Producto 7

A11 Control de accesos

El control de acceso es posterior a la autenticacion, se debe acceder unicamente a los recursos que tenga derecho

- Debe de existir una politica de control de accesos documentada y periodicamente revisada, basada en niveles de seguridad
- Se deben de documentar y concientizar
  niveles y responsabilidades
  Documentacion correcta
- Control de acceso a sistemas operativos
- Control de acceso a infomacion y aplicaciones
- Evaluacion y control desde acceso remoto

A12 ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN DESARROLLO Y MANTENIMIENTO

- Procesamiento correcto en aplicaciones
  Validacion de datos, implementación de contooles internos
  proteccion de integridad de datos

- Controles criptograficos
  Para la protección de datos, integridad y autentricidad de la informacrón

- Seguridad en los sistemas de archivos
  Permisos de lectura escritura en directorios y archivos

A13 ADMINISTRACIÓN DE SISTEMAS DE SEGURIDAD

- Reportes de eventos de seguridad de la informacion y debilidades
  Metodologio para la generación, monitorizacion y seguimiento de reportes

- Administración de incidente de seguridad de la información y mejoras
  Preparacion para los incidentes

A14 Administracion de la continuidad del negocio

El objetivo es contemplar las medidas para que el sistema no interrumpa la actividad de la empresa

Debe de conocerse los procesos de la empresa para poder asegurar los sistemas

Las medidas que se adopten para solucionar, minimizar o asumir esos riesgos deberan expresarse por medio de planes de continuidad del negocio.