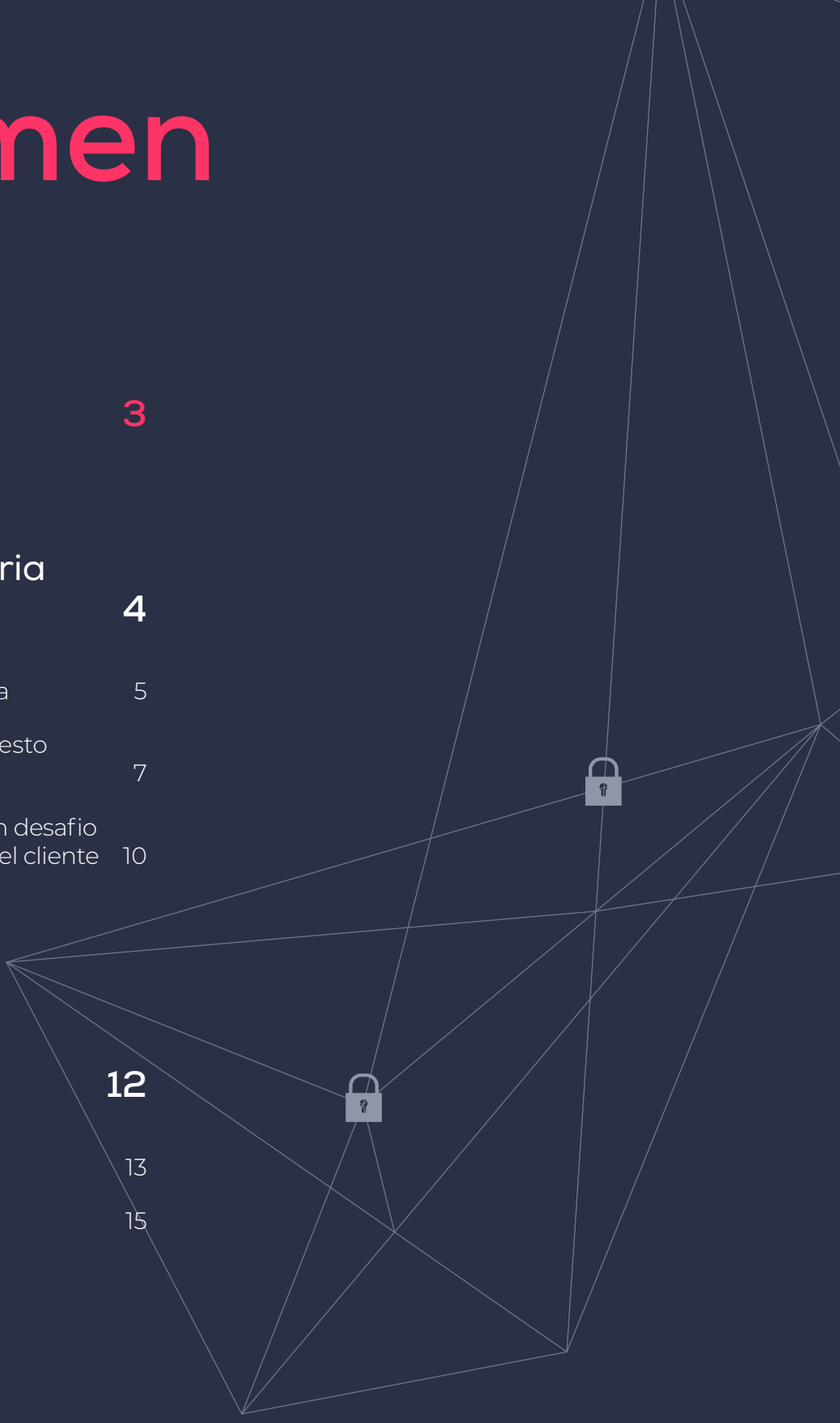
Ciberseguridad en el centro de contacto:

¿cuáles son los riesgos y cómo *protegerse con el modelo SaaS?*

odigo | aws

Resumen



Introducción

Cada vez más empresas optan por equiparse con una solución de contact center as a Service (CCaaS) para aumentar la eficiencia de sus agentes y optimizar la experiencia del cliente. Gracias a la omnicanalidad, la automatización y el uso de la inteligencia artificial (IA). Según un informe publicado por Allied Market Research, se espera que el mercado mundial de CCaaS, valorado en 4.300 millones de dólares en 2021, alcance los 19.800 millones de dólares en 2031. Esta transformación de los centros de contacto, acelerada por la crisis de la Covid-19, en la actualidad acompaña el cambio hacia el teletrabajo y genera nuevos casos de usos.

Sin embargo, el auge del CCaaS, a menudo utilizado por equipos geográficamente dispersos, plantea algunas cuestiones relacionadas con la ciberseguridad. En particular, la seguridad de los datos de los clientes se ha convertido en un tema al que las empresas están prestando mucha atención y plantea el doble reto de garantizar la accesibilidad y la confidencialidad de estos datos.

Al igual que cualquier tecnología basada en la nube que permite a los usuarios acceder a los sistemas de información (SI) y a los datos de las organizaciones desde Internet, el CCaaS aumenta la superficie de exposición a los riesgos del CiberContact Center. Esto conlleva un aumento de la necesidad de seguridad y un cambio de paradigma con el paso de un modelo perimetral (con una barrera de defensa única) a un modelo de «defensa en profundidad», que supone asegurar cada subconjunto de los SI superponiendo varios mecanismos de protección. Por ejemplo, en esta lógica se inscribe el enfoque Zero Trust, basado en particular en los controles de acceso a los recursos regulares y granulares.

¿Cuáles son los principales riesgos en materia de ciberseguridad? ¿Cómo puede proteger mejor su contact center y los datos de sus clientes? ¿Y cuáles son los medios implementados por Odigo, líder mundial en CCaaS, que ha establecido una sólida colaboración con el proveedor de servicios en la nube Amazon Web Services (AWS) en materia de gestión de riesgos? En este libro blanco encontrará todas las respuestas.

1 ERA Parte Los riesgos en materia de Ciberseguridad

I. Situación de la ciberamenaza

En su «Panorama de la cybermenace» («Panorama de la ciberamenaza»), la agencia francesa de seguridad de los sistemas de información (Agence nationale de la sécurité des systèmes d'information, ANSSI) hace un balance de las tendencias que marcaron el año 2022. El informe muestra que el nivel general de amenaza observado en 2021 se mantuvo en 2022 y, además, se produjo un desplazamiento a entidades menos protegidas. Los actores maliciosos, advierte la ANSSI, continúan perfeccionando sus capacidades. Esto se traduce, en particular, en una «segmentación periférica» que ofrece un acceso más discreto y persistente a los sistemas y redes de las entidades públicas y privadas. Este enfoque no solo se centra en los equipos periféricos, sino también en los actores que gravitan alrededor de las víctimas, como socios, proveedores de servicios, subcontratistas, etc.

Lo mismo constata ENISA, que señala que los grupos maliciosos se están especializando cada vez más en técnicas de ataque a la cadena de suministro y a los proveedores de servicios gestionados (MSP). Los ataques contra los datos se encuentran entre las ocho principales amenazas identificadas por la Agencia de Seguridad Cibernética de la Unión Europea realizadas con fines de lucro (más comúnmente), espionaje y desestabilización política.

Independientemente de las motivaciones de los atacantes y de si su contact center es el objetivo principal o un vector de ataque indirecto, cualquier incidente de seguridad conlleva peligros potenciales para su organización, sus socios y sus clientes. Estos son los principales riesgos cibernéticos a los que podría enfrentarse:

- Pérdidas financieras, directas e indirectas, vinculadas a la pérdida de explotación, de material, al pago de un rescate o de una multa, etc.
- Interrupción de la actividad, debido a la paralización y posterior puesta en marcha de los sistemas informáticos.
- Daño a su reputación.
- Robo, divulgación o pérdida de datos.
- Creación de brechas en su sistema de información.

La buena noticia es que las organizaciones también están fortaleciendo sus capacidades basándose en nuevos enfoques (como el Zero Trust), nuevas herramientas de detección y protección y la experiencia de proveedores externos.

«Gracias a la nube y al modelo SaaS, las empresas pueden delegar parte de la gestión de riesgos en actores con competencias y recursos mucho mayores en este ámbito. Así, se benefician del uso de soluciones industrializadas disponibles bajo demanda, mucho más fáciles de instalar, configurar y mantener.»

Matthieu Bouthors
Security Solutions Architect de AWS

II. ¿A qué amenazas está expuesto su centro de contacto?

Los contact centers, on-premise o no en la nube, están en el punto de mira de los actores maliciosos, que pueden actuar a través del teléfono, IVR o Internet con el fin de robar dinero o información sensible sobre las empresas o sus clientes. Las llamadas fraudulentas, los ataques de denegación de servicio telefónico o el phishing son algunos de los ataques a los que debe prestar especial atención.

Llamadas fraudulentas

Las llamadas fraudulentas forman parte de los ataques más comunes contra los centros de contacto. Los actores maliciosos emplean dos tipos de ataques:

- La piratería de equipos (como el IP PABX)

- El spoofing y la suplantación de identidad con la ayuda de herramientas que permiten suplantar números de teléfono, direcciones IP e identificadores de llamadas, o técnicas de ingeniería social para hacerse pasar por clientes o empleados reales.

El fraude de las llamadas de larga distancia (toll fraud) es un problema mundial que cuesta a las organizaciones millones de euros al año. Se produce cuando un usuario no autorizado accede al sistema telefónico del contact center (normalmente infiltrándose en el sistema IVR) para realizar un gran número de llamadas de larga distancia, lo cual produce facturas exorbitantes. Este tipo de fraude también puede saturar las líneas telefónicas de la víctima, movilizando sus recursos informáticos y humanos y creando las condiciones para una denegación de servicio telefónico (TDoS).

Los ciberdelincuentes pueden interactuar con los agentes del contact center utilizando datos robados, como datos personales (el nombre de un cliente real, su número de seguridad social, su fecha de nacimiento, etc.) o un número de tarjeta de crédito, que eventualmente habrán probado realizando un reconocimiento en el IVR. Su intención será obtener más información sobre el usuario legítimo, convencer al agente para que le dé acceso a su cuenta o activar

ciertas acciones, como comprar productos, transferir dinero o modificar los datos de conexión. También podrían intentar obtener información sobre la organización y el funcionamiento interno de la empresa.

En la actualidad, eludir y detectar estas estafas es más complejo debido al uso de llamadas automáticas y el empleo emergente de herramientas basadas en IA.

Deepfakes: ¿una nueva amenaza?

En los últimos años, los espectaculares avances de la IA han propiciado la aparición de tecnologías que permiten producir contenidos de audio ficticios ultrarrealistas. Aunque estas herramientas cada vez son más sofisticadas, el acceso a ellas también es cada vez más fácil .

Varios equipos de investigación han logrado crear clones vocales muy convincentes con la ayuda de los llamados modelos «generativos» con solo unos segundos de grabación de personas reales. Aunque esta tecnología aporta perspectivas prometedoras, ya se está utilizando con fines maliciosos. Por ejemplo, se puede utilizar para hacer una llamada fraudulenta para interactuar con los IVR, e incluso engañar a agentes humanos, reproduciendo la voz humana y manipulando el contenido de audio. Los deepfakes, en particular, despiertan un interés creciente entre los especialistas en seguridad y el público en general.

Los “deepfakes” son contenidos ficticios especialmente creíbles (imágenes, vídeos o grabaciones de audio) elaborados con la ayuda de técnicas de IA y de aprendizaje automático a partir de un material fuente. El método más popular se basa en redes antagonistas generativas (GANs), que son arquitecturas compuestas por dos redes neuronales artificiales que compiten entre sí con el objetivo de lograr falsificaciones que sean lo más realistas posibles (piense en la dinámica entre el falsificador y el detective). En el caso de los deepfakes de audio, el proceso permite

capturar, analizar y reproducir las características de la voz y la forma de hablar a partir de muestras vocales (extractos de discursos, conversaciones telefónicas, etc.).

Los deepfakes de audio son motivo de preocupación para los contact centers, ya que podrían facilitar los ataques basados en ingeniería social, como el phishing de voz, porque no se pueden detectar las imitaciones y las manipulaciones. Aunque algunos deepfakes son increíbles, los especialistas aclaran que no siempre producen resultados perfectos. Algunos escenarios de ataque, que incluyen interacciones en tiempo real, requieren importantes capacidades informáticas y un hardware de origen potente tanto en cantidad como en calidad.

Ataques de denegación de servicio telefónico

Los ataques de denegación de servicio telefónico (TDoS) suponen otra amenaza real para los centros de contacto. Su objetivo es hacer que un sistema telefónico deje de estar disponible para los usuarios legítimos al agotar todos los recursos para que no se puedan recibir ni realizar llamadas. Los ciberdelincuentes recurren a ellos, en ocasiones, para obtener dinero con extorsiones como parte de una nota de rescate; también lo hacen los hacktivistas para acosar u obstaculizar la actividad de su objetivo.

«La elasticidad en la nube, es decir, la capacidad de adaptar los recursos informáticos a las necesidades rápidamente, y la mayor posibilidad de automatizar el suministro de estos recursos, permiten ser menos sensibles o gestionar mejor este tipo de ataques.»

Matthieu Bouthors
Security Solutions Architect de AWS

III. La privacidad de los datos: un desafío de cumplimiento y confianza del cliente

Los ataques descritos anteriormente pueden provocar una violación de datos (cualquier incidente de seguridad que ponga en riesgo la integridad, la confidencialidad o la disponibilidad de los datos), un peligro que es especialmente pernicioso. Según un estudio realizado por IBM Security, el 83 % de las empresas se han visto afectadas por este tipo de ataque en más de una ocasión. Más allá del impacto financiero que tienen, también hay que tener en cuenta el daño que producen en la reputación del objetivo y los perjuicios sufridos por sus empleados o clientes.

Según el último Verizon data breach investigation report (DBIR), publicado en 2022, los datos de autenticación y los datos personales son los dos tipos de datos más codiciados. Estos últimas representan una «fuente de ingresos inagotable» para los ciberdelincuentes, cuyas motivaciones, precisa el informe, son financieras en un 90 %. No solo se pueden utilizar para establecer un fraude financiero, sino que también se pueden revender en el mercado negro.

Así pues, la protección de los datos personales de los clientes representa un desafío importante para las empresas, que están obligadas por ley, como «responsables del tratamiento de los datos», a tomar las precauciones necesarias para garantizar su seguridad y confidencialidad. La cuestión es tanto más importante cuanto que los ciudadanos cada vez se preocupan más por la privacidad de datos —la confidencialidad de los datos—. Se ha convertido en una cuestión de confianza de los clientes. Según una encuesta de EY sobre la protección de la privacidad del consumidor realizada durante la pandemia de la Covid-19, el 63 % de los encuestados afirma que solo comparte sus datos con una organización cuando está seguro de que se recopilarán y almacenarán de forma segura. En este «nuevo panorama de la protección de datos personales», las empresas ya no pueden contentarse con reforzar únicamente sus propias defensas. También deben asegurarse de que sus proveedores de soluciones en la nube sean expertos en seguridad de datos.

En el contexto de las amenazas actuales, la cuestión no es si se va a producir un ataque cibernético o no, sino cuándo va a suceder. Sin embargo, si bien el aumento de los riesgos es inexorable, la vulnerabilidad y las consecuencias de los ataques no lo son. La implantación de una estrategia sólida y sostenible de gestión de riesgos en el contact center (que incluya la aplicación de una política estricta de control de privilegios) y el desarrollo de capacidades de detección y tratamiento de incidencias en coordinación con su proveedor de CCaaS ayudarán a minimizar el riesgo de ataques y el impacto en su organización.

2DA PARTE

Cómo optimizar la seguridad con el modelo CCaaS

I. Prácticas recomendadas

¡Todos somos responsables de la seguridad!

El modelo CCaaS consta de tres actores principales, que contribuyen a la seguridad de la plataforma y los datos alojados en la nube, de acuerdo con una serie de normas o regulaciones.

- El proveedor de alojamiento en la nube gestiona la seguridad de la nube. Se encarga de garantizar la protección de la infraestructura que ejecuta los servicios, la cual incluye software, red y servidores. Ofrece diferentes niveles de configuración de seguridad y proporciona servicios avanzados de seguridad y cumplimiento.

- El proveedor de servicios CCaaS gestiona la seguridad de la plataforma alojada en la nube. Se encarga de proporcionar actualizaciones y herramientas de gestión de datos para asegurar y proteger el software del centro de contacto al máximo.

Nota: *Los proveedores de servicios digitales en breve estarán sujetos a la nueva Directiva NIS (NIS2), que refuerza los requisitos de seguridad e introduce la obligación de enviar notificaciones sobre los incidentes.*

- Por último, el ordenante supervisa todos los aspectos de la seguridad del contact center y despliega los medios necesarios para proteger el acceso a los servicios y datos alojados en la nube (seguridad de los equipos de trabajo y móviles, política de acceso, formación y sensibilización de los usuarios, etc.). Como responsable del tratamiento de los datos de conformidad con el RGPD, debe implementar las medidas técnicas y organizativas necesarias para proteger los datos personales y garantizar que sus subcontratistas y proveedores también presenten las garantías suficientes.

Al elegir una solución de contact center de Odigo, estará beneficiándose de la experiencia combinada de nuestros equipos y de nuestro socio en la nube AWS, que se encarga de parte de la seguridad siguiendo un modelo de responsabilidad compartida.

Nuestras recomendaciones para gestionar los riesgos en un centro de contacto

Nuestro primer consejo es poner en marcha una política de gestión de identidades y acceso (IAM) sólida para evitar el a sus recursos por parte de usuarios no autorizados. Este enfoque consiste en implementar un conjunto de procesos y herramientas para gestionar las identidades digitales de sus usuarios y los permisos de acceso asociados (quién puede acceder a qué y durante cuánto tiempo). Muchas empresas eligen soluciones IAM en modo SaaS, ya que son más fáciles de implementar y administrar.

Nuestro segundo consejo es que se asegure de que su proveedor de soluciones CCaaS dispone de medios suficientes en materia de ciberseguridad y protección de datos. Para ello, compruebe que cuenta con certificaciones reconocidas y que cumple con las normas específicas de su sector de actividad. También puede realizar auditorías y pruebas para evaluar la seguridad de sus infraestructuras y soluciones, y su cumplimiento con respecto a su política de seguridad.

Por último, puede aprovechar su proyecto de migración a la nube para beneficiarse al máximo de las últimas innovaciones. Las soluciones SaaS le permiten acceder a nuevas capacidades para la ciberseguridad y la protección de datos, a la vez que controla los costes y la complejidad de una implementación on-premise.

II. La seguridad con Odigo

Estas capacidades incluyen la detección de vulnerabilidades con IA, la protección de las interacciones con sus clientes gracias a un IVR inteligente, el cifrado y la segmentación de los datos de sus clientes mediante el uso de técnicas avanzadas y el seguimiento de las actividades en tiempo real con herramientas de gestión de eventos e información de seguridad (SIEM).

Nuestro enfoque: control de riesgos y mejora continua

Odigo se adhiere al principio de «Security by Design», que implica integrar la seguridad desde el diseño de nuestros productos, y adopta un enfoque de seguridad basado en riesgos, detección de amenazas y evaluación de las necesidades. Estas necesidades pueden surgir, por ejemplo, como consecuencia de la aprobación de nuevas normas o regulaciones. La implementación del STIR/SHAKEN aporta una solución para luchar contra la suplantación de la identidad de las personas que llaman al centro de contacto, pero también conlleva riesgos, ya que introduce nuevos mecanismos, en este caso de certificación digital, en el proceso de entrega de productos.

Nuestro enfoque se basa en el análisis, la categorización y el tratamiento de los riesgos, e incluye análisis de sensibilidad, procesos de vigilancia permanente de amenazas y vulnerabilidades y medidas de protección contra spoofing y ataques DDoS. Se traduce en la implementación de acciones regulares para mejorar continuamente la seguridad: implementación de las prácticas recomendadas del sector, tareas de certificación, diseño de soluciones a medida para nuestros clientes en consonancia con su estrategia empresarial y las necesidades del negocio previamente identificadas, y enriquecimiento constante de nuestro catálogo de servicios para integrar las últimas innovaciones tecnológicas. Este enfoque de vigilancia y mejora continua se aplica tanto a la seguridad como a la calidad y el cumplimiento.

«La ciberseguridad no es un tema que se solucione de una vez por todas, sino un bucle de mejora continua que requiere que la arquitectura de seguridad evolucione constantemente y estar siempre al corriente de las amenazas.»

Matthieu Bouthors
Security Solutions Architect de AWS

Nuestros medios: un sistema de seguridad coherente, completo y reactivo

Entonces, ¿cómo pueden ayudarle Odigo y sus socios de AWS a identificar los riesgos, proteger su contact center, y detectar y responder a los incidentes de seguridad?

Bertrand Deroubaix, Risks, Quality & Security Director de Odigo explica: «Nuestro dispositivo integra la gestión de amenazas, la prevención de vulnerabilidades y el control y la monitorización. Nos aseguramos de que todas estas funciones esenciales sean interoperables y se comuniquen entre sí, para construir un sistema de gestión de la seguridad coherente y reactivo, capaz de responder a todos los desafíos de nuestros clientes. Todo ello garantizando el refuerzo de la protección de los datos y del cumplimiento normativo. «Nuestras palabras clave son gobernanza, resiliencia y soberanía», añade el experto.

Estas son algunas de las medidas puestas en marcha:

- Sistemas de prevención de intrusiones, antimalware, firewalls y parches, de manera que se reduce su exposición a las amenazas y a las vulnerabilidades.

- Sistemas de microsegmentación, cifrado de datos almacenados y en tránsito y autenticación única (SSO), los cuales garantizan la confidencialidad e integridad de sus datos.

- Herramientas SIEM, que garantizan un seguimiento en tiempo real de las incidencias y transmiten las alertas a nuestro centro de operaciones de seguridad (SOC). Estas herramientas se complementan con auditorías anuales y campañas de pruebas de intrusión.

«Todos los clientes que alojan sus aplicaciones en la nube de AWS se benefician de una serie de herramientas, activadas de forma predeterminada. Por ejemplo, mecanismos de protección contra ataques DDoS o de cifrado sobre la marcha de los flujos de red. Los servicios de AWS bajo demanda permiten llegar aún más lejos. Por ejemplo, Odigo ha implementado el cifrado de datos en reposo utilizando AWS Key Management Service.»

Matthieu Bouthors
Security Solutions Architect de AWS

▸ Mecanismos de alta disponibilidad en nuestros centros de datos, ubicados en diferentes lugares, que garantizan la disponibilidad y la resiliencia de los servicios.

«La inteligencia artificial y el aprendizaje automático enriquecen progresivamente todas estas herramientas, que permiten detectar, analizar y reaccionar a las amenazas en tiempo real, además de anticipar los riesgos», señala Bertrand Deroubaix. Por ejemplo, Odigo utiliza herramientas basadas en el aprendizaje automático, como Amazon GuardDuty, para detectar anomalías mediante el análisis comportamental de las entidades y los usuarios (UEBA).

En caso de que se produzca un ataque, Odigo cuenta con un sistema de gestión de incidencias en funcionamiento las 24 horas del día, los 7 días de la semana. Informamos al cliente objetivo de que se está tratando el incidente y restauramos los servicios a un modo de funcionamiento normal en menos de dos horas minimizando el impacto negativo en la actividad del centro de contacto.

Nuestras certificaciones: un grado de exigencia muy elevado

Al elegir Odigo, estarás obteniendo una solución y una infraestructura certificadas. Odigo y su socio AWS poseen las certificaciones ISO-27001 e ISO-9001, lo cual constata nuestra experiencia en materia de seguridad de datos (ISO-27001) y gestión de calidad para todos nuestros servicios (ISO-9001). Intentamos obtener certificaciones internacionales interprofesionales, complementadas con certificaciones locales, que demuestren el cumplimiento de normas específicas en diferentes sectores.

Por ejemplo, Odigo tiene el certificado HDS para el alojamiento de datos de salud de carácter personal y PCI DSS para el alojamiento de datos de tarjetas de pago. «Hoy en día, muchos clientes eligen los módulos de servicios de pago de Odigo, ya que podemos cobrar pagos a través del centro de contacto a nivel mundial y, posteriormente, dirigirlos a su sistema de información con un grado de seguridad y

cumplimiento mayor», afirma Bertrand Deroubaix. Por su parte, AWS se adhiere al CISPE. Este código de conducta de protección de datos garantiza a las organizaciones que su proveedor de servicios de infraestructura en la nube cumple con los requisitos del RGPD. Más de 100 servicios de AWS han sido declarados conformes con el código CISPE.

La gestión de riesgos en su centro de contacto debe ser una parte integral de su estrategia de ciberseguridad. Le permitirá prevenir ataques informáticos y proteger los datos para garantizar la continuidad del negocio y el cumplimiento de la normativa vigente, además de reforzar la confianza de sus clientes. El modelo CCaaS, a través del uso de proveedores externos que asumen parte de esta misión, le permite evitar tener que depender solo de sus propios recursos y le brinda la oportunidad de ir más allá en materia de seguridad y cumplimiento. Esta elección le aporta acceso a capacidades avanzadas de detección y protección y a nuevas posibilidades de automatización, además de simplificar el uso de algunas tecnologías que son difíciles de implementar on-premise. Odigo y sus socios de primera clase le acompañan en todas las etapas de la seguridad de su plataforma.

odigo

Acerca de Odigo

Odigo ofrece soluciones de Contact Center as a Service (CCaaS) que facilitan la comunicación entre grandes organizaciones y particulares gracias a una solución global de gestión omnicanal. Gracias a su innovador enfoque basado en la empatía y la tecnología, Odigo permite a las marcas conectar con el elemento humano crucial de la interacción, a la vez que saca el máximo partido de las posibilidades digitales. Pionera en el mercado de la experiencia del cliente (CX), la compañía atiende las necesidades de más de 250 grandes clientes empresariales en más de 100 países.

Visítanos en:
www.odigo.com/es

Contáctanos:
contacto@odigo.com

Customer experience inspired by empathy, driven by technology