Política de Seguridad de la Información de Alpek

1. PROPÓSITO

1.1. Proveer lineamientos de seguridad sobre la información, ya sea de ALPEK o de terceros bajo su custodia, en la infraestructura donde se ubique, con el propósito de implementar controles que ayuden a minimizar cualquier riesgo que pueda poner en peligro la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

2.1. Esta política es aplicable a:

- Alpek, sus subsidiarias y organizaciones bajo su control, en todos los países donde tenga operaciones.
- Todo empleado, ejecutivo, director o miembro del consejo de la empresa, sin importar niveles jerárquicos o funciones.

3. RESPONSABILIDADES

3.1. Empleados de ALPEK / Individuos con cualquier relación con ALPEK:

- Realizar sus actividades diarias en cumplimiento con lo dispuesto en este documento.

3.2. Empresas de ALPEK:

- Asegurar que todo lo aquí dispuesto se aplique.

3.3. Auditoría Interna de ALFA:

- Verificar que todo lo aquí dispuesto se aplique.

3.4. Comité Ejecutivo de Seguridad de la Información:

- Validar y proponer Políticas y Lineamientos de Seguridad de la Información.
- Promover en todas las áreas de ALPEK y sus Empresas la necesidad e importancia de la Seguridad de la Información.
- Asegurar que se implemente el programa de Seguridad de la Información en ALPEK.

3.5. Comité Táctico de Seguridad de la Información:

- Definir y documentar políticas, lineamientos y estándares de Seguridad de la Información.
- Mantenerse actualizado sobre amenazas de Seguridad de la Información que puedan impactar a la organización, así como sobre leyes y regulaciones externas aplicables.
- Investigar, evaluar y proponer proyectos y tecnologías para mantener actualizadas las prácticas de Seguridad de la Información de ALPEK.

3.6. Comité de Seguridad de la Información de la Empresa:

- Promover la implementación de metodologías, estándares y lineamientos aplicables a las funciones de este Comité. Promover la cultura de Seguridad de la Información en su Empresa.

4. LINEAMIENTOS Y PROCEDIMIENTOS

4.1. Definiciones

4.1.1. Confidencialidad

- Característica que garantiza que la información solo se proporcione a individuos autorizados.

4.1.2. Control

- Políticas, procedimientos, prácticas, tecnologías y estructuras organizacionales diseñadas para lograr objetivos de negocio y prevenir, detectar y corregir eventos no deseados.

4.1.3. Infraestructura de TI

- Hardware o software utilizado para almacenar, procesar o transmitir información.

4.1.4. Lineamiento

- Medida de seguridad que debe implementarse.

4.1.5. Operación Segura

- Operación libre de incidentes de seguridad o interrupciones que puedan poner en peligro la confidencialidad, disponibilidad e integridad de la información.

4.1.6. Bienes en custodia

- Característica que garantiza que la información solo se proporcione a individuos autorizados. Bienes bajo la custodia de ALPEK pero que no son de su propiedad.

4.1.7. Seguridad de la Información

- Medidas, procedimientos y controles destinados a preservar la confidencialidad, integridad y disponibilidad de la información de acuerdo con los requerimientos de la Empresa.

4.1.8. Sistemas de TI

- Software de propósito específico que apoya parcial o totalmente los procesos de negocio de las Empresas.

4.1.9. Software Malicioso

- Código informático introducido intencionalmente en un sistema para propósitos no autorizados.

4.1.10. Incidente

- Evento no planificado que impacta la operación de una Empresa.

4.2. Lineamientos

- Es política de ALPEK que todas sus Empresas implementen las medidas adecuadas para mantener la seguridad mientras la información es gestionada y controlada, para protegerla contra el uso indebido, modificación y destrucción no autorizada, y para garantizar su confidencialidad, integridad y disponibilidad.

ALPEK y sus subsidiarias deberán cumplir con los siguientes Lineamientos de Seguridad:

4.2.1. Organización de la Seguridad

- ALPEK ha definido un Comité Ejecutivo de Seguridad de la Información para coordinar todos los esfuerzos relacionados con la definición y mantenimiento de esta Política y sus Lineamientos. Asimismo, cada Subsidiaria deberá tener roles claramente definidos y asignados dentro de su organización para gestionar la seguridad de la información conforme a lo aquí dispuesto.

4.2.2. Clasificación de la Información

- Cada Empresa de ALPEK deberá clasificar su información con base en su sensibilidad, criticidad y valor para regular su uso, resguardo y destrucción.

4.2.3. Control de Infraestructura de TI

- Cada Empresa de ALPEK deberá implementar un proceso para gestionar los activos de infraestructura de TI a fin de mantener el control sobre su ubicación y definir las medidas de protección adecuadas.

4.2.4. Gestión del Personal

- Cada Empresa de ALPEK deberá implementar controles de Seguridad de la Información en los procesos de Selección, Reclutamiento y Gestión de Recursos Humanos para asegurar que esta Política sea conocida y observada por todo el personal, ya sea interno, subcontratado o externo que preste servicios a ALPEK.

4.2.5. Seguridad Física

- Cada Empresa de ALPEK deberá implementar controles para establecer y mantener una operación segura de su infraestructura de TI con el propósito de prevenir la pérdida o el robo de información.

4.2.6. Gestión de Sistemas y Redes de TI

- Cada Empresa de ALPEK deberá tener procesos y controles para asegurar que la información esté protegida mientras la infraestructura de TI está en operación, garantizando la confidencialidad, disponibilidad e integridad.

4.2.7. Control de Acceso Lógico

- Cada Empresa de ALPEK deberá implementar controles de protección para asegurar que la infraestructura de TI y la información sean accedidas únicamente por personal autorizado y conforme a los lineamientos definidos para tal propósito.

4.2.8. Desarrollo y Mantenimiento de Sistemas

- Cada Empresa de ALPEK deberá implementar controles de seguridad durante el desarrollo, despliegue, procesamiento y mantenimiento de sistemas de TI en uso para proteger la propiedad intelectual de ALPEK y garantizar la integridad, confidencialidad y disponibilidad de la información.

4.2.9. Continuidad del Negocio

- Cada Empresa de ALPEK deberá implementar programas de Continuidad del Negocio para los activos de información que soportan procesos críticos que puedan afectar las operaciones si se interrumpen debido a causas de fuerza mayor, causas naturales o acciones de individuos.

4.2.10. Cumplimiento de Leyes y Regulaciones

- Cada Empresa de ALPEK deberá cumplir con los requisitos de seguridad establecidos por las leyes y/o regulaciones contractuales de los países donde opera, implementando los controles necesarios en el diseño, operación y uso de su infraestructura de TI y sistemas de información.

4.2.11. Gestión de Incidentes de Seguridad de la Información

- Cada Empresa de ALPEK deberá asegurar que la gestión de incidentes esté organizada y sea efectiva para habilitar una comunicación que permita la detección y corrección oportuna de incidentes.

4.2.12. Gestión de Proveedores

- Cada Empresa de ALFA deberá garantizar que la información y la infraestructura de TI estén protegidas cuando se establezcan relaciones comerciales con proveedores de servicios.

Cada Empresa de ALPEK es responsable de implementar un proceso de Gestión de Riesgos de Seguridad de la Información orientado a la infraestructura de TI y su operación de acuerdo con esta Política.

Cada Empresa de ALPEK deberá realizar revisiones periódicas para asegurar el cumplimiento de esta Política. En caso de detectarse fallas, deberán implementarse planes de acción correctiva.

Premisa general: Todas las subsidiarias de Alpek deben alinearse con el marco normativo establecido en las Políticas de Alpek. Las políticas de cada subsidiaria pueden tener condiciones distintas, pero nunca menos restrictivas que el marco establecido por la Política de Alpek.

Aprobaciones

Nombre	Puesto	Fecha de Autorzación
José Armando Ramos Cantú	Vicepresidente de Capital Humano	26 de febrero de 2021
José Carlos Pons de la Garza	Director Financiero	26 de febrero de 2021
José de Jesús Valdez Simancas	Director General	26 de febrero de 2021