POLÍTICA DE SEGURIDAD

Carlos Castilla Ingenieros, S.A., [de ahora en adelante **Grupo Castilla**] depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas son administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada y de los servicios prestados.

Conscientes de la trascendencia de la seguridad de la información, y en consonancia con el camino que marca nuestra propia identidad, desde **Grupo Castilla** se ha impulsado el establecimiento de:

- Un Sistema de Gestión de la Seguridad de la Información de acuerdo con los requisitos de la norma ISO 27001 (en adelante, SGSI) con el fin de identificar, evaluar y minimizar los riesgos a los que se expone su información y la de sus clientes, así como garantizar el cumplimiento de los objetivos establecidos.

- Y de un Sistema de Gestión de la Seguridad de la Información según los requisitos del Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).

El objetivo de la presente Política de Seguridad es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente y supervisando la actividad diaria, así como proporcionar un marco de referencia para el establecimiento de los objetivos de seguridad que permitan a **Grupo Castilla** desarrollar una cultura de empresa, una forma de trabajar y de tomar decisiones, alineada con la seguridad de la información y que el respeto a los datos personales sean una constante.

Los sistemas TIC están protegidos contra amenazas de rápida evolución, cuyo daño potencial incide en la confidencialidad, integridad, disponibilidad, uso previsto (trazabilidad) y valor de la información (autenticidad) de los servicios. Para defenderse de estas amenazas, se ha definido una estrategia que se adapta a los cambios en las condiciones del entorno para garantizar la prestación continua de nuestros servicios.

Desde los diferentes departamentos de **Grupo Castilla** se asegura que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Grupo Castilla está preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS, por ello se ha actuado en aras de potenciar distintos aspectos de la seguridad TIC:

i. En materia de prevención

Todos los departamentos implicados deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se implementarán las medidas de seguridad determinadas por el ENS, así como controles adicionales identificados a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por terceros para obtener una evaluación independiente.
- Evaluar el riesgo existente ante la posibilidad de conectarse a otros sistemas de información interconectados.

ii. En materia de detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, **Grupo Castilla** monitoriza la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 y Art.12 del ENS. Por ello, se establecen mecanismos de detección, análisis y reporte que informan a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

iii. En materia de respuesta

Desde **Grupo Castilla** se han implementado procedimientos con el fin de:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad en virtud de lo establecido en el Art. 12.6.m) del ENS,
- Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados,
- Establecer protocolos para el intercambio de información relacionada con el incidente.

iv. En materia de recuperación

Para garantizar la disponibilidad de los servicios críticos y en base a los requisitos establecidos en el Art. 11.6.n) del ENS, desde Grupo Castilla se han desarrollado planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Esta Política de Seguridad de la información se alineará con las políticas generales de la compañía y servirá de marco a otros sistemas de gestión interna, como las de calidad.

En Riudoms, a 29 de febrero de 2024

Carles Castilla
Consejero delegado