Informe de recomendaciones de mitigación

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	**26 de mayo de 2024**
Director del Proyecto	**Daniel Alexander Gonzales Castillo**

1. Resumen

Las recomendaciones de mitigación son estrategias y acciones específicas diseñadas para reducir el impacto y la probabilidad de ocurrencia de riesgos asociados con los activos de información de una empresa. Estas recomendaciones se basan en la identificación y evaluación de riesgos y vulnerabilidades, y están alineadas con las mejores prácticas de seguridad de la información. El propósito de estas recomendaciones es fortalecer la postura de seguridad de la empresa y proteger sus activos críticos contra amenazas potenciales.

2. Objetivos

- **Reducir Riesgos**: Implementar medidas efectivas para minimizar la probabilidad y el impacto de los riesgos identificados.
- **Aumentar la Resiliencia:** Fortalecer la capacidad de la empresa para resistir y recuperarse rápidamente de incidentes de seguridad.
- **Proteger Activos Críticos:** Salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información clave.
- **Cumplir con Normativas:** Asegurar el cumplimiento de las normas y regulaciones de seguridad de la información, como ISO 27001 y 27005.
- **Fomentar una Cultura de Seguridad:** Promover la concientización y la adopción de buenas prácticas de seguridad entre todos los empleados de la empresa.

3. Alcance

El alcance de las recomendaciones de mitigación incluirá:

- **Evaluación Inicial:** Revisión de la evaluación de riesgos y vulnerabilidades realizada previamente para identificar áreas críticas que requieren medidas de mitigación.
- **Desarrollo de Estrategias:** Formulación de estrategias de mitigación específicas para cada riesgo identificado, considerando la naturaleza del riesgo y el activo afectado.
- **Implementación de Controles:** Aplicación de controles técnicos, administrativos y físicos para mitigar los riesgos. Esto incluye medidas como cifrado de datos, autenticación multifactor, actualizaciones de seguridad y políticas de acceso.
- **Capacitación y Concientización:** Programas de capacitación para el personal sobre las nuevas políticas, procedimientos y mejores prácticas de seguridad.
- **Monitoreo y Revisión:** Establecimiento de mecanismos de monitoreo continuo para evaluar la efectividad de las medidas de mitigación implementadas y realizar ajustes cuando sea necesario.

- **Documentación y Reporte:** Documentación detallada de todas las actividades de mitigación y generación de informes regulares para la dirección y otras partes interesadas.

4. Recomendaciones

Nombre de activo	Riesgo	Vulnerabilidad	Nivel de exposición al riesgo	Medida	Recomendación
Información de proyectos en curso	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.	207,84	Transferir	Se recomienda contratar un seguro de ciberseguridad que cubra la divulgación no autorizada de información sensible. Además, implementar un sistema de control de acceso basado en roles.
Información de 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.	98,901	Aplazar	Realizar evaluaciones de seguridad periódicas en portales utilizados con proveedores y establecer protocolos seguros para la transferencia de datos, como el uso de VPN y cifrado de extremo a extremo.
Computadoras de escritorio	Están sujetas a riesgos de pérdida de datos por robo o acceso no autorizado, lo que podría resultar en la	Falta de actualizaciones de seguridad y parches en sistemas operativos	98,901	Aplazar	Implementar gestión de parches para mantener los sistemas actualizados y utilizar software de protección

	exposición de información sensible o la interrupción de las operaciones.	y software instalado.			contra virus y malware, así como autenticación multifactor y cifrado de disco completo.
AutoCAD	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.	108,999	Aplazar	Asegurar que AutoCAD esté actualizado con los últimos parches de seguridad, implementar controles de acceso estrictos y realizar copias de seguridad regulares de los archivos de diseño.
Estrategias y planes de negocios	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.	320	Mitigar	Implementar controles de acceso estrictos, utilizar cifrado robusto para documentos confidenciales, y realizar auditorías de seguridad periódicas. Además, se recomienda capacitar al personal en la importancia de la confidencialidad y en prácticas seguras de manejo de información.
Planes de negocios	Similar a las estrategias, los planes de negocios enfrentan el riesgo de	Acceso no autorizado a documentos confidenci	320	Mitigar	Reforzar los controles de acceso y utilizar cifrado robusto para la transmisión y

	divulgación no autorizada, lo que podría comprometer la confidencialidad de los objetivos financieros y estratégicos.	ales de estrategia empresarial.			almacenamiento de planes de negocios. Implementar autenticación multifactor y políticas de acceso basadas en roles para asegurar que solo el personal autorizado pueda acceder a estos documentos.
Comunicaciones internas y externas	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.	Intercepta ción de comunicac iones debido a protocolos de seguridad débiles en correos electrónic os o mensajerí a instantáne a.	38,97	Aceptar	Aunque se ha decidido aceptar el riesgo, es recomendable utilizar protocolos de cifrado para correos electrónicos y mensajería instantánea, y educar al personal sobre prácticas seguras de comunicación para minimizar posibles interceptaciones.
Información de empleados	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 empleado s debido a políticas de acceso débiles o falta de autenticaci ón multifactor .	373,6	Mitigar	Asegurar que la información de empleados esté cifrada y almacenada de manera segura, implementar autenticación multifactor y restringir el acceso a personal autorizado. Realizar auditorías de seguridad

					periódicas y capacitar al personal en la importancia de proteger la información personal.
Registros de 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.	Acceso no autorizado a datos de nómina debido a insuficiente protección de acceso y cifrado de datos.	401,62	Mitigar	Implementar controles de acceso estrictos y cifrado robusto para los datos de nómina. Utilizar autenticación multifactor para asegurar que solo el personal autorizado pueda acceder a estos datos, y realizar auditorías de seguridad periódicas para garantizar la protección de los registros de nómina.
Informes financieros	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.	583,75	Mitigar	Implementar controles de acceso estrictos, incluyendo autenticación multifactor y políticas de acceso basadas en roles. Utilizar cifrado robusto para la transmisión y almacenamiento de informes financieros. Realizar auditorías de seguridad periódicas y capacitar al

					personal en prácticas seguras de manejo de información financiera.
Registros contables	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.	583,75	Mitigar	Implementar medidas de seguridad robustas en las bases de datos contables, como cifrado de datos y autenticación multifactor. Establecer políticas de acceso restringido y realizar auditorías de seguridad regulares para asegurar la integridad y disponibilidad de los registros contables.
Datos bancarios	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.	545,2225	Mitigar	Implementar cifrado robusto para la transmisión y almacenamiento de datos bancarios. Utilizar autenticación multifactor y controles de acceso estrictos para asegurar que solo el personal autorizado tenga acceso a esta información. Realizar auditorías de seguridad periódicas y

					capacitar al personal en prácticas seguras de manejo de información bancaria.
Información de 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.	277,12	Transferir	Contratar un seguro de ciberseguridad para cubrir posibles violaciones de privacidad. Implementar controles de acceso estrictos y cifrado robusto para la transmisión y almacenamiento de información de clientes. Además, educar al personal sobre la importancia de proteger los datos personales y las consecuencias de su exposición.
Información 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	Acceso no autorizado a registros de ventas que podrían revelar estrategias comerciales y datos financieros sensibles.	346,4	Mitigar	Implementar controles de acceso basados en roles y autenticación multifactor para los registros de ventas. Utilizar cifrado para la transmisión y almacenamiento de datos sensibles. Realizar auditorías periódicas y capacitar al personal en

					prácticas seguras de manejo de información de ventas.
Contratos	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.	280,2	Transferir	Contratar un seguro de responsabilidad profesional para cubrir posibles disputas contractuales. Implementar controles de acceso estrictos y utilizar cifrado para la transmisión y almacenamiento de contratos. Capacitar al personal en la importancia de la confidencialidad y en prácticas seguras de manejo de información contractual.
Planes 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.	Falta de control de acceso y versionamiento adecuado en documentos de planificación de proyectos.	256	Transferir	Contratar un seguro de ciberseguridad que cubra la alteración o pérdida de información de planificación de proyectos. Implementar sistemas de control de versiones y acceso basado en roles. Realizar auditorías de seguridad periódicas y capacitar al

					personal en la gestión segura de documentos de planificación de proyectos.
Documentación técnica	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.	132,12	Aplazar	Mientras se decide una medida definitiva, mejorar la seguridad física de los documentos técnicos y restringir el acceso a personal autorizado. Evaluar la implementación de sistemas de cifrado y autenticación multifactor en un futuro cercano para proteger la documentación técnica.
Inventario de herramientas	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.	39,1956	Aceptar	Aceptar riesgo
Inventario de materiales de instalación	Este activo enfrenta riesgos de gestión ineficiente o pérdida de componentes esenciales, lo	Acceso no autorizado a registros de inventario que podrían afectar la	42,72	Aceptar	Aceptar riesgo

	que podría afectar la ejecución y el cumplimiento de proyectos de infraestructura.	disponibilidad de materiales críticos.			
Impresoras	Dispositivos utilizados para la impresión de documentos físicos desde equipos informáticos.	Acceso no autorizado a documentos impresos que contienen información confidencial.	21,36	Aceptar	Aceptar riesgo
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.	20,826	Aceptar	Aceptar riesgo
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.	10,68	Aceptar	Aceptar riesgo