ADENDA DE SEGURIDAD DE RINGCENTRAL

1. Alcance

En este documento se describen las medidas de seguridad de la información (**"Medidas"**) que RingCentral aplica al tratar los Datos Protegidos a través de los Servicios de RingCentral.

2. Definiciones

A los efectos de esta Adenda de Seguridad únicamente, los términos en mayúsculas, no definidos de otro modo en el presente documento, tienen el significado establecido en el Contrato.

A. **"Servicios de Ring Central"**, o **"Servicios"**, significa los servicios ofrecidos por RingCentral y adquiridos por el Cliente.

B. **"Cliente"** se refiere a la entidad que celebró el Contrato con RingCentral.

C. **"Datos Protegidos"** se refiere a los datos del Cliente y de los partners tratados por los Servicios de RingCentral, tal y como se definen en la DPA o el Contrato de RingCentral aplicable, incluidos los "datos personales" y la "información personal" tal y como se definen en las leyes de privacidad aplicables, los datos confidenciales tal y como se definen en el Contrato, los datos de la cuenta, los datos de configuración, el contenido de las comunicaciones, incluidos los mensajes, el buzón de voz y la grabación de vídeo.

D. **"Contrato"** significa el acuerdo vigente entre RingCentral y el Cliente para la prestación de los Servicios.

E. **"Personal"** se refiere a los empleados, contratistas o personal de servicios profesionales subcontratados de RingCentral.

3. Gestión de la Seguridad de la Información

A. Programa de Seguridad

RingCentral mantiene un programa escrito de seguridad de la información que:

i. Incluye políticas o normas documentadas apropiadas para regir el manejo de los Datos Protegidos de conformidad con el Contrato y con la legislación aplicable.

ii. Está dirigido por un empleado de alto nivel jerárquico responsable de supervisar y aplicar el programa.

iii. Incluye salvaguardas administrativas, técnicas y físicas razonablemente diseñadas para proteger la confidencialidad, integridad y disponibilidad de los Datos Protegidos.

iv. Es apropiado para la naturaleza, el tamaño y la complejidad de las operaciones comerciales de RingCentral.

B. Gestión de políticas de Seguridad

Políticas, normas y procedimientos de seguridad de RingCentral:

i. Alinearse con las normas industriales establecidas en materia de seguridad de la información.

ii. Están sujetos a una revisión continua.

iii. Puede revisarse para reflejar los cambios en las mejores prácticas de la industria.

C. Gestión de Riesgos

RingCentral:

i. Realiza evaluaciones de riesgos de ciberseguridad para identificar las amenazas a su negocio u operaciones al menos una vez al año.

ii. Actualiza las políticas, los procedimientos y las normas de RingCentral según sea necesario para hacer frente a las amenazas a los negocios o las operaciones de RingCentral.

4. Evaluaciones de Seguridad Independientes

A. Auditoría Externa

RingCentral:

i. Utiliza auditores independientes cualificados para realizar auditorías de seguridad que cubran los sistemas, entornos y redes en los que se procesan los Datos Protegidos, incluyendo:

a. SOC2 Tipo II.

b. IES/ISO 27001.

ii. mantiene auditorías y certificaciones de cumplimiento adicionales según sea apropiado para el negocio de RingCentral y según se identifique en www.ringcentral.com/trust-center.html.

B. Distribución de Informes

Copias de los informes de auditoría y certificaciones pertinentes:

i. Se facilitará al Cliente si lo solicita.

ii. Están sujetos a un acuerdo de confidencialidad.

C. Cuestionario Anual de Evaluación de Riesgos

El Cliente podrá, en una (1) ocasión dentro de cualquier período de doce (12) meses, solicitar a RingCentral que complete un cuestionario de evaluación de riesgos de terceros en un plazo razonable.

En caso de conflicto entre esta sección y la sección equivalente en el DPA de RingCentral, el DPA tiene prioridad.

5. Seguridad de los Recursos Humanos

A. Comprobación de Antecedentes

RingCentral exige que se realicen comprobaciones previas a la contratación de todos los empleados. RingCentral realiza la búsqueda de antecedentes penales de sus empleados en la medida permitida por la ley. Cada comprobación de antecedentes en EE.UU. incluye:

i. Una verificación de identidad (rastreo del SSN).

ii. Comprobación de los antecedentes penales de hasta siete (7) años por delitos graves y leves a nivel local, estatal y federal, en su caso.

iii. Búsqueda en la lista de terroristas (OFAC), según lo autorizado por la ley.

A nivel internacional, la comprobación de los antecedentes penales se lleva a cabo según lo autorizado por la legislación local.

Las comprobaciones de antecedentes son realizadas por un miembro de la National Association of Professional Background Screeners o por una empresa competente reconocida por el sector en la jurisdicción local.

B. La Formación

RingCentral se asegurará de que todos los empleados, incluidos los contratistas:

i. Complete la formación anual para demostrar que está familiarizado con las políticas de seguridad de RingCentral.

ii. Completar la formación anual para los requisitos de seguridad y privacidad, incluida la concienciación sobre ciberseguridad, el GDPR y la CCPA.

iii. Tener la capacidad y la experiencia razonables para el empleo y la colocación en un puesto de confianza dentro de RingCentral.

C. Seguridad del Puesto de Trabajo

RingCentral se encarga de ello:

i. Los empleados de RingCentral utilizan dispositivos propios y gestionados por RingCentral en el desempeño de sus funciones o dispositivos Bring Your Own Device (BYOD).

ii. Todos los dispositivos, ya sean propiedad de RingCentral y estén gestionados o sean dispositivos Bring Your Own Device (BYOD), están inscritos en el programa completo de dispositivos gestionados de RingCentral.

D. Prevención de la Pérdida de Datos

RingCentral emplea un sistema integral para evitar que los datos de RingCentral y los datos protegidos se vean comprometidos de forma involuntaria o intencionada.

E. Diligencia Debida Sobre los Subcontratistas

RingCentral se compromete a:

i. Mantener un proceso de seguridad para llevar a cabo la debida diligencia antes de contratar a subcontratistas.

ii. Evaluar periódicamente las capacidades de seguridad de dichos subcontratistas para asegurar la capacidad de los mismos de cumplir con las Medidas descritas en este documento.

iii. Aplicar requisitos de seguridad de la información por escrito que obliguen a los subcontratistas a adherirse a las políticas y normas clave de seguridad de la información de RingCentral que sean coherentes con estas Medidas y no menos protectoras.

F. Confidencialidad

RingCentral se asegura que los empleados y contratistas/subcontratistas que procesan Datos Protegidos están obligados por escrito a cumplir con las obligaciones de confidencialidad.

6. Seguridad Física

A. General

RingCentral:

i. Restringe el acceso, controla y supervisa todas las áreas físicas en las que los servicios de RingCentral procesan datos protegidos (**"Zonas Seguras"**).

ii. Mantiene los controles de seguridad física adecuados durante las 24 horas del día y los 7 días de la semana (**"24/7"**).

iii. Revoca cualquier acceso físico a las Zonas Seguras con premura después de que cese la necesidad de acceder a los edificios y sistemas.

iv. Realiza una revisión de los derechos de acceso al menos una vez al año.

B. Procesos de Acceso y Autorización

RingCentral mantiene un proceso documentado de autorización de acceso y registro. El proceso de autorización y registro incluirá como mínimo:

i. Informes en los que se detallan todos los accesos a las Zonas Seguras, incluidas las identidades y las fechas y horas de acceso.

ii. Los informes deben conservarse durante al menos un año, tal y como permite la ley.

iii. Equipo de videovigilancia para supervisar y grabar la actividad en todos los puntos de entrada y salida de las Zonas Seguras las 24 horas del día, los 7 días de la semana, en la medida en que lo permitan las leyes y reglamentos aplicables.

iv. La grabación de vídeo debe mantenerse durante al menos 30 días o según las políticas del proveedor de la ubicación física.

C. Centros de Datos

En la medida en que RingCentral opere o utilice un centro de datos, RingCentral se asegura de que los controles de seguridad física estén en consonancia con las normas del sector, como la ISO 27001 y la SSAE 16 o la ISAE 3402 o una norma similar que incluya:

i. Seguridad del perímetro, incluyendo vallas/barreras y videovigilancia.

ii. Acceso seguro con guardia de seguridad/recepción.

iii. Acceso interior controlado mediante tarjetas RFID, 2FA, controles antirretorno.

iv. Alimentación redundante de utilidades y apoyo a la entrega continua a través de sistemas de respaldo.

v. Conexión de red redundante de varios proveedores.

7. Seguridad Lógica

A. Identificación y Autenticación de Usuarios

RingCentral:

i. Mantiene un proceso documentado de gestión del ciclo de vida de los usuarios que incluye procesos manuales y/o automatizados para la creación, eliminación y modificación de cuentas aprobadas para todos los recursos de información y en todos los entornos.

ii. Se asegura que los usuarios de RingCentral tengan una cuenta individual para una trazabilidad única.

iii. Se asegura que los usuarios de RingCentral no utilicen cuentas compartidas; en los casos en los que las cuentas compartidas son técnicamente necesarias, existen controles para asegurar la trazabilidad.

iv. Las contraseñas de usuario de RingCentral están configuradas de acuerdo con las directrices actuales del NIST.

Para las aplicaciones orientadas al cliente, los clientes pueden optar por integrarse con SSO (Single Sign on) para que el cliente mantenga el control sobre la configuración de sus contraseñas requeridas, incluyendo las soluciones MFA/2FA existentes del cliente.

B. Autorización de Usuarios y Control de Acceso

RingCentral:

i. Configura el acceso remoto a todas las redes que almacenan o transmiten Datos Protegidos para requerir la autenticación de múltiples factores para dicho acceso.

ii. Revoca el acceso a los sistemas y aplicaciones que contienen o procesan Datos Protegidos rápidamente después de que deje de ser necesario acceder a los sistemas o aplicaciones.

iii. Tiene la capacidad de detectar, registrar y notificar el acceso al sistema y a la red o los intentos de violar la seguridad del sistema o de la red.

RingCentral emplea mecanismos de control de acceso destinados a:

i. Limitar el acceso a los Datos Protegidos sólo al Personal que tenga una necesidad razonable de acceder a dichos datos para permitir a RingCentral cumplir con sus obligaciones en virtud del Contrato.

ii. Impedir el acceso no autorizado a los datos protegidos.

iii. Limite el acceso a los usuarios que tienen una necesidad comercial de saber.

iv. Seguir el principio del menor privilegio, permitiendo el acceso sólo a la información y los recursos que sean necesarios.

v. Realice una revisión de los controles de acceso con una periodicidad mínima anual para todos los sistemas de RingCentral que transmitan, procesen o almacenen datos protegidos.

8. Seguridad de las Telecomunicaciones y de las Redes

A. Gestión de la Red

RingCentral:

i. Mantiene un programa de seguridad de la red que incluye protección de cortafuegos estándar del sector y autenticación de dos factores para el acceso a las redes de RingCentral.

ii. Despliega un Sistema de Detección de Intrusos (IDS) y/o un Sistema de Prevención de Intrusos (IPS) para generar, supervisar y responder a las alertas que podrían indicar un compromiso potencial de la red y/o del host.

iii. Supervisa el tráfico web de Internet y de fuentes internas para detectar ciberataques, incluidos los ataques de denegación de servicio distribuidos (DDoS) contra sitios y servicios web, y para bloquear el tráfico malicioso.

B. Segmentación de la Red

RingCentral:

i. Implementa la segmentación de la red entre la red corporativa de la empresa y las instalaciones de alojamiento de los servicios.

ii. Se asegura de la separación entre los entornos dedicados al desarrollo, la puesta en escena y la producción.

iii. Restringe el acceso entre entornos a los dispositivos autorizados.

iv. Controla la configuración y la gestión de la segregación de la red y las reglas del cortafuegos mediante un proceso formal de solicitud y aprobación.

C. Exploración de la Vulnerabilidad de la Red

RingCentral:

i. Realiza escaneos de vulnerabilidad de la red interna y externa contra los sistemas de procesamiento de información al menos trimestralmente.

ii. Evalúa los hallazgos basándose en la puntuación CVSS (si procede) y en la evaluación del impacto, la probabilidad y la gravedad.

iii. Remedia los hallazgos siguiendo los plazos estándar de la industria.

9. Seguridad de las Operaciones

A. Gestión de Activos

RingCentral:

i. Mantiene un registro de activos preciso y actualizado que abarca los activos de hardware y software utilizados para la prestación de servicios.

ii. Mantiene la responsabilidad de los activos a lo largo de su ciclo de vida.

iii. Mantiene los procesos para borrar o destruir físicamente los activos físicos antes de su eliminación.

B. Gestión de la Configuración

RingCentral:

i. Mantiene las configuraciones básicas de los sistemas de información y las aplicaciones basadas en las mejores prácticas del sector, incluyendo:

a. Eliminación de todas las contraseñas proporcionadas por el proveedor.

b. Eliminar/desactivar servicios y configuraciones no utilizadas.

c. Protección antimalware/de punto final según sea técnicamente posible.

ii. Aplica los ajustes de configuración de seguridad de los sistemas utilizados en la prestación de los Servicios.

iii. Se asegura que los relojes de todos los sistemas de procesamiento de la información estén sincronizados con una o varias fuentes de tiempo de referencia.

C. Protección Contra Códigos Maliciosos

i. En la medida de lo posible, RingCentral cuenta con protección de puntos finales, en forma de software de detección y respuesta de puntos finales (EDR) y/o antivirus, instalado y funcionando en servidores y estaciones de trabajo.

ii. Las alertas de EDR se supervisan y se toman medidas inmediatas para investigar y remediar cualquier comportamiento anormal.

iii. Cuando se utilice, el software antivirus estará actualizado y en funcionamiento para buscar y eliminar rápidamente o poner en cuarentena los virus y otros programas maliciosos en los servidores y estaciones de trabajo de Windows.

D. Vulnerabilidad, Parches de Seguridad

RingCentral:

i. Supervisa las vulnerabilidades y las exposiciones divulgadas públicamente para determinar el impacto en los sistemas de información y los productos del proveedor.

ii. Se asegura de las pruebas de garantía de calidad de los parches antes de su despliegue.

iii. Se asegura que todos los hallazgos resultantes de la exploración de las vulnerabilidades de la red y las vulnerabilidades y exposiciones pertinentes divulgadas públicamente se remedien de acuerdo con las mejores prácticas del sector, incluida la puntuación CVSS y la evaluación del impacto, la probabilidad y la gravedad, y se remedien siguiendo los plazos estándar del sector.

E. Registro y Supervisión

RingCentral se asegurará que:

i. Todos los sistemas, dispositivos o aplicaciones asociados al acceso, tratamiento, almacenamiento, comunicación y/o transmisión de Datos Protegidos, generan registros de auditoría.

ii. El acceso a los datos protegidos se registra.

iii. Los registros incluyen suficientes detalles para que puedan ser utilizados para detectar actividades no autorizadas significativas.

iv. Los registros están protegidos contra el acceso, la modificación y el borrado no autorizados.

v. Los registros se envían a una ubicación centralizada para su agregación y supervisión.

10. Desarrollo y Mantenimiento de Software

A. Ciclo de Vida de Desarrollo Seguro

RingCentral:

i. Aplica las prácticas del ciclo de vida del desarrollo seguro, incluso durante los ciclos de diseño, desarrollo y prueba.

ii. Se asegura que los productos se someten a una revisión del diseño de seguridad que incluye consideraciones sobre amenazas y prácticas de manejo de datos.

iii. Se asegura que los servicios se someten a una revisión de liberación segura antes de pasar a producción.

B. Pruebas de Seguridad

Como parte del ciclo de desarrollo seguro, RingCentral:

i. Realiza pruebas de seguridad rigurosas, incluyendo, según sea técnicamente posible:

a. Análisis de código estático.

b. Revisiones por pares del código fuente.

c. Pruebas de seguridad dinámicas e interactivas.

d. Lógica de seguridad, o pruebas de “QA” de seguridad.

ii. Se asegura que las aplicaciones orientadas a Internet se someten a revisiones y pruebas de evaluación de la seguridad de las aplicaciones para identificar las vulnerabilidades de seguridad comunes identificadas por organizaciones reconocidas del sector (por ejemplo, las 10 principales vulnerabilidades de OWASP, las 25 principales vulnerabilidades de CWE/SANS).

iii. Para todas las aplicaciones móviles (es decir, que se ejecutan en Android, Blackberry, iOS, Windows Phone) que recogen, transmiten o muestran Datos Protegidos, lleva a cabo una revisión de la evaluación de la seguridad de la aplicación para identificar y corregir las vulnerabilidades reconocidas por la industria específicas de las aplicaciones móviles.

iv. NO utiliza datos protegidos para las pruebas.

v. Realiza todos los esfuerzos razonables para identificar y corregir las vulnerabilidades del software antes de su publicación.

C. Pruebas de Penetración Anuales

RingCentral:

i. Contrata a terceros cualificados e independientes para que realicen pruebas de penetración anuales contra sus productos y los entornos en los que se alojan los Datos Protegidos.

ii. Requiere que los subencargados realicen pruebas de penetración similares contra sus sistemas, entornos y redes.

iii. Se asegura la corrección de todos los hallazgos en un período de tiempo comercialmente razonable.

D. Gestión de la Vulnerabilidad de los Productos

RingCentral:

i. Utiliza esfuerzos comercialmente razonables para identificar regularmente las vulnerabilidades de seguridad del software en los Servicios de RingCentral.

ii. Proporciona actualizaciones, mejoras y correcciones de errores pertinentes para las vulnerabilidades de seguridad de software conocidas, para cualquier software proporcionado o en el que se procesen Datos Protegidos.

iii. Se asegura que todos los hallazgos resultantes de las pruebas internas y externas se evalúan de acuerdo con las mejores prácticas del sector, incluida la puntuación CVSS y la evaluación del impacto, la probabilidad y la gravedad, y se corrigen siguiendo los plazos estándar del sector.

E. Software de Código Abierto y de Terceros

RingCentral:

i. Mantiene un registro de activos de todo el software de terceros (TPS) y del software de código abierto (OSS) incorporado a los Servicios.

ii. Utiliza esfuerzos comercialmente razonables para asegurar el desarrollo seguro y la seguridad del software de código abierto y del software de terceros utilizado por RingCentral.

iii. Utiliza esfuerzos comercialmente razonables para evaluar, rastrear y remediar las vulnerabilidades del software de código abierto (OSS) y otras bibliotecas de terceros que se incorporan a los Servicios.

11. Manejo de Datos

A. Clasificación de los Datos

RingCentral mantiene normas de clasificación de datos que incluyen:

i. Datos públicos, datos que están generalmente disponibles o que se espera que sean conocidos por el público.

ii. Datos confidenciales, datos que no están disponibles para el público en general.

Los datos protegidos se clasifican como datos confidenciales de RingCentral.

B. Segregación de Datos

RingCentral:

i. Se asegura la separación física o lógica de los datos protegidos de los datos de otros clientes.

ii. Se asegura la separación física y el control de acceso para separar los datos protegidos de los datos de RingCentral.

C. Cifrado de Datos

RingCentral:

i. Se asegurará el cifrado de los datos protegidos en formato electrónico en tránsito por todas las redes públicas alámbricas (por ejemplo, Internet) y todas las redes inalámbricas (excluyendo la comunicación a través de las redes telefónicas públicas conmutadas).

ii. A excepción de la función Engage Communities de Engage Digital, deberá asegurar el cifrado de los Datos Protegidos en formato electrónico cuando se almacenen en reposo.

iii. Utiliza algoritmos de encriptación estándar del sector y fortalezas de las claves para encriptar los datos protegidos en tránsito por todas las redes públicas por cable (por ejemplo, Internet) y todas las redes inalámbricas.

D. Destrucción de Datos

RingCentral deberá:

i. Asegurar la eliminación segura de los datos cuando ya no sean necesarios.

ii. Asegurar que los medios electrónicos que se hayan utilizado en la prestación de los Servicios al Cliente serán desinfectados antes de su eliminación o reutilización, mediante un proceso que garantice la eliminación de los datos e impida su reconstrucción o lectura.

iii. Destruya cualquier equipo que *contenga* Datos Protegidos *que esté dañado o no funcione.*

12. Respuesta a Incidentes

La capacidad de respuesta a incidentes de RingCentral está diseñada para cumplir con las obligaciones legales y reglamentarias que rigen la respuesta a incidentes. Como tal, RingCentral:

A. Mantiene una capacidad de respuesta a incidentes para responder a eventos que puedan afectar a la confidencialidad, integridad y/o disponibilidad de los servicios y/o datos, incluidos los datos protegidos.

B. Tiene un plan documentado de respuesta a incidentes basado en las mejores prácticas del sector.

C. Dispone de un proceso para el manejo de las pruebas que salvaguarda la integridad de las pruebas recogidas hasta permitir la detección del acceso no autorizado a las mismas.

D. Adoptarán los pasos y las medidas adecuadas para cumplir con las obligaciones legales y reglamentarias que rigen la respuesta a los incidentes.

Cuando RingCentral tenga conocimiento o descubra un evento de seguridad que afecte a los Datos Protegidos, RingCentral lo notificará al Cliente sin demora indebida y tomará medidas comercialmente razonables para aislar, mitigar y/o remediar dicho evento.

13. Continuidad de la Actividad y Recuperación de Desastres

A. Continuidad del Negocio

RingCentral:

i. Se asegura que las responsabilidades de la continuidad del servicio están claramente definidas y documentadas y se han asignado a una persona con suficiente autoridad.

ii. Dispone de un plan de continuidad del negocio (BCP) diseñado para proporcionar la prestación continua de los Servicios al Cliente.

iii. Desarrolla, implementa y mantiene un programa de gestión de la continuidad del negocio para abordar las necesidades del negocio y de los Servicios prestados al Cliente. Para ello, RingCentral completa un nivel mínimo de análisis de impacto empresarial, gestión de crisis, continuidad del negocio y planificación de recuperación de desastres.

iv. Se asegura que el alcance del PCN abarca todos los lugares, el personal y los sistemas de información pertinentes utilizados para prestar los servicios.

v. Se asegura que su BCP incluya, entre otros, elementos tales como las soluciones de localización, las soluciones de aplicación, las soluciones de los proveedores y las soluciones de personal, que se ejerciten como mínimo anualmente.

vi. Revisa, actualiza y pone a prueba el PCB al menos una vez al año.

B. Recuperación de Desastres

RingCentral:

i. Mantiene un plan de recuperación en caso de catástrofe, que incluye, entre otras cosas, los detalles de la infraestructura, la tecnología y los sistemas, las actividades de recuperación, e identifica a las personas/equipos necesarios para dicha recuperación, que se ejercita al menos anualmente.

ii. Se asegura que el plan de recuperación de desastres aborda las acciones que RingCentral tomará en caso de una interrupción prolongada del servicio.

iii. Asegura que sus planes abordan las acciones y los recursos necesarios para proporcionar (i) el funcionamiento continuo de RingCentral, y (ii) en el caso de una interrupción, la recuperación de las funciones necesarias para permitir RingCentral para proporcionar los servicios, incluidos los sistemas necesarios, hardware, software, recursos, personal y datos de apoyo a estas funciones.