Universidad Interamericana de Panamá

**Estudiante:**

Francisco Rubio

**Cédula:**

4-848-1301

**Materia:**

Auditoria de sistemas

**Asignación:**

Investigación de conceptos

# Glosario de Conceptos de Auditoria de Sistemas

**Control interno**: Procesos y medidas implementadas para garantizar la eficacia, eficiencia y confiabilidad de las operaciones y la presentación de informes en un sistema.

**Riesgo de auditoría**: Probabilidad de que existan errores significativos en los estados financieros o incumplimientos en los controles internos, que puedan pasar desapercibidos durante la auditoría.

**Marco de referencia**: Conjunto de estándares y principios utilizados como guía para llevar a cabo la auditoría de sistemas, asegurando coherencia y consistencia en la evaluación.

**Evaluación de riesgos**: Proceso de identificar y analizar posibles amenazas a la integridad y confidencialidad de la información, así como a la efectividad de los controles, con el objetivo de minimizar impactos negativos.

**Control interno:** Procesos y medidas implementadas para garantizar la eficacia, eficiencia y confiabilidad de las operaciones y la presentación de informes en un sistema.

**Riesgo de auditoría**: Probabilidad de que existan errores significativos en los estados financieros o incumplimientos en los controles internos, que puedan pasar desapercibidos durante la auditoría.

**Marco de referencia:** Conjunto de estándares y principios utilizados como guía para llevar a cabo la auditoría de sistemas, asegurando coherencia y consistencia en la evaluación.

**Evaluación de riesgos:** Proceso de identificar y analizar posibles amenazas a la integridad y confidencialidad de la información, así como a la efectividad de los controles, con el objetivo de minimizar impactos negativos.

**Pruebas de auditoría**: Exámenes detallados y evidencia recopilada para evaluar la efectividad de los controles internos y la precisión de la información financiera o de sistemas.

**Muestreo estadístico**: Técnica que utiliza una muestra representativa para evaluar y extrapolar la efectividad de los controles o la precisión de la información en el conjunto completo de datos.

**Planificación de auditoría**: Proceso de desarrollo de enfoques y estrategias para llevar a cabo una auditoría de sistemas de manera efectiva y eficiente.

**Seguridad de la información**: Medidas y controles implementados para proteger la confidencialidad, integridad y disponibilidad de la información en un sistema.

**Gobierno de TI**: Estructuras y procesos que garantizan la alineación de la tecnología de la información con los objetivos y estrategias organizacionales.

**Políticas y procedimientos**: Directrices establecidas para guiar el comportamiento y las acciones relacionadas con la seguridad y el uso adecuado de los sistemas de información.

**Cumplimiento normativo**: Asegurarse de que las operaciones y prácticas de TI cumplan con las leyes, regulaciones y estándares establecidos.

**Segregación de funciones**: Distribución de tareas y responsabilidades para prevenir conflictos de interés y fraudes al requerir la cooperación de varias personas.

**Seguridad física**: Medidas para proteger los recursos físicos del sistema, como servidores y centros de datos, contra amenazas como robos o desastres naturales.

**Continuidad del negocio**: Planificación y preparación para mantener operaciones críticas después de eventos adversos, garantizando la recuperación rápida de los sistemas.

**Auditoría forense**: Investigación especializada que utiliza técnicas de auditoría para analizar y recopilar evidencia de posibles actividades delictivas en sistemas de información.

**Auditoría de aplicaciones**: Examen de la integridad, seguridad y eficiencia de las aplicaciones informáticas utilizadas en un sistema.

**Auditoría de bases de datos**: Evaluación de la seguridad, integridad y eficiencia de las bases de datos que almacenan información crítica.

**Auditoría de redes**: Revisión de la arquitectura y controles de red para garantizar su seguridad y eficacia.

**Auditoría de sistemas operativos**: Evaluación de la configuración, seguridad y rendimiento de los sistemas operativos utilizados en un entorno de tecnología de la información.

**Auditoría de seguridad de datos**: Análisis de las medidas implementadas para proteger la confidencialidad y la integridad de los datos.

**Auditoría de controles de acceso**: Revisión de los mecanismos que regulan el acceso a sistemas y datos para garantizar su adecuación y seguridad.

**Auditoría de cumplimiento**: Verificación de que las operaciones y prácticas cumplen con los estándares internos y externos establecidos.

**Auditoría de gestión de cambios**: Evaluación de los procedimientos para gestionar modificaciones en sistemas y procesos, asegurando la integridad y seguridad.

**Auditoría de respaldo y recuperación**: Revisión de las estrategias y procesos para respaldar y restaurar datos, garantizando la disponibilidad continua.

**Auditoría de gestión de incidentes**: Evaluación de la capacidad de respuesta ante eventos de seguridad, asegurando una gestión eficiente de incidentes.

**Análisis de vulnerabilidades**: Identificación y evaluación de posibles debilidades en sistemas para mitigar riesgos de seguridad.

**Pruebas de penetración**: Simulación de ataques controlados para evaluar la resistencia de un sistema y mejorar sus defensas.

**Auditoría de gestión de activos**: Revisión de los procesos para adquirir, mantener y dar de baja activos de TI, garantizando su uso eficiente.

**Auditoría de gestión de proyectos**: Evaluación de la planificación y ejecución de proyectos de TI para asegurar el logro de objetivos.

**Auditoría de terceros**: Evaluación de la gestión de riesgos asociados con proveedores externos de servicios y tecnologías.

**Auditoría de sistemas en la nube**: Revisión de la seguridad y eficiencia de los sistemas y datos alojados en entornos de computación en la nube.

**Auditoría de servicios de TI:** Evaluación de la calidad y cumplimiento de los servicios de TI proporcionados interna o externamente.

**Auditoría de ciberseguridad**: Revisión de las medidas de seguridad para proteger los sistemas contra amenazas cibernéticas.

**Auditoría de controles de TI**: Evaluación de los controles generales de tecnología de la información para garantizar su eficacia.

**Control de acceso**: Implementación de medidas para regular y supervisar el acceso a sistemas y datos.

**Monitoreo de eventos**: Seguimiento constante de actividades en sistemas para detectar y responder a eventos de seguridad.

**Seguridad de la red**: Implementación de controles para proteger la infraestructura de red contra amenazas.

**Auditoría de cumplimiento de PCI DSS**: Verificación de conformidad con los estándares de seguridad de datos para la industria de tarjetas de pago.

**Auditoría de cumplimiento de HIPAA**: Evaluación de prácticas para garantizar la privacidad y seguridad de la información de salud.

**Auditoría de cumplimiento de GDPR**: Revisión de medidas para cumplir con los requisitos de protección de datos personales establecidos por el Reglamento General de Protección de Datos.

**Auditoría de cumplimiento de SOX**: Evaluación de controles internos financieros según la Ley Sarbanes-Oxley.

**Auditoría de cumplimiento de ISO 27001**: Verificación de conformidad con estándares internacionales para la gestión de la seguridad de la información.