Informe de recomendaciones de mitigación

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. Resumen

El proceso de mitigación de riesgos se centra en identificar y aplicar medidas específicas para reducir la probabilidad y el impacto de riesgos que pueden afectar a los activos críticos de la empresa. Este procedimiento es fundamental para proteger la información sensible, garantizar la continuidad operativa y mantener la integridad y confidencialidad de los datos. Las acciones incluyen la implementación de controles de acceso, cifrado de datos, soluciones de gestión de seguridad, auditorías periódicas y capacitación del personal. Estas medidas ayudan a prevenir la divulgación no autorizada, la manipulación de información, la pérdida de datos y otros incidentes que podrían tener consecuencias legales, financieras y operacionales.

3. Metodología utilizada

La metodología aplicada se dividió en las siguientes etapas clave:

- **Identificación de Activos Críticos**: Se realizó una revisión detallada del inventario de activos de información críticos, incluyendo activos físicos, lógicos y de información, identificados previamente utilizando los principios de la ISO/IEC 27001 Control 8.
- **Identificación de Amenazas y Vulnerabilidades:** Se emplearon técnicas de análisis para identificar las posibles amenazas que podrían afectar a cada activo crítico, así como las vulnerabilidades específicas que podrían ser explotadas por estas amenazas.
- **Evaluación de Riesgos:** Se evaluaron los riesgos asociados a cada amenaza identificada, considerando la probabilidad de ocurrencia y el impacto potencial en la confidencialidad, integridad y disponibilidad de la información.

- **Análisis y Priorización de Riesgos:** Se asignaron valores numéricos para la probabilidad y el impacto de cada riesgo identificado, utilizando una escala del 1 al 5 conforme a la metodología de la ISO/IEC 27005. Los riesgos fueron priorizados en función de su nivel de riesgo calculado, determinando aquellos que requieren medidas de mitigación inmediatas.

4. **Medidas de mitigación recomendadas**

Nombre de activo	Descripción del activo	Riesgo	Nivel de exposición al riesgo	Medidas de mitigación
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.	207,84	Implementar controles de acceso estrictos y cifrado de documentos para proteger la documentación técnica y estratégica de los proyectos activos. Utilizar soluciones de gestión de derechos digitales (DRM) para restringir la divulgación no autorizada. Realizar auditorías regulares y capacitaciones de seguridad para el personal involucrado en los 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.	98,9	Aplicar cifrado a los datos de contacto y contratos con proveedores. Establecer acuerdos de confidencialidad y realizar auditorías periódicas de seguridad. Implementar sistemas de gestión de acceso para garantizar que solo

				el personal autorizado pueda acceder a esta información.
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.	98,9	Instalar software de seguridad robusto, como antivirus y firewalls. Implementar políticas de uso aceptable y realizar capacitaciones de seguridad para los empleados. Utilizar cifrado de discos y asegurar que los datos sensibles se almacenen en servidores seguros en lugar de en los dispositivos locales.
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.	109	Utilizar soluciones de autenticación multifactor (MFA) para acceder al software. Implementar políticas de seguridad de contraseñas y cifrado de archivos de diseño. Realizar copias de seguridad regulares y auditorías de acceso para detectar y prevenir accesos no autorizados.
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.	320	Proteger los documentos mediante cifrado y controles de acceso. Utilizar sistemas de gestión de derechos digitales (DRM) para restringir la divulgación y compartir documentos de forma segura. Realizar revisiones de

				seguridad periódicas y capacitaciones para el personal clave.
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.	320	Aplicar medidas similares a las estrategias de negocios, incluyendo el cifrado de documentos y controles de acceso. Utilizar soluciones de gestión de documentos que ofrezcan seguimiento y auditoría de accesos. Realizar simulacros de seguridad y revisar regularmente las políticas de confidencialidad.
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.	143,01	Implementar cifrado de extremo a extremo para correos electrónicos y mensajes instantáneos. Utilizar soluciones de seguridad para prevenir la interceptación y manipulación de comunicaciones. Capacitar al personal sobre la identificación de ataques de phishing y otras amenazas.
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.	373,6	Proteger la información personal y profesional mediante cifrado y controles de acceso. Implementar políticas de privacidad y realizar auditorías de seguridad. Utilizar soluciones de gestión de identidades y

				accesos (IAM) para asegurar que solo el personal autorizado tenga acceso a estos datos.
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.	401,62	Aplicar cifrado a los registros de compensación y beneficios. Implementar controles de acceso estrictos y realizar auditorías periódicas. Utilizar soluciones de gestión de seguridad de datos (DLP) para prevenir la pérdida de información confidencial.
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.	583,75	Utilizar cifrado y controles de acceso para proteger los informes financieros. Implementar soluciones de gestión de riesgos financieros y realizar auditorías de seguridad regulares. Capacitar al personal en la identificación de amenazas y el manejo seguro de información financiera.
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	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.	583,75	Aplicar cifrado y controles de acceso a los registros contables. Implementar políticas de integridad de datos y realizar auditorías periódicas. Utilizar soluciones de respaldo y

	necesario para mantener la precisión y transparencia financiera.			recuperación de datos para asegurar la precisión y disponibilidad de los registros financieros.
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.	545,22	Proteger la información bancaria mediante cifrado y autenticación multifactor (MFA). Implementar políticas de gestión de riesgos financieros y realizar auditorías regulares. Utilizar soluciones de detección y prevención de fraudes para proteger contra el robo de identidad y el fraude financiero.
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.	277,12	Implementar cifrado y controles de acceso para proteger los datos de clientes. Establecer políticas de privacidad y realizar auditorías de seguridad. Utilizar soluciones de gestión de relaciones con clientes (CRM) seguras y capacitar al personal sobre la protección de datos personales.
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	Está sujeta a riesgos de manipulación o divulgación no autorizada, lo que podría afectar las estrategias comerciales y la competitividad en el merca	346,4	Aplicar medidas de seguridad como cifrado y controles de acceso a los registros de ventas. Utilizar soluciones de gestión de ventas seguras y realizar auditorías periódicas.

	relacionada con las actividades de ventas.			Implementar políticas de integridad de datos y capacitar al personal sobre la manipulación segura de información comercial.
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.	280,2	Utilizar cifrado y soluciones de gestión de contratos seguras. Implementar controles de acceso y realizar auditorías regulares para asegurar la integridad y confidencialidad de los contratos. Capacitar al personal sobre la interpretación y manejo seguro de documentos contractuales.
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.	256	Proteger los planes de proyectos mediante cifrado y controles de acceso. Utilizar soluciones de gestión de proyectos que ofrezcan seguimiento y auditoría de accesos. Realizar revisiones de seguridad periódicas y capacitar al personal sobre la gestión segura 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,	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.	132,12	Aplicar medidas de cifrado y controles de acceso a la documentación técnica. Utilizar soluciones de gestión de documentos seguras y realizar auditorías regulares. Capacitar al personal

	materiales y procesos técnicos.			técnico sobre la protección y manejo seguro de información técnica.
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.	39,19	Implementar soluciones de seguimiento y control de inventario para prevenir la pérdida o daño físico. Realizar auditorías periódicas y establecer políticas de manejo y almacenamiento seguro de herramientas. Capacitar al personal sobre el uso y mantenimiento adecuado de las herramientas.
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.	42,72	Utilizar soluciones de gestión de inventarios para asegurar el control y seguimiento de los materiales. Implementar políticas de almacenamiento seguro y realizar auditorías regulares. Capacitar al personal sobre la gestión eficiente y segura de materiales de instalación.