LINEA BASE DEL ALCANCE

Enunciado del Alcance del Proyecto

El proyecto consiste en Implementar medidas y controles de seguridad de la información para proteger los activos críticos de CKS contra amenazas cibernéticas y físicas, garantizando la integridad, confidencialidad y disponibilidad de la información de la empresa

Criterios de Aceptación

Criterios	Nivel Esperado	Frecuencia
Cumplimiento de Normativas: Todas las medidas implementadas deben cumplir con las normativas y regulaciones peruanas aplicables, como la Ley de Protección de Datos Personales y el Reglamento de Seguridad de la Información	Alto	Monitoreo Continuo
Cobertura de Activos Críticos: Todos los activos de información crítica de CKS, incluyendo datos de clientes e información financiera y propiedad intelectual, deben estar protegidos según lo establecido en el proyecto.	Alto	Monitoreo Continuo
Efectividad de Controles de Seguridad: Los controles de seguridad implementados, incluyendo controles de acceso, autenticación, monitoreo y detección de amenazas deben garantizar la protección adecuada de los activos de información.	Alto	Monitoreo Continuo
Capacitación del Personal: Todo el personal relevante de CKS debe haber sido adecuadamente capacitado en mejores prácticas de seguridad de la información y estar preparado para reconocer y responder a posibles amenazas.	Medio	Bimensual
Respaldo y Recuperación de Datos: Se debe haber establecido un plan de copia de seguridad y recuperación de datos eficaz para garantizar la disponibilidad y la integridad de la información en caso de fallos del sistema o incidentes de seguridad.	Alto	Monitoreo Continuo
Actualización y Mantenimiento: Los procedimientos deben estar establecidos para garantizar que los sistemas y aplicaciones se mantengan actualizados con las últimas actualizaciones y parches de seguridad, y que se realicen evaluaciones periódicas para identificar nuevas amenazas y vulnerabilidades	Medio	Monitoreo Continuo
Seguimiento de Incidente: Proceso establecido para el seguimiento y la gestión de incidentes de seguridad, incluyendo la documentación adecuada, la investigación de causas raíz y la implementación de medidas correctivas y preventivas.	Alto	Monitoreo Continuo

Entregables del Proyecto:

- Informe de Investigación y recopilación de datos
- Informe de análisis de activos de información
- Informe de identificación de riesgo y vulnerabilidades
- Informe de análisis y priorización de riesgos
- Informe de recomendaciones de mitigación
- Políticas de seguridad
- Manual de procedimientos de seguridad
- Informe de Controles de accesos
- Informe de pruebas de funcionalidad y seguridad
- Plan de copias de seguridad
- Implementación de procedimientos de copias de seguridad
- Informe de pruebas de recuperación de datos
- Material de capacitación
- Programación y Coordinación de Sesiones de Capacitación
- Formulario de evaluación de la efectividad de la capacitación

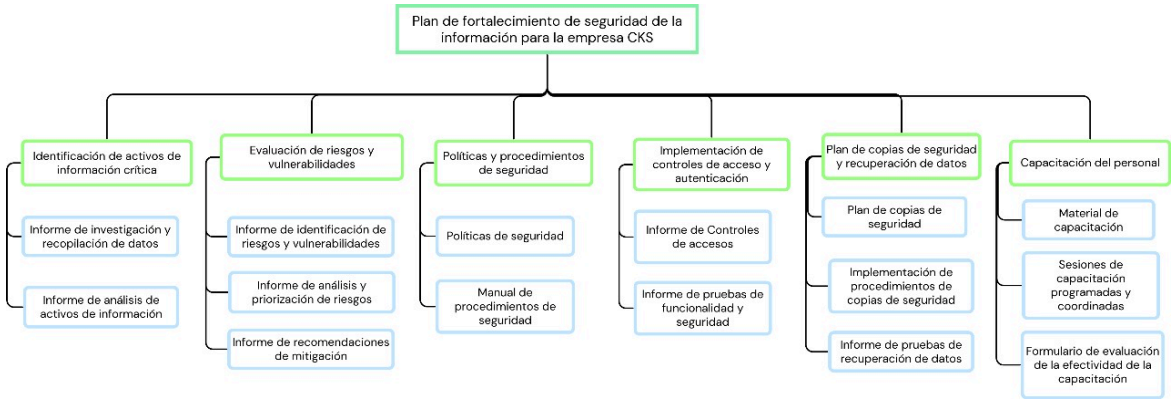
Exclusiones del Proyecto

- Desarrollo de nuevas normativas o regulaciones: El proyecto no incluye la creación o modificación de normativas o regulaciones, se enfoca en cumplir con las existentes.
- Auditorías externas independientes: El proyecto puede incluir evaluaciones internas de seguridad, pero no cubre auditorías externas independientes por terceros.
- Gestión de crisis de seguridad graves: Si bien se incluye el seguimiento de incidentes, las crisis graves que requieran respuestas inmediatas pueden estar fuera del alcance del proyecto.
- Capacitación en aspectos no relacionados con la seguridad de la información: El proyecto se centra en la capacitación del personal en mejores prácticas de seguridad de la información, excluyendo otros temas no relacionados.

Restricciones

Tipo	Descripción de la Restricción
Costo	No se permitirá la adquisición de recursos adicionales que no estén incluidos en el presupuesto aprobado.
Tiempo	No se pueden realizar implementaciones que afecten la disponibilidad de los sistemas críticos durante horas pico de operación sin la debida autorización.
Calidad	No se puede comprometer la calidad del trabajo realizado para cumplir con los plazos establecidos.

Estructura de Desglose del Trabajo (EDT)



Diccionario de la EDT

DICCIONARIO DEL EDT		
Componente	Descripción del trabajo	Responsable
1.1. Identificación de activos de información crítica	Identificar y clasificar los activos de información crítica de la organización.	Ciriaco Esquivel Omar
1.1.1. Informe de investigación y recopilación de datos	Investigar y recopilar datos sobre los activos de información crítica de la organización.	Ciriaco Esquivel Omar
1.1.2. Informe de análisis de activos de información	Analizar los activos de información para identificar su importancia y criticidad.	Ciriaco Esquivel Omar
1.2. Evaluación de riesgos y vulnerabilidades	Realizar evaluaciones de riesgos y vulnerabilidades en los activos de información crítica.	Gonzales Castillo Daniel
1.2.1. Informe de identificación de riesgos y vulnerabilidades	Identificar y documentar los riesgos y vulnerabilidades en los activos de información.	Gonzales Castillo Daniel
1.2.2. Informe de análisis y priorización de riesgos	Analizar y priorizar los riesgos identificados para la toma de decisiones.	Gonzales Castillo Daniel
1.2.3. Informe de recomendaciones de mitigación	Proporcionar recomendaciones para mitigar los riesgos y vulnerabilidades identificados.	Gonzales Castillo Daniel
1.3. Políticas y procedimientos de seguridad	Implementar normativas y estándares de seguridad para garantizar la protección de los activos críticos.	Soto Obregon Milagros
1.3.1. Políticas de seguridad	Desarrollar políticas para establecer las normas y directrices de seguridad de la información.	Soto Obregon Milagros

1.3.2. Manual de procedimientos de seguridad	Documentar los procedimientos operativos estándar para la implementación de las políticas de seguridad.	Soto Obregon Milagros
1.4. Implementación de controles de acceso y autenticación	Establecer y configurar controles de acceso y autenticación para restringir el acceso no autorizado.	Huanuco Vicuña James
1.4.1. Informe de Controles de accesos	Implementar controles de acceso para garantizar la seguridad de los activos de información.	Huanuco Vicuña James
1.4.2. Informe de pruebas de funcionalidad y seguridad	Realizar pruebas para asegurar la funcionalidad y seguridad de los controles de acceso.	Huanuco Vicuña James
1.5. Plan de copias de seguridad y recuperación de datos	Elaborar un plan de copias de seguridad para garantizar la disponibilidad y recuperación de datos críticos.	Yauricasa Mendoza Miguel
1.5.1. Plan de copias de seguridad	Desarrollar un plan para realizar copias de seguridad de los datos críticos de la organización.	Yauricasa Mendoza Miguel
1.5.2. Implementación de procedimientos de copias de seguridad	Implementar procedimientos para llevar a cabo las copias de seguridad de manera efectiva.	Yauricasa Mendoza Miguel
1.5.3. Informe de pruebas de recuperación de datos	Realizar pruebas para garantizar la efectividad de la recuperación de datos en caso de incidentes.	Yauricasa Mendoza Miguel
1.6. Capacitación del personal	Brindar capacitación en seguridad de la información al personal de la organización.	Vasquez Leiva Antony
1.6.1. Material de capacitación	Desarrollar materiales de capacitación para el personal sobre seguridad de la información.	Vasquez Leiva Antony
1.6.2. Sesiones de capacitación programadas y coordinadas	Programar y coordinar sesiones de capacitación para el personal.	Vasquez Leiva Antony
1.6.3. Formulario de evaluación de la efectividad de la capacitación	Evaluar la efectividad de la capacitación mediante formularios de retroalimentación.	Vasquez Leiva Antony