okticket

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD

1. Contenido

2. Principios de seguridad

Los principios de seguridad en los que se sustenta esta política son:

- Análisis y Gestión del Riesgo. Se realizan aquellos procesos necesarios de análisis y gestión de riesgos que permitan determinar, reducir, eliminar, evitar o asumir los riesgos asociados al Sistema.
- Mínima Funcionalidad. Solo están disponibles las funciones, protocolos y servicios necesarios para cumplir con el requisito operacional o funcional del sistema.
- Mínimo Privilegio. Los usuarios de los sistemas que manejen información confidencial solo dispondrán de los privilegios y autorizaciones que se requieran para la realización de las obligaciones asociadas a su puesto de trabajo.
- Verificación de la Seguridad. La aplicación de estos principios y su consecuente implementación en medidas de protección deberá ser inicial y periódicamente verificada.
- Monitorización, Vigilancia y Respuesta a Incidentes. Se dispone de una capacidad de vigilancia y respuesta que permita la reacción oportuna y adecuada a cualquier incidente de seguridad.

3. Alcance

Esta política se aplica a todos los sistemas TIC de OKTICKET y por extensión a todo el personal de la organización conforme al Esquema Nacional de Seguridad.

4. Misión

OKTICKET es una startup enmarcada en el sector SaaS Fintech cuya misión es proporcionar una solución de digitalización y gestión de los pagos y gastos de viajes de negocios, con foco en: la mejor experiencia usuario, la flexibilidad funcional, la integración avanzada con el ecosistema de software del cliente, la optimización del proceso en todas sus etapas, así como el control y trazabilidad de la información.

Nuestro propósito fundamental es convertir nuestra solución en el estándar de facto de la gestión de gastos de viaje profesionales. Siempre desde la perspectiva que establecen nuestros valores corporativos:

- El rigor profesional orientado a objetivos
- El compromiso con la organización
- La comunicación orientada al cliente y,
- El trabajo en equipo

5. Política de seguridad

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.

Se tienen en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información: El eslabón más débil de la cadena es el elemento humano por lo que se prestará máxima atención a las acciones de concienciación y formación. Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

b) Gestión de la seguridad basada en los análisis y gestión de los riesgos de manera continua y actualizada.

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- 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.

c) Prevención para reducir la probabilidad de materialización de las amenazas, detección de ciberincidentes: Medidas de respuesta con el fin de recuperar la información y los servicios y conservación; con el fin de minimizar las vulnerabilidades y lograr que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que se maneja o a los servicios que presta.

d) Existencia de líneas de defensa (con medidas organizativas, físicas y lógicas): constituida por múltiples capas de seguridad y prevención ante otros sistemas de información interconectados. Se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

e) Integridad y actualización del sistema: OKTICKET ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal. Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

f) Gestión de personal y profesionalidad: Todos los empleados deberán recibir información, formación y concienciación en materia de seguridad. Se establecerá un programa de concienciación continua. 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.

g) Autorización y control de los accesos: OKTICKET implementará mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

h) Protección de las instalaciones: OKTICKET implementará mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

i) Adquisición de productos de seguridad y contratación de servicios de seguridad: Cuando OKTICKET 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 establecen procedimientos específicos de reporte y resolución de incidencias. Se garantiza que el personal de terceros está adecuadamente concienciado en materia de seguridad al menos al mismo nivel que el establecido en esta Política. OKTICKET tendrá en cuenta, para la adquisición de productos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad. Se siguen las recomendaciones establecidas en la Guía de Seguridad de las TIC CCN-STIC 105, Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación.

j) Prevención ante otros sistemas de información interconectados: En caso de interconexión entre sistemas con terceros, siempre se deberá cumplir que éste disponga de medidas de seguridad dedicadas y adecuadas al grado de interconexión y el tipo de información que sea tratada. Siempre se realizarán mediante conexiones seguras cifradas Será preferentemente a considerar la disponibilidad de certificado de conformidad con ENS.

k) Diferenciación de responsabilidades: Presentando entre las mismas el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos

l) Protección de la información almacenada y en tránsito y continuidad de la actividad: OKTICKET implementará mecanismos para proteger la información almacenada o en tránsito, especialmente cuando ésta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.). Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo. Se desarrollarán procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de OKTICKET. De igual modo, se implementarán mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren los documentos, para garantizar que toda información en soporte no electrónico relacionada estará protegida con el mismo grado de seguridad que la electrónica.

m) Registro de actividad y detección de código dañino: OKTICKET habilitará registros de la actividad de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

n) Incidentes de seguridad: OKTICKET implementará un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, OKTICKET implementará las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

OKTICKET establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un 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. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- Para garantizar la disponibilidad de los servicios, OKTICKET dispondrá de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

o) Mejora continua del proceso de seguridad: El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información. OKTICKET habilitará registros de la actividad de los usuarios, reteniendo la información necesaria para monitorización.

OKTICKET habilitará registros de la actividad de los usuarios, reteniendo la información necesaria para monitorización.

El alcance de certificación es: Los sistemas de información que estén afectados por las medidas y controles de seguridad del Esquema Nacional de Seguridad que son los relacionados con las actividades de diseño, desarrollo, implantación y mantenimiento de soluciones software para la gestión de gastos empresariales.

Se ha determinado que la categoría del sistema de OKTICKET es MEDIA.

6. Marco Normativo

OKTICKET mantiene implantado un procedimiento para la identificación de requisitos legales, normativos y reglamentarios, así como para la evaluación de su cumplimiento. Por medio de este procedimiento se determinan medios para la identificación de nuevos requisitos o cambios en los requisitos ya identificados, y mecanismos para evaluarlos y establecer recursos para asegurar el cumplimiento de las obligaciones aplicables.

7. Organización e implantación del proceso de seguridad

La seguridad del sistema de información de OKTICKET está atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.

El personal de OKTICKET que trabaja dentro del alcance del ENS recibe la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios.

OKTICKET exige de manera objetiva y no discriminatoria que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

La organización de la seguridad de la información se define en un procedimiento interno documentado de responsabilidades y funciones, donde se ha tenido en cuenta la Guía de Seguridad de las TIC CCN-STIC 801 Responsabilidades y Funciones de marzo de 2019 del CCN.

Las designaciones de la tabla anterior serán revisadas en el ciclo de dos años, iniciándose el cómputo del plazo en el proceso de declaración o certificación de conformidad del sistema con respecto al Real Decreto 311/2022. La seguridad del sistema será revisada por los responsables designados de conformidad a los requisitos, la política y los procedimientos aprobados Estas designaciones son recogidas formalmente en un acta de reunión. Estos responsables recibirán obligatoriamente la formación necesaria para el desarrollo seguro en materia de gestión de la información.

El esquema propuesto diferencia los grandes bloques de responsabilidad establecidos en el Real Decreto 311/2022 (Dirección, supervisión y operación), teniendo en cuenta la reducida estructura de OKTICKET:

- El responsable de la Información; esta responsabilidad recae en el Comité de Seguridad de OKTICKET.

  Tiene la responsabilidad última del uso que se haga de una cierta información y por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información). Establece los requisitos de la información en materia de seguridad.

- El responsable del Servicio es el Comité de Seguridad de OKTICKET. Establece los requisitos de la información del servicio del que es responsable.

- El responsable del Sistema: es el Responsable de Sistemas de OKTICKET; es el responsable de operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo su correcto funcionamiento e informando al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. Lleva a cabo las funciones del administrador de la seguridad del sistema.

- El responsable de Seguridad: es el encargado de mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de

responsabilidad, de acuerdo a lo establecido en esta política de seguridad de la información. Promueve formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.

• Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello, se encargará de:

- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.

- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.

- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.

- Elaborar la normativa de Seguridad de la Información para su aprobación.

- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.

- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y, en particular, en materia de protección de datos de carácter personal.

- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la Información.

Los mecanismos de coordinación entre las responsabilidades establecidas se establecen en los procedimientos documentados del Sistema de Gestión de la Seguridad de la Información. OKTICKET establece, en plena observancia de los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, que los conflictos entre distintos elementos de la organización serán resueltos por el superior jerárquico.

8. Desarrollo de la Política de Seguridad de la Información

El sistema de información de OKTICKET está diseñado y configurado de forma que se garantiza la seguridad por defecto:

a) El sistema proporciona la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad son las mínimas necesarias y se asegura que sólo son accesibles por las personas, o desde emplazamientos o equipos autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) Se eliminan mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema es sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Los aspectos que afectan a la protección de las instalaciones e infraestructuras de la sede física de OKTICKET sita en (Zona Intra del Parque Científico Tecnológico de Gijón, Avenida del Jardín Botánico, 1345-Edificio 1, Oficinas 4-5; 33203 de Gijón, Principado de Asturias), así como los aspectos de prevención ante otros sistemas de información interconectados, están

subcontratados a un tercero, estando definidos los requisitos por contrato. (El tercero debe estar certificado en la misma categoría del ENS que se quiera obtener)

En el sistema de información de OKTICKET los soportes de información en tránsito requerirán de un especial cuidado debido a la naturaleza de los mismos. Deberán almacenarse en lugares seguros, evitando el acceso a los mismos por parte de personas no autorizadas siendo recomendable evitar su empleo en lugares públicos donde la información pudiese estar visible para un tercero o bien donde una sustracción del soporte resultase fácil tales como emplazamientos al aire libre que permitan una rápida huida con el soporte sustraído Estos soportes se encontrarán siempre protegidos mediante medidas criptográficos a fin de minimizar el impacto en caso de pérdida o robo. En caso de que el personal al cargo de este soporte pierda el control sobre del mismo bien sea por robo o pérdida, deberá comunicarlo al responsable de seguridad con la mayor premura.

Se registran las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

9. Obligaciones del Personal

Todo el personal de OKTICKET tiene la obligación de conocer y cumplir esta política de seguridad de la información y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal de OKTICKET asiste a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establece un programa de concienciación continua para atender a todos los miembros de OKTICKET, 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.

Las obligaciones del personal están establecidas en la normativa de seguridad. Los mecanismos de faltas y sanciones están descritos en un apartado específico.

10. Terceras Partes

Cuando OKTICKET 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 establecen procedimientos específicos de reporte y resolución de incidencias. Se garantiza que el personal de terceros está adecuadamente concienciado en materia de seguridad al menos al mismo nivel que el establecido en esta Política.

En caso de interconexión entre sistemas con terceros, siempre se deberá cumplir que éste disponga de medidas de seguridad dedicadas y adecuadas al grado de interconexión y el tipo de información que sea tratada. Siempre se realizarán mediante conexiones seguras cifradas Será preferentemente a considerar la disponibilidad de certificado de conformidad con ENS.

OKTICKET tendrá en cuenta, para la adquisición de productos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad. Se siguen las recomendaciones establecidas en la Guía de Seguridad de las TIC CCN-STIC 105, Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación.

11. Control de los Documentos

Los documentos del Sistema de Gestión de la Seguridad de la Información aprobados se conservan en la carpeta en formato electrónico en la estructura de carpetas definida. Los documentos son revisados por el Responsable de Seguridad y aprobados por el Comité de Seguridad, utilizando para ello su firma digital.

El documento declaración de aplicabilidad, estará firmado por el Responsable de Seguridad.

12. Tratamiento de los Datos Personales

El tratamiento de datos personales implica ciertos riesgos que deben ser gestionados adecuadamente para garantizar la seguridad y privacidad de la información. Es crucial implementar medidas de seguridad adecuadas, realizar evaluaciones de riesgos de manera

periódica, proporcionar formación continua al personal y estar en conformidad con la normativa de protección de datos vigente.

En Gijón, a 1 de julio de 2024

La dirección okticket