

# Informe de identificación de riesgos y vulnerabilidades de activos

## 1. Información del proyecto

Nombre del proyecto	Plan de fortalecimiento de la seguridad de la información para la empresa Consulting, Knowledge & Systems (CKS)
Empresa	Consulting, Knowledge & Systems (CKS)
Fecha de elaboración	25/05/2024
Director del proyecto	Daniel Alexander Gonzales Castillo

## 2. Introducción

Este informe tiene como objetivo identificar los riesgos y vulnerabilidades asociados a los activos de información previamente identificados, utilizando la metodología de la norma ISO 27005.

La empresa maneja una variedad de activos de información que incluyen desde documentos estratégicos y financieros hasta datos sensibles de clientes y empleados. Dado que actualmente no cuenta con medidas de seguridad implementadas ni documentadas, es crucial realizar una evaluación detallada para entender las amenazas potenciales que podrían afectar la confidencialidad, integridad y disponibilidad de estos activos.

El informe proporcionará una base sólida para la implementación de controles de seguridad adecuados, destinados a mitigar los riesgos identificados y fortalecer la postura de seguridad de la empresa. Esto no solo protegerá la información crítica de la empresa, sino que también fortalecerá la confianza de los clientes y socios comerciales en sus operaciones.

## 3. Metodología

Para realizar el inventario de los activos, se basó en el Control 8 de la norma ISO 27001 para la gestión de activos de información dentro de la organización. Este control proporciona un marco estructurado para identificar, clasificar y gestionar activos de información que son críticos para la operación y la seguridad de la empresa.

- **Identificación de Activos:**

- Se realizó un inventario exhaustivo de todos los activos de información, incluyendo activos físicos (como equipos informáticos y dispositivos de red) y activos lógicos (como software y datos).
- Cada activo fue clasificado según su importancia para la operación y su sensibilidad a la seguridad de la información.
- **Clasificación de Activos:**
  - Los activos fueron clasificados de acuerdo con su nivel de confidencialidad, integridad y disponibilidad requeridos para protegerlos adecuadamente.
  - Se consideraron los impactos potenciales en caso de pérdida, acceso no autorizado o alteración de cada activo.
- **Valoración de Amenazas y Vulnerabilidades:**
  - Se aplicó la norma ISO 27005 para identificar los riesgos y vulnerabilidades asociados con cada activo.
  - Para cada activo identificado, se evaluaron las posibles amenazas que podrían afectar y las vulnerabilidades específicas que podrían ser explotadas por estas amenazas.

#### Niveles de amenazas

Clasificación	Descripción
Muy alta (5)	Existen amenazas con una probabilidad extremadamente alta
Alta (4)	Existen amenazas con una probabilidad sustancial
Moderado (3)	Existen amenazas que podrían materializarse con una probabilidad significativa
Bajo (2)	La probabilidad de que ocurra es baja, pero no se puede descartar por completo
Muy bajo (1)	La probabilidad de ocurrencia es extremadamente baja

#### Niveles de vulnerabilidades

Clasificación	Descripción
---------------	-------------

Muy alta (5)	Las medidas de seguridad actuales son inadecuadas y dejan al activo de información altamente expuesto
Alta (4)	Existen amenazas con una probabilidad sustancial
Moderado (3)	Existen amenazas que podrían materializarse con una probabilidad significativa
Bajo (2)	La probabilidad de que ocurra es baja, pero no se puede descartar por completo
Muy bajo (1)	La probabilidad de ocurrencia es extremadamente baja

#### 4. Evaluación de amenazas y vulnerabilidades de cada activo

Nombre de activo	Descripción del activo	Riesgo	Nivel de amenaza	Nivel de 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.	4	3
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.	3	3
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	3	3

		las operaciones.		
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.	3	3
Estrategias y planes de negocios	Documentos que delinean la dirección estratégica de la empresa, incluyendo objetivos a largo plazo, planes de expansión, políticas corporativas y enfoques comerciales.	Los riesgos principales incluyen la divulgación a competidores, lo que podría afectar la ventaja competitiva y la dirección estratégica de la empresa.	4	4
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.	4	4
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.	3	3
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.	4	5

Registros de nómina	Registros de compensación y beneficios de los empleados, incluyendo detalles de salarios, deducciones, beneficios, impuestos y otra información relacionada con la nómina.	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 cumplimiento normativo.	4	5
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.	5	5
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 transparencia financiera.	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.	5	5
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.	5	5

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.	4	4
Información de ventas	Registros de todas las transacciones de ventas realizadas por la empresa, incluyendo ventas realizadas, productos vendidos, precios, descuentos, comisiones y otra información relacionada con las actividades de ventas.	Está sujeta a riesgos de manipulación o divulgación no autorizada, lo que podría afectar las estrategias comerciales y la competitividad en el merca	5	4
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.	5	3
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 la gestión de proyectos.	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.	4	4

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.	3	3
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.	2	2
Inventario de materiales de instalación	Componentes esenciales utilizados en proyectos de cableado estructurado y sistemas de seguridad. Incluyen cables de red, conectores, canaletas, dispositivos de montaje y equipos de switching y enrutamiento, etc.	Este activo enfrenta riesgos de gestión ineficiente o pérdida de componentes esenciales, lo que podría afectar la ejecución y el cumplimiento de proyectos de infraestructura.	2	2