# UNIDAD 1 – INFORMACION – SEGURIDAD LOGICA

# (ANEXO 1)

- **Identificación y Autenticación:** Permiten prevenir el ingreso de personas no autorizadas al sistema. La base para el seguimiento de las actividades de los usuarios.
  **Identificación:** momento en el que el usuario se da a conocer en el sistema.
  **Autenticación:** verificación que realiza el sistema sobre la identificación. Poseen 4 técnicas que pueden ser utilizadas en conjunto o de manera individual:
    - Algo que solamente el individuo conoce (password, PIN, etc)
    - Algo que la persona posee (tarjeta magnética)
    - Algo que el individuo es y que lo identifica unívocamente (huellas digitales)
    - Algo que el individuo es capaz de hacer (patrones de escritura)

  Es conveniente que los usuarios sean identificados y autenticados una sola vez pudiendo acceder a todas las funcionalidades del sistema ("Single Login" o sincronización de password).
  La seguridad informática se basa en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esto abarca diferentes puntos:

    - Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios.
    - Identificación de los usuarios definida de acuerdo con una norma homogénea para toda la organización.
    - Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos.
    - Revisiones orientadas a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas.
    - Detección de actividades no autorizadas.
    - Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado.
    - Procedimientos a tener en cuenta en caso de desvinculaciones del personal.

- **Modalidad de Acceso:** Refiere al modo de acceso que se permite al usuario sobre los recursos y la información.
    - **Lectura:** solo puede leer o visualizar la información
    - **Escritura:** permite agregar datos, modificar o borrar información
    - **Ejecución:** ejecutar programas
    - **Borrado:** eliminar recursos del sistema (considerado forma de modificación)
    - **Todas las anteriores**

- **Creación:** crear nuevos archivos
- **Búsqueda:** listar archivos

- **Control de Acceso Interno**
  - **Palabras claves:** se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. No es recomendable debido a su fácil deducción.
    - Sincronización de Passwords: permite que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, en caso de actualización de la misma, que se modifique para todos. No es recomendable.
    - Caducidad y Control: mecanismo que controla cuando pueden y/o deben cambiar sus passwords los usuarios.
  - **Cifrado:** la información solo puede ser descifrada por aquellos que tengan la clave apropiada.
  - **Listas de Control de Accesos:** registro donde figuran los nombres de los usuarios que obtuvieron acceso a un determinado recurso del sistema.
  - **Limites Sobre la Interfaz de Usuario:** Restringen a los usuarios a funciones específicas y están en conjunto con las listas de control de accesos.
  - **Etiquetas de Seguridad:** Designaciones otorgadas a los recursos.

- **Control de Acceso Externo**
  - **Dispositivos de Control de Puertos:** Autorizan el acceso a un puerto determinado pudiendo estar físicamente separados o incluidos en otro dispositivo.
  - **Firewalls o Puertas de Seguridad:** Dispositivo de red que crea una separación entre redes publicas y privadas mediante un análisis del trafico de datos.
    - **Características Básicas**
      - Dispositivos de defensa perimetral que separan redes
      - Filtran el tráfico dependiendo reglas predefinidas
      - No protegen de ataques internos
      - No protegen de accesos no autorizados
      - No protegen de la totalidad de ataques dañinos
    - **Clasificación de Firewalls**
      - Tipo de software
      - Appliances o dispositivos de hardware

    - **Funcionalidades Accesorias**

        - Punto de conexión de VPNs
        - VPN host a red
        - VPN red a red
        - Escaneo de Virus
        - Filtrado de Contenidos/anti Spam
        - Balanceo de carga de Firewalls (BCFW)
        - Alta Disponibilidad (AD)
    - **Defensa en Profundidad**
      La utilización de varios firewalls en serie puede otorgar el beneficio de todos y no ser vulnerable a la debilidad de uno solo.
    - **DMZ – Zona Desmilitarizada**
      Área de configuración del firewall con reglas especificas orientada a manejar equipos que deben tener mayor exposición en la infraestructura.
    - **Tipos de Firewall**
      Por su tipo de filtrado:
        - Packet Filters: monitorea las IP de origen y destino verificando puertos, pero no el contenido (IP)
        - Circuit Level Gateways: permite conexiones a través de él y crea un circuito para monitorear la conexión con una verificación de contenido limitada. (TCP/IP)
        - Applications Level Gateways: igual que los anteriores pero específicos para cada aplicación/protocolo. (Proxies)
        - State-Full Multilayer Inspection: combinación de los tres anteriores, control de paso de contenidos a través de reglas de validación.
    - **Consideraciones Sobre el Uso de Firewalls**
        - La combinación de factores hace el mejor firewall
        - Depende de como se implementen las políticas
        - Se justifica reduciendo el impacto y/o probabilidad de amenazas que reduzcan el riesgo.
        - Debe ser administrado, revisado y actualizado periódicamente
        - Se puede implementar combinaciones de firewalls
        - Son parte de un plan se seguridad general
- **Firewalls Personales:** Dispositivos lógicos que se instalan en la propia terminal y permiten aplicar filtros a la información de red correspondiente a cada interfaz y/o aplicación.
- **IDS – Sistema de Detección de Intrusiones:** Elemento que detecta, identifica y responde a actividades no autorizadas o anormales.

- **Modelo de Funcionamiento General**
  - Recolección de datos
  - Análisis
  - Respuesta
- **Clasificaciones**

  Por su fuente de datos:
  - HIDS: (Sistema de Detección de Intrusiones de Maquina) utilizan registros de auditoría, sistema, aplicaciones y archivos. *(Tipwire, Prelude, Imsafe, GFI, LANguard, S.E.L.M.)*
  - NIDS y NNIDS: (Sistema de Detección de Intrusiones de Red y Sistema de Detección de Intrusiones de Nodo de Red) utilizan paquetes de red (TCP, UPD, IP) con posibilidad de utilizar agentes (IDS Distribuido) *(Snort, Bro, Prelude, Suricata)*

  Por su metodología de análisis:

  - Por detección de uso indebido *(Snort, Bro)*
  - Por detección de anomalías *(Imsafe, Prelude)*

  Por su modo de respuesta:

  - Respuesta pasiva
  - Respuesta activa

- **IPS – Sistema de Prevención de Intrusiones:** Combinación de un IDS + Firewall en respuesta activa. Detectan el curso de ataque y lo bloquean antes de que suceda. *(IntruShield, Hogwash, Radware, Storm watch. ISS, Juniper, Tipping Point (3Com), Cisco, Suricata)*
- **Dispositivos UTM:** Firewalls de red que manejan diferentes servicios en un mismo equipo.
  - **Funciones**
    - Función de un firewall de inspección de paquetes
    - Función de VPN
    - Antispam
    - Antiphishing
    - Antispyware
    - Filtrado de contenidos
    - Antivirus de perímetro
    - Detección/prevención de intrusos
  - **Modos**

- Proxy: uso de proxies para procesar y redirigir todo el tráfico interno.
- Transparente: procesan los paquetes y son capaces de analizarlos en tiempo real.

- **NGFW – Next Generation Firewalls:** Se basa en la inspección profunda de paquetes, sumada a la tecnología para evitar intrusiones y de firewalls tradicionales.
- **WAF – Web Application Firewall:** Dispositivo fisico o logico que analiza el trafico de web (entre servidor web y WAN), los datos recibidos por parte del usuario y protege de diferentes ataques web como: SQL Injection, Buffer Overflows, etc. Mayor alcance que un IDS/IPS.
    - **Modelos de Seguridad WAF**
        - Modelo de Seguridad Positiva: deniegan todas las transacciones y solamente aceptan las que identifica como seguras o validas determinadas por una serie de reglas predefinidas anteriormente. Destentaja – falsos positivos.
        - Modelo de Seguridad Negativa: acepta todas las transacciones y deniega las que detecta como una posible amenaza o un ataque. Desventaja – constante actualización.
    - **Proceso de Aprendizaje**

      Petición:

      ```
      GET http://sitepath.com/show_article.php?id=15
      ```

      Regla:

      ```
      GET http://sitepath.com/show_article.php?id=15' or 1=1
      ```

      Resultado: Error 404.

    - **Riesgos de un WAF**

      Deben estar muy bien configurados, de lo contrario detectaran muchos falsos positivos generando así muchas transacciones denegadas. A su vez, también pueden producir un cierto retardo en las transacciones.
    - **Modos de Funcionamiento**

      Pueden funcionar en modo bridge, router, proxy o plugin. Disponibles en hardware y software. Puede denegar operaciones dependiendo de su posición geográfica.

- **Acceso de Personal Contratado o Consultores**

- **Administración de Seguridad**
  Es necesario implementar una eficiente administración de medidas de seguridad lógica. La política de seguridad que se desarrolle debe guiar a las decisiones referidas a la determinación de los controles de accesos establecidas para cada perfil de usuario. Los permisos de acceso requieren determinar cuál será el nivel de seguridad necesario sobre los datos, para ello es imprescindible el clasificar la información. Una vez clasificados, deberán establecerse medidas de seguridad para cada uno de los niveles.

  - **Administración del Personal y Usuarios – Organización del Personal**
    - Definición de puestos
    - Determinación de la sensibilidad del puesto
    - Elección de la persona para cada puesto
    - Entrenamiento inicial y continuo del empleado

---

# SEGURIDAD FISICA

- **Incendios**
  Causados por el uso indebido de combustibles, fallas de instalaciones eléctricas defectuosas y almacenamiento y traslado de sustancias peligrosas. Posibles factores para contemplar:
    - El área de cómputos debe estar en un local que no sea combustible o inflamable
    - El área de cómputos no debe situarse cerca de áreas donde se procesen, fabriquen o almacenen materiales inflamables.
    - Las paredes deben estar hechas de materiales incombustibles
    - Construcción de falso piso con materiales incombustibles
    - No se debe fumar
    - Muebles incombustibles y cestos metálicos
    - Piso y techos impermeables

  - **Seguridad del Equipamiento**
    El acceso a los centros de cómputos debe ser solamente para personal autorizado. Deben contar con mecanismos de ventilación y detección de incendios.
  - **Recomendaciones**
    El sistema de detección de incendios debe activar la extinción. El personal debe estar capacitado para usar extinguidores. Implementar pareces contra incendios.

- **Condiciones Climatológicas**
  La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción del edificio.

    - **Terremoto**
- **Instalación Eléctrica**
  Problemática que abarca desde el usuario hogareño hasta la gran empresa.
    - **Picos y Ruidos Electromagnéticos**
    - **Cableado**
    - **Cableado de Alto Nivel de Seguridad**
    - **Pisos de Placas Extraíbles**
    - **Sistema de Aire Acondicionado**
    - **Emisiones Electromagnéticas**
- **Ergometría**
  Disciplina que se encarga de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean.
    - **Trastornos Óseos y/o Musculares**
    - **Trastornos Visuales**
    - **Salud Mental**
    - **Ambiente Luminoso**
    - **Ambiente Climático**
- **Utilización de Guardias**
    - **Control de Personas**
    - **Control de Vehículos**
    - **Desventajas de la Utilización de Guardias**
- **Sistemas Biométricos**
    - **Emisión de Calor**
    - **Huella Digital**
    - **Verificación de Voz**
    - **Verificación de Patrones Oculares**
- **Protección Electrónica**
    - **Barreras Infrarrojas y de Micro-Ondas**
    - **Detector Ultrasónico**
    - **Detectores Pasivos Sin Alimentación**
    - **Sonorización y Dispositivos Luminosos**
    - **Circuitos Cerrados de Televisión**
    - **Edificios Inteligentes**