Aspectos de seguridad

Seguridad de la solución.

image-1674752561299.png

image-1674752585129.png

image-1674752728665.png

Encriptación.

Con motivo de proteger los datos y las conversaciones que suceden dentro de **uContact**, el sistema garantiza máxima seguridad de la voz y de mensajería con encriptación TLS, Websockets Secure (WSS) y SRTP, entre otros.

image-1674752783702.png

Requisito de autenticación. Cada licencia de **uContact** consumida por un cliente deberá tener un usuario y contraseña asociado, que será propiedad de cada usuario. De esta forma, no solo es posible contar con información de la identidad de quienes hacen uso de la solución, sino también proteger los datos allí alojados de cualquier usuario externo al cliente; pudiendo definirse requisitos de complejidad para la contraseña (caracteres, largo, etc). Por último, cabe destacar que el sistema cuenta con la certificación de seguridad ISO 27001, que permite asegurar la confidencialidad e integridad de los datos y de la información	**Roles & Restricciones.** **uContact** utiliza una arquitectura de seguridad basada en tres roles: agente, supervisor o administrador; cada uno brindándole acceso al set de herramientas que mejor se ajuste a las tareas asociadas a cada perfil. De esta forma, ningún usuario podrá ver más de lo estrictamente exigido por las tareas asociadas a su cargo.
Acceso a datos. Los datos de cada instancia de **uContact** solo serán accedidos por sus dueños; es decir, nuestros clientes. Los integrantes de **uContact net2phone** accederán a ellos únicamente en aquellos casos en los que se solicite soporte técnico, se deba realizar algún desarrollo y/o se requiera alguna capacitación o recomendación de uso de la plataforma	**GDPR.** En el caso de nuestros clientes de GDPR, previo al comienzo de su relación comercial con nosotros se les solicita la firma de un acuerdo de confidencialidad de datos

Seguridad de Google Cloud.

Gracias a nuestro partnership oficial con Google Cloud, ofrecemos su nube –y todos sus beneficios– como implementación estándar y además sumamos sus protocolos de seguridad a nuestra propia capa de detección de ataques de fuerza bruta y comunicaciones encriptadas.

image-1674753069540.png

Disponibilidad de la infraestructura.

Tal como lo define Google Cloud, la instancia multizona en la que está alojado **uContact** cuenta con un 99,9% de disponibilidad. En este enlace podrán encontrar más información acerca de los SLA definidos por la compañía mencionada anteriormente.

image-1674753109153.png

Respaldos automatizados: Mediante herramientas disponibles en GCP, en todas las soluciones cloud de **uContact** contamos dentro de la creación de instancias con respaldos automatizados. Estos respaldos permiten tener una imagen completa de la instancia diariamente, por un periodo de 10 días, permitiendo recuperación de información que se desee y también puntos de restauración ante incidentes.	**Auditoría de Logs Centralizada:** Cada instancia cloud cuenta con un sistema de recopilación de logs del sistema de forma centralizada. Esto permite guardar datos históricos de todos los logs del sistema operativo, auditoria de seguridad y logs del sistema **uContact**. Con esta información centralizada se toman acciones detectando anomalías, posibles brechas de seguridad y recomendaciones en el uso de la plataforma.
Alertas Proactivas: Todas nuestras instancias tienen activadas alertas proactivas, que están monitoreando constantemente el estado de cada instancia, avisando de posibles errores antes de que sucedan, para que nuestro equipo de Soporte pueda visualizar y tomar acciones antes de tiempo.	**Monitoreo automatizado:** Nuestro equipo de soporte cuenta con varias herramientas que constantemente monitorean el estado de cada servidor, en variados parámetros (CPU,uso de memoria, uso de red, disponibilidad de conexión y uptime). Tanto sea por notificaciones directas a nuestro personal como también en nuestro cuadro de mando, se pueden tomar acciones de mejora o preventivas para optimizar el uso de la plataforma

Operativas de seguridad.

Análisis de vulnerabilidad.

Con el fin de garantizar la seguridad de los datos y de las instancias de nuestros clientes, nuestro equipo técnico utiliza herramientas para realizar pruebas periódicas en el sistema para analizar y detectar posibles vulnerabilidades. Solo con
un monitoreo constante es que se puede minimizar los riesgos. Por otra parte, cabe destacar que se utilizan herramientas
tales como Inmuniweb y OWASP® Zed Attack Proxy (ZAP) para poder realizar pruebas de vulnerabilidad más completas y
así ser más exhaustivos en la detección de posibles vulnerabilidades.

image-1674753405860.png

Pruebas de penetración.

Con el fin de garantizar la seguridad de los datos y de las instancias de nuestros clientes, nuestro equipo técnico utiliza herramientas para realizar pruebas periódicas en el sistema para analizar y detectar posibles vulnerabilidades. Solo con un monitoreo constante es que se puede minimizar los riesgos.

image-1674753445396.png

Control de cambios.

Todos los cambios o desarrollos a realizar en **uContact** están a cargo de nuestro equipo de desarrolladores, quienes se
encargan de recibir y evaluar los cambios sugeridos por los clientes u otras áreas de la empresa con el fin de determinar si
son viables o no. En caso de que lo sean, son aplicados y testeados múltiples veces para luego ser

implementados en la
solución y comunicados oficialmente.

image-1674753484378.png

Gestión de incidentes

En caso de que existiera alguna eventualidad que pusiera en riesgo la seguridad o la confidencialidad de los datos, nuestro equipo técnico cuenta con un plan de contingencia elaborado para dar respuestainmediata a este tipo de situaciones.
En primer lugar, se identifica la fuente originaria del incidente para, en segundo lugar, determinar qué se debe evaluar para
resolverlo. En tercer lugar, se aplican los pasos a seguir para resolver o enfrentar el incidente. Por último, el cuarto paso a
seguir se corresponde con el reporte del incidente y su solución como método de prevención para próximas oportunidades

image-1674753540088.png

Revision #3
Created 26 January 2023 16:54:26 by Alejandra Vega
Updated 3 February 2023 16:41:35 by Mauricio Coronel