**CHECKLIST DE AUDITORÍA DE UN SISTEMA INFORMÁTICO**

**1. Seguridad de la Información**

* **Control de accesos:** Verificar permisos y roles de usuario.
* **Gestión de contraseñas:** Validar políticas de contraseñas, requisitos de cambio y almacenamiento seguro.
* **Protocolos de seguridad en la red:** Revisar configuración de firewalls, VPN, y sistemas de detección de intrusos (IDS/IPS).

**4. Respaldo y Recuperación de Desastres**

* **Plan de respaldo:** Verificar periodicidad, integridad y seguridad de los respaldos.
* **Plan de recuperación de desastres (DRP):** Asegurarse de que exista un DRP y se pruebe regularmente.
* **Disponibilidad de redundancia:** Comprobar si el sistema tiene redundancia para minimizar tiempos de inactividad.

**7. Integridad y Disponibilidad de los Datos**

* **Control de integridad de datos:** Comprobar que los datos se mantengan íntegros durante almacenamiento y procesamiento.
* **Disponibilidad del sistema:** Evaluar diseño y medidas para reducir el tiempo de inactividad.

**8. Auditoría y Monitoreo de Actividades**

* **Registro de eventos (logs):** Verificar que las actividades críticas estén registradas y accesibles.
* **Monitoreo continuo:** Asegurar monitoreo para detectar actividades anómalas.

**10. Documentación**

* **Documentación del sistema:** Confirmar que arquitectura, procesos y cambios estén documentados y accesibles.
* **Manual de usuario y capacitación:** Verificar existencia de guías y entrenamientos para usuarios y personal técnico.

**CHECKLIST DE AUDITORÍA DE SEGURIDAD DE LOS DATOS**

**1. Políticas y Gobernanza de Seguridad de Datos**

* **Política de seguridad de datos:** Confirmar que exista una política de seguridad de datos formal y actualizada.
* **Gobernanza de datos:** Verificar que haya un comité o equipo responsable de la seguridad y manejo de datos.
* **Clasificación de datos:** Asegurarse de que los datos estén clasificados en niveles de sensibilidad (confidenciales, internos, públicos).
* **Políticas de retención y eliminación:** Revisar las políticas para la retención, archivado y eliminación segura de los datos.

**2. Control de Acceso a los Datos**

* **Roles y permisos:** Verificar que cada usuario tenga asignados permisos adecuados según su rol.
* **Autenticación multifactor (MFA):** Asegurar que se utilice MFA para acceder a datos sensibles.
* **Registro de accesos:** Confirmar que los accesos a los datos críticos se registren y revisen regularmente.
* **Principio de menor privilegio:** Evaluar que los permisos estén basados en el acceso mínimo necesario para realizar funciones específicas.

**3. Protección de Datos en Tránsito y en Reposo**

* **Cifrado de datos en tránsito:** Asegurar que los datos sean cifrados durante la transmisión, usando protocolos seguros (como TLS).
* **Cifrado de datos en reposo:** Confirmar que los datos almacenados estén cifrados, especialmente los datos sensibles o confidenciales.
* **Gestión de claves de cifrado:** Revisar que las claves de cifrado estén protegidas y gestionadas de manera segura.

**4. Seguridad de Bases de Datos y Almacenamiento**

* **Seguridad de bases de datos:** Verificar configuraciones de seguridad en bases de datos, incluyendo restricciones de acceso y autenticación.
* **Parcheo y actualizaciones:** Confirmar que el software de bases de datos y almacenamiento esté actualizado y con los parches de seguridad aplicados.
* **Seguridad de almacenamiento en la nube:** Asegurarse de que se apliquen políticas de seguridad para los datos almacenados en la nube.

**5. Copias de Seguridad y Recuperación de Datos**

* **Copias de seguridad periódicas:** Revisar la frecuencia y la seguridad de las copias de respaldo de datos.
* **Pruebas de recuperación:** Confirmar que se realicen pruebas de recuperación de datos de forma periódica.
* **Almacenamiento seguro de respaldos:** Asegurarse de que los respaldos se almacenen en ubicaciones seguras y se cifren si es posible.

**6. Protección contra Amenazas y Vulnerabilidades**

* **Evaluación de vulnerabilidades:** Confirmar que existan procedimientos de evaluación y mitigación de vulnerabilidades.
* **Detección de intrusiones:** Verificar la implementación de sistemas de detección de intrusiones (IDS/IPS) para proteger los datos.
* **Protección contra malware y antivirus:** Revisar que existan herramientas actualizadas de detección y prevención de malware.

**7. Monitoreo y Registro de Actividades**

* **Registro de actividades (logs):** Asegurarse de que se registren las actividades relacionadas con el acceso y manipulación de datos.
* **Monitoreo continuo:** Confirmar que haya monitoreo en tiempo real para detectar actividad sospechosa.
* **Alertas de seguridad:** Revisar que existan alertas configuradas para incidentes de seguridad de datos.

**8. Cumplimiento de Normativas y Regulaciones**

* **Cumplimiento de normativas:** Asegurar cumplimiento con regulaciones como GDPR, HIPAA, CCPA, o las aplicables.
* **Evaluación de privacidad de datos:** Confirmar que se realicen evaluaciones periódicas de impacto en la privacidad y seguridad de datos.
* **Notificación de brechas de seguridad:** Revisar los procedimientos de notificación de incidentes de seguridad según normativas.

**9. Concientización y Capacitación de Seguridad**

* **Capacitación de empleados:** Asegurarse de que haya programas de capacitación continua en seguridad de datos para todos los empleados.
* **Simulaciones de ataques:** Evaluar la realización de pruebas o simulaciones de phishing y otras amenazas para evaluar la preparación del personal.
* **Política de uso aceptable:** Confirmar que todos los empleados conozcan y acepten la política de uso de datos y recursos informáticos.

**10. Planes de Respuesta a Incidentes**

* **Plan de respuesta a incidentes:** Verificar que exista un plan detallado para responder a incidentes de seguridad de datos.
* **Equipo de respuesta a incidentes:** Asegurarse de que exista un equipo capacitado para manejar brechas de seguridad.
* **Simulacros de respuesta:** Confirmar que se realicen simulacros para evaluar la efectividad del plan de respuesta.

Los objetivos principales, a grandes rasgos y de forma resumida, de la auditoría de sistemas pueden agruparse en:

* Determinar si los controles implementados son eficientes y suficientes;
* Identificar las causas de los problemas existentes en los sistemas de información y a su vez las áreas de oportunidad que puedan encontrarse, determinando las acciones preventivas y correctivas necesarias para mantener a los sistemas de información confiables y disponibles;
* Identificar causas y soluciones a problemas específicos de los sistemas de información, que pueden estar afectando a la operación y a las estrategias del negocio, como el cumplimiento de licencias de software, las incompatibilidades de hardware y software, errores en bases de datos con problemas de seguridad, fallas en el control de versiones, etc.;
* Incrementar la satisfacción y seguridad de los usuarios de dichos sistemas informatizados;
* Educar sobre el control de los sistemas de información, puesto que se trata de un sector muy cambiante y relativamente nuevo, por lo que es preciso educar a los usuarios de estos procesos informatizados;
* Mejorar la relación coste-beneficio de los sistemas de información

Por lo tanto, la auditoría de sistemas es una forma de control y evaluación que no solo abarca los equipos informáticos en sí, sino que su ámbito de aplicación abarca también el control de los sistemas de entrada a dichos equipos y el uso que se le da a los mismos.

Tipos de auditoría de sistemas:

Las auditorías de sistemas pueden ser aplicadas a diferentes niveles corporativos, pudiendo realizarse una auditoría de sistemas a toda la entidad, a un departamento, a un área o incluso a una actividad concreta. Por otro lado, dentro de la auditoría de sistemas, y en función de los procedimientos de auditoría aplicados y el objetivo que se quiere valorar, pueden distinguirse diferentes tipos:

* Auditoría de la gestión: se verifica el uso de los sistemas para la contratación de bienes y servicios, documentación de los programas, etc.
* Auditoría legal del Reglamento de Protección de Datos: se verifica el cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley de Protección de Datos de Carácter Personal.
* Auditoría de los datos: en la que se verifica el uso de los sistemas para la clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
* Auditoría de las bases de datos: en la que se verifica el uso de los sistemas en cuanto a los controles de acceso a las bases, de actualización, de integridad y calidad de los datos.
* Auditoría de la seguridad: referida a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y principio de no repudio.
* Auditoría de la seguridad física: referida a la ubicación de la organización, evitando ubicaciones de riesgo, y asegurando que los servidores y bases de datos se encuentran físicamente protegidos y en un entorno favorable (arcos de seguridad, CCTV, vigilantes, etc.).
* Auditoría de la seguridad lógica: referida a los métodos de autenticación de los sistemas de información.
* Auditoría de la seguridad en producción: mediante la cual se evalúan los riesgos y las respuestas frente a errores, accidentes y fraudes.