Plan de gestión de accesos y monitoreo

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

1. Resumen

Este documento detalla el plan estratégico para la gestión y monitoreo de accesos en CKS, fundamentado en las políticas y procedimientos rigurosos establecidos conforme a la norma ISO 27001. El objetivo principal es garantizar la protección integral de los sistemas de información y activos críticos de la empresa. El plan incluye la implementación de políticas detalladas para la asignación de roles y privilegios, asegurando que todos los accesos sean justificados y minimizados según el principio de "menor privilegio". Se establecerán procedimientos robustos para la creación, modificación y eliminación de cuentas de usuario, respaldados por una estricta autenticación multifactor (MFA) para fortalecer la verificación de identidades. Además, se contempla la aplicación de controles físicos como sistemas de tarjetas de acceso y CCTV para proteger las instalaciones críticas. El plan también abarca un sistema integral de monitoreo continuo y auditoría regular para evaluar la efectividad de los controles implementados y asegurar el cumplimiento con las normativas de seguridad establecidas. Esto se complementa con un enfoque en la capacitación del personal, garantizando una comprensión profunda de las políticas y prácticas de seguridad, promoviendo así una cultura de conciencia y responsabilidad en la protección de la información sensible de CKS.

2. Objetivos

Se definen los siguientes objetivos:

- **Establecer un marco claro para la gestión efectiva del acceso a los sistemas y datos críticos de CKS:**

  El objetivo es desarrollar políticas claras y documentadas que regulen cómo se gestionará el acceso a los sistemas y datos críticos dentro de la organización. Esto incluye definir roles y responsabilidades para la administración de accesos, establecer criterios para la asignación de privilegios basados en las necesidades laborales específicas, y asegurar que todos los accesos estén alineados con las normativas de seguridad establecidas.

- **Proponer controles robustos para prevenir accesos no autorizados y proteger la información sensible:**

  Se propondrán medidas de seguridad sólidas para prevenir accesos no autorizados a los sistemas y datos sensibles de CKS. Esto implica la adopción de autenticación multifactor (MFA), el uso de cifrado para la protección de datos confidenciales, y la aplicación del principio de menor privilegio para restringir el acceso solo a los usuarios necesarios.
- **Proponer mecanismos de monitoreo continuo para detectar y responder rápidamente a incidentes de seguridad relacionados con accesos:**

  Se propondrá la implementación de sistemas de monitoreo continuo para supervisar y analizar el uso de sistemas y redes dentro de CKS. Esto permitirá identificar de manera proactiva cualquier actividad sospechosa o acceso no autorizado, facilitando una respuesta rápida y efectiva ante posibles incidentes de seguridad. Además de auditorías periódicas para evaluar la efectividad de los controles de acceso implementados y asegurar el cumplimiento con las políticas de seguridad establecidas.

3. Alcance

Este plan cubre todos los sistemas de información, redes y áreas físicas críticas de CKS, asegurando que todas las políticas y procedimientos de control de accesos sean aplicables y efectivas.

4. Controles físicos de acceso

a. Sistemas de Tarjetas de Acceso:

- **Implementación**: Se deberán instalar sistemas de tarjetas de acceso en todas las entradas principales y áreas restringidas de las instalaciones de CKS.
- **Funcionamiento**: Cada empleado autorizado deberá recibir una tarjeta de acceso personalizada que deberá usar para ingresar a áreas específicas según sus niveles de privilegio.
- **Registro y Gestión:** Se llevará un registro detallado de las tarjetas emitidas y los accesos realizados para garantizar la trazabilidad y la gestión adecuada de accesos.

b. Sistemas de CCTV:

- **Instalación:** Se deberán colocar cámaras de circuito cerrado de televisión (CCTV) estratégicamente en áreas críticas y de acceso restringido de las instalaciones.
- **Cobertura**: Las cámaras proporcionarán cobertura continua y grabación de video para monitorear y registrar actividades en tiempo real.

- **Monitoreo**: El sistema de CCTV estará conectado a un centro de monitoreo dedicado o será accesible para el personal de seguridad de CKS, asegurando la vigilancia constante y la capacidad de respuesta rápida ante incidentes.

c. Otras Medidas de Seguridad Física:

- **Control de puertas y cercas**: Se implementarán sistemas adicionales de control de puertas y cercas perimetrales para reforzar la protección física de las instalaciones.
- **Seguridad de instalaciones críticas**: Las áreas que albergan activos críticos, como salas de servidores y centros de datos, contarán con medidas adicionales de seguridad física, como sistemas de bloqueo electrónico y monitoreo ambiental.

5. Proceso de monitoreo

a. Selección de herramientas de monitoreo

- **Identificación de herramientas**: Seleccionar herramientas avanzadas de monitoreo que permitan la supervisión constante de actividades de acceso a sistemas y redes. Estas herramientas deben ser capaces de registrar eventos, detectar patrones anómalos y generar alertas automáticas ante actividades no autorizadas o sospechosas.
- **Implementación de herramientas:** Instalar y configurar las herramientas de monitoreo en los sistemas críticos de CKS, asegurando que cubran todas las áreas y tipos de acceso relevantes, incluyendo acceso físico y acceso remoto a través de redes internas y externas.

b. Definición de parámetros de monitoreo

- **Establecimiento de umbrales**: Definir umbrales y límites normales de actividad para cada tipo de acceso y usuario, basados en roles y privilegios específicos.
- **Monitoreo en tiempo real**: Configurar los sistemas para monitorear en tiempo real, evaluando continuamente las transacciones y actividades de acceso para identificar desviaciones de los patrones normales de uso.

c. Generación de alertas y respuestas

- **Configuración de alertas:** Configurar alertas automáticas para notificar al equipo de seguridad de la información sobre actividades no autorizadas o comportamientos anómalos.
- **Procedimientos de respuesta**: Establecer procedimientos claros y documentados para responder rápidamente a las alertas generadas, incluyendo la investigación de incidentes, la mitigación de riesgos y la recuperación de sistemas afectados.

6. Procedimientos de auditoría

a. Planificación de auditoría

- **Frecuencia:** Establecer la frecuencia de las auditorías, considerando la criticidad de los sistemas y la sensibilidad de la información accesible.
- **Calendario:** Crear un calendario de auditorías regulares que garantice una cobertura adecuada de todos los controles de acceso implementados.
- **Notificación:** Notificar a todas las partes interesadas sobre las fechas programadas para las auditorías y el alcance de las mismas.

b. Ejecución de auditoría

- **Equipo auditor:** Designar un equipo de auditoría competente, que puede incluir personal interno capacitado o auditores externos certificados.
- **Recopilación de evidencia:** Recolectar evidencia suficiente y adecuada durante las auditorías, incluyendo revisiones de registros de acceso, entrevistas con personal relevante y evaluación de la efectividad de los controles implementados.
- **Pruebas de penetración**: Realizar pruebas de penetración, si es necesario, para evaluar la resistencia de los controles de acceso ante posibles vulnerabilidades.

c. Informe de auditoría

- **Documentación**: Preparar un informe detallado que documente los hallazgos de la auditoría, incluyendo áreas de cumplimiento y no cumplimiento con las políticas definidas y la normativa ISO 27001.
- **Recomendaciones:** Incluir recomendaciones específicas para mejorar los controles de acceso identificados durante la auditoría, priorizando acciones correctivas y preventivas.

d. Seguimiento y cierre de hallazgos

- **Plan de acción correctiva:** Desarrollar un plan de acción detallado para abordar y corregir las deficiencias identificadas durante la auditoría.
- **Seguimiento**: Realizar un seguimiento regular para verificar la implementación efectiva de las acciones correctivas y el cumplimiento continuo con las políticas y estándares de seguridad.

7. Proceso de revisión y actualización

a. Programación de revisiones

- **Frecuencia:** Definir la frecuencia de las revisiones del plan de gestión de accesos y monitoreo. Generalmente, las revisiones deben realizarse al menos

anualmente, aunque puede ser necesario ajustar la frecuencia según cambios significativos en la organización o en el entorno tecnológico.

- **Calendario**: Establecer un calendario específico para las revisiones, asegurando que se programen con anticipación y se coordinen con otras actividades de seguridad y cumplimiento.

b. Evaluación de eficacia

- **Recolección de retroalimentación:** Recopilar retroalimentación de partes interesadas clave, incluyendo el equipo de seguridad de la información, administradores de sistemas y usuarios finales, sobre la efectividad de las políticas y procedimientos actuales.
- **Análisis de Resultados:** Analizar los resultados de las evaluaciones de cumplimiento, auditorías internas e incidentes de seguridad para identificar áreas que necesiten revisión o mejora en el plan de gestión de accesos y monitoreo.

c. Actualización de políticas y procedimientos

- **Identificación de cambios**: Identificar y documentar cambios tecnológicos, regulaciones nuevas o actualizadas, y mejores prácticas emergentes que puedan impactar los controles de acceso y monitoreo.
- **Revisión y aprobación:** Revisar y actualizar las políticas y procedimientos existentes para reflejar estos cambios, asegurando la aprobación por parte de la dirección ejecutiva y el equipo de seguridad de la información.

d. Implementación de cambios

- **Comunicación y capacitación:** Comunicar los cambios actualizados a todo el personal relevante y proporcionar capacitación adicional si es necesario, asegurando la comprensión y la adherencia a las nuevas políticas y procedimientos.
- **Monitoreo de implementación**: Supervisar la implementación de los cambios y realizar un seguimiento para asegurar que se integren adecuadamente en las prácticas operativas diarias de CKS.