IntPowers × GENESYS

DOSSIER DE SEGURIDAD · GENESYS CLOUD

Video transaccional en Genesys Cloud

Respuestas a un cuestionario de riesgo de proveedor para cuentas Genesys Cloud. Cada control indica quién responde: nosotros, la infraestructura o tu organización.



Desde 2019
Genesys AppFoundry Premium Partner

AWS
Infraestructura en nodos dedicados por cliente

EU · US
Regiones con asignación de almacenamiento

Login Genesys
El agente entra con su cuenta de Genesys Cloud

02 Alcance y modelo de responsabilidad compartida

PROVEEDOR AWS CLIENTE

Qué cubre este documento y quién responde de cada capa. Tu plataforma Genesys Cloud forma parte de tu organización: aparece como «Cliente».

CAPA	QUIÉN RESPONDE	QUÉ INCLUYE
Infraestructura física y de red	AWS	Centros de datos, hipervisor, red troncal y su programa de conformidad.
Plataforma y pasarela SPLIT	Proveedor	Nodos dedicados por cliente, transcodificación, STUN / TURN por región y enlace SIP con tu Genesys Cloud.
Cifrado de la pata WebRTC	Proveedor	Siempre activo, con certificados de 256 bits y renovación automática.
SPLIT trunking	Proveedor	Conexión SIP entre la pasarela y tu Genesys Cloud; SRTP disponible según tu política.
Identidad del agente	Cliente	El agente entra con su cuenta de Genesys Cloud; los widgets SPLIT usan esa sesión.
Política de grabación y retención	Cliente	La voz la graba Genesys según tu política; el video, solo si activas Video REC.
Monitorización y copias	Proveedor	Sistema propio de monitorización ITSM y copias sobre AWS.
Escritorio de agente y red	Cliente	Atiende en Genesys Cloud con los widgets SPLIT; red según los requisitos CCaaS.

EN UNA FRASE La voz entra en Genesys como una llamada más. El video va por nuestra pasarela, cifrado.

03 Integración con Genesys Cloud

PROVEEDOR AWS CLIENTE

Cómo se integra Video RTC en tu organización Genesys Cloud y quién responde de cada punto de contacto con la plataforma.

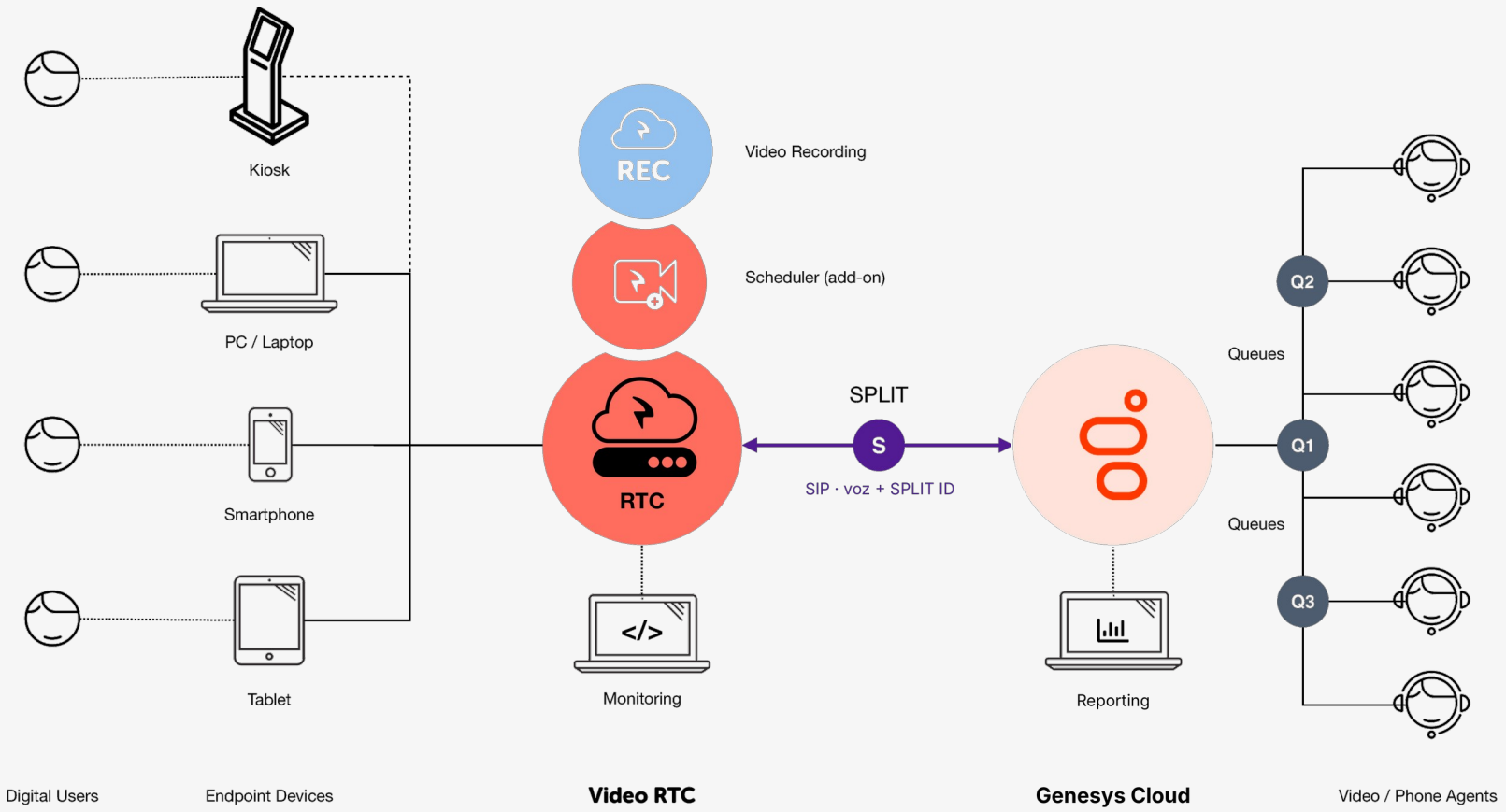
PUNTO DE INTEGRACIÓN	QUIÉN RESPONDE	QUÉ IMPLICA
Ficha en Genesys AppFoundry	**Proveedor**	Video RTC for Genesys, Premium Partner desde 2019; se contrata con Interactive Powers.
SPLIT trunking	**Proveedor**	La videollamada entra en tu organización Genesys Cloud como una llamada más, por SPLIT trunking: la conexión SIP con la que enlazamos cualquier CCaaS.
Enrutamiento	**Cliente**	Architect, colas, skills y prioridades de Genesys: la llamada no sale de tu flujo.
Control del agente	**Cliente**	Atender, retener, transferir y consultar desde la barra de la interacción y el dialpad.
Widgets SPLIT	**Proveedor**	Video Session, Scheduled, Reverse, Messaging y Remote Viewer, con la sesión Genesys.
Video del agente	**Proveedor**	Ventana SPLIT Agent y PiP; el video llega cifrado por WebRTC desde la pasarela.
Grabación	**Cliente**	La voz, en la grabación de Genesys; el video, en Video REC solo si lo activas.
Contexto y reporting	**Cliente**	Datos del widget en cabeceras SIP para Architect; la videollamada cuenta en tus KPI.

EN UNA FRASE La interacción vive en tu Genesys Cloud; nosotros aportamos el video y su pasarela.

04 Arquitectura y flujo de datos

PROVEEDOR AWS CLIENTE

Los componentes de una videollamada transaccional en Genesys Cloud y por dónde pasa cada uno. La grabación de video es una pieza aparte: se activa, no viene puesta.



EN UNA FRASE

La voz la enruta Genesys; el video, nuestra pasarela. Un identificador SPLIT las une.

05 Inventario de datos, residencia y retención

PROVEEDOR AWS CLIENTE

Qué datos trata el servicio, dónde residen, cómo van protegidos y quién decide cuánto tiempo se conservan.

DATO	DÓNDE RESIDE	PROTECCIÓN	RETENCIÓN
Audio y video en tiempo real	Pasarela, en la región asignada	WebRTC cifrado	No se almacena salvo grabación activada
Voz de la videollamada	Tu Genesys Cloud, con su grabación	SRTP, si lo activas	Tu política en Genesys
Grabaciones de video	Video REC, región asignada	AES 256 en exportación	Programada por servicio
SPLIT ID y parámetros	Tu Genesys y la pasarela	Solo los de la sesión	Sin copia de datos Genesys
Logs de sistema	Nodos por región	Sin acceso exterior	Bajo NDA
Credenciales del agente	Tu organización Genesys Cloud	No las custodiamos	Tuyas

EN UNA FRASE Asignación regional EU o US por contrato. La voz y su grabación se quedan en tu Genesys Cloud.

06 Cifrado y gestión de claves

PROVEEDOR · AWS · CLIENTE

Qué protege cada tramo y quién lo activa. Las comunicaciones en tiempo real van cifradas con protocolos estándar, incluidas las conexiones WebRTC entre pares y la transcodificación híbrida.

TRAMO	MECANISMO	QUIÉN LO ACTIVA
Cliente ↔ pasarela	WebRTC cifrado de extremo a extremo, con STUN / TURN propios por región y certificados de 256 bits.	Siempre activo
Pasarela ↔ Genesys Cloud	Pata de voz por SPLIT trunking (SIP); SRTP disponible según tu política.	Lo activas tú
Pasarela ↔ widget del agente	Video WebRTC cifrado hasta el navegador del agente, dentro de Genesys Cloud.	Siempre activo
Exportación de grabaciones	AES de 256 bits sobre todo registro que sale del almacenamiento.	Siempre activo
Red y administración	Cortafuegos, SSH, SSL / TLS y VPN sobre todos los sistemas.	Siempre activo

DETALLE BAJO ACUERDO DE CONFIDENCIALIDAD: Cifrado en reposo del almacenamiento de grabaciones · Custodia de claves, rotación y uso de KMS · Asignación de llaves dedicadas por cliente: procedimiento

EN UNA FRASE Tres tramos. El que entra en Genesys va por SPLIT trunking, con SRTP si lo activas.

07 Identidad y control de acceso

PROVEEDOR AWS CLIENTE

El agente no tiene cuenta nuestra: entra en Genesys Cloud y los widgets SPLIT usan esa sesión. El entorno de grabación de video es aparte y de uso corporativo.

Autenticación del agente

Su cuenta de Genesys Cloud; los widgets SPLIT usan esa sesión.

Permisos del agente

Roles y colas de tu organización Genesys; no creamos cuentas de agente.

Restricción por red

Filtrado por rangos de IP sobre la autenticación por directorio.

Acceso a Video REC

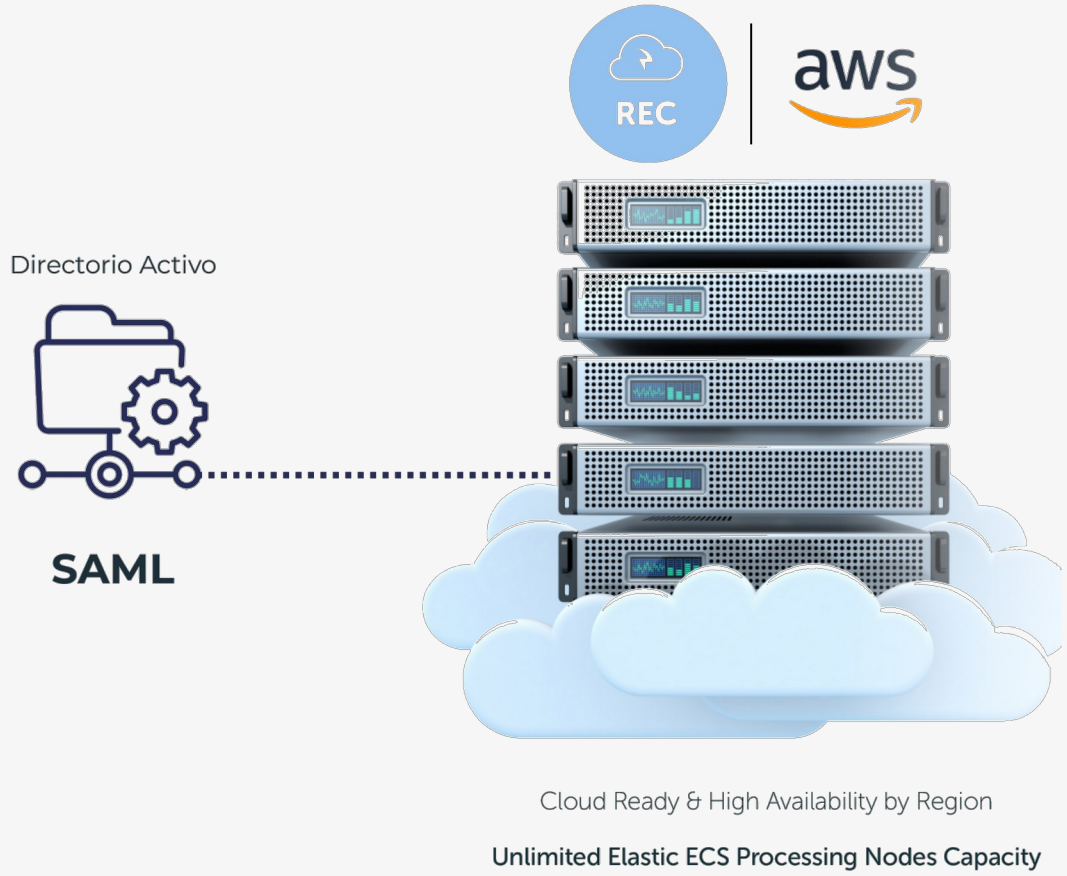
Directorio Activo por SAML 2.0 o SSO externo; cuentas nominales.

Borrado

Desactivado por defecto; solo a petición expresa del cliente.

MFA en cuentas administrativas

Bajo NDA.



EN UNA FRASE La contraseña del agente no sale de Genesys. Nosotros no la vemos ni la guardamos.

08 Segregación y aislamiento entre clientes

PROVEEDOR AWS CLIENTE

Cómo se separan los datos y el proceso de un cliente de los de otro, capa por capa.

CAPA	MECANISMO DE AISLAMIENTO	ALCANCE
Nodos de proceso	CPaaS sobre nodos dedicados que no comparten acceso entre sí.	Por cliente
Almacenamiento	Unidades de almacenamiento dedicadas, activables por servicio.	Por servicio
Llaves y cuentas	Opciones específicas de activación para asignar llaves y cuentas dedicadas.	Por cliente
Servicios de red	STUN / TURN propios por región, desplegables como IP dedicadas.	Por región o por cliente
Región	Asignación regional de datos: EU, US y las que fije el contrato.	Por contrato
Infraestructura	Aislamiento físico y de hipervisor, bajo el programa de conformidad de AWS.	**AWS**

EN UNA FRASE Tus datos no conviven con los de otro cliente: ni en proceso, ni en almacenamiento, ni en red.

09 Registro, auditoría y monitorización

PROVEEDOR · AWS · CLIENTE

Hay dos capas de registro y conviene no confundirlas: la trazabilidad de la interacción, que vive en Genesys Cloud, y los logs del sistema, que viven en nuestros nodos.

QUÉ SE REGISTRA	DÓNDE	QUIÉN ACCEDE	CÓMO SE ENTREGA
Eventos, grabación de voz y reporting	En Genesys Cloud, como una llamada más	Tú, con las herramientas de Genesys	Ya es tuyo
Metadatos de sesión y parámetros de entrada	Con el identificador único SPLIT	Tu Genesys, CRM o script de agente	Por integración
Logs de sistema: eventos, errores, avisos	Nodos por región; sin contenido de servicio	Solo desde dentro del nodo	Trazas concretas, bajo requerimiento
Marcadores de auditoría de grabaciones (Flags)	Almacenamiento REC	Usuarios con el permiso	En el panel
Indicadores ITSM por región, nodo y servicio	Monitorización propia sobre AWS	Nuestro equipo; tu TI si el contrato lo prevé	Paneles compartidos

DETALLE BAJO ACUERDO DE CONFIDENCIALIDAD: Periodo de retención de los logs de sistema · Integración con el SIEM del cliente

EN UNA FRASE Los logs de nodo no se exponen a sistemas externos. Se activan trazas concretas y se entregan bajo requerimiento.

10 Grabaciones: ciclo de vida completo

PROVEEDOR AWS CLIENTE

La voz la graba Genesys con su política. El video solo se graba si activas Video REC, y desde ahí cada paso queda bajo tu política.

Activación

La fija tu política de seguridad. Tipo de grabación según plan: RAW; SD con MP4; HD.

Acceso

Cuentas nominales con permisos por servicio; previsualización y metadatos según permiso.

Retención

Periodos de almacenamiento programados por servicio.

Post-proceso

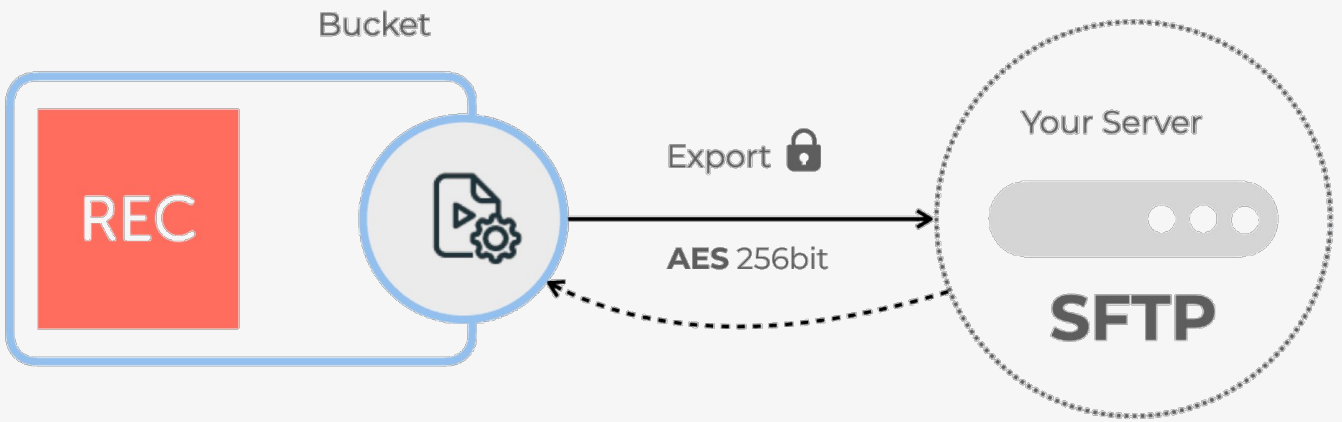
Instrucciones al recibir cada registro: borrado automático, exportación SFTP, archivado, copia.

Exportación

Programable y automática, cifrada con AES de 256 bits, a tu propio servidor.

Borrado

Permiso desactivado por defecto; se activa solo a petición expresa.



SSH

amazon SFTP

EN UNA FRASE Voz en Genesys y video en Video REC: las dos grabaciones bajo tu política, con el mismo identificador SPLIT.

11 Gestión de vulnerabilidades y desarrollo seguro

PROVEEDOR · AWS · CLIENTE

Los criterios con los que se desarrolla y se opera la plataforma, y el proceso que los sostiene.

PRINCIPIO	QUÉ IMPLICA EN LA PRÁCTICA
Seguridad de aplicación	Impedir el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de la aplicación y sus datos.
Seguridad de red	Cortafuegos, SSH, SSL, TLS y VPN, con controles que evolucionan con conocimiento específico.
Seguridad probada de producto	Todos los accesos con certificados de 256 bits para cifrar comunicaciones y protocolos.
Gestión del centro de datos	Automatización, monitorización y gestión sobre AWS.
Los datos pertenecen al cliente	Nodos dedicados sin acceso compartido entre servicios.

DETALLE BAJO ACUERDO DE CONFIDENCIALIDAD: Cadencia de parcheo de sistemas y dependencias · Pruebas de intrusión externas: frecuencia y último informe · Programa de divulgación responsable · Revisión de código y gestión de cambios

EN UNA FRASE Los principios están escritos. El proceso que los audita se entrega con el expediente.

12 Continuidad y recuperación

PROVEEDOR AWS CLIENTE

Existe un Plan de Recuperación ante Desastres documentado y un sistema documental de seguridad. Estas son sus cifras de recuperación por región.

Copia de datos · EU

Mínimo 1 día · estándar 7 días · máximo 14 días. AWS Backup.

Sincronización de directorio · EU

Mínimo 1 mes · estándar 2 meses · máximo 1 año. Directory Sync.

Copia de datos · US

Mínimo 1 día · estándar 7 días · máximo 14 días. AWS Backup.

Sincronización de directorio · US

Mínimo 1 mes · estándar 2 meses · máximo 1 año. Directory Sync.



DETALLE BAJO ACUERDO DE CONFIDENCIALIDAD:

RTO por nivel de severidad · Procedimiento de restauración y responsables por servicio

EN UNA FRASE Servidores y servicios críticos conectados a copias de varias semanas o meses, con restauración por región.

13 Respuesta a incidentes

PROVEEDOR AWS CLIENTE

Qué hay ya en este documento para cada fase, y qué se entrega bajo NDA: el procedimiento de respuesta a incidentes completo.

FASE	LO QUE YA ESTÁ EN ESTE DOCUMENTO	SECCIÓN
Detección	Sistema propio de monitorización ITSM por región, nodo y servicio, con paneles compartidos con tu equipo.	9
Trazabilidad	Logs de sistema en nodos por región, sin acceso exterior; trazas concretas entregadas bajo requerimiento.	9
Contención	Nodos de proceso, almacenamiento y claves dedicados por cliente, sin acceso compartido entre servicios.	8
Recuperación	Copias AWS Backup y sincronización de directorio por región, con restauración por servicio.	12

DETALLE BAJO ACUERDO DE CONFIDENCIALIDAD

- Clasificación de incidentes y niveles de severidad
- Plazo de notificación al cliente y a la autoridad de control
- Cadena de escalado y responsables
- Comunicación durante el incidente y análisis posterior
- Coordinación con el equipo de seguridad del cliente

Existe y se entrega con el expediente completo. Pídelo antes de la fase de due diligence.

EN UNA FRASE Un banco no pregunta si tienes procedimiento. Pregunta en cuántas horas le llamas.

14 Subprocesadores y terceros

PROVEEDOR AWS CLIENTE

Quién más interviene en la prestación del servicio y con qué alcance.

FUNCIÓN	QUIÉN LA PRESTA	DÓNDE Y CÓMO	REGIÓN
Cómputo, red y almacenamiento	**AWS**	Nodos y unidades de almacenamiento dedicados por cliente, dentro del programa de conformidad de AWS.	EU · US, según contrato
Copias de seguridad	**AWS**	AWS Backup, con retención de 1, 7 y 14 días.	Por región
Pasarela SPLIT y transcodificación	**Proveedor**	Nodos propios. No se subcontrata.	Por región
STUN / TURN	**Proveedor**	Servidores propios con IPs dedicadas, desplegables por cliente.	Por región
Identidad del agente	**Cliente**	Tu organización Genesys Cloud. No custodiamos credenciales.	La tuya
Voz y grabación de voz	**Cliente**	Tu Genesys Cloud, conectado por SPLIT trunking; SRTP disponible.	La tuya

DETALLE BAJO ACUERDO DE CONFIDENCIALIDAD: Lista completa de subprocesadores y su acuerdo de tratamiento · Proveedores de conectividad SIP y de red, si aplican · Procedimiento de notificación de cambios en la lista

EN UNA FRASE Somos AWS Standard Technology Partner. La infraestructura no se subcontrata a nadie más.

15 Certificaciones y atestaciones

PROVEEDOR · AWS · CLIENTE

Un sello de la infraestructura no es un sello del proveedor. Los separamos para que nadie tenga que averiguarlo a mitad de una evaluación.

Lo que atesta Interactive Powers

En su ficha de Video RTC en Genesys AppFoundry

GDPR

HIPAA

Si tu proceso de compra exige una atestación que no está en esta columna, dilo en la primera reunión: es una conversación de plazos.

Lo que certifica la infraestructura

Programa de conformidad de Amazon Web Services, donde ejecutamos. Los sellos de la derecha, ISO 27001 incluido, son de AWS, no de Interactive Powers.

Verificable en aws.amazon.com/compliance. Interactive Powers es AWS Standard Technology Partner.



SOC 1



SOC 2



SOC 3



ISAE 3402



PCI



MPAA



FISMA



ISO27001



HIPAA

EN UNA FRASE Ni SOC 2 ni ISO 27001 están atestados hoy por Interactive Powers: son de AWS. Lo decimos aquí para no tener que explicarlo después.

16 Documentación disponible bajo NDA

PROVEEDOR AWS CLIENTE

Lo que existe por escrito y se entrega con el acuerdo de confidencialidad. Pídelo antes de la fase de due diligence, no durante.

Plan de Recuperación ante Desastres

Objetivos de recuperación, RTO por severidad, responsables y procedimiento por servicio. Sección 12.

Sistema documental de seguridad

Procedimientos internos de seguridad y su control de versiones. Sección 11.

Gestión de claves

Custodia, rotación, KMS y asignación de llaves dedicadas. Sección 6.

Gestión de vulnerabilidades

Cadencia de parcheo, informes de pentest, divulgación responsable. Sección 11.

Respuesta a incidentes

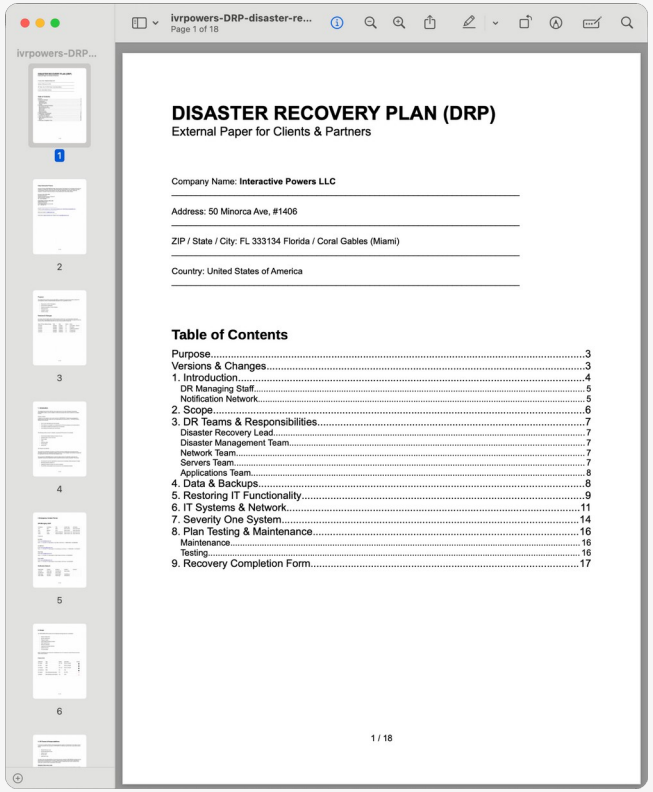
Clasificación, plazos de notificación, escalado y comunicación. Sección 13.

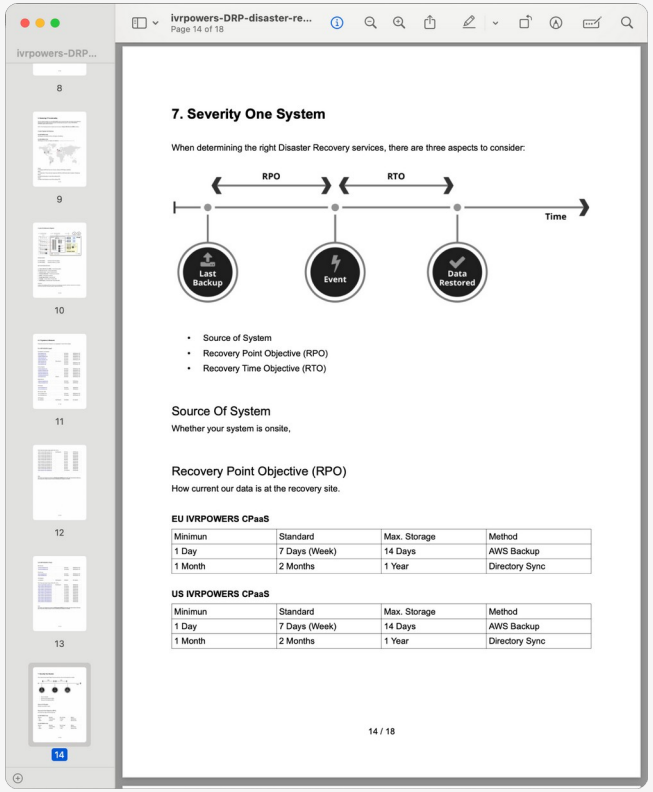
Subprocesadores

Lista completa y acuerdos de tratamiento. Sección 14.

Retención de logs y SIEM

Periodos de retención y opciones de integración. Sección 9.





EN UNA FRASE Pon a tu equipo de seguridad en la primera reunión, no en la última.

IntPowers × GENESYS

La conversación de seguridad es mejor tenerla al principio.

Lo que no esté resuelto lo decimos en la primera reunión, no en la última.



Hablar con Ingeniería

Solicitar el expediente

Bajo NDA

Siete documentos, listados en la sección 16

Madrid · Miami

Soporte en horario CET y EST

AppFoundry

Premium Partner de Genesys desde 2019

AWS Partner

Standard Technology Partner

Interactive Powers, SL (Europa) o LLC (America) operan como IntPowers o IVRPowers