POLÍTICA DE SEGURIDAD

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 o confidencialidad 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 a 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 de acuerdo a los requisitos del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, 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 incida en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y 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 7 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 parte de terceros con el fin de obtener una evaluación independiente.

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 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,
- 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, 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.

La presente Política de Seguridad de la información se hallará siempre alineada con las políticas generales de la compañía y con las que sirvan de marco a otros sistemas de gestión interna, como son las políticas de calidad.

En Riudoms, a 19 de noviembre de 2020

Carles Castilla
CEO Grupo Castilla

Aprobación y entrada en vigor

Esta Política de Seguridad de la Información es efectiva desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política en vigor debidamente aprobada y publicada.

Alcance

Esta política se aplica a todos los sistemas TIC propiedad de **Grupo Castilla** y a todos los miembros de la organización implicados en dicha solución.

Misión

Grupo Castilla es una de las compañías líder en desarrollo e implantación de soluciones de software de gestión del capital humano (HCM) en España, con una amplia trayectoria desde su fundación en el 1979. Aportamos valor a nuestros clientes a través de un servicio integral, personalizado y adaptado a todas sus necesidades, con una apuesta constante por el desarrollo tecnológico. Nuestra máxima preocupación es conseguir que cada uno de nuestros clientes se sienta atendido en todo momento, proporcionarles respuestas ágiles y especializadas con un excelente servicio postventa.

Marco Normativo

Grupo Castilla se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

- Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- El convenio colectivo aplicable.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico.
- Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista, que viene a modificar varios artículos de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, a fin de adecuar su régimen a la nueva redacción dada, por la Directiva 2009/136/CE, a la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia (actualización 08/07/2020).

El marco de referencia que da cobertura legal a este documento se establece en virtud de lo dispuesto en el Artículo 12 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Marco Organizativo de la Seguridad TIC

La seguridad TIC compromete a todos los miembros de la organización sujetos al alcance de la presente política. Para ello, en virtud de los establecido en el Anexo II, sección 3.1 del Real Decreto 3/2010, de 8 de enero, se han identificado de forma fehaciente responsables de velar por su cumplimiento y deberá ser conocida por todos los miembros de la organización.

i. Organización de la seguridad

Grupo Castilla ha nombrado un Comité de Seguridad TIC que supervisará el seguimiento y cumplimiento del SGSI y del ENS. El Comité de Seguridad TIC está formado por cargos corporativos y de responsabilidad dentro de la organización.

Según lo descrito en el Procedimiento de Seguridad creado el efecto, el Comité de Seguridad TIC tendrá las siguientes funciones y responsabilidades:

- Coordinar todas las actividades relacionadas con la seguridad de las TIC.
- Es responsable de la redacción de la Política de Seguridad.
- Es responsable de la creación y aprobación de las normas que enmarcan el uso de los servicios TIC.
- Aprobará los procedimientos de actuación en lo relativo al uso de los servicios TIC.
- Aprobará los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.

Asimismo, se han definido las funciones y responsabilidades del Responsable de Seguridad de la Información y su relación con el Comité de Seguridad TIC, así como las funciones y responsabilidades en materia de Seguridad TIC para todos los empleados implicados.

El Responsable de Seguridad de la Información será nombrado por la Dirección a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

ii. Liderazgo y compromiso de la dirección

La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos, la valoración de la disponibilidad, integridad y confidencialidad de su información y aún más la de sus clientes y partes interesadas. Así, se compromete a desarrollar, implantar, mantener y mejorar continuamente la presente política de Seguridad y su **Sistema de Gestión** con el objetivo de la mejora continua en la forma en que prestan sus servicios y en que tratan la información. Por ello, es política de **Grupo Castilla** que:

- Se establezcan anualmente objetivos con relación a la Seguridad de la Información.
- Se cumpla con los requisitos legales, contractuales y del negocio.
- Se realicen actividades de formación y concienciación en materia de los procesos de Seguridad de la Información para todo el personal.
- Se desarrolle un proceso de análisis, gestión y tratamiento del riesgo sobre los activos de información.
- Se establezcan los objetivos de control y los controles correspondientes para mitigar los riesgos detectados.
- Se establezca la responsabilidad de los empleados en relación con:
    - Reportar las violaciones a la seguridad;
    - Preservar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los activos de información en cumplimiento de la presente política;
    - Cumplir las políticas y procedimientos inherentes a la presente Política de Seguridad.
    - Reportar por los canales previstos, los problemas o vulnerabilidades detectadas en materia de seguridad TIC.
    - Proponer mejoras del SGSI al Comité de Seguridad TIC.

iii. Política de seguridad de la información

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes interesadas.

iv. Datos de carácter personal

Grupo Castilla trata datos de carácter personal. En este sentido, y en cumplimiento con la legislación vigente en materia de protección de datos, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, **Grupo Castilla** ha aplicado medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- la seudonimización y el cifrado de datos personales;
- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

v. Gestión de riesgos

Todos los sistemas sujetos a esta Política han sido evaluados mediante un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

vi. Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de la Información se encuentra alineada con el Sistema de Gestión de Seguridad de la Información implementado bajo el referencial ISO 27001 y complementa las políticas de seguridad de **Grupo Castilla** en diferentes materias:

- Manual Seguridad TIC.
- Procedimientos de Seguridad:
    - Organización de la seguridad de la información
    - Seguridad de los recursos humanos
    - Gestión de activos
    - Control de acceso
    - Criptografía
    - Seguridad física y del entorno
    - Seguridad de las operaciones
    - Seguridad de las comunicaciones
    - Adquisición, desarrollo y mantenimiento de sistemas
    - Relación con proveedores
    - Incidencias de seguridad de la información
    - Aspectos de la seguridad de la información en la continuidad del negocio
    - Cumplimiento
- Procedimientos Operativos.

Esta Política se desarrollará siguiendo la normativa en materia de seguridad de la información. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en

particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones sujetos al alcance de certificación.

La normativa de seguridad estará disponible en la intranet de **Grupo Castilla.**

vii. Obligaciones del personal

Todos los miembros de **Grupo Castilla** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC aplicar las medidas necesarias para que la información llegue a los afectados.

Todos los empleados recibirán una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Asimismo, se establecerá un programa de concienciación continua para sensibilizar a todos los miembros de **Grupo Castilla**, en particular a los de nueva incorporación, el cual se encuentra alineado con el estándar ISO 9001 actualmente implantado.

viii. Terceras partes

Cuando **Grupo Castilla** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **Grupo Castilla** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.