidos
- Manipulación de información
- Pérdida de información

Imágenes tomadas y utilizadas conforme a la licencia de Shutterstock.com

Algunas de las consecuencias o reacciones de las vulnerabilidades antes mencionadas pueden ser de tipo: **legal, social, financiero** y, en otros casos, se pueden presentar **daños físicos** al equipo.

Además, para conocer los requerimientos en términos de confiabilidad, disponibilidad, integridad y no rechazo de información, como parte de la seguridad de la información, se presenta el estándar **IEC/TS 62351,** donde se pueden observar los métodos y objetivos para asegurar la seguridad en el control de la red eléctrica a través de las redes de comunicación.

El alcance de la serie del estándar **IEC/TS 62351**, está enfocada en la seguridad de la información especialmente para las operaciones del control de la red eléctrica. Sus dos principales objetivos se pueden agrupar como:

Los principales estándares definidos por la **IEC TC 57** y están formulados especialmente para:

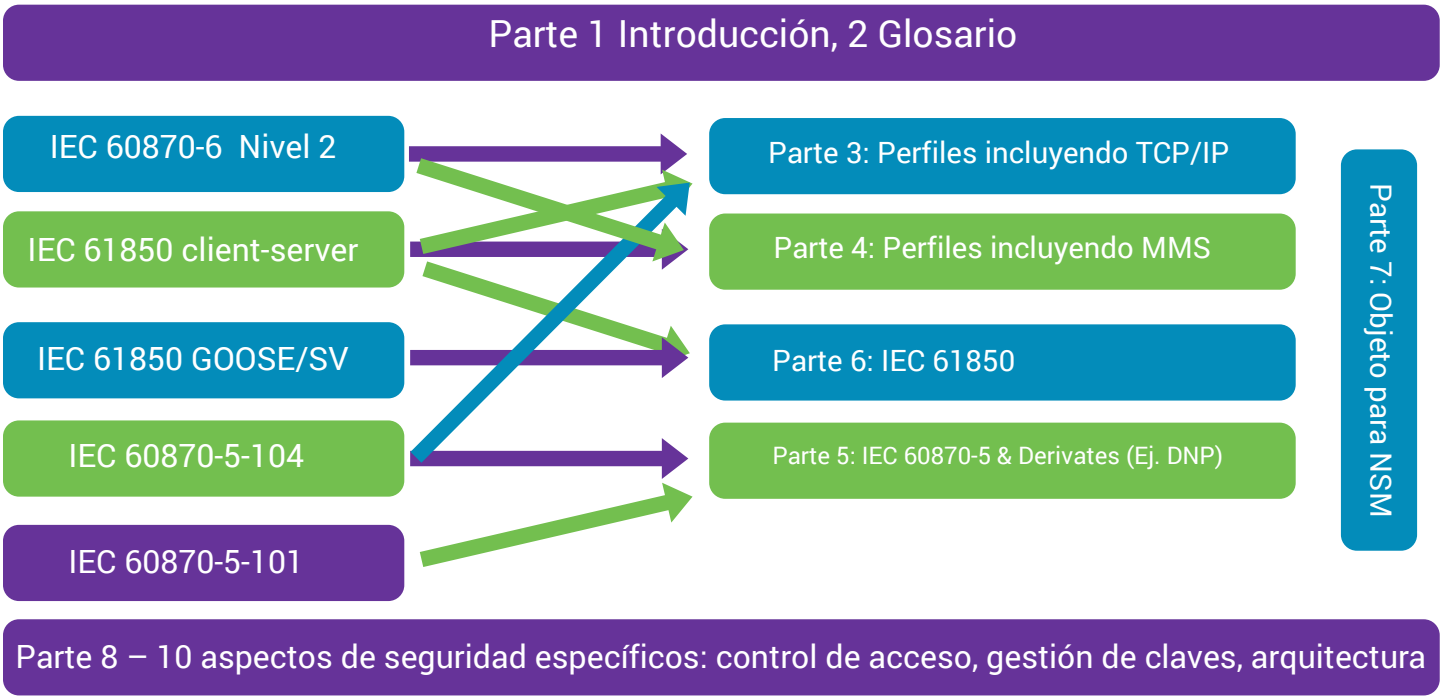
- La serie **IEC 60870-5**, en los siguientes apartados:

    - 101 y 104 para el centro de control de la subestación.
    - 102 para medición.
    - 103 para la protección de comunicación.

- La serie **IEC 60870-6** para el control interno del centro de comunicaciones.
- La serie **IEC 61850** para la comunicación multinivel en los sistemas eléctricos.
- La serie **IEC 61970** para la administración de datos a nivel transmisión.
- La serie **IEC 61968** para la administración de datos a nivel distribución.

El desarrollo de estándares o reportes técnicos de soluciones finales de seguridad.

La estructura de la serie del estándar **IEC/TS 62351**, consiste en diferentes partes las cuales consideran objetivos específicos de seguridad de información. En la siguiente imagen, se muestra la estructura en relación con los estándares de comunicación:



En la **parte 1** da una introducción de las partes subsecuentes del estándar, introduce varios aspectos de seguridad de información de acuerdo a la operación de la red eléctrica. Así, en la **parte 2** se presenta un glosario de términos.

De la **parte 3 a la 6,** se especifican los estándares de seguridad para los protocolos de comunicación **IEC TC 57** y los perfiles de las capas especiales **TCP/IP and MMS** (Manufacturing Message Specification), los cuales proveen varios niveles de seguridad en la comunicación, dependiendo sobre el protocolo y los parámetros que se definen en determinada implementación.

La **parte 7** es un área específica de la seguridad extremo a extremo. También conocida como **administración del sistema de red o NSM (Network System Management)**, esta provee la administración de la infraestructura de la comunicación de la red, y de forma análoga, la **SNMP** (simple network management protocol) la cual es aplicada al control de la red local para la comunicación de las PC.

De las **partes 8 a la 10,** se define la administración de aspectos de seguridad específicos, los cuales también son validados por el administrador de base de datos aplicando el CIM (Common information model).

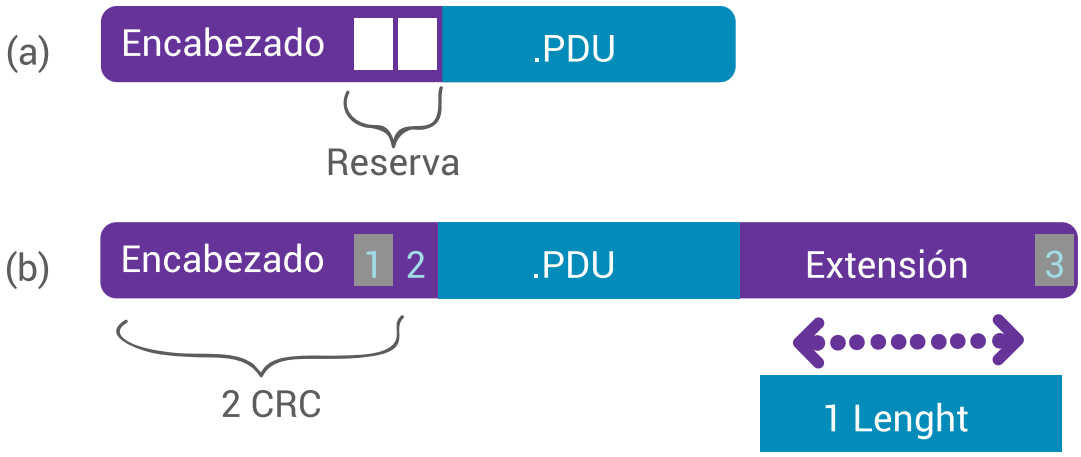
Las diferentes partes del estándar definen una gran variedad de mediciones y protecciones contra:

- Acceso a información sin autorización.
- Modificación o robo de información sin autorización.
- Pérdida de información.
- Denegar el servicio o prevención de acceso sin autorización.
- Responsabilidad para la pérdida de información, la cual incluye:
- Denegar los eventos que tomaron lugar.
- Hacer peticiones de eventos que no tomaron lugar.

Adicionalmente (para las características como la encriptación, firewalls, antivirus/spyware, passwords, etc.), un elemento clave en las medidas de seguridad de la información consiste en la introducción de la autorización mediante el **control de acceso basado en rol o RBAC (Role-Based Access Control)** a través de una firma digital agregada al protocolo de cada paquete enviada desde el cliente al servidor o fabricante.

Imágenes tomadas y utilizadas conforme a la licencia de Shutterstock.com

Por otra parte, la **HMAC (Keyed-Hash Message Authentication Code)**, es un método para la construcción y el cálculo del código de autentificación del mensaje, el cual incluye datos de una función criptográfica en combinación con una llave. La diferencia entre estos dos métodos se puede observar en la siguiente imagen, donde el ejemplo (a) no cuenta con autenticación y el (b) si:



Por último, el trabajo acerca del desarrollo de la estandarización de la seguridad de datos y comunicación para la administración y operación de la red eléctrica, aún está en crecimiento debido al desarrollo e implementación de la actualización de la red eléctrica, con el objetivo de detectar problemas y amenazas en las áreas de la seguridad de la información.