POLÍTICA DE SEGURIDAD

Histórico de Versiones		
Número	**Fecha**	**Modificación**
1	23/04/25	Versión inicial
2	16/02/26	Se firma por nuevo CEO y se hacen modificaciones leve del texto

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

El Comité de Seguridad ha revisado y aprobado el texto en la fecha 01/06/2023. En adelante, cuando hagamos referencia al Sistema de Seguridad de la Información, nos referiremos a él como SGSI (Sistema de Gestión de la Seguridad de la Información) debido a su integración. El Comité de Seguridad de la Información de TEAM2GO podrá llevarse a cabo al mismo tiempo, teniendo en cuenta nuestro alcance y recursos. Esta Política de Seguridad de la Información estará vigente desde la fecha indicada hasta que sea sustituida por una nueva versión.

2. INTRODUCCIÓN

Con el fin de cumplir su Misión y alcanzar los objetivos establecidos, TEAM2GO se apoya en Tecnologías de Información y Comunicaciones (TIC) para la prestación de los Servicios identificados. Es esencial gestionar estos sistemas con agilidad y diligencia, implementando las medidas de seguridad necesarias para salvaguardarlos de posibles daños accidentales o intencionados que puedan comprometer la disponibilidad, integridad y confidencialidad de la información procesada y los servicios proporcionados. El propósito fundamental de la seguridad de la información es garantizar la calidad de la información y la continuidad de los servicios dentro del alcance establecido. Para lograrlo, se deben adoptar medidas preventivas, supervisar de forma constante la actividad diaria y responder de manera eficiente a los incidentes de seguridad. Asimismo, es fundamental asegurar el cumplimiento de las obligaciones legales, así como la confidencialidad, integridad y disponibilidad de los sistemas de información. Los sistemas de tecnología de la información y comunicaciones (TIC) deben estar protegidos contra las amenazas en constante evolución que pueden comprometer la confidencialidad, integridad, disponibilidad, así como la trazabilidad, autenticidad, uso y valor de la información y los servicios. Para defenderse eficazmente de estas amenazas, se requiere una estrategia adaptable a los cambios del entorno, con el objetivo de garantizar la continuidad de los servicios en el ámbito establecido. Esto implica que el área de Sistemas de la organización debe aplicar las medidas de seguridad mínimas establecidas por el Esquema Nacional de Seguridad e ISO 27001, monitorear de manera continua los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades informadas, y prepararse para responder de manera eficiente y eficaz ante los incidentes de seguridad, asegurando así la continuidad de los servicios en el ámbito establecido. Cada departamento debe comprender que la seguridad de las TIC es una parte integral de todas las etapas del ciclo de vida del sistema, desde su concepción hasta su retirada del servicio, incluyendo las decisiones de desarrollo o adquisición y las actividades de operación. Los requisitos de seguridad y las necesidades de financiamiento deben identificarse e incorporarse en la planificación, en las solicitudes de propuestas y en los pliegos de licitación para los proyectos de TIC. Los departamentos involucrados deben estar preparados para prevenir, detectar, reaccionar y recuperarse de los incidentes de acuerdo con el Artículo 7 del ENS, bajo la supervisión y coordinación del Área de Sistemas.

Prevención de incidentes

Con el fin de evitar o minimizar en la medida de lo posible los impactos negativos en la información y los servicios dentro del alcance establecido, es necesario que los diferentes departamentos tomen medidas preventivas. El área de Sistemas es responsable de implementar las medidas de seguridad mínimas establecidas por el ENS e ISO 27001, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, junto con los roles y responsabilidades de seguridad de todo el personal, deben ser claramente definidos y documentados. Para asegurar el cumplimiento de la política, el departamento de Sistemas debe:

- 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.

Monitorización y detección de incidentes

- Dado el riesgo de degradación rápida de los servicios dentro del alcance debido a incidentes que pueden variar desde pequeñas interrupciones hasta la completa interrupción, es fundamental llevar a cabo una monitorización continua de la operación. Esto permitirá detectar cualquier anomalía en los niveles de rendimiento de los servicios y tomar las medidas correspondientes de acuerdo con lo establecido en el Artículo 9 del ENS. La monitorización cobra especial importancia cuando se implementan líneas de defensa según lo establecido en el Artículo 8 del ENS. Se implementarán mecanismos de detección, análisis y reporte que informen regularmente a los responsables y que alerten sobre desviaciones significativas de los parámetros establecidos como normales. Los sistemas de detección de intrusos desempeñan un papel fundamental al supervisar y revisar los recursos, asegurando el cumplimiento de las políticas de seguridad y tratando de identificar de manera rápida, efectiva y eficiente cualquier actividad maliciosa. Según las necesidades, se establecerán las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.
- De acuerdo con el Reglamento General de Protección de Datos, en sus artículos 33 y 34, se requiere la notificación de las violaciones de seguridad

que involucren datos personales a la Agencia Española de Protección de Datos y a los individuos afectados cuando exista un riesgo para ellos. Por lo tanto, es necesario establecer controles internos para identificar y clasificar este tipo de incidencias relacionadas con datos personales, y comunicarlas al Responsable de Seguridad.

Respuesta ante Incidentes

Las áreas o departamentos involucrados deben:

- Responder eficazmente a los incidentes de seguridad, mediante los mecanismos establecidos por el área de Sistemas.
- Designar un único punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Ejecutar los protocolos para el intercambio de información relacionada con el incidente, establecidos por el área de Sistemas. Esto incluye comunicaciones, mediante el formulario, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Recuperación ante Incidentes

Para garantizar la disponibilidad de los servicios críticos, el departamento de Sistemas debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Los sistemas de información que dan soporte a los procesos de servicio de implantación, mantenimiento y soporte técnico de la aplicación informática MyTeam2Go para la gestión de recursos humanos, de acuerdo con el documento de aplicabilidad vigente a fecha de emisión de certificado.

4. MISIÓN

TEAM2GO es una empresa de implantación y desarrollo de su propio software MyTeam2Go que se fundamenta sobre la gestión del talento, la innovación en la digitalización de políticas de recursos humanos y la flexibilidad, que son los valores más importantes para la organización. El Sistema Integrado de Gestión de la Seguridad de la Información tiene como finalidad conseguir unos servicios competitivos, comprometiéndonos a cumplir con los requisitos derivados de las necesidades de nuestros clientes, con una gestión transparente,

eficiente y responsable. Para ello, el Sistema Integrado de Gestión de la Seguridad de la Información tiene como objetivos principales:

- Gestión y control eficaz de los servicios objeto del alcance.
- Implementar con eficacia la continuidad del servicio objeto del alcance.
- Mejorar de forma continua nuestros Sistemas Integrados de Gestión.
- Cumplimiento de los requisitos legales aplicables y otros requisitos de los clientes.
- Asegurar la confidencialidad, disponibilidad e integridad de la información, así como su trazabilidad y autenticidad.
- Asegurar una prestación de los servicios, objeto del alcance, eficiente y eficaz.
- Cumplir los requisitos acordados mediante acuerdos de nivel de servicio.
- Garantizar un servicio continuado y la gestión adecuada de las incidencias.
- Gestionar los riesgos eficientemente.
- Fomentar la comunicación segura, interna y externa.
- Asignación eficiente de funciones, recursos y responsabilidades.
- Concienciación, formación y motivación del personal de la Compañía, sobre la importancia del desarrollo e implantación de un Sistema Integrado de Gestión de Seguridad de la Información y sobre su implicación en el cumplimiento de las expectativas de los clientes y la protección de su información.
- Adaptación a la evolución y tecnologías del mercado.

5. MARCO NORMATIVO

El marco legal y normativo en materia de seguridad de la información al que responde la política y el sistema integrado de gestión de seguridad de la información lo definen:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales de 13 de diciembre.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- UNE-ISO/IEC 27001:2017.

6. PRINCIPIOS BÁSICOS DEL ESQUEMA NACIONAL DE SEGURIDAD

La seguridad en TEAM2GO se considera un proceso integral que abarca todos los aspectos relacionados con el sistema de información, recursos humanos, materiales, técnicos, jurídicos y organizativos. La implementación del sistema de gestión de seguridad de la información basado en ISO 27001 y el ENS, tiene este enfoque integral, evitando actuaciones puntuales o soluciones temporales.

Prestamos especial atención a la concienciación de todo el personal involucrado y de los responsables jerárquicos. Es fundamental mitigar riesgos asociados al desconocimiento, la falta de organización, de coordinación y de instrucciones claras. Para ello, se realizan formaciones y se dan directrices continuas, asegurando que todos los miembros de la empresa comprendan y actúen conforme a las políticas de seguridad establecidas.

El análisis y la gestión de riesgos son fundamentales para nuestro proceso de seguridad siendo actividades continuas y constantemente actualizadas. Mantenemos un entorno controlado mediante la identificación y evaluación constante de riesgos, con el objetivo de reducirlos a niveles aceptables. Esto se logrará aplicando medidas de seguridad adecuadas y equilibradas, en función de la naturaleza de la información tratada, los servicios prestados y los riesgos identificados. Esta gestión proactiva permite asegurar que las medidas de seguridad son siempre pertinentes y efectivas, protegiendo así los activos y la integridad de la empresa.

La seguridad del sistema en nuestra empresa incluye acciones de prevención, detección y respuesta para minimizar vulnerabilidades y proteger la información y los servicios.

- Prevención: Implementamos medidas destinadas a disuadir y reducir la exposición a riesgos. Estas medidas eliminan o disminuyen el impacto de las amenazas se puedan materializarse.

- Detección: Establecemos mecanismos para identificar rápidamente la presencia de incidentes y cualquier actividad sospechosa que pueda comprometer el sistema.

- Respuesta: Desarrollamos procedimientos para actuar de manera eficiente y oportuna en caso de incidentes, con el fin de restaurar la información y los servicios afectados.

Garantizamos la conservación de los datos e información en soporte electrónico y mantenemos los servicios disponibles durante todo el ciclo de vida de la información digital. Los procedimientos del sistema asegurarán la preservación del patrimonio digital, respetando siempre los principios básicos y requisitos establecidos.

Nuestro sistema de información cuenta con una estrategia de protección basada en múltiples capas de seguridad. Esta estrategia se garantiza que, si una capa de seguridad es comprometida, se logren los siguientes objetivos:

- Reacción frente a incidentes: Se implementan mecanismos para desarrollar una respuesta adecuada a los incidentes que no pudieron evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su totalidad.

- Minimización del impacto: Se toman medidas para minimizar el impacto en el sistema y limitar los efectos adversos en la información y los servicios.

Las líneas de defensa están compuestas por medidas de naturaleza organizativa, física y lógica, creando un entorno de seguridad robusto y efectivo.

La vigilancia continua es esencial para detectar actividades o comportamientos anómalos y permitir una respuesta oportuna. Además, realizamos una evaluación permanente del estado de seguridad de nuestros activos, lo que nos permitirá medir su evolución, identificar vulnerabilidades y detectar deficiencias de configuración.

Las medidas de seguridad son reevaluadas y actualizadas periódicamente para garantizar que su eficacia se ajuste a la evolución de los riesgos y los sistemas de protección. En caso necesario, se realiza un replanteamiento de la seguridad para mantener un entorno seguro y protegido.

En nuestros sistemas de información, se definen claramente los roles de los responsables, que influyen al responsable de la información, al responsable del servicio, al responsable de la seguridad y al responsable del sistema. La responsabilidad de la seguridad de los sistemas de información está claramente diferenciada de la responsabilidad sobre la explotación de estos.

Se especifican las atribuciones de cada uno de estos responsables, así como los mecanismos para la coordinación entre ellos y para la resolución de posibles conflictos.

7. ORGANIZACIÓN DE LA SEGURIDAD

Comité: Funciones y Responsabilidades

TEAM2GO dispone de un **Comité de Seguridad** de la Información, para la gestión del Sistema y la vigilancia del cumplimiento de las políticas y normas implantadas en la organización. El Comité está compuesto por los siguientes responsables:

- Dirección de la Entidad

- Responsable de Seguridad
- Responsable del Sistema

El Comité es el encargado de realizar las siguientes funciones:

- Apoyar al Responsable Técnico de Seguridad para que sus decisiones sean llevadas a cabo con éxito.
- Coordinar y gestionar todos los servicios y soluciones prestados por la organización para asegurar que se satisfacen todos los requisitos definidos
- Decidir, tras las revisiones del sistema, aquellas acciones necesarias para la mejora continua en cuanto a Seguridad de la Información.
- Revisar y Aprobar las Políticas de Seguridad de la organización anualmente o cuando se produzcan cambios significativos en la misma.
- Definir el enfoque que se debe dar a la evaluación y gestión de riesgos para la consecución de los objetivos definidos.
- Asegurar que los activos se gestionan conforme a los requisitos legales y regulatorios vigentes.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización.

El Comité, con plena autoridad para tomar decisiones, asumirá la responsabilidad de los riesgos identificados en los análisis correspondientes. Para ello, se asegurará de que se realicen correctamente los análisis de riesgos, se establezca un nivel aceptable de riesgo, se apruebe el plan de tratamiento de riesgos y se acepten los riesgos residuales. El Comité poseerá conocimientos sobre la metodología de análisis de riesgos.

El Comité se reunirá al menos una vez al año para verificar la eficacia de los Sistemas de Gestión implementados en la organización. En caso de que el Comité lo considere necesario, también se podrán convocar reuniones extraordinarias según sea requerido. Se podrá invitar a las reuniones del Comité a todas aquellas personas que se consideren necesarias, en función de los temas a tratar.

Las decisiones adoptadas durante las reuniones del Comité son registradas en un acta, que se aprueba o corrige al comienzo de la siguiente sesión del Comité por todos los participantes. Estas actas se guardan como evidencia de la asistencia y el registro de las deliberaciones del Comité, y se archivan como documentación que respalda las decisiones tomadas por el Comité.

Roles: Funciones y Responsabilidades

En función de nuestro alcance y recursos, se definen los siguientes nivele y roles:

Nivel de Gobierno

1. Dirección de la entidad

La Dirección de la Entidad (Alta Dirección) es fundamental para establecer, liderar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI) y garantizar el cumplimiento normativo.

Las funciones son las siguientes:

a. Determinar los niveles de seguridad de la información.
b. Determinar y aprobar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, así como autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad (ENS).
c. Determinar la categoría del sistema y su aprobación dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad (ENS).
d. Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
e. Es el responsable del uso que se haga de la información y de su protección.
f. Es el responsable de gestionar cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
g. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
h. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles.
i. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de la organización.

2. Responsable de la Información

El Responsable de la Información tiene funciones orientadas a garantizar la protección, disponibilidad, integridad y confidencialidad de la información dentro de la organización.

a. Determinar los niveles de confidencialidad, integridad y disponibilidad de la información.

b. Aplicar el principio de proporcionalidad para definir controles adecuados.
c. Garantizar que la información se gestione conforme a su nivel de protección.
d. Definir quién puede acceder a la información y con qué permisos.
e. Aprobar las solicitudes de acceso y garantizar la correcta segregación de funciones.
a. Revisar periódicamente los accesos y asegurar la revocación de permisos innecesarios.
b. Asegurar que el tratamiento de la información cumple con el ENS, la normativa vigente y las políticas internas.
c. Coordinar con el Responsable de Seguridad para aplicar las medidas necesarias.
d. Vigilar que los usuarios hagan un uso adecuado de la información.
e. Asegurar que los datos se mantengan actualizados y sean fiables.
f. Colaborar en la identificación, análisis y respuesta a incidentes de seguridad.
g. Informar sobre cualquier brecha de seguridad que afecte a la información bajo su responsabilidad.

3. Responsable del servicio.

El Responsable del Servicio es el encargado de garantizar la correcta prestación y seguridad del servicio bajo su responsabilidad.

Tiene atribuidas las siguientes funciones:

a. Asegurar que el servicio cumple con los requisitos de seguridad definidos en el ENS.
b. Coordinar la integración de los controles de seguridad en el diseño y operación del servicio.
c. Garantizar la disponibilidad, integridad y confidencialidad del servicio.
d. Asegurar que el servicio cumple con las regulaciones y normativas aplicables.
e. Colaborar con el Responsable de Seguridad y el Responsable de la Información para alinear las medidas de seguridad.
f. Verificar que los proveedores de servicios cumplen con los requisitos de seguridad exigidos.
g. Definir y supervisar acuerdos de nivel de servicio (SLA) y acuerdos de seguridad.
h. Evaluar los riesgos de seguridad asociados al servicio.
i. Aplicar controles de mitigación adecuados según la criticidad del servicio.
j. Definir y aplicar planes de respuesta ante incidentes de seguridad del servicio.

k. Garantizar la recuperación y continuidad del servicio en caso de interrupciones.
l. Participar en auditorías de seguridad y en la revisión periódica del estado del servicio.
m. Proponer mejoras para garantizar la eficiencia y seguridad del servicio.

Nivel de supervisión

4. Responsable de Seguridad

El Responsable de Seguridad juega un papel clave en la gestión y protección de la información dentro de la organización y será nombrado por la Dirección.

Tiene atribuidas las siguientes funciones:

a. Determinar las medidas de seguridad aplicables, dentro del marco establecido en el Anexo II del Esquema Nacional de Seguridad (ENS) y el Anexo A de ISO 27001.
b. Coordinar y mantener el Sistema Integrado de Gestión de Seguridad de la Información que cubre los aspectos relativos a la seguridad conforme al ENS y a la ISO 27001.
c. Asegurar el cumplimiento de planes y objetivos del Sistema Integrado de Gestión de la Seguridad de la Información.
d. Revisar y mantener, la documentación, el análisis y evaluación de riesgos, revisando regularmente los resultados para asegurar la idoneidad, eficacia y efectividad Sistema de Gestión Integrado de Seguridad de la Información, así como de los controles y medidas implantados.
e. Garantizar que el Sistema funciona, reaccionando ante cualquier evento y mejorando de manera continua.
f. Analizar los informes de auditoría y elevar al Comité las conclusiones de este análisis.
g. Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias en que pudieran incurrir en caso de incumplimiento.
h. Velar por el correcto cumplimento de la normativa legal aplicable, especialmente en materia de protección de datos personales y propiedad intelectual.
i. Solicitar opinión al Delegado de Protección de Datos sobre las violaciones de seguridad de datos personales y en su caso, recomendar la notificación a la Agencia Española de Protección de Datos y/o a los interesados.

5. Delegado de protección de datos

El rol de la Delegada de Protección de Datos (DPO, por sus siglas en inglés) es fundamental en la gestión de la privacidad y el cumplimiento del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) en España.

Su labor está estrechamente relacionada con el Responsable de Seguridad y el Responsable de la Información, ya que debe garantizar que los datos personales sean tratados de manera segura y conforme a la normativa vigente.

Aunque su función no está regulada directamente en el Esquema Nacional de Seguridad (ENS) ni en la ISO/IEC 27001:2023, su trabajo se alinea con ambos marcos, ya que la protección de datos es un elemento clave dentro de la seguridad de la información.

a. Gestión de riesgos: Identificación y mitigación de riesgos de seguridad que puedan afectar a datos personales.
b. Medidas de seguridad: Implementación de controles para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.
c. Gestión de incidentes: Supervisión de brechas de seguridad y coordinación con el Responsable de Seguridad.
d. Auditoría y mejora continua: Evaluación periódica del cumplimiento normativo y actualización de las políticas de seguridad.

Nivel operativo

6. Responsable del Sistema

El responsable del Sistema es la persona encargada de la seguridad y operatividad de los sistemas de información.

El responsable del sistema será nombrado por el Comité de Seguridad.

Tiene atribuidas las siguientes funciones:

a. Gestionar el Sistema.
b. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
c. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de la empresa.
d. Acordar la suspensión del tratamiento de información o la prestación de servicio si existiesen deficiencias graves de seguridad. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
e. Hacer de intermediario entre la organización y todas las personas involucradas bajo el alcance del sistema.
f. Establecer directrices y medidas.

g. Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
h. Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
i. Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de instalación, configuración y prueba.
j. Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
k. Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
l. Elaborar procedimientos operativos de seguridad.
m. Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
n. Aprobar los cambios que afecten a la seguridad del Sistema.
o. Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
p. Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
q. Comunicar, tan pronto como se tenga constancia, las violaciones de seguridad que afecten a datos personales, al Responsable de Seguridad.

7. Administrador de Seguridad

El administrador de seguridad es el encargado de la gestión operativa de la seguridad en los sistemas de información, asegurando que las medidas técnicas y organizativas se implementan y funcionan correctamente.
El administrador de seguridad, será nombrado por el Comité de Seguridad.

El Administrador de Seguridad tiene atribuidas las siguientes funciones:

a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
b. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
c. Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

d. Como administrador de todos los accesos a los ficheros y recursos de la instalación pueden tener per se acceso a los mismos.
e. Analizar posibles transgresiones e irregularidades en los accesos.
f. Evaluar la seguridad de paquetes, aplicaciones, productos y dispositivos, antes de su adquisición o implantación.
g. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
h. Asegurar que los controles y medidas de seguridad establecidos son adecuadamente observados.
i. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
j. Dar soporte técnico en materia de seguridad, a los desarrolladores, técnicos y usuarios en general.
k. Se encarga de administrar y monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
l. Informar al Responsable de la Seguridad de cualquier vulnerabilidad relacionada con la seguridad.
m. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
n. Por otro lado, tiene atribuidas las siguientes obligaciones:
o. Guardará secreto de la información de carácter personal que conozca en el desempeño de su función, aún después de haber abandonado la organización.
p. Velará porque se concedan y revoquen oportunamente las autorizaciones para acceder a los datos de los cuales sea responsable.
q. Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
r. No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos, informar de posibles debilidades en los controles, y no poner en peligro la disponibilidad de los datos, ni su confidencialidad o integridad.
s. No ceder ni comunicar a otros las contraseñas, que son personales, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros; los usuarios serán responsables de todos los accesos y actividades que se puedan haber realizado utilizando su código de usuario y contraseña.
t. Proteger las copias de datos que estuvieran en su poder.

u. No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles y medidas que se hayan establecido.

8. Personal Técnico

El Personal Técnico tiene las siguientes responsabilidades:

a. Desarrollo del código efectivo de las aplicaciones que le sean asignadas, basándose en los requerimientos previos del producto manager.
b. Realizar una codificación libre de errores, efectuando las pruebas necesarias para tal efecto.
c. Realizar una correcta gestión de versiones en el desarrollo.
d. Mantener el código organizado en repositorios que permitan realizar una correcta trazabilidad sobre todos los cambios.
e. Documentar, tanto en el propio código, insertando comentarios que faciliten su compresión, como en la documentación del proyecto, detallando los procesos, algoritmos y funciones empleados en la solución de cada uno de los desarrollos.
f. Realizar su desarrollo aplicando prácticas seguras de codificación desde el punto de vista de la seguridad de la información (Desarrollo Seguro).
g. Informar en todo momento del estado y situación de cada uno de los proyectos en los que está involucrado.
h. Mantener el código actualizado y funcional, en base de los nuevos requerimientos que le sean solicitados.
i. Desarrollar las tareas asignadas en tiempo y forma de implantación y soporte.
j. Informar al Product Manager de cualquier desviación en sus tareas por cualquier motivo.
k. Analizar y estimar los pedidos que le asigne el Product Manager.

9. Personal Funcional

Las funciones y obligaciones atribuidas al personal de TEAM2GO, son las siguientes:

a. Acceder únicamente a los datos que necesite para el ejercicio de sus funciones.
b. Todos los datos de carácter personal que con motivo del desempeño de los trabajos que les sean encomendados conozcan los usuarios, son confidenciales y habrán de guardar estricta reserva al respecto, no divulgándolos más allá de lo estrictamente necesario para realizar su trabajo.
c. Cualquier incidencia acaecida habrá de ser comunicada de acuerdo con lo indicado en el Procedimiento de Gestión de incidencias.

d. El deber de no sacar fuera del ámbito de TEAM2GO ninguna clase de datos sin autorización expresa del Responsable de la Información.
e. El deber de no dejar su pantalla de acceso a los Sistemas e información activa cuando por cualquier causa deje su puesto de trabajo desatendido.
f. La obligación de disponer de clave de acceso a los ordenadores y modificarla cuando así se establezca.
g. El cumplimiento estricto de las normas, políticas y procedimientos de seguridad.
h. Queda expresamente prohibido destruir, alterar o dañar de cualquier otra forma los datos, programas o documentos electrónicos.
i. Queda expresamente prohibido intentar borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
j. Ejecución de los servicios del alcance.
k. Procedimiento de Designación
l. Política de Seguridad de la Información

El Comité de Seguridad tiene como responsabilidad llevar a cabo una revisión anual de esta Política de Seguridad de la Información y proponer su revisión o mantenimiento. La aprobación de la Política recae en el Comité de Seguridad, y se debe difundir para que todas las partes involucradas la conozcan.

8. DATOS DE CARÁCTER PERSONAL

En la prestación de los servicios dentro del alcance establecido, es necesario procesar datos personales. TEAM2GO cuenta con un análisis de riesgos de seguridad que incluye controles y medidas para mitigar o eliminar los riesgos identificados en tratamientos con un nivel alto de riesgo. Para ello, se ha llevado a cabo una evaluación de impacto en la protección de datos, que identifica los riesgos en términos de seguridad y propone medidas y controles para que el riesgo residual sea aceptable.

9. DELEGADO DE PROTECCIÓN DE DATOS

El delegado de Protección de Datos (DPD) será designado de forma única para toda la organización, y su nombramiento y cese serán informados a la Agencia Española de Protección de Datos. El DPD desempeñará las funciones establecidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, así como en otras disposiciones legales pertinentes. A continuación, se enumeran las funciones y responsabilidades del DPD, basadas tanto en el RGPD como en la LOPD (LOPDGDD 3/2018), así como en las recomendaciones del Grupo 29:

a. Informar y asesorar al responsable o al encargado y a los trabajadores sobre las obligaciones que impone la normativa de protección de datos.
b. Supervisar el cumplimiento de la normativa
c. Asesorar respecto de la evaluación de impacto relativa a la protección de datos, para lo que deberá aconsejar sobre:
d. si se debe llevar a cabo o no una evaluación de impacto de la protección de datos.
e. qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.
f. si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
g. qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados.
h. si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con la normativa general de protección de datos.
i. Cooperar con la autoridad de control
j. Actuar como punto de contacto para cuestiones relativas al tratamiento
k. Ayudar al responsable o el encargado del tratamiento a controlar el cumplimiento interno del RGPD, para lo que necesitará:
l. recabar información para determinar las actividades de tratamiento,
m. analizar y comprobar la conformidad de las actividades de tratamiento,
n. informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
o. Deberá considerar debidamente el riesgo asociado a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.
p. Elaborar inventarios y mantener un registro de las operaciones de tratamiento basados en la información que les proporcionan los diversos departamentos de su organización responsables del tratamiento de datos personales.
q. Comunicar a los órganos de administración y dirección del RT o del ET la existencia de una vulneración relevante en materia de protección de datos, y proporcionar las medidas necesarias para evitar la persistencia de esta conducta.
r. Recibir las reclamaciones contra un RT o ET presentadas por un afectado, comunicar al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.
s. Recibir las reclamaciones contrato un RT o ET por parte de un afectado, directamente de Agencia Española de Protección de Datos o, de las autoridades

autonómicas de protección de datos, cuando el afectado se ha dirigido a las autoridades de control directamente, debiendo dar respuesta en el plazo de un mes.

10. GESTIÓN DE RIESGOS

Los sistemas sujetos a esta Política deben realizar un análisis de riesgos para evaluar las amenazas y riesgos a los que están expuestos. Este análisis de riesgos servirá como base para determinar las medidas de seguridad que se deben implementar, además de las requeridas por el Esquema Nacional de Seguridad, como se establece en el Artículo 6 del ENS y el Anexo A de ISO 27001. El proceso de gestión de riesgos, que abarca la categorización de los sistemas, el análisis de riesgos y la selección de medidas de seguridad proporcionales y justificadas, debe ser revisado y aprobado anualmente por el Comité de Seguridad. El análisis y tratamiento de riesgos deben ser actividades recurrentes de acuerdo con el Artículo 9 del ENS. Por lo tanto, el análisis de riesgos se repetirá periódicamente para mantener la seguridad de los sistemas:

- 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

El Comité de Seguridad establecerá una valoración de referencia para los distintos tipos de información gestionada y los servicios prestados. Además, impulsará la asignación de recursos necesarios para satisfacer las necesidades de seguridad de los diferentes sistemas, fomentando inversiones de carácter transversal.

Una vez completado el análisis de riesgos de los activos dentro del alcance, el Comité de Seguridad deberá aprobar los resultados obtenidos. Posteriormente, se deben aprobar los niveles de riesgo aceptables para la organización.

Para aquellos activos en los que no se puedan asumir riesgos asociados, se deberá establecer un plan de tratamiento de riesgos que incluya la definición de controles a implementar, plazos, responsabilidades y descripción de las actividades a realizar. El plan de tratamiento de riesgos también contendrá información sobre el seguimiento de las actividades para permitir la visualización del estado actual de cada control. Además de la aplicación de controles, existe la opción de transferir o asumir los riesgos.:

a. Los riesgos se pueden transferir a través de acuerdos con compañías de seguros o proveedores.
b. En cuanto a la posibilidad de asumir riesgos, esta acción debe ser realizada con el consentimiento escrito de la Dirección.

En cualquiera de los casos mencionados anteriormente, el Responsable de Seguridad será el responsable de gestionar el riesgo. Para garantizar el buen funcionamiento del proceso de gestión de riesgos, es necesario llevar a cabo un seguimiento periódico de la ejecución del plan de tratamiento de riesgos. Esto implica monitorear el estado de cada uno de los controles, asegurando el compromiso con la mejora continua del sistema de gestión. También se debe verificar si se han proporcionado los recursos necesarios para implementar los controles y tratar adecuadamente los riesgos que la organización no puede asumir.

Una vez implementados los controles, al menos una vez al año, se realizará una reevaluación de riesgos para analizar la eficacia y el desempeño de los controles implementados, así como su influencia en las variables que influyen en el cálculo del riesgo. Esta reevaluación de riesgos también debe tener en cuenta cualquier cambio, incidente u otro evento que haya afectado las variables del cálculo de riesgo, así como cualquier previsión futura de situaciones que puedan afectar la seguridad de la información de la organización.

Después de finalizar la reevaluación de riesgos, se presentarán los resultados en una Revisión por la Dirección, donde se revisarán los riesgos residuales, en caso de existir. Estos riesgos residuales deberán ser aprobados por el Responsable del Proceso en conjunto con el Responsable del riesgo en cuestión. Los resultados de la reevaluación servirán como información de entrada para la toma de decisiones, como establecer objetivos de seguridad, definir cambios en el nivel de riesgo aceptable o asumible, o determinar la estrategia de seguridad de la información a seguir por parte de la organización.

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad de la Información es el resultado de la integración de las políticas de seguridad de TEAM2GO según ENS e ISO 27001. La finalidad es establecer un marco común y coherente que aborde la seguridad de la información en todas sus dimensiones y asegure la protección adecuada de los activos de información de la organización.

Esta integración abarca políticas relacionadas con aspectos como la gestión de riesgos, la protección de datos personales, la seguridad de los sistemas y redes, la continuidad del negocio, la seguridad física, entre otros. Al unificar estas políticas, se busca garantizar una visión holística de la seguridad de la información y promover la aplicación de medidas y controles coherentes en toda la organización.

La Política de Seguridad de la Información establece los principios, objetivos y responsabilidades en materia de seguridad de la información, y proporciona una base sólida para la implementación de medidas de seguridad adecuadas. Asimismo, sirve como referencia para la toma de decisiones y la asignación de recursos en relación con la seguridad de la información.

Al integrar las políticas de seguridad, TEAM2GO busca asegurar una gestión eficaz y eficiente de la seguridad de la información, protegiendo los activos de información frente a amenazas y riesgos, y cumpliendo con los requisitos legales y normativos aplicables. Además, se fomenta la concienciación y el compromiso de todos los miembros de la organización en la protección de la información y la promoción de buenas prácticas de seguridad.

La implementación de esta Política se llevará a cabo a través de la normativa de seguridad, que contendrá la definición detallada de los aspectos específicos relacionados con la seguridad de la información. Esta normativa será accesible para todos los miembros de la organización que necesiten conocerla, especialmente aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La Política de Seguridad de la Información estará disponibles para su consulta en la página web corporativa de TEAM2GO. Además, se pondrá a disposición del personal interno a través de la carpeta compartida de SharePoint, junto con la normativa de seguridad, asegurando así que todos los miembros de la organización tengan acceso a esta información clave.

La disponibilidad de la Política y la normativa de seguridad en formatos accesibles facilitará su consulta y garantizará que los empleados estén informados sobre las medidas y los procedimientos establecidos para mantener la seguridad de la información. Esto fomentará una cultura de seguridad sólida en la organización y promoverá el cumplimiento de las políticas y las mejores prácticas en materia de seguridad de la información.

El Responsable de Seguridad es el responsable directo del mantenimiento de esta política, prestando consejo y guía para su implementación y correcciones ante desviaciones en su cumplimiento.

12. RESOLUCIÓN DE CONFLICTOS.

En caso de que surja algún conflicto entre los diferentes responsables que forman parte de la estructura organizativa de la Política de Seguridad de la Información, se establece que la decisión final será tomada por el Comité de Seguridad.

El mecanismo de coordinación y resolución de conflictos se basará en la discusión y el análisis de las diferentes perspectivas y argumentos presentados por los responsables involucrados. El Comité evaluará los aspectos relevantes, analizará las implicaciones de las decisiones y buscará alcanzar un consenso en la resolución del conflicto.

En última instancia, la decisión del Comité será vinculante y prevalecerá sobre cualquier discrepancia o conflicto existente entre los responsables. Esto asegura una autoridad centralizada y un enfoque coherente en la toma de decisiones relacionadas con la seguridad de

la información, evitando posibles desavenencias y garantizando la aplicación uniforme de la Política de Seguridad en toda la organización, mediante:

- Análisis de la situación
- Identificar el origen del conflicto
- Identificar todos los implicados
- Identificar la opinión de los implicados
- Definir un objetivo
- Proponer posibles soluciones
- Elegir una propuesta
- Aplicar la solución elegida
- Evaluar el resultado
- Si el conflicto se ha solucionado: Lecciones aprendidas para que el conflicto no vuelva a aparecer en el futuro.
- Si el conflicto NO se ha solucionado: En este caso, volver a analizar el resto de las alternativas propuestas que se descartaron. y con la experiencia de haber intentado solucionar el conflicto una vez, elegir la solución correcta con mayor garantía de éxito.

13. OBLIGACIONES DEL PERSONAL

En TEAM2GO, se establece que todo el personal involucrado en el alcance del sistema de seguridad de la información tiene la obligación de conocer y cumplir la Política de Seguridad de la Información y la Normativa de Seguridad. Es responsabilidad del Comité de Seguridad asegurarse de que la información llegue a todos los afectados y disponer los medios necesarios para ello.

Con el objetivo de promover la concienciación y el cumplimiento de la Política de Seguridad de la Información, se llevarán a cabo actividades formativas específicas. Estas actividades estarán orientadas a la capacitación de los empleados involucrados en el sistema. Se prestará especial atención a la formación de los nuevos empleados, así como a la difusión de la Política de Seguridad y su desarrollo normativo entre todos los empleados.

Las personas con responsabilidad en el uso, operación o administración de sistemas de Tecnologías de la Información y Comunicación (TIC) recibirán formación adecuada para el manejo seguro de los sistemas en la medida en que lo necesiten para desempeñar sus funciones. Esta formación será obligatoria antes de asumir cualquier responsabilidad, ya sea en el caso de una primera asignación, un cambio de puesto de trabajo o una modificación en las responsabilidades dentro del mismo.

De esta manera, se busca garantizar que todo el personal esté debidamente informado y capacitado en cuanto a las medidas de seguridad de la información, promoviendo un ambiente de trabajo seguro y fomentando una cultura de seguridad.

14. TERCERAS PARTES

Cuando TEAM2GO preste servicios o maneje información de terceros, se les informará sobre esta Política de Seguridad de la Información y se establecerán canales de comunicación y coordinación con los respectivos Comités de Seguridad. Además, se establecerán procedimientos de actuación para reaccionar ante incidentes de seguridad.

En el caso de que utilice servicios de terceros o comparta información con terceros, también se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad correspondiente a dichos servicios o información. Estas terceras partes estarán sujetas a las obligaciones establecidas en la normativa y podrán desarrollar sus propios procedimientos operativos para cumplirla.

Se establecerán procedimientos específicos para el reporte y la resolución de incidencias relacionadas con terceros. Asimismo, se garantizará que el personal de terceros esté debidamente consciente de las medidas de seguridad, al menos al mismo nivel que se establece en esta Política.

En caso de que alguna parte de la Política no pueda ser cumplida por una tercera parte, como se menciona anteriormente, se requerirá un informe del Responsable de Seguridad que identifique los riesgos involucrados y la manera de abordarlos. Antes de proceder, este informe deberá ser aprobado por los responsables de la información y los servicios afectados.

De esta manera, se busca asegurar que tanto los proveedores de servicios como aquellos con quienes se comparte información cumplan con los requisitos de seguridad establecidos, y se establecen los mecanismos adecuados para garantizar la colaboración, el reporte y la resolución de incidentes de seguridad.