IntPowers

DOSSIER DE SEGURIDAD Y CUMPLIMIENTO

Video transaccional para contact centers

Respuestas a las preguntas de un cuestionario de riesgo de proveedor, en su orden. Cada control indica quién responde de él: nosotros, la infraestructura o tu organización.



Desde 2016
En producción con clientes de banca y seguros

AWS
Infraestructura en nodos dedicados por cliente

EU · US
Regiones con asignación de almacenamiento

SAML 2.0
Identidad en tu propio directorio

02 Alcance y modelo de responsabilidad compartida

PROVEEDOR AWS CLIENTE

Qué cubre este documento y quién responde de cada capa. Es la primera pregunta de cualquier evaluación y condiciona todas las demás.

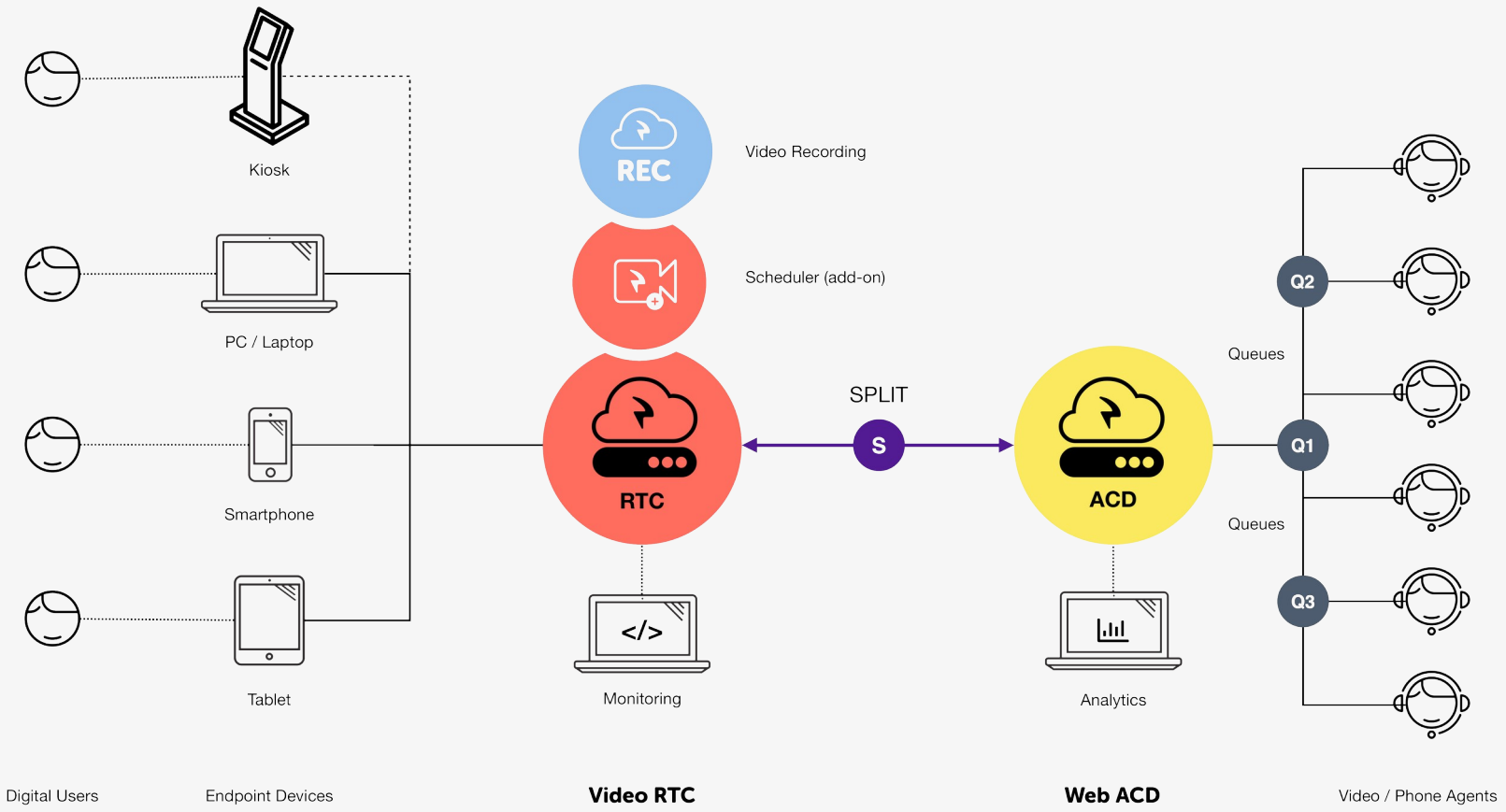
CAPA	QUIÉN RESPONDE	QUÉ INCLUYE
Infraestructura física y de red	**AWS**	Centros de datos, hipervisor, red troncal y su programa de conformidad.
Plataforma y pasarela SPLIT	**Proveedor**	Nodos dedicados por cliente, transcodificación, STUN / TURN por región, almacenamiento de grabaciones.
Cifrado de la pata WebRTC	**Proveedor**	Siempre activo, con certificados de 256 bits y renovación automática.
SRTP en la troncal SIP	**Cliente**	Disponible al conectar la troncal; lo activa el cliente según su política.
Identidad y directorio	**Cliente**	Directorio Activo o SSO del cliente por SAML 2.0; el proveedor lo integra.
Política de grabación y retención	**Cliente**	El cliente decide qué se graba y cuánto se conserva; el proveedor lo ejecuta.
Monitorización y copias	**Proveedor**	Sistema propio de monitorización ITSM y copias sobre AWS.
Escritorio de agente y red interna	**Cliente**	El agente atiende desde su herramienta habitual; la red del cliente no cambia.

EN UNA FRASE Solo una pata de la sesión entra en tu red. Todo lo que ocurre en ella lo controlas tú.

03 Arquitectura y flujo de datos

PROVEEDOR AWS CLIENTE

Los componentes que intervienen en una videollamada transaccional y por dónde pasa cada uno. La grabación y el agendamiento son piezas aparte del motor: se activan, no vienen puestas.



EN UNA FRASE El motor de video, tu distribuidor y tus agentes: tres piezas, un solo enlace SPLIT entre ellas.

04 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
Señalización y contexto SIP	Tu troncal y tu plataforma	SRTP, si lo activas	La de tu plataforma
Grabaciones RAW / MP4	Almacenamiento REC, región asignada	AES 256 en exportación	Programada por servicio
Metadatos de sesión (SPLIT ID)	Tu plataforma y REC	Con la interacción	Con la interacción
Logs de sistema	Nodos por región	Sin acceso exterior	Bajo NDA
Credenciales de acceso a REC	Tu directorio (SAML)	No las custodiamos	Tuyas

EN UNA FRASE

Asignación regional EU o US por contrato; llaves, cuentas y unidades de almacenamiento dedicadas cuando lo exiges.

05 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, desplegables como IP dedicadas.	Siempre activo
Pasarela ↔ tu troncal SIP	SRTP sobre SIP, disponible al conectar tus troncales VoIP.	Lo activas tú
Certificados	Longitud mínima de 256 bits, activación privada y renovación automática.	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 Dos patas, dos cifrados. La que entra en tu red usa el que tú ya sabes operar: SRTP.

06 Identidad y control de acceso

PROVEEDOR AWS CLIENTE

El entorno de grabación es de uso corporativo, reservado a un número limitado de usuarios señalados por reglas de seguridad. No da servicio a nivel de agente.

Autenticación

Directorio Activo del cliente por SAML 2.0, o SSO externo (Google, Microsoft).

Cuentas

Nominales por servicio, con recuperación de contraseña por correo.

Restricción por red

Filtrado por rangos de IP sobre la autenticación por directorio.

Permisos por servicio

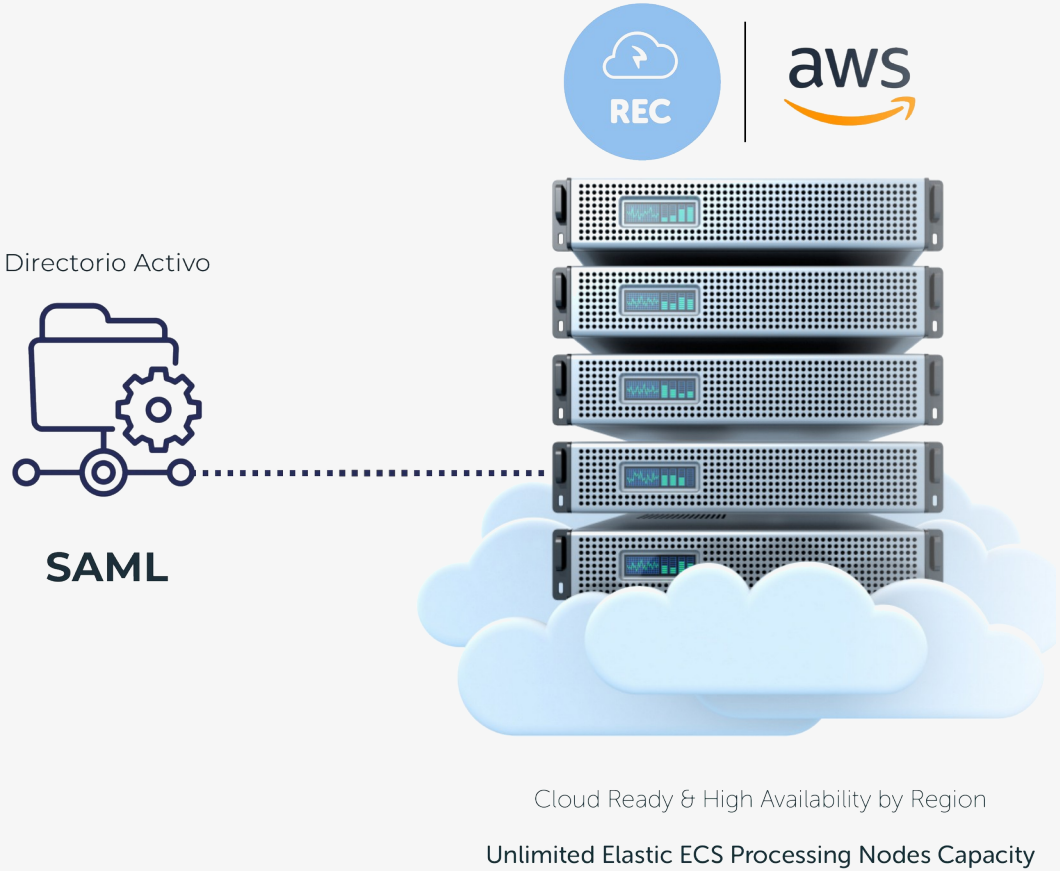
Auto-processing, HD, MP4 Player, Metadata, Flags y Borrado.

Borrado

Desactivado por defecto; solo a petición expresa del cliente.

MFA en cuentas administrativas

Bajo NDA.



EN UNA FRASE La contraseña no sale de tu directorio. Nosotros no la vemos ni la guardamos.

07 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.

08 Registro, auditoría y monitorización

PROVEEDOR · AWS · CLIENTE

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

QUÉ SE REGISTRA	DÓNDE	QUIÉN ACCEDE	CÓMO SE ENTREGA
Eventos, grabación y reporting de cada videollamada	En tu plataforma, como una llamada más	Tú, con tus herramientas	Ya es tuyo
Metadatos de sesión y parámetros de entrada	Con el identificador único SPLIT	Tu CRM, ERP 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.

09 Grabaciones: ciclo de vida completo

PROVEEDOR · AWS · CLIENTE

Activar la grabación no es directamente operativo, por razones de seguridad y privacidad: es una decisión del cliente. Desde ahí, cada paso queda bajo su 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

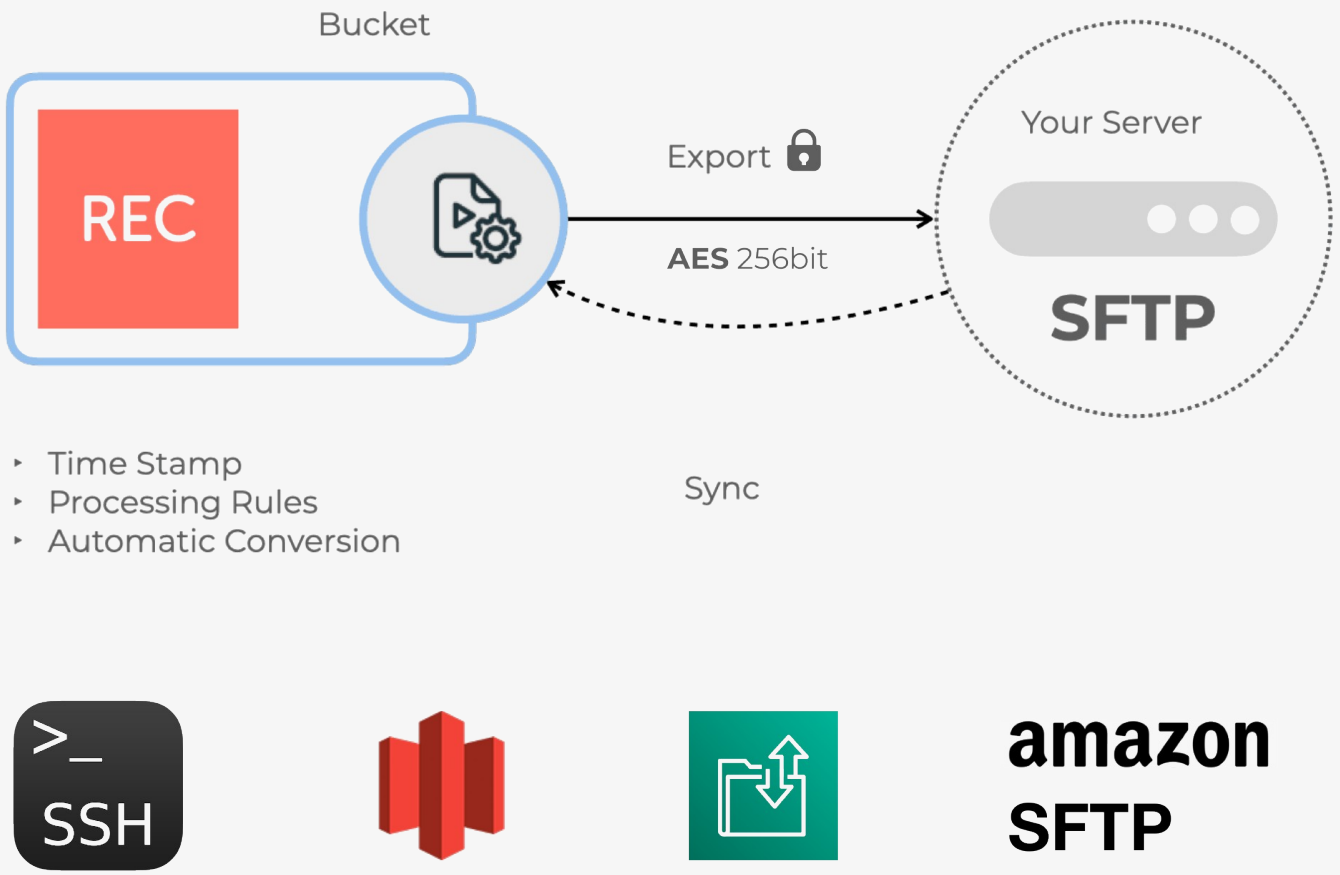
Instrucciones al recibir cada registro: borrado automático, exportación SFTP, archivado, copia.

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.



EN UNA FRASE

Es la diferencia con una sala de video de terceros: allí la grabación vive en otro sistema, con otra retención y otro responsable.

10 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.

11 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.

12 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.	8
Trazabilidad	Logs de sistema en nodos por región, sin acceso exterior; trazas concretas entregadas bajo requerimiento.	8
Contención	Nodos de proceso, almacenamiento y claves dedicados por cliente, sin acceso compartido entre servicios.	7
Recuperación	Copias AWS Backup y sincronización de directorio por región, con restauración por servicio.	11

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.

13 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	**Cliente**	Tu Directorio Activo o SSO. No custodiamos credenciales.	La tuya
Conectividad SIP	**Cliente**	Tu troncal y tu operador; SRTP disponible al conectarla.	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.

14 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



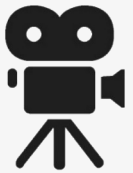
SOC 3



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.

15 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 11.

Sistema documental de seguridad

Procedimientos internos de seguridad y su control de versiones. Sección 10.

Gestión de claves

Custodia, rotación, KMS y asignación de llaves dedicadas. Sección 5.

Gestión de vulnerabilidades

Cadencia de parcheo, informes de pentest, divulgación responsable. Sección 10.

Respuesta a incidentes

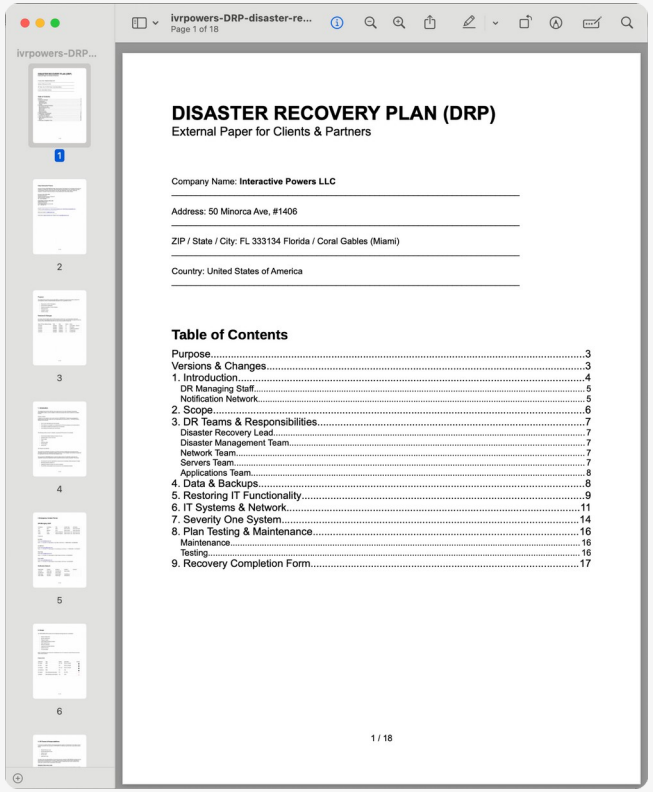
Clasificación, plazos de notificación, escalado y comunicación. Sección 12.

Subprocesadores

Lista completa y acuerdos de tratamiento. Sección 13.

Retención de logs y SIEM

Periodos de retención y opciones de integración. Sección 8.



DISASTER RECOVERY PLAN (DRP)
External Paper for Clients & Partners

Company Name: **Interactive Powers LLC**

Address: 50 Minorca Ave, #1406

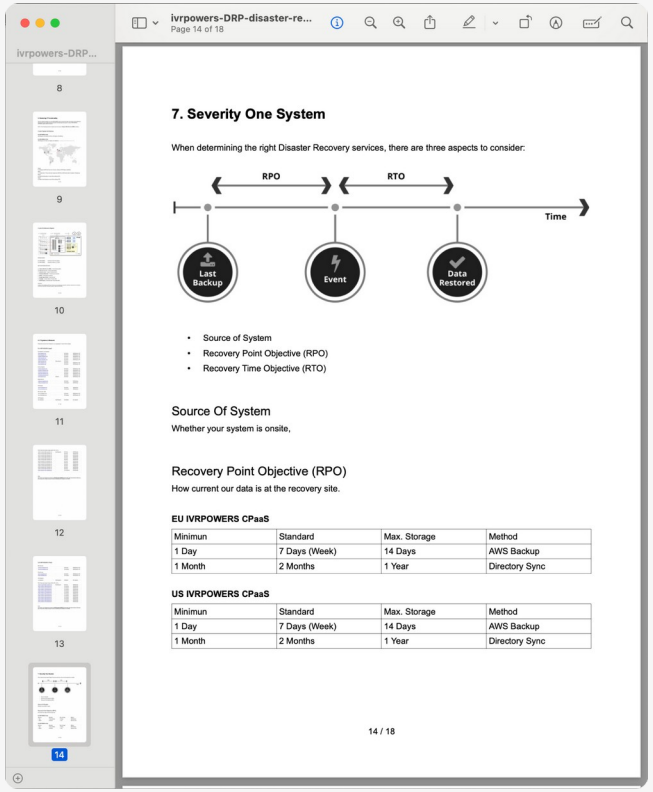
ZIP / State / City: FL 333134 Florida / Coral Gables (Miami)

Country: United States of America

Table of Contents

Purpose....3
Versions & Changes....3
1. Introduction....4
DR Managing Staff....5
Notification Network....5
2. Scope....6
3. DR Teams & Responsibilities....7
Disaster Recovery Lead....7
Disaster Management Team....7
Network Team....7
Servers Team....7
Applications Team....8
4. Data & Backups....8
5. Restoring IT Functionality....9
6. IT Systems & Network....11
7. Severity One System....14
8. Plan Testing & Maintenance....16
Maintenance....16
Testing....16
9. Recovery Completion Form....17

1 / 18



7. Severity One System

When determining the right Disaster Recovery services, there are three aspects to consider:

RPO RTO Time

Last Backup — Event — Data Restored

- Source of System
- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)

Source Of System

Whether your system is onsite,

Recovery Point Objective (RPO)

How current our data is at the recovery site.

EU IVRPOWERS CPaaS

Minimun	Standard	Max. Storage	Method
1 Day	7 Days (Week)	14 Days	AWS Backup
1 Month	2 Months	1 Year	Directory Sync

US IVRPOWERS CPaaS

Minimun	Standard	Max. Storage	Method
1 Day	7 Days (Week)	14 Days	AWS Backup
1 Month	2 Months	1 Year	Directory Sync

14 / 18

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

IntPowers

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 15

Madrid · Miami
Soporte en horario CET y EST

interactivepowers.com
Documentación pública de plataformas

AWS Partner
Standard Technology Partner

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