Informe de controles de acceso

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 informe detalla los controles de acceso propuestos para los cinco departamentos de Consulting, Knowledge & Systems (CKS), alineados con los requisitos de la norma ISO 27001 sobre seguridad de la información. El objetivo principal es asegurar la confidencialidad, integridad y disponibilidad de los activos críticos de información de la empresa, implementando políticas y procedimientos adecuados de control de acceso. Se propone un enfoque estructurado que incluye evaluación de riesgos, selección de controles, implementación, operación, y monitoreo continuo para garantizar la efectividad y adecuación de los controles de acceso en cada departamento.

2. Objetivos

- **Proteger la confidencialidad de la información:** Garantizar que solo las personas autorizadas dentro de cada departamento tengan acceso a la información confidencial de CKS. Esto se logrará mediante la implementación de controles de acceso físicos y lógicos robustos que restrinjan el acceso no autorizado a los sistemas y datos sensibles.
- **Preservar la integridad de los datos**: Asegurar que los datos críticos no sean modificados, alterados o destruidos de manera no autorizada. Esto implica establecer mecanismos de control que eviten cambios no autorizados en los sistemas y datos, así como la implementación de registros de auditoría para rastrear cualquier actividad sospechosa.
- **Garantizar la disponibilidad de los sistemas y datos**: Asegurar que los sistemas y datos estén disponibles y accesibles cuando sea necesario para las operaciones comerciales. Esto incluye la implementación de medidas de seguridad que mitiguen los riesgos de interrupciones o pérdidas de servicio debido a incidentes de seguridad o fallas técnicas.
- **Cumplir con los requisitos legales y contractuales:** Asegurar que los controles de acceso implementados cumplan con todas las leyes, regulaciones y acuerdos

contractuales relevantes. Esto incluye normativas específicas de protección de datos y cualquier requisito contractual establecido por clientes o socios comerciales de CKS.

- **Promover una cultura de seguridad informática**: Fomentar la conciencia y la responsabilidad entre los empleados de CKS en relación con las mejores prácticas de seguridad informática. Esto se logrará mediante la capacitación regular, la sensibilización sobre los riesgos de seguridad y la promoción de políticas internas que refuercen la importancia de la protección de la información.

3. Alcance

Las medidas de control de acceso según la norma ISO 27001 se aplicarán de manera integral a todos los activos de información crítica de la empresa CKS, abarcando específicamente los siguientes elementos dentro de cada uno de sus cinco departamentos:

Departamento de Ventas:

- **Sistemas Informáticos:** Incluyendo estaciones de trabajo y dispositivos móviles utilizados por el personal de ventas para la gestión de clientes, propuestas comerciales y comunicaciones.
- **Datos Electrónicos:** Información relacionada con prospectos, clientes actuales, historiales de ventas y reportes financieros generados por el departamento de ventas.
- **Redes:** Configuraciones de red que facilitan la comunicación segura con clientes y socios comerciales, incluyendo acceso a bases de datos de clientes y CRM.

Gerencia General:

- **Sistemas Informáticos:** Incluyendo acceso a sistemas de gestión empresarial (ERP), reportes ejecutivos y sistemas de comunicación interna.
- **Datos Electrónicos**: Información estratégica y de planificación, incluyendo presupuestos, estrategias corporativas y análisis de mercado.
- **Redes**: Acceso a redes corporativas seguras que facilitan la comunicación y la toma de decisiones estratégicas.

Departamento de Proyectos:

- **Sistemas Informáticos:** Incluyendo herramientas de gestión de proyectos, documentos técnicos y software de diseño utilizado para la ejecución de proyectos.
- **Datos Electrónicos:** Información relacionada con especificaciones de proyectos, cronogramas, presupuestos y comunicaciones internas y externas.
- **Redes:** Configuraciones de red que permiten la colaboración segura con clientes, contratistas y proveedores durante la ejecución de proyectos.

Departamento de Recursos Humanos:

- **Sistemas Informáticos:** Incluyendo sistemas de gestión de recursos humanos, bases de datos de empleados y sistemas de nómina.
- **Datos Electrónicos:** Información personal y confidencial de empleados, políticas de recursos humanos y registros de capacitación y desarrollo.
- **Redes**: Acceso seguro a redes internas que gestionan la comunicación y las operaciones del departamento de recursos humanos.

Departamento de Contabilidad:

- **Sistemas Informáticos:** Incluyendo sistemas contables, software de gestión financiera y sistemas de control presupuestario.
- **Datos Electrónicos:** Información financiera confidencial, registros contables, auditorías internas y reportes financieros.
- **Redes:** Configuraciones de red que permiten el acceso seguro a sistemas bancarios en línea, intercambio de archivos financieros y comunicaciones con auditores externos.

4. Controles de acceso

a. **Autenticación Multifactor (MFA)**:

- **Objetivo:** Asegurar que el acceso a sistemas críticos y datos sensibles requiera más de una forma de autenticación para verificar la identidad del usuario.
- **Política:** Todos los empleados deben utilizar autenticación multifactor para acceder a sistemas que manejan información crítica. Esto incluye al menos dos de los siguientes factores: algo que el usuario sabe (contraseña), algo que el usuario posee (token o dispositivo físico) y algo que el usuario es (biometría).
- **Implementación:** Utilizar soluciones de autenticación multifactor compatibles con los sistemas existentes en CKS. Establecer procedimientos claros para registrar y gestionar los factores de autenticación.

b. Gestión de Contraseñas:

- **Objetivo**: Garantizar contraseñas seguras y su correcta gestión para proteger los sistemas y datos de accesos no autorizados.
- **Política:** Las contraseñas deben cumplir con estándares mínimos de complejidad, incluyendo longitud, combinación de caracteres (mayúsculas, minúsculas, números y caracteres especiales).
    - Las contraseñas deben ser rotadas periódicamente según la política de seguridad establecida.
    - Queda prohibido el uso de contraseñas compartidas o fácilmente deducibles (como nombres, fechas de nacimiento, etc.).
- **Implementación:** Utilizar herramientas de gestión de contraseñas si es necesario para asegurar el cumplimiento de las políticas. Educar a los empleados sobre la importancia de una buena gestión de contraseñas y proporcionar capacitación regular.

c. Control de Acceso a Redes y Equipos:

- **Objetivo**: Proteger la infraestructura de red de CKS contra accesos no autorizados y asegurar su funcionamiento seguro y eficiente.
- **Política**:
    - Configurar firewalls, routers y switches según las mejores prácticas de seguridad y las necesidades específicas de CKS.
    - Realizar auditorías periódicas de configuraciones de red para identificar y corregir posibles vulnerabilidades.

- Implementar procedimientos para la gestión de parches y actualizaciones de seguridad en equipos de red.

d. Control de Acceso Físico:

- **Objetivo**: Restringir el acceso físico a instalaciones y áreas críticas de CKS para prevenir intrusiones y proteger los activos físicos.
- **Política:**
  - Utilizar sistemas de control de acceso físico como tarjetas de proximidad o biometría para limitar la entrada a áreas sensibles.
  - Mantener registros de acceso físico y realizar revisiones regulares para asegurar que solo personal autorizado tenga acceso.
- **Implementación:** Implementar controles de acceso físico adecuados según las instalaciones y recursos disponibles. Educar al personal sobre la importancia de mantener la seguridad física y reportar cualquier incidente de acceso no autorizado.

e. Control de Acceso a la Información:

- **Objetivo**: Proteger la información confidencial y crítica de CKS mediante políticas y procedimientos que regulen quién puede acceder y cómo se accede a la información.
- **Política:**
  - Definir roles y permisos de acceso basados en el principio de privilegios mínimos, limitando el acceso solo a la información necesaria para realizar las funciones laborales.
  - Encriptar datos sensibles durante su almacenamiento y transmisión para protegerlos contra accesos no autorizados.
- **Implementación:** Implementar soluciones de cifrado adecuadas para los sistemas de información críticos. Establecer procedimientos para la revisión y actualización de permisos de acceso de manera regular.