FACTORES AMBIENTALES

Los factores ambientales de la empresa Consulting, Knowledge & Systems (Cks) pueden ampliar o limitar las opciones de gestión de proyectos, teniendo un impacto tanto positivo como negativo en los resultados.

Entre sus factores ambientales de la empresa, se incluyen:

1. **Regulaciones y Normativas:**

- Norma Técnica Peruana ISO/IEC 27001
  - Gestión de Seguridad de la Información: Esta norma nacional adopta el estándar internacional ISO/IEC 27001 sobre gestión de seguridad de la información. Algunos aspectos importantes de esta norma son:

  - Identificación de riesgos de seguridad de la información: La norma establece procesos para identificar y evaluar los riesgos de seguridad de la información que pueden afectar a la organización.

  - Implementación de controles de seguridad: Se define la implementación de controles de seguridad de la información para mitigar los riesgos identificados y proteger la confidencialidad, integridad y disponibilidad de la información.

  - Auditorías y revisiones periódicas: La norma requiere la realización de auditorías y revisiones periódicas para garantizar la efectividad del sistema de gestión de seguridad de la información.

- Ley N° 29733- Ley de Protección de Datos Personales

  Esta ley es relevante para el proyecto de fortalecimiento de la seguridad de la información en CKS, ya que establece disposiciones importantes para el tratamiento adecuado de los datos personales y la seguridad de la información.

2. **Cultura Organizacional:**

   En CKS brinda los servicios de: Switching, Redes Inalámbricas y Videovigilancia y Cableado Estructurado De Cobre Y Enlaces De Fibra Óptica, además la empresa cuenta con cuatro áreas principales que abarcan distintos aspectos de sus operaciones: el Departamento de Recursos Humanos, encargado de gestionar talento humano y promover un ambiente laboral positivo; el Departamento de Contabilidad y Finanzas, responsable de administrar recursos financieros y garantizar la salud financiera de la empresa; el Departamento de Ventas, dedicado a impulsar el crecimiento del negocio mediante la adquisición y retención de clientes; y finalmente, el Departamento de Proyectos, encargado de llevar a cabo la planificación y ejecución de iniciativas clave para el éxito de la empresa.

La comunicación actualmente se da de forma directa, en persona, es fundamental para fomentar la colaboración y el trabajo en equipo entre los empleados durante la jornada laboral, la cual se extiende de lunes a sábado. Valores como la puntualidad y el respeto son pilares fundamentales que guían nuestras acciones y relaciones en el día a día, reflejando nuestro compromiso con la excelencia y el profesionalismo en todas nuestras interacciones.

3. **Visión**

   Ser líderes en el mercado nacional de soluciones tecnológicas, ofreciendo innovación constante y garantizando la excelencia en nuestros servicios para impulsar el crecimiento sostenible de nuestros clientes.

4. **Misión**

   Proporcionar soluciones tecnológicas integrales de alta calidad y última generación a empresas de todos los tamaños en el Perú, asegurando la satisfacción del cliente, la protección de su inversión y el desarrollo de relaciones a largo plazo basadas en la confianza y el compromiso.

5. **Evolución del Entorno Cibernético:**

   Actualmente tenemos cada vez más presente el entorno cibernético en constante evolución, y para CKS, la seguridad de la información es de suma importancia. La creciente sofisticación de las amenazas cibernéticas y el rápido avance de las tecnologías digitales destacan la necesidad de abordar de manera proactiva nuestros sistemas de seguridad.

   Esto implica una atención constante a la actualización de políticas, la capacitación del personal y la implementación de medidas de seguridad física y de red para proteger nuestros activos críticos y mantener la integridad de nuestros sistemas.

6. **Impacto Económico:**

   Para CKS la asignación de recursos financieros para la implementación de medidas de seguridad, incluyendo la adquisición de tecnología y la capacitación del personal es importante y tiene cierta prioridad, debido a que es el cuidado de la información que tienen.

   Además se puede considerar el retorno de la inversión a largo plazo, donde la mitigación de riesgos cibernéticos evitará en este mundo actual los costosos incidentes de seguridad que afecten la continuidad del negocio y la reputación de la empresa.

7. **Riesgos Ambientales:**
   - **Fallo de Energía Eléctrica:** Interrupciones repentinas en el suministro eléctrico podrían afectar la operación de sistemas de seguridad física, como cámaras de vigilancia o sistemas de alarma, comprometiendo la protección de los activos de información.
   - **Desastres Naturales:** Eventos como inundaciones, incendios o terremotos podrían dañar la infraestructura física, incluidos los dispositivos de seguridad, y afectar la capacidad de respuesta ante incidentes de seguridad.
   - **Acceso No Autorizado:** La falta de controles de acceso físico adecuados podría permitir que personas no autorizadas ingresen a áreas críticas de la empresa, comprometiendo la seguridad de los activos de información y la efectividad de las medidas de seguridad física.

- **Despliegue Inadecuado de Medidas de Seguridad:** Errores en la instalación o configuración de sistemas de seguridad física podrían resultar en vulnerabilidades que podrían ser explotadas por intrusos, comprometiendo la seguridad de la información.
- **Errores Humanos:** La falta de capacitación adecuada del personal en procedimientos de seguridad física y en el manejo de equipos de seguridad podría dar lugar a errores que comprometen la efectividad de las medidas de seguridad implementadas.
- **Insuficiente Mantenimiento de Equipos de Seguridad:** La falta de mantenimiento regular de equipos de seguridad física, como cerraduras, sistemas de alarma o cámaras de vigilancia, podría reducir su efectividad y aumentar el riesgo de incidentes de seguridad.

8. Gestión de Activos

a. Gestión del Conocimiento y la Información:

Sistemas de Gestión del Conocimiento: Implementar un sistema formal para la gestión del conocimiento puede mejorar la eficiencia y la capacidad de innovación. Esto incluye la documentación de procesos, la creación de repositorios de conocimientos accesibles y la promoción del intercambio de conocimientos entre empleados.

Seguridad de la Información: Dado que actualmente no existen medidas formales de seguridad de la información, es crucial desarrollar e implementar políticas y procedimientos para proteger la información crítica. Esto incluye controles de acceso, cifrado de datos, y la realización de auditorías regulares.

b. Capital Humano:

Desarrollo de Talento: Invertir en la formación y desarrollo de los empleados puede aumentar la competencia y adaptabilidad de la empresa. Ofrecer programas de capacitación continua y oportunidades de desarrollo profesional es clave para retener talento y fomentar la innovación.

Cultura Organizacional: Fomentar una cultura organizacional que valore la innovación, la colaboración y la mejora continua puede tener un impacto positivo en la moral y el desempeño de los empleados.

c. Activos Físicos:

Garantizar que la infraestructura física, como oficinas y centros de datos, esté bien mantenida y protegida contra riesgos físicos (incendios, inundaciones, robos). Implementar medidas de seguridad física adecuadas, como sistemas de vigilancia y control de acceso.