ANÁLISIS DE CAUSA RAÍZ (RCA)

PROYECTO	Plan de fortalecimiento de la seguridad de la información para la empresa CKS.
EMPRESA	Empresa Consulting, Knowledge & Systems (CKS)
AUTOR	Ciriaco Esquivel Omar Antonio
APROBADO POR	Gonzales Castillo Daniel Alenxander
FECHA CREACIÓN	01/07/2024
FECHA APROBACIÓN	05/07/2024

DETALLES DEL PROBLEMA		EMISIÓN A INFORMAR				POSIBLE CAUSA RAÍZ			SOLUCIONES SUGERIDAS				
				CALIFIQUE QUÉ TAN CRÍTICO			PROBABILIDAD	DETALLES		CALIFIQUE LA POSIBLE SOLUCIÓN		DESCRIBIR LA MEDICIÓN DEL ÉXITO	
FECHA DEL PROBLEMA NOTIFICADO	**NOMBRE**	**DESCRIBIR EL PROBLEMA**	**EXPLICAR LA FUENTE**	*Califique qué tan crítico: Bajo, Medio o Alto*	*Justificación*	**DESCRIBIR LA CAUSA**	*Probabilidad de tasa: Baja, Media o Alta*	*Enumerar las pruebas para su aclaración*	**DESCRIBIR LA SOLUCIÓN**	*Tasa de probabilidad de riesgos: Baja, Media o Alta*	*Modificación*	*Describir las pruebas*	*Describir los resultados*
1/6/2024	Acceso no autorizado a información sensible	Un usuario no autorizado accedió a información sensible.	Falta de controles de acceso adecuados.	Alto	La información sensible compromete la seguridad de la empresa.	Configuración incorrecta de permisos de usuario.	Media	Revisión de logs de acceso y configuración de permisos.	Implementar controles de acceso estrictos y revisar configuraciones	Baja	Actualización de políticas de acceso y capacitación del personal.	Simulación de acceso no autorizado.	Accesos no autorizados eliminados.
5/6/2024	Respaldo de datos incompleto o fallido	Respaldo de datos no se completó correctamente.	Falta de verificación de respaldos.	Medio	Posible pérdida de datos críticos.	Errores en el software de respaldo.	Alta	Revisión de proceso de respaldo.	Implementar una rutina de verificación de respaldos.	Baja	Actualización de procedimientos de respaldo.	Pruebas periódicas de restauración de datos.	Respaldos completados correctamente.
12/6/2024	No cumplimiento de políticas de seguridad	Empleados no siguen políticas de seguridad.	Falta de concientización y capacitación.	Alto	Compromete la seguridad de la información.	Capacitación insuficiente.	Media	Encuestas y auditorías internas.	Realizar capacitaciones y talleres de concientización .	Baja	Programas de capacitación regular.	Evaluaciones post-capacitación.	Mejora en el cumplimiento de políticas.
18/6/2024	Tiempo de respuesta lento ante incidentes de seguridad	Respuesta lenta a incidentes de seguridad.	Procedimientos de respuesta no claros.	Medio	Aumenta el impacto de los incidentes.	Falta de un plan de respuesta a incidentes.	Media	Revisión de incidentes pasados.	Implementar un plan de respuesta a incidentes.	Baja	Actualización de manuales y procedimientos.	Simulaciones de incidentes.	Mejora en el tiempo de respuesta.
25/6/2024	Gestión inadecuada de activos	Falta de control sobre los activos de información.	Inventario de activos incompleto.	Medio	Riesgo de pérdida o mal uso de activos.	Falta de procedimientos de gestión de activos.	Alta	Auditoría de activos.	Implementar un sistema de gestión de activos.	Baja	Procedimientos de registro y seguimiento de activos.	Revisiones periódicas de inventarios.	Control adecuado de activos.
1/7/2024	No seguimiento de incidentes de seguridad	Incidentes de seguridad no se registran ni se sigue su resolución.	Falta de un sistema de seguimiento de incidentes.	Alto	Incapacidad de aprender de incidentes pasados.	Ausencia de políticas de seguimiento.	Media	Revisión de incidentes anteriores.	Implementar un sistema de registro y seguimiento de incidentes.	Baja	Procedimientos de seguimiento de incidentes.	Auditorías internas.	Todos los incidentes registrados y seguidos.
5/7/2024	Deficiencias en la gestión de cambios	Cambios en el sistema no se gestionan adecuadamente.	Falta de un proceso de gestión de cambios.	Medio	Cambios no controlados pueden introducir vulnerabilidades	Falta de políticas de gestión de cambios.	Alta	Revisión de cambios recientes.	Implementar políticas y procedimientos de gestión de cambios.	Baja	Manual de gestión de cambios.	Revisión de cambios después de la implementación.	Cambios gestionados adecuadamente.
10/7/2024	Incumplimiento de procedimientos establecidos	Procedimientos de seguridad no se siguen correctamente.	Falta de supervisión y monitoreo.	Alto	Compromete la integridad del sistema de seguridad.	Supervisión insuficiente.	Media	Auditorías y revisiones de procesos.	Implementar monitoreo y auditorías regulares.	Baja	Políticas de supervisión.	Auditorías de cumplimiento.	Cumplimiento mejorado.