Informe de identificación de riesgos y vulnerabilidades

Nombre del proyecto	**Plan de fortalecimiento de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)**
Empresa/Organización	**Consulting Knowledge & Systems (CKS)**
Fecha de elaboración	**22 de mayo de 2024**
Director del Proyecto	**Daniel Alexander Gonzales Castillo**

1. Resumen

Este informe tiene como objetivo evaluar los riesgos y vulnerabilidades de seguridad de la información en "Consulting, Knowledge & Systems", basándose en el inventario de activos previamente realizado. Se busca identificar amenazas potenciales y evaluar su impacto en los activos críticos de la empresa, con el fin de recomendar acciones para fortalecer la seguridad de la información y proteger los intereses del negocio.

2. Objetivos

Los objetivos del informe son los siguientes:

- Identificar y analizar los riesgos de seguridad de la información que podrían afectar a "Consulting, Knowledge & Systems".
- Evaluar la probabilidad y el impacto de los riesgos identificados, considerando los activos críticos previamente catalogados.
- Priorizar los riesgos según su criticidad para la organización, enfocándose en aquellos que podrían tener el mayor impacto en la confidencialidad, integridad y disponibilidad de la información.
- Proporcionar recomendaciones específicas y prácticas para mitigar los riesgos identificados, alineadas con las mejores prácticas de seguridad de la información.

3. Alcance

El informe abordará los siguientes aspectos:

- Análisis detallado del entorno operativo y organizacional de "Consulting, Knowledge & Systems", utilizando como base el inventario de activos previamente documentado.
- Evaluación estructurada de los riesgos de seguridad de la información, aplicando metodologías como la norma ISO 27005.
- Identificación y documentación de vulnerabilidades significativas que podrían afectar a los activos críticos de la empresa.
- Exclusión de la implementación directa de controles de seguridad; el enfoque estará en la identificación y evaluación de riesgos y vulnerabilidades.

4. Identificación de riesgos, amenazas y vulnerabilidades

Nombre de activo	Descripción del activo	Riesgo	Vulnerabilidad
Información de proyectos en curso	Documentación técnica y estratégica de los proyectos activos.	Este activo está expuesto al riesgo de divulgación no autorizada, lo que podría comprometer la propiedad intelectual y estratégica de los proyectos en desarrollo.	Acceso no autorizado debido a permisos inadecuados en sistemas de gestión de proyectos.
Información de proveedores	Datos de contacto y contratos con proveedores.	Puede enfrentar riesgos de seguridad relacionados con la confidencialidad de los contratos y la información financiera de los proveedores, lo que podría afectar las relaciones comerciales y la competitividad.	Brechas de seguridad en los portales o plataformas de intercambio de información con proveedores.
Computadoras de escritorio	Equipos utilizados por el personal para tareas generales.	Están sujetas a riesgos de pérdida de datos por robo o acceso no autorizado, lo que podría resultar en la exposición de información sensible o la interrupción de las operaciones.	Falta de actualizaciones de seguridad y parches en sistemas operativos y software instalado.
AutoCAD	Software de diseño asistido por computadora (CAD).	Este software puede estar expuesto a riesgos de acceso no autorizado que podrían comprometer diseños y propiedad intelectual valiosa de la empresa.	Exploits de seguridad conocidos en versiones no actualizadas de AutoCAD.
Estrategias y planes de negocios	Documentos que delinean la dirección estratégica de la empresa, incluyendo objetivos a largo plazo,	Los riesgos principales incluyen la divulgación a competidores, lo que podría afectar la ventaja competitiva y la dirección estratégica de la empresa.	Acceso no autorizado a documentos confidenciales de estrategia empresarial.

	planes de expansión, políticas corporativas y enfoques comerciales.		
Planes de negocios	Documentos que detallan la estrategia de negocio de la empresa, incluyendo análisis de mercado, modelos financieros, planes de marketing y estrategias de crecimiento.	Similar a las estrategias, los planes de negocios enfrentan el riesgo de divulgación no autorizada, lo que podría comprometer la confidencialidad de los objetivos financieros y estratégicos.	Acceso no autorizado a documentos confidenciales de estrategia empresarial.
Comunicaciones internas y externas	Correos electrónicos, mensajes instantáneos y otros medios de comunicación utilizados para la interacción tanto interna como externa de la empresa.	Existe el riesgo de interceptación o manipulación de comunicaciones, lo que podría resultar en la divulgación de información confidencial o la manipulación de acuerdos comerciales.	Interceptación de comunicaciones debido a protocolos de seguridad débiles en correos electrónicos o mensajería instantánea.
Información de empleados	Información personal y profesional de los empleados para la gestión de recursos humanos	Está sujeta al riesgo de violaciones de privacidad y pérdida de datos personales, lo que podría llevar a problemas legales y de reputación para la empresa.	Acceso no autorizado a registros de empleados debido a políticas de acceso débiles o falta de autenticación multifactor.
Registros de nómina	Registros de compensación y beneficios de los empleados, incluyendo detalles de salarios, deducciones,	Este activo enfrenta riesgos de acceso no autorizado o pérdida de datos financieros confidenciales, lo que podría afectar la confianza de los empleados y el	Acceso no autorizado a datos de nómina debido a insuficiente protección de acceso y cifrado de datos.

	beneficios, impuestos y otra información relacionada con la nómina.	cumplimiento normativo.	
Informes financieros	Documentos que proporcionan información detallada sobre el rendimiento financiero de la empresa, incluyendo balances, estados de resultados, flujos de efectivo, análisis financieros y otra información relevante para la toma de decisiones financieras.	Existen riesgos de manipulación o divulgación no autorizada de información financiera sensible, lo que podría afectar la reputación y la toma de decisiones estratégicas.	Acceso no autorizado a informes financieros críticos debido a controles de acceso deficientes.
Registros contables	Registros detallados de todas las transacciones financieras realizadas por la empresa, incluyendo registros de ingresos, egresos, activos, pasivos, capital contable y cualquier otro registro contable necesario para mantener la precisión y	Sujetos a riesgos de alteración no autorizada o pérdida de datos, lo que podría afectar la precisión de los informes financieros y el cumplimiento normativo.	Falta de seguridad en bases de datos contables que podría resultar en robo de datos o fraudes contables.

	transparencia financiera.		
Datos bancarios	Información relacionada con las cuentas bancarias de la empresa, incluyendo números de cuenta, saldos, movimientos, información de tarjetas de crédito, préstamos y otra información financiera confidencial.	Están expuestos a riesgos de robo de identidad, fraude financiero y violación de normativas de protección de datos, lo que podría tener consecuencias legales y financieras graves para la empresa.	Riesgo de robo de identidad o fraude financiero debido a accesos no autorizados a datos bancarios.
Información de clientes	Datos relacionados con los clientes de la empresa, incluyendo información de contacto, historial de compras, preferencias, comentarios y otra información relevante para la gestión de relaciones con los clientes.	Este activo enfrenta riesgos de violación de privacidad y divulgación no autorizada, lo que podría dañar la confianza del cliente y la reputación de la empresa.	Violaciones de privacidad debido a la exposición de datos personales de clientes.
Información de ventas	Registros de todas las transacciones de ventas realizadas por la empresa, incluyendo ventas realizadas, productos vendidos, precios,	Está sujeta a riesgos de manipulación o divulgación no autorizada, lo que podría afectar las estrategias comerciales y la competitividad en el merca	Acceso no autorizado a registros de ventas que podrían revelar estrategias comerciales y datos financieros sensibles.

	descuentos, comisiones y otra información relacionada con las actividades de ventas.		
Contratos	Documentos que detallan acuerdos y compromisos entre la empresa y sus clientes, proveedores, socios comerciales y otras partes interesadas, incluyendo términos y condiciones, acuerdos de nivel de servicio, contratos de ventas y cualquier otro documento contractual relevante.	Los riesgos incluyen la interpretación errónea o la violación de términos contractuales, lo que podría llevar a disputas legales y financieras con partes interesadas.	Acceso no autorizado a detalles contractuales confidenciales.
Planes de proyectos	Documentos que describen los objetivos, alcance, recursos, presupuestos y cronogramas de los proyectos de la empresa. Incluyen estrategias de ejecución y cualquier otra información relevante para	Existen riesgos de alteración no autorizada o pérdida de información crítica de planificación y ejecución de proyectos, lo que podría afectar la entrega y la eficiencia operativa.	Falta de control de acceso y versionamiento adecuado en documentos de planificación de proyectos.

	la gestión de proyectos.		
Documentación técnica	Documentos técnicos que detallan especificaciones, planos, diagramas, manuales y otra información técnica necesaria para la ejecución y el mantenimiento de proyectos. Incluyen información sobre equipos, materiales y procesos técnicos.	Este activo enfrenta riesgos de acceso no autorizado o pérdida, lo que podría afectar la capacidad de la empresa para mantener y operar sistemas técnicos de manera segura y eficiente.	Acceso no autorizado a especificaciones técnicas y diseños de productos.
Inventario de herramientas	El inventario de herramientas comprende una variedad de herramientas manuales y equipos de medición utilizados por los técnicos durante la instalación y el mantenimiento de sistemas de cableado y seguridad.	Sujeto a riesgos de pérdida o daño físico, lo que podría afectar la capacidad de los técnicos para realizar instalaciones y mantenimiento de manera efectiva.	Riesgo de pérdida o robo de herramientas críticas no gestionadas adecuadamente.
Inventario de materiales de instalación	Componentes esenciales utilizados en proyectos de cableado estructurado y sistemas de seguridad. Incluyen cables	Este activo enfrenta riesgos de gestión ineficiente o pérdida de componentes esenciales, lo que podría afectar la ejecución y el cumplimiento de proyectos de	Acceso no autorizado a registros de inventario que podrían afectar la disponibilidad de materiales críticos.

	de red, conectores, canaletas, dispositivos de montaje y equipos de switching y enrutamiento, etc.	infraestructura.	
Impresoras	Dispositivos utilizados para la impresión de documentos físicos desde equipos informáticos.	Acceso no autorizado a documentos impresos que contienen información confidencial.	Falta de autenticación adecuada para acceder a funciones de impresión y escaneo, lo que podría permitir a personas no autorizadas obtener información sensible.
Microsoft Teams	Microsoft Teams es una plataforma de colaboración empresarial que permite la comunicación y el trabajo en equipo a través de chat, reuniones y colaboración en documentos.	Exposición de datos sensibles debido a configuraciones de privacidad inadecuadas.	Vulnerabilidades de seguridad en la plataforma que podrían ser explotadas para acceder a conversaciones o archivos compartidos sin autorización.
Zoom	Zoom es una herramienta de videoconferencia ampliamente utilizada para reuniones virtuales y colaboración en tiempo real.	Interrupciones del servicio que podrían afectar la disponibilidad de reuniones críticas.	Vulnerabilidades de seguridad que podrían ser aprovechadas para interceptar comunicaciones durante las videoconferencias, comprometiendo la confidencialidad de la información discutida.