

Activitat 4 - Diseño de un plan integral de seguridad informática

Pol de la Viuda

Contenido

Servicios de Seguridad	3
Integridad	3
Confidencialidad.....	3
Disponibilidad.....	3
Autenticación.....	3
No repudio.....	3
Control de Acceso	4
Mecanismo de Seguridad Concretos	4
Confidencialidad.....	4
Integridad	4
Disponibilidad.....	4
Autenticación.....	4
No Repudio.....	4
Control de Acceso	4
Medidas de Seguridad Logia.....	5
Firewall y segmentación de red	5
Antivirus y anti-malware	5
Actualizaciones automáticas	5
Medidas de Seguridad Física	5
Control de acceso al edificio.....	5
Cámaras de vigilancia	5
Protección de servidores	5
Enfoque Global de la Seguridad.....	6
Edificio	6
Hardware y red interna	6
Sistemas Operativos y Software	6
Conexión de Internet.....	6
Información	6
Virus USB.....	6
Activo.....	6
Amenaza	7

Vulnerabilidad.....	7
Impacto.....	7
Riesgo	7
Servicios	7
Mecanismos	7

Servicios de Seguridad

Integridad

La empresa tendría que asegurarse de que la información no sea modificada de forma no autorizada, para evitar problemas en la base de datos

Confidencialidad

La empresa ha de proteger los datos de sus clientes, empleados y proyectos, para que solo lo pueda ver la gente que este autorizada para ello

Disponibilidad

Mantener los sistemas operativos, aplicaciones y servidores accesibles, incluso ante fallos de luz o ataques, ya sea con generadores externos o con antivirus

Autenticación

Comprobar que los usuarios que acceden a la red están autorizados y que sean quien realmente dicen que son

No repudio

Registrar las acciones de los usuarios en sistemas críticos para que no puedan cambiar datos

Control de Acceso

Limitar el acceso según el puesto de trabajo

Mecanismo de Seguridad Concretos

Confidencialidad

Cifrado de discos y base de datos, es preventivo, esto evita el acceso no autorizado a datos

Integridad

Suma de verificación en archivos críticos, es detector, te permite comprobar si un archivo ha sido modificado

Disponibilidad

Sistema de alimentación ininterrumpida, es preventivo, evita caídas de servidores cuando hay un corte de luz

Autenticación

Contraseñas, es preventivo, te garantiza que solo entren usuarios autorizados

No Repudio

Firmas digitales, es detector, esto te ayuda a saber que usuario ha hecho que cosa

Control de Acceso

Role-Based Access Control, es preventivo, restringe recursos según el puesto de trabajo

Medidas de Seguridad Logia

Firewall y segmentación de red

Separar la red administrativa de la contable y del Wi-Fi de invitados

Antivirus y anti-malware

Detectar y bloquear virus introducidos mediante USB u otros medios

Actualizaciones automáticas

Mantener sistemas operativos y aplicaciones al día

Medidas de Seguridad Física

Control de acceso al edificio

Tarjetas magnéticas o biometría para empleados.

Cámaras de vigilancia

Registro de entradas y zonas críticas.

Protección de servidores

Sala con acceso restringido, climatización y SAI.

Enfoque Global de la Seguridad

Edificio

Controla el acceso físico

Hardware y red interna

Firewalls, segmentación de red y acceso a servidores

Sistemas Operativos y Software

Actualizaciones, antivirus, control de versiones, cifrado

Conexión de Internet

VPN, filtrado de tráfico, IDS/IPS, cifrado TLS

Información

Backups automáticos, cifrado de datos, control de acceso basado en el puesto de trabajo

Virus USB

Activo

Datos de la empresa (clientes, proyectos).

Amenaza

Malware introducido por dispositivo USB externo.

Vulnerabilidad

Falta de control sobre dispositivos extraíbles.

Impacto

Pérdida o corrupción de información crítica; posibles interrupciones del servicio.

Riesgo

Alto, ya que la información sensible podría verse comprometida.

Servicios

Confidencialidad, integridad y disponibilidad.

Mecanismos

Antivirus y antimalware actualizado (preventivo), bloqueo de puertos USB no autorizados (preventivo), copias de seguridad automáticas (corrector), monitorización de sistemas (detector).