Políticas y procedimientos de control de accesos

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	**01 de junio de 2024**
Director del Proyecto	**Daniel Alexander Gonzales Castillo**

1. Resumen

Este documento detalla las políticas y procedimientos de control de accesos de Consulting, Knowledge & Systems (CKS) para el el establecimiento de lineamientos que cumplan con los estándares de la norma ISO 27001, específicamente el control "Control de Accesos". El proyecto tendrá en cuenta controles específicos como la asignación basada en roles para derechos de acceso, la implementación de procedimientos formales para la creación y eliminación de cuentas de usuario, y la obligación de autenticación multifactor (MFA) para todos los accesos. Adicionalmente, se establecerán medidas rigurosas para el control de acceso físico a áreas críticas mediante tarjetas de acceso y sistemas de CCTV, así como la segregación de redes internas para minimizar riesgos. Los procedimientos detallados incluirán la solicitud formal y aprobación de accesos, revisiones periódicas de privilegios, monitoreo continuo de actividades de acceso, y auditorías regulares para garantizar el cumplimiento y la efectividad de las políticas establecidas, alineadas con los controles de acceso específicos exigidos por la norma ISO 27001.

2. Objetivos

Para cumplir con el objetivo principal de establecer controles adecuados para gestionar y restringir el acceso a la información y sistemas de información en Consulting, Knowledge & Systems (CKS), se propone lo siguiente:

- **Implementar Políticas de Control de Acceso**: Desarrollar e implementar políticas claras y detalladas de control de acceso que definan cómo se gestionarán los derechos de acceso a los sistemas y datos dentro de la organización. Esto incluirá la asignación de privilegios basada en roles específicos y la definición de procedimientos para la solicitud, aprobación y revocación de accesos.
- **Establecer Mecanismos de Autenticación Robustos:** Implementar mecanismos de autenticación fuertes, como la autenticación multifactor (MFA), para verificar la identidad de los usuarios antes de permitirles el acceso a sistemas críticos. Esto ayudará a

proteger contra accesos no autorizados mediante la validación de múltiples factores de identificación.

- **Aplicar el Principio de Menor Privilegio**: Adoptar el principio de menor privilegio, asegurando que los usuarios tengan acceso solo a la información y recursos necesarios para cumplir con sus responsabilidades laborales específicas. Esto reducirá la superficie de ataque y mitigará los riesgos asociados con accesos innecesarios a datos sensibles.
- **Monitorear y Auditar Accesos**: Establecer procedimientos para monitorear y auditar regularmente los accesos a sistemas e información confidencial. Esto permitirá detectar y responder rápidamente a actividades sospechosas o no autorizadas, fortaleciendo la seguridad de la información y cumpliendo con los requisitos de auditoría.
- **Capacitar y Sensibilizar al Personal:** Proporcionar capacitación continua al personal sobre las políticas y procedimientos de control de acceso, así como sobre las mejores prácticas de seguridad de la información. Promover una cultura de seguridad donde todos los empleados comprendan la importancia de proteger la información de la organización.
- **Revisar y Mejorar Continuamente los Controles:** Establecer un proceso de revisión periódica de los controles de acceso para evaluar su efectividad y realizar mejoras según sea necesario. Esto asegurará que CKS esté alineado con las últimas amenazas de seguridad y regulaciones, garantizando así la protección continua de la información crítica.

3. Alcance

Esta política de control de acceso se extiende a todos los empleados, contratistas, consultores y terceros que requieran acceso a los sistemas de información de Consulting, Knowledge & Systems (CKS) para desempeñar sus funciones laborales o brindar servicios a la organización. Esto incluye, pero no se limita a, personal interno de todas las áreas funcionales como ventas, gestión general, proyectos, recursos humanos y contabilidad. Además, abarca a contratistas y consultores externos que trabajan en proyectos específicos o brindan servicios temporales a CKS, así como a terceros proveedores de servicios que requieran acceso para cumplir con acuerdos contractuales. Todos los individuos cubiertos por esta política deben cumplir con los controles de acceso establecidos, seguir los procedimientos definidos para la gestión de privilegios y participar en la capacitación continua en seguridad de la información proporcionada por la empresa. La aplicación de esta política es fundamental para asegurar que solo aquellos con autorización adecuada tengan acceso a los activos de información críticos de CKS, minimizando así el riesgo de acceso no autorizado o mal uso de datos sensibles.

4. **Políticas de de control de acceso**

   a. **Gestión de accesos de usuario**

   - **Asignación de derechos de acceso**

     Los derechos de acceso serán asignados de acuerdo con las necesidades específicas de cada puesto dentro de Consulting, Knowledge & Systems (CKS). Esto implica que cada empleado, contratista o consultor recibirá accesos solo a los sistemas y datos requeridos para el cumplimiento efectivo de sus responsabilidades laborales. Los privilegios de acceso deberán ser revisados regularmente para garantizar que sigan siendo apropiados y necesarios según la evolución de las funciones y responsabilidades de cada individuo.

   - **Creación y eliminación de cuentas**

     Todas las cuentas de usuario deben ser solicitadas y aprobadas por el gerente de TI o la autoridad designada antes de su creación. Además, se establecerán procedimientos claros para la eliminación inmediata de cuentas al finalizar el contrato laboral o cuando no sean necesarias. Esto asegura que el acceso a los sistemas de CKS esté limitado únicamente a individuos autorizados y activos.

   - **Autenticación**

     Todos los usuarios de CKS deben autenticarse utilizando credenciales únicas y seguras. Se fomentará el uso de autenticación multifactor (MFA) siempre que sea posible, para agregar una capa adicional de seguridad al proceso de inicio de sesión. Esto no solo protege contra el acceso no autorizado, sino que también fortalece la verificación de identidad de los usuarios antes de permitirles acceder a sistemas sensibles o datos críticos.

   b. **Control de acceso físico**

   - **Acceso a áreas sensibles:**

     El acceso físico a áreas críticas donde se encuentran ubicados los servidores y equipos de red estará estrictamente restringido a personal autorizado. Esto se logrará mediante el uso de medidas de seguridad física como cerraduras electrónicas, tarjetas de acceso y sistemas de videovigilancia. Solo aquellos con una necesidad específica y autorización explícita podrán ingresar a estas áreas para mantener la integridad operativa de los sistemas de información de CKS.

   - **Registros de accesos:**

     Se mantendrán registros detallados de acceso físico a todas las áreas sensibles y críticas. Estos registros serán revisados regularmente como parte de las actividades de monitoreo y auditoría, garantizando así que cualquier acceso no

autorizado o inusual sea identificado y respondido de manera oportuna y adecuada.

c. Control de acceso a redes y sistemas

- **Acceso a la red:**

  Solo dispositivos autorizados y registrados podrán conectarse a la red corporativa de CKS. Se implementarán medidas de control de acceso robustas para asegurar que cada dispositivo cumpla con los requisitos de seguridad establecidos antes de permitir el acceso a la red. Además, el acceso remoto a los sistemas corporativos estará sujeto a procedimientos estrictos de autenticación y protección para mitigar los riesgos asociados con conexiones externas.

- **Segregación de redes:**

  Las redes internas de CKS serán segmentadas de manera efectiva para minimizar el riesgo de accesos no autorizados entre diferentes áreas de la infraestructura de red. Esta segregación no solo protege la integridad de los datos y sistemas críticos, sino que también limita la propagación potencial de amenazas internas. Cada segmento de red estará diseñado para operar de manera independiente, con controles adecuados de firewall y políticas de acceso que refuercen la seguridad general de la infraestructura de TI de CKS.

5. Cumplimiento y sanciones

El incumplimiento de las políticas de control de acceso puede resultar en acciones disciplinarias, incluyendo la terminación del contrato laboral.