Política de Seguridad de la Información

Aprobada por el Consejo de Administración
el 26 de marzo de 2024

1 Objetivo de la política

El objeto de este documento denominado Política de Seguridad de la Información es definir los principios y las reglas básicas para garantizar la seguridad de la información de Truck & Wheel, en adelante TW Group y minimizar los riesgos de naturaleza no financiera y que esto resulte en una mejora de la seguridad de los servicios que la compañía ofrece a sus clientes y en los propios procesos internos de la organización.

2 Alcance

El alcance de la presente Política abarca toda la información de las sociedades de TW Group con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.
Por su carácter de política general es de obligado conocimiento y cumplimiento por parte de todas las direcciones de TW Group, tanto en sus relaciones internas como con otras organizaciones.

3 Principios generales de seguridad de la información

La presente responde a las recomendaciones recogidas en el Estándar Internacional ISO/IEC 27001, así como el cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que en el ámbito de la seguridad de la información puedan afectar a TW Group.
Esta política se establece para alcanzar la adopción, implantación y operatividad continuada de protocolos y procedimientos que se cimenten en los tres componentes básicos de la seguridad de la información:

- Confidencialidad. Garantizar el acceso a sistemas y datos únicamente por las personas autorizadas para ello.
- Integridad. Garantizar la exactitud de la información y de los sistemas contra la pérdida o destrucción ya sea de forma accidental o intencionada.
- Disponibilidad. Garantizar que la información y los sistemas puedan ser utilizados en la forma y tiempos requeridos.

Además, TW Group, establece los siguientes principios básicos como directrices fundamentales de la seguridad de la información que han de tenerse presentes en las actividades relaciones con el tratamiento de la información:

- Alcance estratégico. La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de dirección de TW Group de forma que pueda estar coordinada e integrada en todas las iniciativas estratégicas para conformar un marco de trabajo coherente y eficaz.
- Seguridad integral. La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos y debe considerarse como parte de la operativa habitual.
- Gestión de riesgos. El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información y permitirá el mantenimiento de un entorno controlado, minimizado los riesgos hasta niveles aceptables. La reducción de los niveles de riesgo se realizará mediante el despliegue de medidas de seguridad y se establecerá un equilibrio

entre la información y su tratamiento, el impacto y probabilidad de los riesgos a los que está expuesta y la eficacia y coste de las medidas de seguridad.

- Proporcionalidad. El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.
- Seguridad por defecto. Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

TW Group, considera que esta política es de obligado conocimiento de todo el personal de la organización por lo que deberá ser comprendida y asumida por todos los niveles de la organización.
La Política deberá estar disponible en la página web corporativa de TW www.tw-group.com y en un repositorio común de TW Group, de forma que sea accesible por todas las personas del grupo.

4 Compromisos de la dirección

La dirección de TW Group, consiente de la importancia de la seguridad de la información declara los siguientes compromisos:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los empleados de TW Group.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

5 Roles y responsabilidades

TW Group se compromete a velar por la seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las distintas normativas y leyes aplicables.
La función de seguridad de la información recae en el departamento de Ciberseguridad, Sistemas e Infraestructuras en la figura del CISO quien es el responsable de definir, implementar y monitorizar las medidas de ciberseguridad y seguridad de la información.
Todo usuario de los sistemas de información es responsable del uso adecuado que haga de los mismos y de cumplir con los controles y recomendaciones establecidas en los correspondientes protocolos elaborados de manera alineada a esta Política.

Por otro lado, los empleados tienen la obligación de obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

6 Objetivos de seguridad de la información.

TW Group definirá un conjunto de objetivos medibles que contribuyen a minimizar y controlar los riesgos de la organización.
Dichos objetivos deberán ser medidos al menos semestralmente y revisados anualmente con el fin de encontrase alineados con la estrategia de la organización.

7 Cumplimiento normativo

TW Group tiene el compromiso de dotar los recursos necesario para dar cumplimiento a toda la legislación, normativa o regulación aplicable devenida de la protección y seguridad de la información y establecer la responsabilidad de dicho cumplimiento a todos los miembros de la organización.
Se identificarán los requerimientos de las leyes aplicables en el tratamiento y seguridad de la información y se establecerán los mecanismos y medidas adecuadas y razonables para su cumplimiento. Se tendrán en cuenta también las normas que provengan de organismos supranacionales de los que España sea miembro y la normativa comunitaria y/o extracomunitaria, en razón a las áreas de presentación de servicios por parte de TW Group.
Se tendrán en cuenta, también, las normas o códigos de conducta procedentes de TW Group.

8 Aplicación de la política de seguridad

Para aplicar los principios expuestos en esta política, se deberán definir, elaborar, implantar y mantener planes de actuación o de acciones de mejora continua. La elaboración de estos planes y acciones se deberán basar en procesos formales de análisis de riesgos, criterios de evaluación y gestión de riegos o necesidades objetivas de negocio, que permitan implantar las soluciones más idóneas.
A nivel operativo, la organización desarrollará sus propios procedimientos, estándares y guías de seguridad, que garanticen la integridad, confidencialidad y disponibilidad de la información.
Igualmente, se definirán las normas de gestión de seguridad de la información necesarias, acordes con estándares internacionales reconocidos, para asegurar el seguimiento acciones en seguridad de manera efectiva y eficiente, así como de los procesos de revisión y mejora continua de la seguridad.

9 Clasificación y tratamiento de la información

La información de la organización deberá ser clasificada en virtud de su importancia y deberá ser tratada de acuerdo con dicha clasificación. Para ello se deberá definir un modelo de clasificación de la información que permita determinar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad e integridad.
TW Group deberá clasificar la información en función del soporte en el que está siendo utilizado:

- Soporte lógico. Información que esté siendo utilizada mediante medios ofimáticos, correo electrónico o sistemas de información.
- Soporte físico. Información que esté en papel, soportes magnéticos como usb, dvd, etc.

En función de la sensibilidad de la información, TW Group deberá catalogar la información en cinco niveles.

- Uso público
- Difusión limitada
- Información confidencial
- Información reservada
- Información secreta

Véase definición en la norma de niveles de clasificación.

10 Formación y concienciación

La organización deberá establecer planes formativos a todo el personal en materia de seguridad de la información. Estos planes deberán ser acorde al área destinataria y público objetivo según se considere necesario. Así mismo, se realizarán campañas periódicas de concienciación sobre seguridad de la información dirigidas a todo el personal a través del medio que se considere más efectivo.
Asimismo, los empleados deberán ser informados de las actualizaciones de las políticas y procedimientos de seguridad de los que se vean afectados y de las amenazas existentes, de manera que puedan garantizar el cumplimiento de esta política.

11 Gestión de la continuidad del negocio

TW Group deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis.
El Plan de Continuidad de Negocio deberá ser actualizado y aprobado periódicamente junto con el Plan de Recuperación de Desastres alineado con la continuidad del negocio, abarcando la continuidad del funcionamiento de las tecnologías de la información y comunicación.
Adicionalmente se deberá formar y capacitar a los empleados en materia de Continuidad de Negocio. La cuál deberá ser revisada periódicamente con el objetivo de que este alineada con el Plan existente.

12 Auditoría de seguridad y gestión de vulnerabilidades

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo con su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.
Una vez identificadas las vulnerabilidades, la organización deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

13 Incumplimiento y sanciones disciplinarias

El incumplimiento o desviaciones de los principios o directrices en la presente política deberán justificarse por motivos de negocio y deberán ser consensuadas con el departamento de Ciberseguridad, Sistemas e Infraestructuras.
En caso contrario, el incumplimiento total o parcial de los recogido en este documento tendrá como resultado la toma de acciones disciplinarias de acuerdo con el proceso interno de TW Group. Es responsabilidad de todos los empleados de TW Group notificar al responsable de Seguridad de la información de cualquier evento o situación que pudiera suponer un incumplimiento de alguna de las directrices definidas por la presente política.

14 Mejora Continua

TW Group considera fundamental vigilar por la mejora continua, por ello, definirá acciones que permitan mejorar el desempeño de la organización en cuanto a la disponibilidad, integridad y confidencialidad de la información.

15 Vigencia

La Política de Seguridad de la Información entrará en vigor desde el mismo día de su publicación.
Esta política será revisada y aprobada anualmente por el Consejo de Administración. No obstante, si tuvieran lugar cambios relevantes en la sociedad o se identificarán cambios significativos en el entorno de amenazas y riesgos, ya sea de tipo legal, operativo, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario.