INSTITUTO SUPERIOR TECNOLÓGICO QUITO

Seguridad Web

Unidad 1: Fundamentos

1.1 Seguridad de la Información y Seguridad Informática

- La seguridad de la Información es un concepto con un enfoque holístico orientado a proteger.
- La seguridad informática comprende herramientas tecnológicas de protección.
- La seguridad de la Información es un concepto más amplio que incluye a la seguridad informática.

1.1 Seguridad de la Información y Seguridad Informática

Sin seguro

Con seguro

1.2 Confidencialidad, Integridad y Disponibilidad

- **CIA Triad:** Confidentiality, Integrity and Availability.
- Define tres propiedades que como mínimo debe garantizar la seguridad de la información.
- **Confidencialidad:** Únicamente los usuarios autorizados puedan acceder a la información.
- **Integridad:** Orientada a evitar operaciones de modificación o eliminación.
- **Disponibilidad:** Garantiza que los recursos se encuentren disponibles cuando se los requiera.

1.2 Confidencialidad, Integridad y Disponibilidad

- **Confidencialidad:** La confidencialidad está orientada a precautelar el secretismo de un mensaje.
- El principal medio para lograr esto es a través de métodos de criptografía.
- Criptografía: Busca garantizar el secretismo del mensaje.
- Criptoanálisis: Busca romper el secretismo de mensaje.

Criptología = Criptografía + Criptoanálisis.

1.2 Confidencialidad, Integridad y Disponibilidad

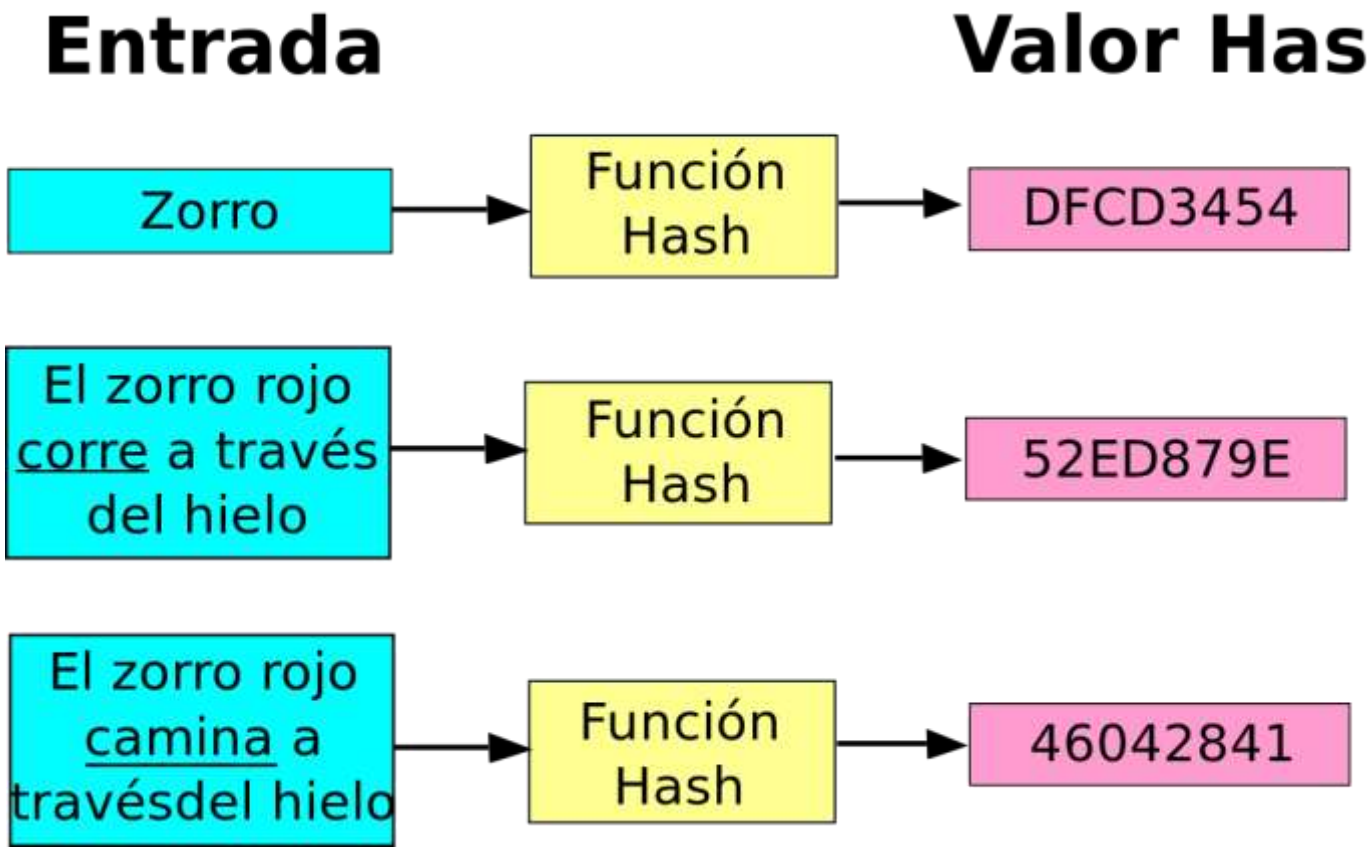
- El mejor ejemplo está en el caso de la Enigma del ejército alemán.
- Alan Turing junto con su equipo de trabajo rompió los código cifrados.

1.2 Confidencialidad, Integridad y Disponibilidad

1.2 Confidencialidad, Integridad y Disponibilidad

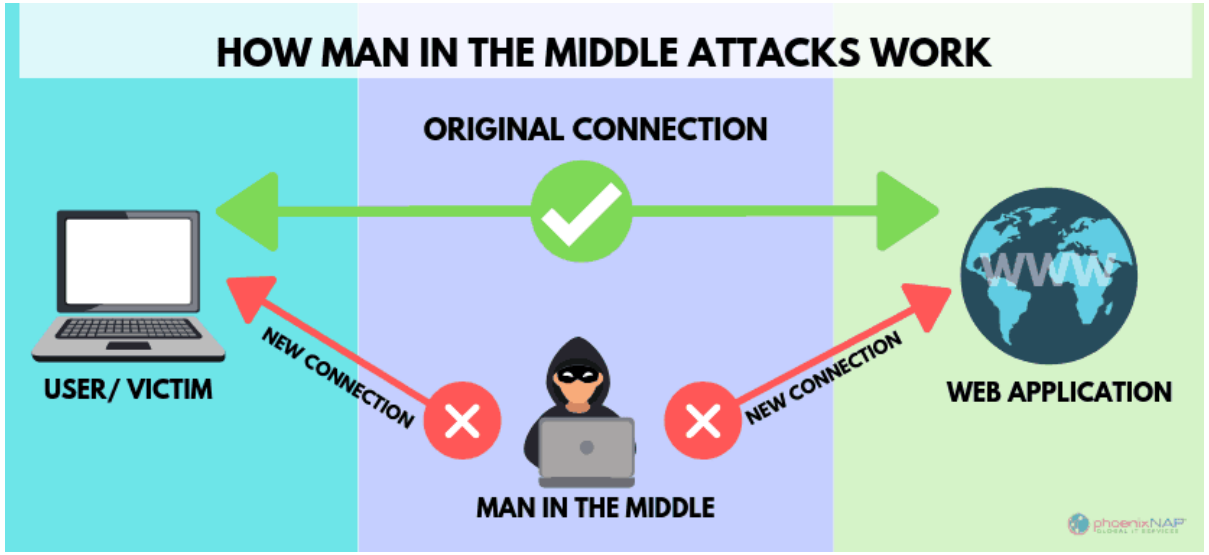
- **Integridad:** Se logra a través de códigos hash (digests o resúmenes).
- El código hash es único para cada mensaje.
- El código hash no es reversible, es decir, no se puede obtener el mensaje original a partir del mismo.
- Si dos mensajes son iguales entonces sus códigos hash serán los mismos.
- Esto permite identificar modificaciones al mensaje original.

1.2 Confidencialidad, Integridad y Disponibilidad



1.2 Confidencialidad, Integridad y Disponibilidad

- **Principales ataques:**
- Eavesdropping.
- Modificaciones no autorizadas.
- Man in the middle.



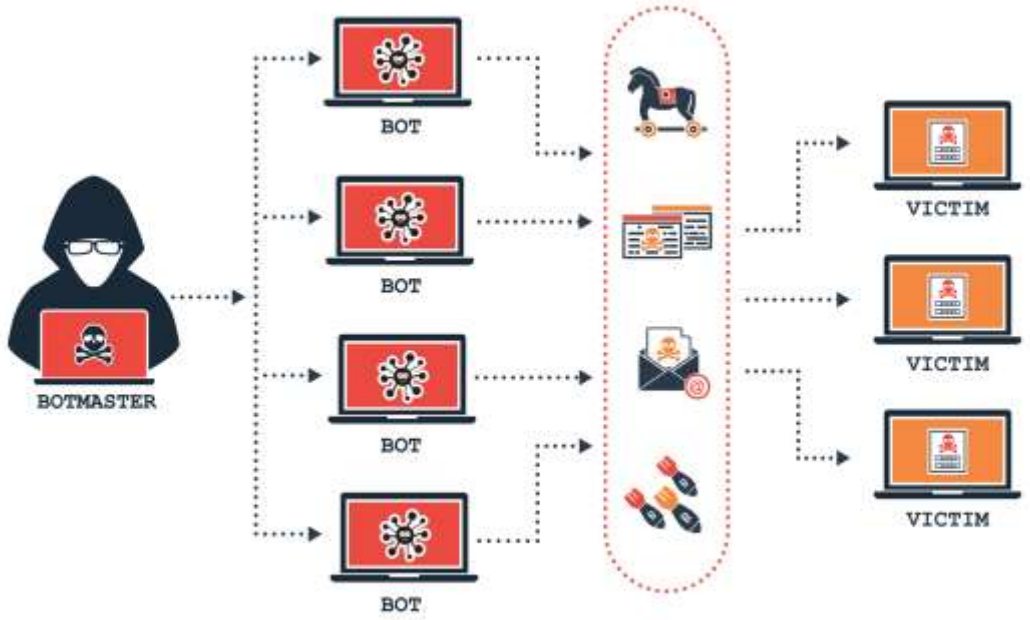
1.2 Confidencialidad, Integridad y Disponibilidad

- **Disponibilidad:** Busca garantizar que los recursos estén disponibles cuando se los requiera.
- El no garantizar este principio ha hecho perder millones de dólares a cientos de compañías alrededor del mundo.

- **Principales amenazas:**
- Denial of Services (DoS)
- DDoS
- Buffer overflow
- Cortes de energía!

1.2 Confidencialidad, Integridad y Disponibilidad

- **Botnet:** Red de computadores comprometidos para perpretar ataques de DDoS.



1.2 Confidencialidad, Integridad y Disponibilidad

- **Hackers:** Generalmente se distinguen tres tipos: White hat, Grey hat and Black hat.
- Se han propuestos otros colores como el Blue hat para testers y el Green o Yellow hat para newbies.

Kevin Mitnick

1.3 Autenticación, Autorización y Auditoría

- **Autenticación:** Comprobar que la entidad es quien dice ser.
- **Autorización:** Limitar las acciones del usuario autenticado.
- **Auditoría:** Generar mensajes de log que ayuden a corroborar y correlacionar eventos.

1.3 Autenticación, Autorización y Auditoría

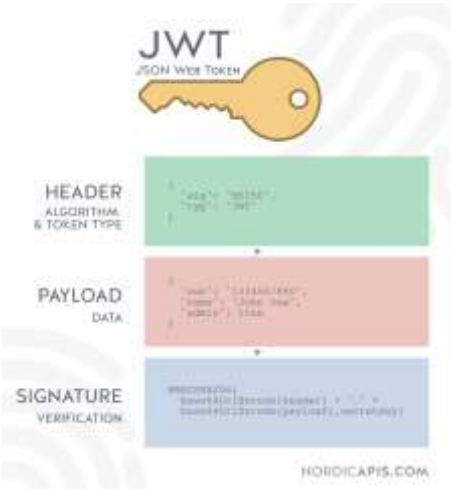
- **Autenticación:** Verificar la identidad de la entidad que hace uso del servicio.

	Descripción	Ejemplos
Conocimiento	Algo que conozco	Password, PIN
Posesión	Algo que poseo	Smart card, badge, token
Características	Algo que soy	Fingerprint, hand geometry, keystroke dynamic

- Se recomienda emplear esquemas de autenticación múltiple.

1.3 Autenticación, Autorización y Auditoría

- **Autenticación Web:** Uso de cookies y tokens.
- **Cookies:** Ficheros que se almacenan en el lado del cliente para guardar su sesión y preferencias de usuario.
- **Token:** Se entrega después de la autenticación del usuario y permite (Ejemplos: Bearer, JWT)



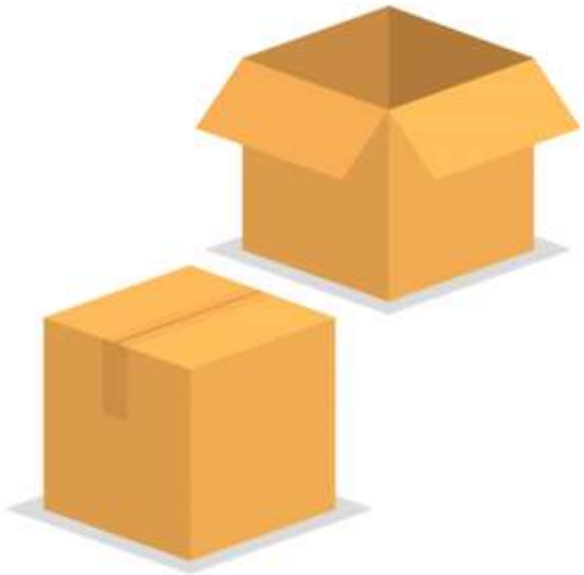
1.3 Autenticación, Autorización y Auditoría

- **Autorización:** Brinda una serie de derecho generalmente a través de reglas o roles.
  - **Reglas:** Conocidas como ACL (Access Control List).
  - **Roles**: Conocido RBAC (Role Based Authentication Control).

- **Denegación implícita:** Los modelos deben tener una sentencia de denegación implícita si no se cumple ningún parámetro de la ACL.
- **Necesidad de saber:** Se brinda los derechos sí y solo sí el usuario lo requiere.

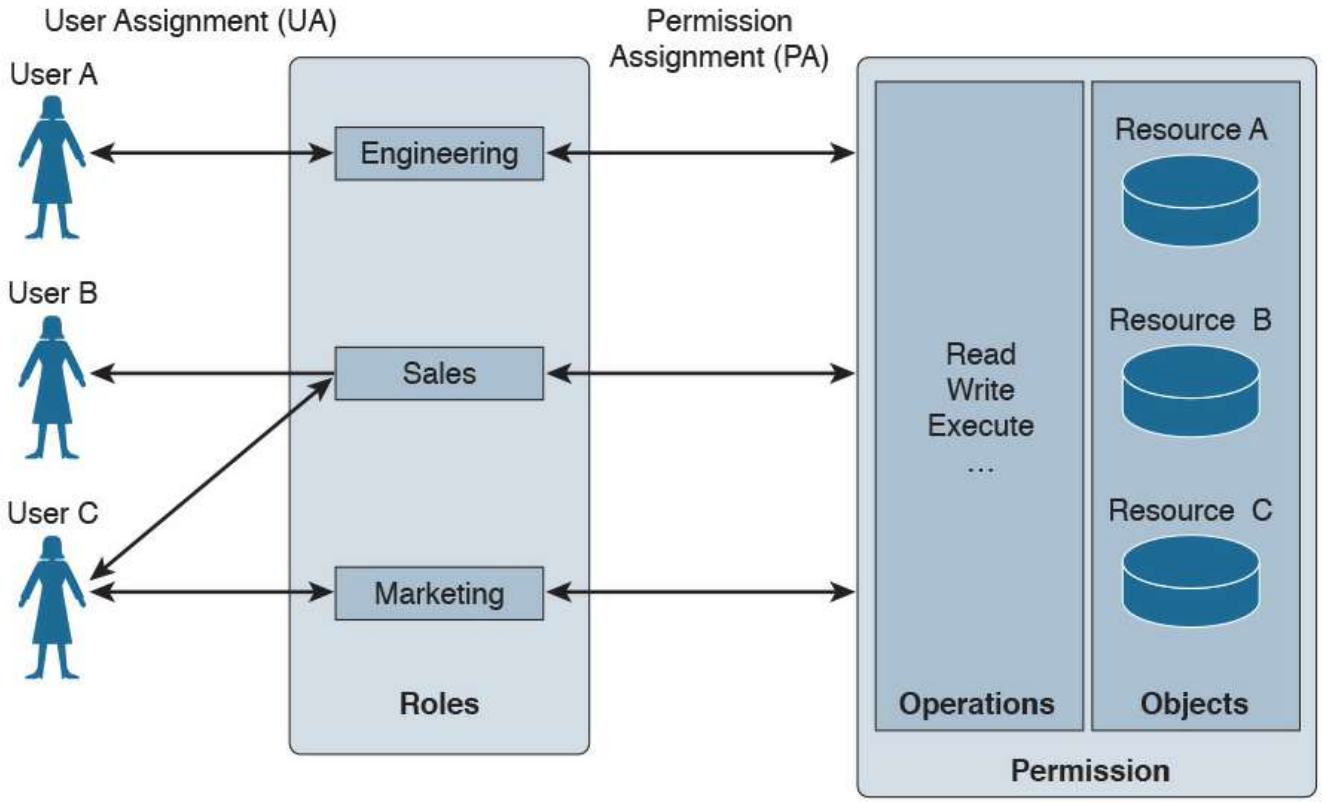
1.3 Autenticación, Autorización y Auditoría

- **Caja abierta:** Comprende en quitar derechos paulatinamente.
- **Caja cerrada:** Comprende en quitar todos los derechos y asignarlos paulatinamente.



1.3 Autenticación, Autorización y Auditoría

- **RBAC**



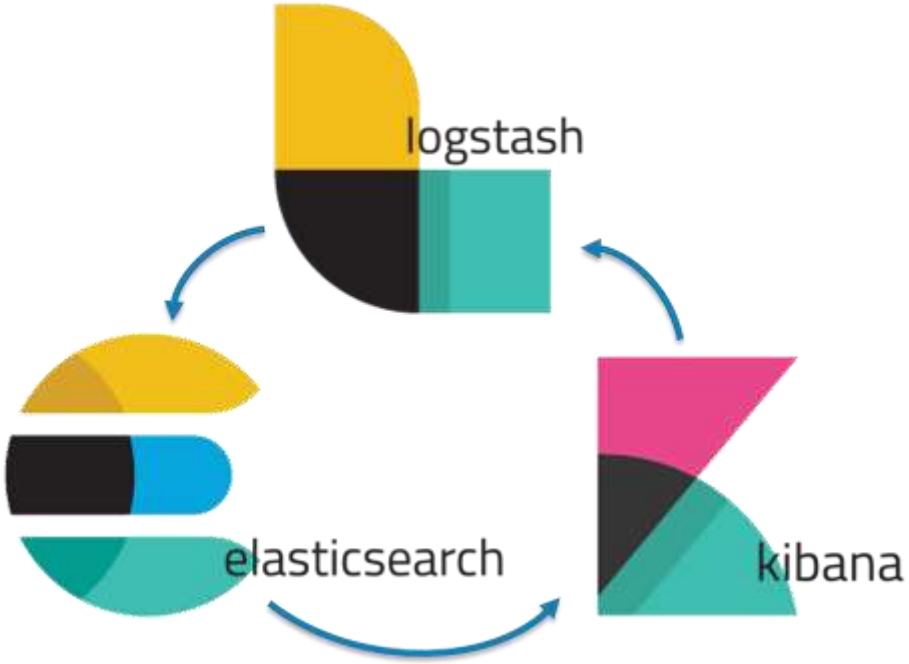
1.3 Autenticación, Autorización y Auditoría

Auditoría

- **Evento:** Todo suceso que tiene lugar en un instante de tiempo determinado.
- **Incidente:** Todo evento que amenaza la seguridad de la información.
- **No todo evento es un incidente, pero todo incidente es un evento.**
- Permite principalmente dos acciones principales:
- **Corroborar:** Confirmar que la acción detectada tuvo lugar y bajo qué parámetros.
- **Correlacionar:** Vincular eventos relacionados de forma que se pueda recrear un ataque.

1.3 Autenticación, Autorización y Auditoría

- **SIEM (Security Information Event Manager):** Alient Vault, QRadar, GrayLog, ELK, entre otros.



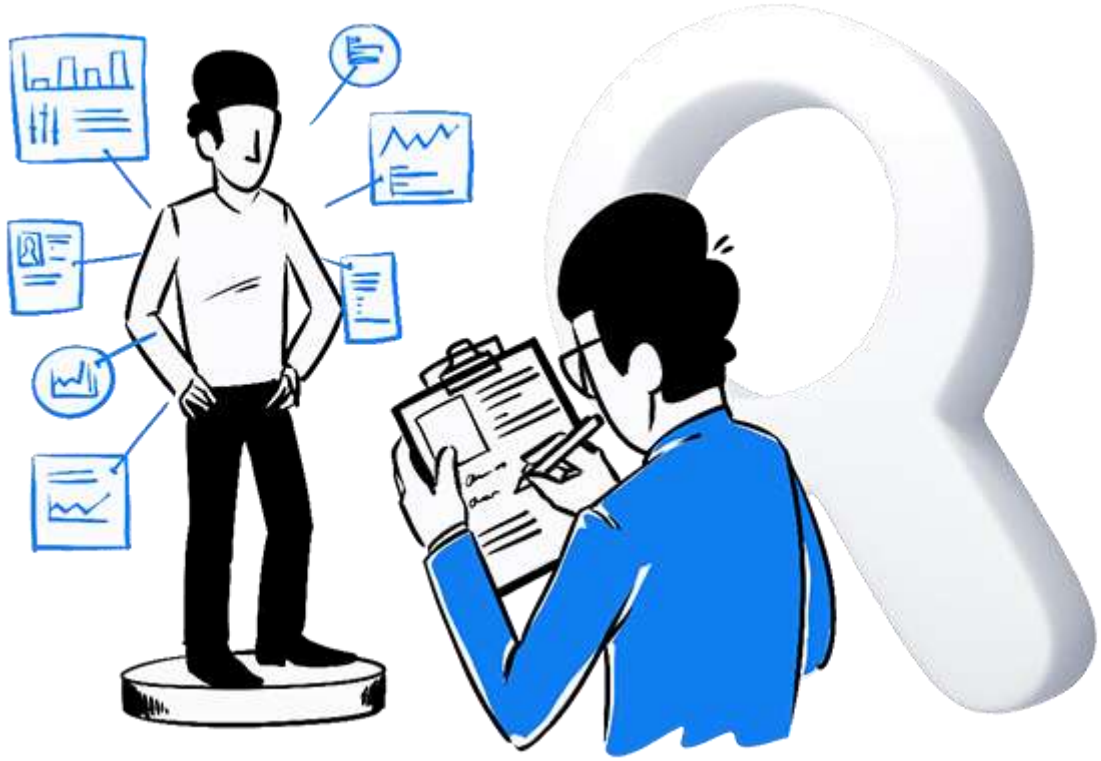
1.4 Privacidad

- Es un derecho humano orientado a precautelar la información personal.
- Sin embargo, el término y alcance del mismo es difícil de definir.
- PII: Personal Identifible Information.
- Ha cobrado gran importancia desde la ejecución del GDPR (General Data Protection Regulation).
- En Ecuador ya se posee una Ley Orgánica de Protección de Datos Personales.
- Sin embargo, no existe ente regulador ni reglamento a la dicha ley.

1.4 Privacidad

Son ejemplos de datos personales:

- Nombre
- Edad
- Teléfono
- Número de identificación
- Número de seguro
- Información médica
- Dirección física
- Dirección electrónica
- Gustos
- Geolocalización
- Historial de actividad
- Nivel de educación



1.5 Esteganografía

- Esteganografía se refiere al ocultamiento de información en multimedia.
- Principalmente se realiza en imágenes, pero no está limitada la técnica únicamente a este medio.
- Es así que también tiene cabida en audio, video, e incluso memoria volátil.
- No es una técnica de cifrado pero puede aplicarse con la misma.
- El estegoanálisis es la ciencia que busca encontrar mensajes ocultos en multimedia

Esteganología = Esteganografía + Estegoanálisis

1.6 Roles de Seguridad de la Información

- Las personas ocupan ciertos roles respecto de la seguridad de la información.
- Cada rol cumple con una función específica que debe cumplirse a cabalidad.
- Los términos no son únicos y dependiendo de cada organización pueden variar entre sí.

1.6 Roles de Seguridad de la Información

NIVEL ESTRATÉGICO:

Es el Nivel Superior donde se toman decisiones estratégicas y no programas.

NIVEL TÁCTICO:

Es el Nivel Medio donde se toman decisiones tácticas, programadas y no programadas.

NIVEL OPERATIVO:

Es el Nivel Técnico donde se toman decisiones tácticas y programadas.

1.6 Roles de Seguridad de la Información

- CISO: Chief Information Security Officer.
- CSO: Chief Security Officer.
- CTO: Chief Technology Officer.
- CIO: Chief Information Officer.
- DPO: Data Protection Offier.
- Custody Technicians.
- Implementation Technicians.


Yo soy ITQ
www.itq.edu.ec