Seguridad

Basándose en estas consideraciones también se deben de tener en cuenta para las políticas de escaneo de los antivirus que puedan estar instalados en los equipos, evitando escaneo o denegaciones de acceso por seguridad.

- Aspectos de seguridad
- ISO 27001
- PCI Compliance
- Consideraciones

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

ISO 27001

> La norma internacional **ISO 27001** permite el aseguramiento, la confidencialidad e integridad de los datos y de la información y de los sistemas que la procesan. Esta permite a las organizaciones el análisis del riesgo y la aplicación de los controles necesarios para eliminarlos.

Si nos dirigimos a la **configuracion del sistema**, nos encontramos con las siguientes opciones que nos ayudaran a establecer un sistema más seguro para nuestros usuarios.

Dentro de la **opcion mensaje de la empresa**, se puede establecer un mensaje de advertencia de la compañía, que aparecerá cada vez que el agente inicie sesión. También el sistema mostrará la fecha y hora de la última sesión iniciada del usuario.

image-1660054612219.png

Dentro de las medidas de seguridad que establece se encuentran:

Expiración de la contraseña luego de determinada cantidad de días. **(Modificable)**

- Solicita cambio obligatorio de contraseña después que se actualiza por supervisor o por la primera vez que el usuario ingresa.

Bloqueo de cuenta luego de determinados intentos fallidos de ingreso de contraseña. **(Modificable)**

En el momento de cambiar la contraseña, no permitir utilizar las últimas X cantidad de contraseñas utilizadas. (Modificable)

El sistema cuenta con tres estados distintos para los usuarios:

- Activo.
- Inactivo.
- Bloqueado **(por intentos de *login* fallidos).**

El usuario es deshabilitado si no entra a **uContact** luego de cierta cantidad de días determinados. **(Modificable)**

Formato de contraseñas establece la complejidad que debe tener las contraseñas de los agentes. Aquí se puede configurar si debe tener:

- Minúsculas
- Mayúsculas
- Números
- Caracteres especiales
- y el largo mínimo de caracteres

Si nos dirijimos a la creacion de agentes, **podemos encontrar los siguientes campos disponibles:**

AGENDA DE LOGIN
image-1660055169066.png
La posibilidad de crear una **agenda de *login***, la cual establece determinados días de la semana y horarios en los cuales el agente puede conectarse al sistema.

CUENTA TEMPORAL

image-1660055244493.png

También está la oportunidad de crear usuarios temporales, es decir, se crea una cuenta que tiene un vencimiento forzado en la fecha que se establezca en los campos.

PCI Compliance

PCI es el estándar de seguridad de datos de la industria de tarjetas de pago, también conocido como PCI DSS (Payment Card Industry – Data Security Estándar) y es un estándar exclusivo de seguridad de la información administrado por el Consejo de Estándares de Seguridad y hace referencia a un estándar que contiene una serie de requerimientos de seguridad que todos los comerciantes, grandes o pequeños, deben cumplir, este estándar se aplica a cualquier empresa que procesa, almacena o transmite datos de tarjetas de crédito, por lo tanto **el comercio debe de contar con un certificado "PCI Certificate"** que garantice que todo su proceso y herramientas que utiliza cumplen con las normas de seguridad necesaria para garantizar la integridad de la información, por lo que el software **uContact de Contact Center Omnicanal es "PCI Compliance"** porque **cumple con los requerimientos más comunes** que el proceso del cliente requiera para su certificación.

Algunos requisitos básicos de cumplimientos que algunos procesos que se requieren y están incluidos en uContact son:

- Utilizar un certificado SSL de 128bits. Resumiendo: Proteger los datos. Cifrar cualquier transmisión pública de los datos.
- ISO 27001 Seguridad de manejo y resguardo de la información
- ISO 27002 proceso de gestión de la continuidad del negocio
- Instalar y mantener una configuración de cortafuegos para proteger de datos.
- No utilices los valores predeterminados del proveedor para las contraseñas del sistema y otros parámetros de seguridad.
- Cifrar la transmisión de los datos de los titulares de las tarjetas a través de redes públicas y abiertas.
- Restringir el acceso a los datos por necesidad de conocimiento de la empresa.
- Asignar un ID único a cada persona con acceso al sistema.
- Realizar auditorías periódicas de acceso y seguridad a los recursos de red y datos.
- Mantén una política de seguridad y asegúrate de que todo el personal la conozca.

Adicionalmente, Google Cloud se somete a una auditoría anual de terceros con el fin de certificar que todos sus productos cumplan con las normas PCI DSS. Esto significa que los servicios proporcionan una infraestructura en la que los clientes pueden compilar sus propios servicios o aplicaciones para el almacenamiento, el procesamiento o la transmisión de datos de titulares de tarjetas.

Es importante señalar que los clientes siguen siendo responsables de garantizar que sus aplicaciones cumplan con las normas PCI DSS. Consulta cómo crear un entorno que cumpla con las normas PCI DSS para aprender a usar Google Cloud Platform a fin de implementar estas normas en tu aplicación.

Consideraciones

En la red donde estén trabajando los agentes se deben de considerar los siguientes puntos:

1. El puerto **3478 UDP/TCP** tiene que estar habilitado al menos para el host stun.ucontactcloud.com
2. El puerto **8089 UDP/TC**P tiene que estar habilitado al menos para el host (ucontactinstance).ucontactcloud.com
3. El puerto **443 UDP/TCP** tiene que estar habilitado al menos para el host (ucontactinstance).ucontactcloud.com
4. Los puertos **10000-20000 UDP** tienen que estar habilitado al menos para el host (ucontactinstance).ucontactcloud.com
5. Tiene que estar habilitado el acceso al los sitios cacerts.geotrust.com/GeoTrustRSACA2018.crt y redirector.gvt1.com/ para permitir a los navegadores validar el certificado SSL de uContact.
6. Tener libre acceso a las siguientes IP **(104.197.204.63 , 74.125.134.127)** usadas por google chrome.
7. Habilitar acceso al sitio de Licenciator para las activaciones de las licencias: us-central1-licenciator.cloudfunctions.net/api/servers/getLicence
8. Habilitar acceso al sitio de Montioreo de la herramienta: monitor.ucontactcloud.com
9. Verificar que SIP - ALG no este activo en los dispositivos de red locales y de borde.
10. Verificar que IPS - detection no este activo ya que puede descartar paquetes Voip y ocasionar problemas de voz (corte de llamadas inesperados etc)
11. dominio *.github.com para updates debe estar habilitado

Basándose en estas consideraciones también se deben de tener en cuenta para las políticas de escaneo de los antivirus que puedan estar instalados en los equipos, evitando escaneo o denegaciones de acceso por seguridad.

Consideraciónes de red para videollamadas

Bandwidth

- 1MB/s simétrico

Latency for toll-quality

- <100 ms total

Jitter

- < 20 ms jitter

Packet loss

- < 1 % for voice calls

Codec

- VP8

Conasideraciones de red para VoIP

Bandwidth

- 256 kbps per call

Latency for toll-quality

- <100 ms total

Jitter

- < 20 ms jitter

Packet loss

- < 1 % for voice calls

Codec

- ulaw, alaw

Equipo de Computo

- Procesador: Core i3 2.0 GHz.
- Memoria: 8GB RAM.
- Resolución mínima: 1366 x 768 (mínimo)
- Disco mínimo: 160 GB

- Explorador internet: Chrome (o cualquier navegador que sea parte del proyecto “CHROMIUM”) (no se recomienda Firefox)
- Enlace 2Mb subida/bajada
- NO MAQUINAS VIRTUALES
