POLÍTICA DE SEGURIDAD

TALENTOMOBILE

Contenido

1. Introducción

TALENTO MOBILE es una empresa tecnológica global. Nos definen nuestro espíritu innovador, nuestras ganas de hacer las cosas bien hechas y nuestra experiencia en proyectos y soluciones digitales.

Aunque ya hemos superado los 5 años de vida, nos gusta vivir cada día como si fuera el primero. Esto nos hace sentir más libres, potenciar la innovación y el flujo de ideas y lo más importante, garantizar que nuestro equipo esté lo más a gusto posible, lo que es directamente proporcional a los resultados que los clientes obtienen de nuestros desarrollos y proyectos.

Los valores que describen a TALENTO MOBILE son los siguientes:

- Simplicidad: Lo hacemos simple y efectivo
- Agilidad: Usamos metodologías ágiles manteniendo la calidad
- Inspiración: Nos importa el valor que aportan los detalles
- Motivación: Nos apasiona nuestro trabajo y se nota

Nuestras soluciones se aplican a la industria Fintech e Insurtech:

- ID Verification: Herramienta de verificación de identidad inteligente y automatizada (OCR). Extrae y valida de manera remota información de **documentos de identificación personal** para la apertura de cuentas o darse de alta como nuevo cliente.
- Liveness & Biometría Facial: Software para validación de usuarios de forma remota, comparando rasgos biométricos en video y fotografías para **evitar la suplantación de identidad**.
- Digital Onboarding: Solución unificada de ID Verification y Liveness & Biometría Facial en un solo producto de fácil integración en aplicaciones. Todo lo necesario para la **creación de clientes verificados de forma remota.** La primera plataforma de onboarding digital low code del mercado.
- Clicquote (Chatbot): Nuestra solución de Chatbot end-to-end para procesos de **contratación de productos y servicios.** Podrás ofrecer una experiencia de usuario única en cualquier canal digital Web, Mobile, Whatsapp en tiempo récord.
- Perito Digital: Nuestra solución de **visión por computación para detección de vehículos, siniestros y matrículas**, que permiten acelerar y digitalizar los procesos de peritaje y contratación de seguros.
- Videoanalytics: Análisis en video y en tiempo real para la **identificación biométrica múltiple** y **detección de objetos** como mascarillas o armas, ayudando a crear espacios abiertos más seguros.

Nuestros servicios se adaptan a las necesidades de cada proyecto con servicios personalizados:

- UX/UI Design (Experiencia de Usuario): Diseño **centrado en el usuario** mediante técnicas de investigación cuantitativas y cualitativas, para ofrecer soluciones que realmente impacten en nuestros usuarios.
- Desarrollo Personalizado (Desarrollo para Crear Impacto): Ayudamos a nuestros clientes a descubrir y aprovechar las innovaciones tecnológicas. Proporcionando experiencia en todas las fases de vida de **desarrollo del producto** o **servicio digital**.
- Programa Kit Digital (Ayuda para la digitalización de Pymes y Autónomos): Desde el gobierno de España se pone en marcha el programa especial **Acelera Pyme**, con el que Talento Mobile colabora como proveedor de servicios y transformación digital.

2. Marco Normativo

El marco normativo en materia de seguridad de la información en el que TALENTO MOBILE desarrolla su actividad, esencialmente, es el siguiente:

- 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.
- Real Decreto 951/2015, de 23 de octubre, de modificación 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.
- Guía de Seguridad CCN-STIC 821: Normas de Seguridad.
- Guía de Seguridad CCN-STIC 804: Guía de Implantación.
- RGPD (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.
- Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de derechos digitales.
- UNE ISO/IEC 27001:2014 Sistemas de gestión de seguridad de la información. Requisitos

3. Alcance

El alcance de la presente política se define de la siguiente forma:

Sistema de gestión de la seguridad de la información utilizado en: Desarrollo, Mantenimiento, e Implantación de los Servicios Informáticos en aplicaciones móviles, y web. Para grandes y pequeñas empresas

TALENTO MOBILE se apoya en sus sistemas TIC para alcanzar sus objetivos. Estos sistemas deben ser 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, o de los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

3.1 Misión y objetivos

Se desarrollarán, al menos, los siguientes objetivos:

a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.

b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.

c) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
d) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
f) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.
g) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.
h) Gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
i) Gestión de la continuidad implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

3.2 Prevención

Para defenderse de las amenazas, los departamentos deben aplicar las medidas mínimas de seguridad, así como cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en las ofertas, y en pliegos de licitación para proyectos de TIC. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

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

- Autorizar los sistemas antes de entrar en operación.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.3 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continuada para detectar anomalías en la prestación de los servicios y actuar en consecuencia.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.4 Respuesta

TALENTO MOBILE y sus departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

3.5 Recuperación

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

4. Organización de la seguridad

La implantación de la Política de Seguridad en TALENTO MOBILE requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

Como parte de la Política de Seguridad de la Información, los principales roles quedan identificados y detallados del modo siguiente:

- Responsable de Seguridad: César Castillo

- Responsable de la Información: Karla
- responsable del Servicio: César Castillo
- Responsable de Sistemas: Javier Román
- DPO: Datages Consulting

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

4.1 Comités: Funciones y Responsabilidades

La Seguridad de la Información es una responsabilidad organizativa que es compartida con la dirección de TALENTO MOBILE. En consecuencia, éste promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vía definida y de apoyo a las iniciativas de seguridad.

Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas y por un presidente que será responsable último de las decisiones adoptadas y que dirigirá las reuniones del Comité de Seguridad, informando, proponiendo y coordinando las actividades y decisiones.

Esta función de presidente inicialmente recae en el responsable de Seguridad.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión de la Política de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación a la Alta dirección.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dicho activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
- Principales incidencias en la Seguridad de la Información.
- Elaboración y actualización de planes de continuidad.
- Cumplimiento y difusión de las Políticas de Seguridad.

4.2 Responsable de Seguridad

Es el responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos en los objetivos estratégicos.

Las funciones del responsable de Seguridad de la Información son las siguientes:

- Asistencia al presidente del Comité de Seguridad en la elaboración del orden del día de las sesiones a celebrar.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de TALENTO MOBILE.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
- La estrategia de seguridad de la información definida por el Comité de Seguridad.
- Las normas y procedimientos contenidos en la Política de Seguridad de la Información de TALENTO MOBILE y normativa de desarrollo.
- Supervisar los incidentes de seguridad producidos en TALENTO MOBILE.
- Difundir en TALENTO MOBILE las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como las funciones y obligaciones en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de TALENTO MOBILE.

4.3 Responsable de Sistemas

Es responsable de asegurar la ejecución de medidas para protección de los activos y servicios de los sistemas de información que soportan la actividad de TALENTO MOBILE.

Las funciones del responsable de Sistemas son las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante el ciclo de vida, especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de TALENTO MOBILE conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en TALENTO MOBILE.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- El responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de la Seguridad, antes de ser ejecutada.

4.4 Responsable de la Información

Es responsable de asegurar la ejecución de medidas para protección de la información, propia o de los clientes, que se utilizan en la actividad de TALENTO MOBILE.

Las funciones del responsable de la Información son las siguientes:

- Establece los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación sobre protección de datos.
- Determina los niveles de seguridad de la información.

4.5 Responsable del Desarrollo del servicio

Es responsable de asegurar la utilización de medidas de seguridad en los servicios y proyectos desarrollados por los equipos de TALENTO MOBILE.

Las funciones del responsable del desarrollo del servicio son las siguientes:

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de los servicios prestados relacionados con el desarrollo.

- Describe los requisitos de Desarrollo
- Vela por el cumplimiento de las metodologías de desarrollo de TALENTO MOBILE, así como de los requisitos de seguridad del producto
- Determina los niveles de seguridad del servicio.

4.6 Procedimientos de Designación

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

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo con la Ley 11/2007 designará al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

4.7 Difusión, actualización y revisión de la 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 el Órgano de Gobierno y será difundida para que la conozcan todas las partes afectadas.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos.

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.

5. Datos de carácter personal

La Política de Protección de Datos y el Manual de Medidas de Seguridad al que tendrán acceso sólo las personas autorizadas, identifican los responsables de los tratamientos de datos personales, detallan estos tratamientos y exponen las medidas de seguridad correspondientes.

Todos los sistemas de información de TALENTO MOBILE se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el Documento de Seguridad.

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos (GDPR), y la nueva LOPD, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.
Se aplicará, asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

6. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar 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

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.
El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal. La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

7. Obligaciones del personal

Todos los miembros de TALENTO MOBILE 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 disponer los medios necesarios para que la información llegue a los afectados.
Todos los miembros de TALENTO MOBILE atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año.

Se establecerá un programa de concienciación continua para atender a todos los miembros de TALENTO MOBILE, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinares que procedan, sin prejuicio de las responsabilidades legales correspondientes.

8. Terceras partes

Cuando TALENTO MOBILE 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.

9. Aprobación del Documento

Documento: Política de Seguridad

Estado: Aprobado

Firmado:

César Castillo


TALENTOMOBILE