

El cumplimiento de ISO/17799 permite ajustarse al cumplimiento de la mayoría de las exigencias de las normas internacionales de seguridad, incluyendo ISO 27001. El implementar los controles necesarios para cumplir con el estándar presupone un gran trabajo operativo, el cual requiere planeamiento y mano de obra especializada que no siempre es posible obtenerla.

SHELLCODE provee la capacidad operativa para llevar a su compañía a adoptar las mejores prácticas en seguridad de la información, ayudando a:

- Mejorar la imagen corporativa en crecimiento
- Aumentar la seguridad efectiva de los sistemas de información
- Mejorar la gestión de seguridad
- Garantizar la continuidad de negocio
- Implementar procesos de auditoría interna.
- Incrementar los niveles de confianza de clientes y socios de negocio.
- Aumentar el valor comercial y mejora de la imagen de la organización.
- Auditorías de seguridad más precisas y fiables.

Estar conforme con dicha norma no solo significa cumplir con las normas internacionales de seguridad de la información, sino que conlleva a una progresiva auditoría en base a riesgos y cumplimientos de políticas, logrando que se cree un proceso cíclico, el cual desde la implementación de ISO 17799 hasta las evaluaciones de su progreso y mantenimiento, deja entrever una estructura de implantación y mejoras en base a Riesgos y Seguridad de la Información que plantea una muy buena imagen corporativa y comercial.

A continuación se listan las consideraciones necesarias para el cumplimiento de los dominios de la norma ISO 17799:

**Consideraciones sobre los dominios de la norma.**

- ***Gestión de comunicaciones y operaciones.***
  - Fiabilidad en los enlaces de comunicación
  - Verificación de configuraciones y seguridad de los sistemas
  - Separación de entornos
  - Gestión de copias de respaldo
  - Procedimientos para la administración y mantenimiento de sistemas.
  - Identificación de puntos de accesos
  - Definición, implementación y auditoría de sistemas de protección (FIREWALLS).
  - Definición, implementación y auditoría de sistemas para el control de intrusos.
  - Administración y mantenimiento de inventario de sistemas
- ***Control de accesos***
  - Definición de roles y perfiles
  - Políticas de contraseñas y privilegios en los servidores
  - Métodos de autenticación
  - Monitoreo de sistemas
- ***Clasificación y control de activos***
  - Inventario de activos
  - Identificación de activos críticos
  - Valorización de la información
- ***Análisis de Políticas de seguridad***
  - Verificación de Políticas de Seguridad de Información
  - Definición de los Alcances y objetivos
  - Niveles de implementación
  - Política de acceso por terceras partes y externalización
- ***Seguridad del Personal***
  - Nivel de concientización
  - Detección de la necesidad de capacitación
  - Definición de roles en los procedimientos

- ***Gestión de continuidad del negocio***
  - Auditoría de planes de recuperación (Back-Up)
  - Análisis de riesgo
  - Riesgo Bruto y Residual
  - Análisis de Impacto al Negocio
  - Estrategias de Recuperación
- **Seguridad física y del entorno**
  - Control de acceso físico
  - Seguridad física de la infraestructura IT