Plan de fortalecimiento de seguridad de la información para la empresa CKS 5. Plan de copias de Identificación de activos 2. Evaluación de riesgos y 4. Controles de acceso y 3. Políticas y procedimientos seguridad y recuperación 6. Capacitación del personal de información crítica autenticación vulnerabilidades de seguridad de datos 5.1 Plan de copias de 6.1 Material de 4.1 Politicas y seguridad capacitación 1.1 Informe de investigación 2.1 Informe de identificación 3.1 Políticas de procedimientos de y recopilación de datos de riesgos y vulnerabilidades seguridad control de accesos 5.1.1 Diseñar plan detallado 6.1.1 Desarrollar material de que describir como se 3.1.1Desarrollar capacitación que realizarán las copias de 2.1.2 Identificar aborde las políticas y políticas de seguridad 3.1.2 Obtener 4.1.1 Documentar los 1.1.2 Recopilar seguridad 1.1.1 Realizar puntos débiles en la 2.1.1 Realizar un procedimientos establecidos que aborden revisión y controles de acceso en los documentos y entrevistas con los el acceso a datos, análisis exhaustivo de red a través de aprobación por sistemas y aplicaciones registros relevantes responsables de cada la infraestructura de herramientas de protección de parte de la sobre los activos de área escaneo de información y gerencia la empresa 5.2 Protocolo de vulnerabilidades respuesta a incidentes recuperación de datos 6.2 Sesiones de 4.2 Plan de gestión de capacitación accesos y monitoreo 3.2 Manual de 2.2 Informe de análisis y programadas y 1.2 Informe de análisis de procedimientos de priorización de riesgos coordinadas 5.2.1 Definir qué datos y activos de información seguridad sistemas tienen la máxima prioridad para la recuperación 4.2.1 Documentar monitoreo 6.2.1 Programar y coordinar según su criticidad de la funcionalidad y sesiones de capacitación 3.2.1 Crear 2.2.2 Priorizar los 2.2.1 Evaluación de seguridad de los controles de para el personal sobre las procedimientos riesgos según su impacto y acceso implementados 1.2.2 Documentar 1.2.1 Analizar la mejores prácticas de 3.2.2 Documentar operativos estándar probabilidad de gravedad y importancia de cada todos los activos de seguridad de la información pasos específicos probabilidad de para la cada riesgo información activo de que deben seguir implementación de identificado ocurrencia. información crítica identificados los empleados las políticas de seguridad 6.3 Formulario de evaluación de la 2.3. Informe de efectividad de la recomendaciones de capacitación mitigación 6.3.1 Evaluar la efectividad de las sesiones de capacitación mediante la 2.3.2 Priorizar las recopilación de retroalimentación y la 2.3.1 Desarrollar acciones de realización de pruebas de estrategias y mitigación en conocimientos. recomendaciones función para mitigar los de la criticidad de riesgos identificados los riesgos