TRABAJOS DE AUDITORÍA DE IT Y CIBERSEGURIDAD

Trabajos de Auditoría	Descripción	Riesgos Mitigados
Auditoría de gobierno de TI	Evaluar la eficacia del gobierno y la alineación de la estrategia de TI con los objetivos del negocio.	Riesgos de desalineación entre TI y el negocio provocando ineficiencia operativa y pérdidas económicas.
Auditoría de la Seguridad de la Información	Evaluar la efectividad de las políticas y controles de seguridad de la información.	Pérdida de integridad, confidencialidad y disponibilidad de la información procesada por la empresa.
Auditoría de Evaluación de controles generales de tecnología (ITGCs)	Evaluación de controles generales de TI que afectan la integridad y la confiabilidad de los sistemas críticos.	Errores de procesamiento, fraudes y cambios o accesos no autorizados en los sistemas.
Auditoría de evaluación de ingeniería social	Simulación de ataques de ingeniería social para evaluar la conciencia y preparación del personal frente a posibles ciberataques.	Obtención de información confidencial y clave de la empresa o de sus colaboradores a través de mecanismos de ingeniería social, como la manipulación o el engaño.
Auditoría integral de controles de aplicación	Revisión de controles funcionales de aplicaciones claves para prevenir y detectar posibles fraudes en los procesos de negocio.	Posibles fraudes y/o pérdidas financieras directas debido a deficiencias en los controles sobre los sistemas de información.
Auditoría de Ciberseguridad	Identificación de vulnerabilidades y debilidades en sistemas e infraestructura crítica.	Riesgos de ciberataques, interrupción del servicio y/o robo de información.
Auditoría de evaluación de proyectos de TI	Evaluación de proyectos de TI antes de su lanzamiento para garantizar su correcto funcionamiento y seguridad en su salida al ambiente de producción.	Errores críticos en los proyectos de TI que provoquen posibles pérdidas de inversión, incumplimiento regulatorio y/o daños a la reputación de la empresa.
Auditoría de segregación de funciones en sistemas de información (SAP / ORACLE) – SoD	Revisión de los permisos y accesos de usuarios en sistemas de información críticos mediante el uso de herramientas especializadas.	Posibles fraudes y/o pérdidas financieras directas debido a deficiencias en los controles sobre los sistemas de información.
Auditoría de gestión de servicios de TI y TO	Revisión de la gestión y entrega de servicios de TI y Tecnología Operativa (sistemas de automatización industrial).	Baja calidad de servicios, incumplimiento de acuerdos de nivel de servicio y/o posibles impactos en las operaciones.

Trabajos de Auditoría	Descripción	Riesgos Mitigados
Auditoría de madurez de la gestión de TI	Evaluación del nivel de madurez en la gestión de TI y la seguridad de la empresa.	Ineficiencias operativas y ausencia de control sobre la gestión y control de las TIC.
Auditoría al proceso de desarrollo de software	Revisión de los procesos de desarrollo de software para asegurar su calidad y seguridad de los sistemas.	Errores en ambientes productivos, vulnerabilidades de seguridad y proyectos retrasados.
Auditoría de centros de procesamiento de datos (Datacenters)	Revisión de la infraestructura y las medidas de seguridad en los centros de datos.	Interrupción del servicio, pérdida de datos y acceso no autorizado.
Auditoría del proceso de adquisición y compra de servicios e infraestructura TI/TO	Evaluación de los procesos de adquisición y contratación de servicios e infraestructura tecnológica.	Adquisiciones inadecuadas, gastos innecesarios y proveedores no confiables.
Auditorías continuas sobre operaciones de TI, procesos financieros y/o operativos	Auditoría constante para garantizar el cumplimiento y la eficacia de las operaciones empresariales con oportunidad y volúmenes de datos apropiados.	Riesgos de incumplimiento, ineficiencia operativa y pérdida financiera.
Auditorías de servicios en la Nube	Revisión de la seguridad y cumplimiento normativo de los servicios en la nube utilizados por la empresa.	Filtración de datos, accesos no autorizados y pérdida de control sobre la información.
Auditorías de cumplimiento en aspectos generales de TI y ciberseguridad	Evaluación del cumplimiento de políticas y normativas en materia de TI y ciberseguridad.	Multas, sanciones y daño a la reputación por incumplimiento normativo.
Auditorías de cumplimiento como derechos de autor y protección de datos personales	Evaluación del cumplimiento de leyes y regulaciones de derechos de autor (Ley 603) y protección de datos personales (Leyes 1581 y 1266).	Procesos legales no deseados, multas y pérdida de confianza de los clientes por incumplimiento de normativas.
Auditoría de continuidad del negocio (BCP) y a los planes de recuperación de desastres (DRP)	Evaluación de la capacidad de la empresa para mantener operaciones en caso de desastres.	Riesgos de interrupción prolongada de operaciones y pérdida de datos críticos.