POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Índice

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1 Introducción

La Política de seguridad de la información es un componente fundamental de la Política Empresarial del Grupo PLANASA. Se trata de un elemento indispensable en el sistema de gestión del Grupo y, como tal, constituye una directriz importante para la adopción y mejora continua de los procesos empresariales del Grupo en la competencia internacional.

La Política de seguridad de la información del Grupo PLANASA aúna políticas y buenas prácticas en este ámbito de responsabilidad con la política de seguridad de la información y buenas prácticas que se definen en la sede del Grupo PLANASA en Valtierra (España).

Estos procesos empresariales dependen cada vez más de la información y de los sistemas de la información. La seguridad de la información y de los sistemas de información es mucho más que la protección de la infraestructura técnica, se extiende a la administración y control de nuestro flujo de información. Esto hace que sea necesario que todos los trabajadores sean conscientes de la importancia de la seguridad de la información como parte de los procesos empresariales, la adopción de infraestructuras y el desarrollo e instalación de sistemas de información.

Esta Política sirve como base para el desarrollo de las normativas correspondientes en materia de seguridad de la información. Por ende, estas normativas se aplican a todos los empleados para garantizar una comprensión firme y clara de las responsabilidades relativas a la seguridad de la información y sirven como guía para la gestión segura de la información del Grupo.

Mediante esta Política de seguridad de la información, el Consejo de PLANASA obliga a los directivos y al personal a utilizar las normativas que se definen y apoyar de forma activa el desarrollo continuo de la seguridad de la información.

El Consejo de PLANASA aprueba las normativas a partir de esta Política de seguridad de la información. Todas las instrucciones que se dicten respecto de la gestión de la seguridad de la información serán, por ende, vinculantes para todos los departamentos y trabajadores.

2 Objetivo

En la Política de seguridad de la información que se describe en ese documento se definen los objetivos, estrategias y responsabilidades básicas para garantizar la seguridad de la información en el Grupo PLANASA.

Esta política está diseñada para establecer un punto de partica común y un marco para el desarrollo progresivo de los procedimientos necesarios, teniendo en cuenta las necesidades específicas en lo que respecta a la seguridad de la información.

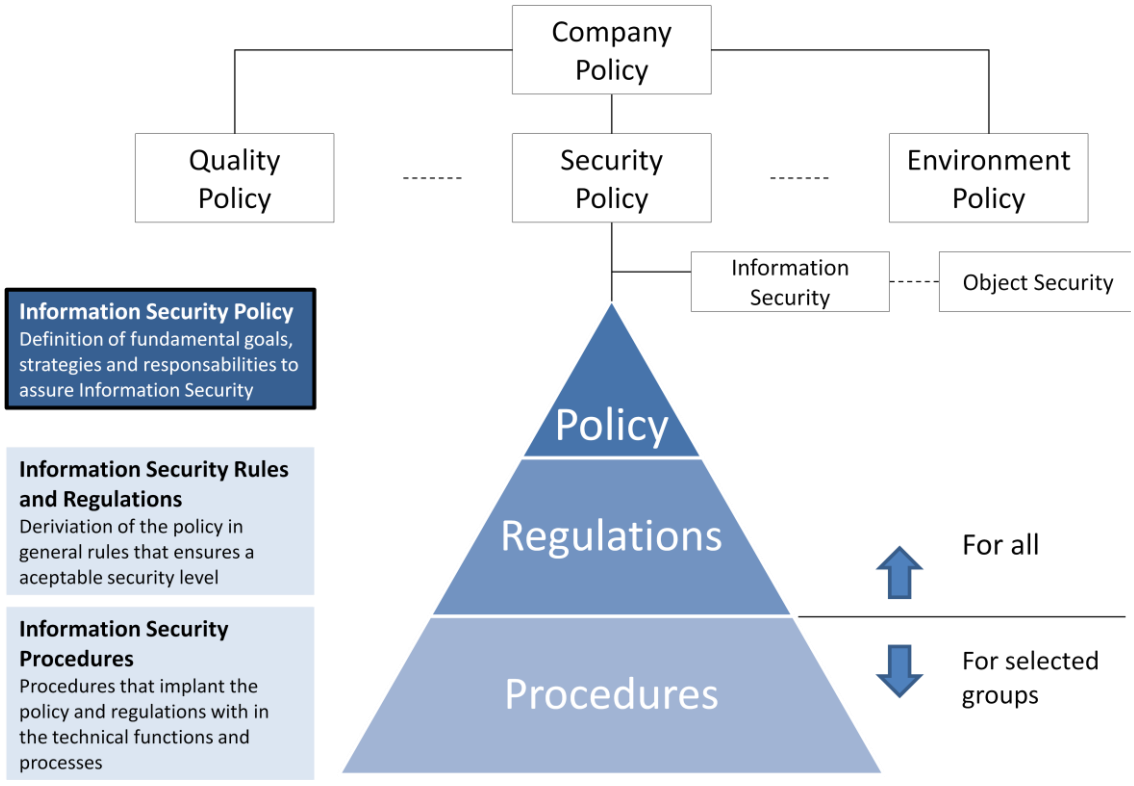
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las necesidades específicas de la Compañía pueden deberse a factores tales como la estructura organizativa, los procesos empresariales, los sistemas de información e, incluso, la ubicación geográfica.

La Política de seguridad de la información se basa en estándares y normativas y su objetivo final es su adopción en todas las empresas que componen el Grupo PLANASA.

3 Contexto

A continuación se muestra cómo debe integrarse la Política de seguridad de la información en las distintas Políticas de la empresa (para servir como modelo):



Las normativas de seguridad de la información complementan a las normativas actuales y relevantes (tales como las condiciones de contratación, Ley de protección de datos local).

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4 Ámbito de aplicación

La Política de seguridad de la información y todas las normativas relacionadas se aplican a todas las empresas que componen el Grupo PLANASA.

5 Seguridad de la información en el Grupo PLANASA

El éxito de la empresa se ve influenciado en gran medida por la experiencia y el saber hacer de sus trabajadores. Las pérdidas de datos no controladas o la manipulación de datos, conocimiento e información (a las que se hará referencia en lo sucesivo como «información») pueden poner en peligro el éxito de la compañía.

La información y la infraestructura disponibles para el tratamiento de datos y para la comunicación son activos sociales valiosos que deben protegerse. En consecuencia, todos los trabajadores tienen la obligación personal de proteger la información y los recursos de comunicación frente a cualquier tipo de pérdida, falsificación o fraude y de manipular las herramientas con el cuidado necesario.

Cumplir con la Política de seguridad de la información constituye una medida importante para garantizar y mejorar la posición del Grupo en el mercado. La adopción continuada de la Política de seguridad de la información en los procesos empresariales mejora la imagen positiva en el mercado y garantiza la confianza en nuestros productos y servicios.

Para poder ser más competitivos, resulta esencial comprender el potencial de utilizar tecnologías de la información modernas. Para ello es necesario adoptar medidas que protejan la confidencialidad, integridad y disponibilidad de la información durante la planificación, desarrollo y adquisición de infraestructura y sistemas de información, así como en el transcurso de las operaciones cotidianas.

Es necesario cumplir con los siguientes principios:

- **Confidencialidad:** aquella información que no esté destinada específicamente para su divulgación pública únicamente deberá estar disponible para las personas autorizadas.
- **Integridad:** debe garantizarse un tratamiento de la información sin errores, así como su protección frente a modificaciones no autorizadas.
- **Disponibilidad:** los activos de información deberán facilitarse dentro de un periodo de tiempo acordado.
- **Responsabilidad:** el acceso a la información que merezca ser protegida y que se utilice en operaciones debe ser innegable.

Para garantizar los principios anteriores deberán adoptarse las siguientes medidas de seguridad:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- **Autentificación:** debe garantizarse la autentificación única para acceder a la información.
- **Autorización:** únicamente deberá concederse acceso a la información a personas autorizadas y deberá limitarse al alcance necesario para el trabajo.
- **Auditoría:** el acceso a la información que merezca la pena proteger debe estar registrado y controlado.

Es necesario revisar de manera periódica los requisitos de seguridad de la información con respecto de los cambios en los requisitos empresariales. Los métodos y herramientas deberán someterse a análisis y auditorías frecuentes para detectar nuevos riesgos y requisitos de seguridad.

6 Responsabilidades

La seguridad de la información se ve afectada en gran medida por el comportamiento responsable de los directivos y empleados, así como de los gestores de los sistemas de información.

Las bases para la adopción de procedimientos de seguridad de la información y el cumplimiento de los principios de seguridad de la información se fundamentan en una concienciación adecuada en lo que respecta a la seguridad por parte de los trabajadores internos y externos. Por ende, deberán tomarse las medidas de información y formación correspondientes, puesto que Planasa considera que los riesgos en materia de tecnologías de la información se relacionan con una falta de conocimiento o uso inapropiado.

El Consejo de PLANASA fomenta de manera activa la seguridad de la información en todas las empresas que forman parte del Grupo, promoviendo acciones para mejorar la seguridad de la información. Además, el Consejo de PLANASA se compromete a:

- Facilitar directrices claras y apoyo visible a las iniciativas de seguridad de la información.
- Fomentar la adopción de medidas relativas a la seguridad de la información.
- Facilitar los recursos necesarios para garantizar el nivel adecuado de seguridad de la información.
- Aprobar el nombramiento de cargos y responsabilidades específicos para velar por la seguridad de la información en el conjunto de la Organización.
- Impulsar planes y programas relativos a la concienciación en materia de seguridad de la información.
- Garantizar el cumplimiento de las normativas existentes en este ámbito de responsabilidad.
- Designar al Departamento de Sistemas de la Información para dirigir la adopción de esta Política en el Grupo PLANASA.

El Grupo PLANASA dispondrá de un **Comité de Seguridad de la Información** liderado por el Departamento de Sistemas que tendrá como objetivos principales:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Desarrollar y mantener la Normativa de Seguridad de la Información del Grupo PLANASA.
- Proponer, fomentar y coordinar, a nivel de Grupo, todos los proyectos relativos a la seguridad de la información.
- Garantizar el cumplimiento de las políticas y directrices en materia de seguridad de la información para definir Planes de Gestión de Seguridad y Planes de Recuperación tras Desastres para los sistemas de información.
- Dirigir y coordinar el desarrollo y adopción de los procedimientos operativos necesarios en cuestión de seguridad de la información.
- Dirigir y coordinar la gestión del conocimiento en el Grupo PLANASA, trabajando en conjunto con los cargos superiores y los expertos los ámbitos relacionados con la seguridad de la información.
- Coordinar acciones para mejorar la seguridad con el responsable para el cumplimiento de la ley local de protección de datos.
- Este comité estará compuesto por los siguientes miembros:
    - Director de Tecnologías de la Información (presidente)
    - Director financiero
    - Los miembros del Departamento de Tecnologías de la Información que resulten necesarios
    - Director de Recursos Humanos
    - Director de Cumplimiento normativo

Cualquier persona a nivel interno o externo (trabajadores del Grupo PLANASA o personal externo) que utilice la información y los sistemas de información necesarios debe prestar la atención necesaria y cumplir con la Política de Seguridad de la información del Grupo PLANASA. Sus responsabilidades principales son:

- Utilizar los sistemas de la información únicamente para realizar tareas autorizadas en cumplimiento con la legislación y la regulación.
- Proteger la información a lo largo de su ciclo de vida desde la creación o recepción mediante el procesamiento, comunicación, transporte, almacenamiento, notificación a terceros o posible destrucción.
- Proteger cualquier tipo de información, informatizada o no, de forma acorde con las normativas de seguridad.
- Proteger la información frente accesos no autorizados, publicación indebida o pérdida.
- Conocer los requisitos legales y normativos de la Organización.
- Cualquier incumplimiento de las normativas de seguridad de la información deberá comunicarse de manera adecuada cuando se detecte.

Aprobación

Elaborado por:	Aprobado por:	Fecha de aprobación:
Director global de Sistemas de la Información	**Junta directiva del Grupo Planasa**	**Febrero de 2020**