Seguridad Lógica. Elementos clave para tener en cuenta para evaluación y análisis

Elemento clave	Descripción y consideraciones
Gestión de identidades y accesos (IAM)	* **Autenticación fuerte:** Utilizar múltiples factores de autenticación (algo que se sabe, algo que se posee, algo que se es) para verificar la identidad de los usuarios.
	* **Autorización:** Establecer roles y permisos claros para cada usuario, limitando el acceso a los recursos estrictamente necesarios.
	* **Gestión de contraseñas:** Implementar políticas sólidas de contraseñas, incluyendo complejidad, rotación regular y prohibición de contraseñas débiles o reutilizadas.
Cifrado	* **Cifrado de datos en reposo:** Proteger los datos almacenados en discos duros, bases de datos y otros sistemas de almacenamiento.
	* **Cifrado de datos en tránsito**: Asegurar la confidencialidad de los datos mientras se transmiten a través de redes.
	* **Algoritmos de cifrado**: Seleccionar algoritmos de cifrado robustos y actualizados, como AES.
Control de acceso a la red	* **Firewall:** Implementar firewalls para filtrar el tráfico de red entrante y saliente, permitiendo solo el tráfico autorizado.
	* **VPN**: Utilizar redes privadas virtuales (VPN) para establecer conexiones seguras a través de redes públicas.
	* **Segmentación de redes**: Dividir la red en segmentos más pequeños para limitar el impacto de posibles brechas de seguridad.
Detección y prevención de intrusiones (IPS)	* **Sistemas de detección de intrusiones:** Implementar sistemas que monitoreen la actividad de la red y detecten comportamientos anómalos o ataques en curso.
	* **Sistemas de prevención de intrusiones:** Utilizar sistemas que bloqueen los ataques antes de que puedan causar daños.
Monitoreo y registro de eventos de seguridad	* **Sistemas de detección de eventos de seguridad (SIEM):** Consolidar y analizar los registros de seguridad de múltiples fuentes para identificar amenazas y detectar incidentes.
	* **Análisis de logs:** Realizar un análisis exhaustivo de los registros para identificar patrones y detectar actividades sospechosas.
Concientización y capacitación de los usuarios	* **Programas de capacitación:** Implementar programas de capacitación regulares para concientizar a los usuarios sobre las mejores prácticas de seguridad y las amenazas más comunes.

	* **Simulaciones de ataques:** Realizar simulaciones de ataques para evaluar la preparación de los usuarios y la efectividad de las medidas de seguridad.
Contingencia y recuperación de desastres	* **Planes de contingencia:** Desarrollar planes detallados para responder a incidentes de seguridad y restaurar los sistemas afectados.
	* **Copias de seguridad:** Realizar copias de seguridad regulares de los datos y probar su restauración.
Actualización de software y parches	* **Gestión de parches:** Aplicar de manera oportuna los parches de seguridad para corregir vulnerabilidades conocidas.
	* **Inventario de software**: Mantener un inventario actualizado del software utilizado en la organización.
Principio de mínimo privilegio	* **Otorgar solo los permisos necesarios:** Otorgar a los usuarios solo los permisos mínimos necesarios para realizar sus tareas.