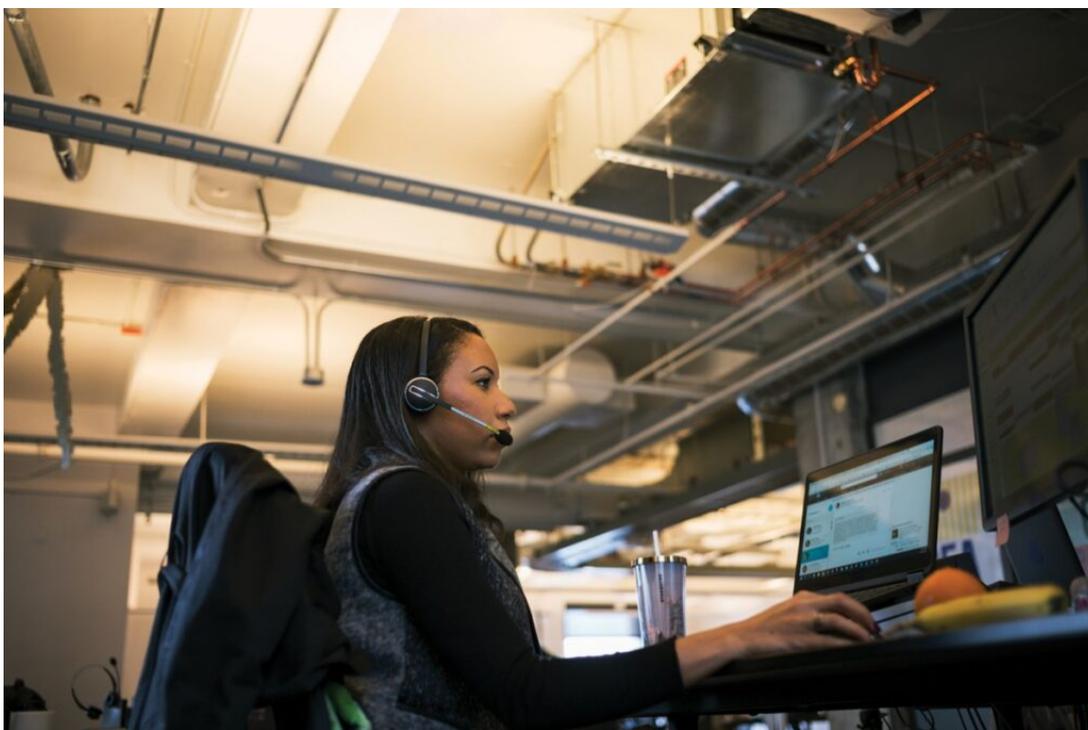


IA para Contact Centers, Interacción con el cliente multicanal

El contact center impulsado por la IA, parte 4: Mejorar la seguridad del contact center con la autenticación biométrica

Tony Lorentzen | General Manager & Senior Vice President, Intelligent Engagement

25 enero 2023



Solución de seguridad biométrica avanzada para verificar la identidad de los clientes de forma rápida, fácil y segura, y proteger las interacciones en todos los canales. Examinamos cómo la integración de Nuance Gatekeeper con las innovaciones de Microsoft en la plataforma Microsoft Digital Contact Center, ayuda a mejorar la experiencia de los clientes y a detectar el fraude.

[Este blog se publicó originalmente, en inglés, en Microsoft.com.](#)

When a customer needs assistance, they not only expect a quick and convenient way to get help, but also for their personal information to be protected. However, when it comes to verifying that people are who they say they are, many contact centers use traditional authentication methods that are no longer fit for purpose. That's why the biometric security solutions included in Microsoft's digital contact center platform are essential. Thanks to biometrics, all types of organizations can verify the identity of their customers quickly, easily and securely across all channels, to operate with complete peace of mind and protect against fraud.

Por qué hay que reforzar la seguridad en los contact centers

Los métodos tradicionales para verificar la identidad de los clientes han quedado obsoletos, son vulnerables y añaden fricción. A punto de comenzar el 2023, los métodos de autenticación aún dependen de la autenticación basada en el conocimiento (KBA), es decir, de los PIN, las contraseñas y las preguntas de seguridad que todos conocemos. Tienen que evolucionar:

1. Para los criminales es muy fácil conseguir información personal de los clientes y suplantar su identidad. Nuestras contraseñas e información personal están expuestas en internet, en distintas plataformas y redes. Además, no podemos olvidar que estamos tratando con verdaderas bandas de cibercrimen organizado. Son profesionales y tienen los recursos y formación necesarios para llevar a cabo un delito sin demasiada dificultad, con este tipo de métodos de autenticación.
2. Los largos procesos de autenticación añaden fricción y una mala experiencia. Además, tenemos que autenticarnos en repetidas ocasiones dentro la misma cuenta cuando pasamos de un canal a otro, o simplemente queremos realizar una nueva operación.
3. Los clientes esperan que las marcas sepan quiénes son desde el primer instante que se ponen en contacto con sus empresas, y no quieren someterse a un interrogatorio para demostrar su identidad.
4. Los clientes a menudo pierden u olvidan la información que necesitan para ser autenticados. Lo que aumenta el tiempo de poder acceder a cualquier consulta u operativa, supone un esfuerzo adicional por ambos lados (empresa y cliente) y la correspondiente frustración al no poder resolver la consulta de forma inmediata por culpa de una contraseña o un protocolo de seguridad ineficiente.

Por eso la seguridad biométrica es tan importante para ayudar a las organizaciones a **proteger a sus clientes y sus propios negocios**.

Con la biometría, las organizaciones pueden ser **más eficientes** y dejar los problemas de los métodos tradicionales de autenticación basados en el conocimiento al permitir una autenticación rápida, segura y sin fricciones, garantizando que las personas con las que interactuamos son realmente quienes dicen ser.

Using inherent biometric elements such as voice biometrics, behavior, and conversational biometrics (how people sound, how they behave, and what they say) with non-biometric factors, a core AI risk engine can make intelligent assessments of authentication and fraud risk. By using biometrics, the system can identify the real person behind the interaction, rather than being limited to the information they have or the device they use.

And now that Nuance Gatekeeper biometric security is integrated with Microsoft products on the [Microsoft Digital Contact Center platform](#), our solutions will multiply the benefits for all our customers.

Autenticación sin interrupciones

The combination of Gatekeeper and Microsoft Dynamics 365 Customer Service in the digital contact center platform will help evolve and strengthen the security of identification and verification (ID&V) processes and provide agents and employees with tools that help them deliver seamless service on any channel. While customer relationship management (CRM) data provides customer identification, multimodal biometrics bolster verification to validate customer identity quickly and accurately.

Por su parte, la validación de llamadas detecta tácticas de fraude habituales, como la suplantación de la identificación automática del número (ANI), y la detección del entorno, cuestionando la fiabilidad de las señales del tipo de dispositivo y la red.

Mayor detección y prevención del fraude

As we have said before, biometric security has a dramatic impact on the ability of organizations to detect and prevent fraud during customer interactions through any channel. [Dynamics 365 Fraud Protection](#) is a perfect complement to biometrics, providing an adaptive AI tool that protects organizations against payment fraud, identity theft, account misappropriation, and many other transactional fraud threats.

Con estas tecnologías trabajando al unísono, la IA dispone de un conjunto de datos enriquecidos para tomar decisiones mejor informadas sobre cuándo utilizar la autenticación escalonada o marcar una transacción o individuo como sospechoso. Gatekeeper identifica a la persona que está detrás de la transacción, mientras que Dynamics 365 examina la transacción en sí. Una potente combinación que

ofrece una oferta única en el mercado de la protección contra el fraude.

Potenciando la personalización

Con la autenticación biométrica, también es mucho más sencillo personalizar las relaciones con los clientes desde el principio. En particular, con la biometría de voz pasiva, donde los clientes pueden ser identificados y su experiencia adaptada en cuestión de segundos mientras explican su necesidad a un agente, un sistema IVR o un asistente virtual.

Las soluciones de biometría de voz simplifican la tarea de ofrecer un servicio personalizado y una asistencia especializada a diversos clientes. Por ejemplo, Telefónica necesitaba encontrar la forma de priorizar la atención de los clientes mayores de 65 años, más vulnerables durante la pandemia, cuando el volumen de llamadas se disparó de tal forma que resultaba imposible priorizar la atención de las personas más necesitadas. **Telefónica utilizó la biometría de voz para identificar a las personas mayores de 65** en función de numerosas características propias de la voz y pudo dirigirlos directamente a una línea de servicio prioritario.

There's also an opportunity to create more personalized experiences for employees. Another exciting benefit of bringing together Nuance and Microsoft products in the digital contact center platform is the integration between Gatekeeper and **Azure Active Directory** (Azure AD). Employees at many companies around the world use Azure AD to sign in to their accounts every day, and that will be made even easier by using biometric authentication instead of usernames and passwords.

Crear un contact center más seguro

Nuestra visión del contact center digital incorpora la seguridad biométrica en todas las interacciones con los clientes para agilizar, personalizar y proteger cada conversación, consulta u operación en todos los canales. Al integrar nuestros productos en una única plataforma, estamos haciendo realidad esa visión, permitiendo a los equipos y departamentos de atención al cliente dar mejor soporte y vender más y mejor, y a los equipos de fraude detectar y prevenir más fraude.

Más información sobre nuestra solución de contact center

Throughout this series of articles, we've explored how to **create engaging and personalized digital experiences, achieve self-service using superior voice solutions**, and build **conversational AI** applications with the protection of advanced biometric security solutions. This is the contact center of the future, made possible by **Microsoft's digital contact center platform**.

Tags: [Fraude](#), [Seguridad y biometria](#), [Plataforma de Contact Center Digital de Microsoft](#)

More Information

Más información

Descubre como Nuance, Dynamics 365 y Microsoft Teams puedan dar forma al futuro de tu contact center.

[Learn more](#)



About Tony Lorentzen

Tony, que cuenta con más de 25 años de experiencia en el sector tecnológico, trabaja en Nuance desde hace 17, donde es vicepresidente de Intelligent Engagement Solutions dentro de la división Enterprise. Previamente lideró varios equipos en la compañía, incluyendo Ingeniería de Ventas, Consultoría de Negocio y Product Management. Con su experiencia, Tony lleva las soluciones de Nuance al mercado empresarial, asociándose con los clientes para garantizar que las implementaciones generen un verdadero retorno de la inversión. Antes de Nuance, trabajó en Lucent y Verizon, donde dirigió equipos que aplicaban las últimas tecnologías para resolver problemas empresariales complejos. Tony se licenció en la Universidad de Villanova y obtuvo un MBA en el Dowling College.



[View all posts by Tony Lorentzen](#)