Política de Seguridad

La Dirección de **SISTEMAS DE MISILES DE ESPAÑA, S.L.,** en su voluntad de garantizar la prestación de servicios y de ofrecer a sus clientes unos productos con mejor calidad cada día en el desarrollo de sus actividades, ha establecido la presente Política de Seguridad, apoyada en su Dirección Estratégica y basada en los siguientes puntos clave:

Objeto

SISTEMAS DE MISILES DE ESPAÑA, S.L. (en adelante "**SMS**" o la "**empresa**") desarrolla la presente ***Política de Seguridad*** (en adelante, la "**Política**") con el propósito de establecer directrices y procedimientos para proteger la confidencialidad, integridad y disponibilidad de la información (clasificada y sensible) de la empresa y de terceros, de los servicios que presta, de sus instalaciones, así como de los sistemas informáticos y recursos asociados (software y hardware), contra cualquier amenaza interna o externa que pueda comprometer su seguridad o provocar pérdidas o daños, no solo a **SMS** sino también a sus clientes y proveedores.

Esta Política es aplicable a todos los activos de información de la empresa, a sus infraestructuras y a todas las personas que interactúen con ellos. La Dirección de la empresa es responsable de aprobar y respaldar las medidas de seguridad de la información y se compromete a asignar recursos y promover una cultura de seguridad adecuada al ámbito del ejercicio y actuación de la empresa.

Para ello, se inician los procesos correspondientes a fin de obtener la certificación en la ISO 27001, cumplimentando asimismo los requisitos exigidos por el Esquema Nacional de Seguridad (ENS), que constituirán los marcos de referencia del desarrollo de **SMS** como compañía.

Ámbito de aplicación

Los destinatarios de la Política (en adelante, "**colaboradores**") son:

- Todos los empleados de **SMS**.
- Los proveedores, subcontratistas y clientes de **SMS**.
- Cualesquiera **terceros** que interactúen con los sistemas y datos de información de **SMS**, con independencia del área de negocio de que se trate, de su ubicación geográfica o de las actividades que desarrollen.

Principios generales de SMS

1.- Acceso y Control de Información

La empresa implementará medidas de control de acceso para garantizar que solo personal autorizado tenga acceso a la documentación (física y electrónica) relevante para el desarrollo de sus funciones laborales. Se establecerán políticas y procedimientos para la gestión adecuada de contraseñas, acceso remoto y compartición de información confidencial. El control de acceso alcanzará a todos los sistemas de la empresa y a todos los datos en función de la autorización que se conceda en cada momento.

Todos los empleados deben proteger sus credenciales de acceso y no compartir sus contraseñas con terceros.

2.- Protección de Datos y activos empresariales

La empresa se compromete a cumplir con todas las leyes y regulaciones de protección de datos aplicables y que se encuentren vigentes, tanto si la empresa es responsable como si es la encargada del tratamiento de los datos, así como a implementar las medidas técnicas y organizativas para proteger los datos personales de todos los colaboradores, realizándose copias de seguridad periódicas de los datos críticos y almacenándolas de forma segura.

Los empleados y demás colaboradores de SMS deberán cumplir con todas las obligaciones establecidas por la normativa vigente en materia de protección de datos.

La protección de la información alcanzará también a los demás activos empresariales, incluyendo, sin limitación, cualesquiera derechos de propiedad industrial e intelectual, patentes, marcas registradas, diseños industriales, derechos de autor, secretos empresariales, datos e información sensible, imagen corporativa, licencias y concesiones, acuerdos y contratos con socios, e información sujeta a restricciones internaciones (ITAR), tanto de la propia empresa como de sus proveedores y clientes.

3.- Seguridad Física

Los dispositivos, los sistemas críticos y la información clasificada se mantendrán en Zonas de Acceso Restringido (ZAR) y Zonas Administrativas de Protección (ZAP) en función de su grado de clasificación.

Existirá un protocolo de limpieza y destrucción segura de datos en dispositivos obsoletos conforme a la legislación vigente.

4.- Gestión de Riesgos

Se llevará a cabo una evaluación regular de riesgos de seguridad de la información para identificar y mitigar posibles amenazas y vulnerabilidades. Se establecerán controles de seguridad adecuados para proteger los activos de información crítica.

5.- Concienciación y Formación:

Con carácter regular se proporcionarán sesiones de formación sobre seguridad a todos los empleados de SMS. Estos deben ser conscientes de las amenazas de ingeniería social y deben desarrollar prácticas seguras en el desarrollo de su trabajo.

Se desarrollará en 3 niveles:

- Un primer nivel por medio de formación / charla individual cuando un empleado cause alta en la empresa.
- Un segundo nivel de formación y concienciación en el momento en el que se decida que el empleado debe contar con una Habilitación Personal de Seguridad.
- Un tercer nivel de formación continua a través de las circulares que el Departamento de Seguridad haga llegar a todos los empleados con carácter regular.

6.- Cumplimiento y Auditoría

Se llevarán a cabo auditorías internas regulares para garantizar el cumplimiento de esta Política y de los controles de seguridad establecidos, tomando medidas correctivas inmediatas para abordar cualquier incumplimiento o vulnerabilidad identificada.

El Coordinador de Protección de Datos y el *Compliance Officer* de la empresa supervisarán aquellas materias que sean de su competencia.

7.- Mejora Continua

La empresa se compromete a mejorar continuamente sus prácticas de seguridad de la información a través de la revisión regular de esta Política, la evaluación de riesgos y la implementación de medidas de seguridad adicionales según sea necesario.

8.- Política de uso de dispositivos

Los empleados que tengan dispositivos corporativos deben de usarlos de forma segura y no instalar software no autorizado por SMS.

Se implementarán controles de seguridad en dispositivos móviles que accedan a la red corporativa.

Incumplimiento

En caso de infracción de las obligaciones contenidas en esta Política, la Dirección de SMS podrá adoptar las medidas que procedan, tanto de carácter disciplinario frente a sus empleados en el ámbito laboral, como frente al resto de colaboradores, incluyendo la terminación de los respectivos contratos o el ejercicio de acciones legales, según corresponda. Estos procedimientos son complementarios con cualquier procedimiento judicial que pueda dirigirse frente al colaborador y con cualquier otra sanción o consecuencia que pueda derivarse de dicho procedimiento conforme a la normativa aplicable.

Actualización

Esta política se revisará anualmente para asegurar su relevancia y eficacia.

Entrada en vigor y difusión

La presente Política de Seguridad ha sido aprobada por el Director General de Sistemas de Misiles de España, S.L en fecha de 24/07/2024, a propuesta del Jefe de Seguridad del Servicio de Protección de **SMS**.

Entrará en vigor desde su publicación y estará disponible para todos los colaboradores.

En Madrid, a 24 de Julio de 2024

D. Luis Mayo Muñiz
Director General de **SISTEMAS DE MISILES DE ESPAÑA S.L.**