Seguridad y cumplimiento regulatorio en AWS

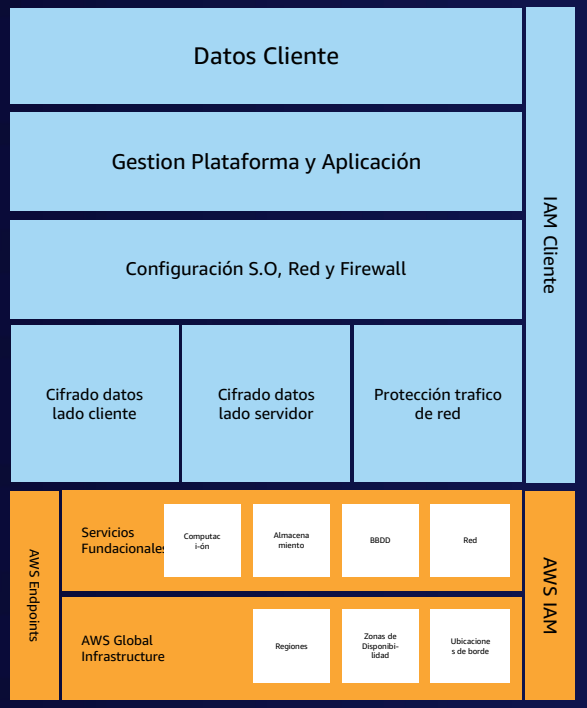
D. Borja Larrumbide Martinez

Responsable de Seguridad de España y Portugal
Amazon Web Service

El modelo de responsabilidad compartida

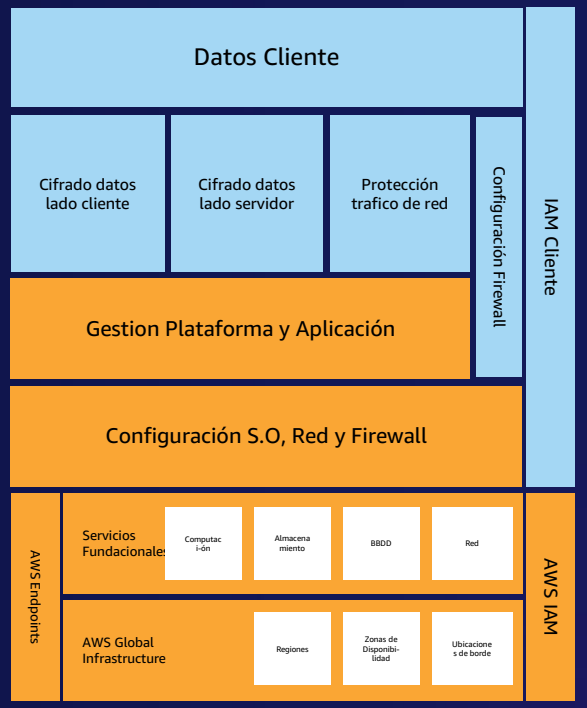
Importante entender para el análisis de riesgo y estrategias de mitigación

1 Servicios de Infraestructura



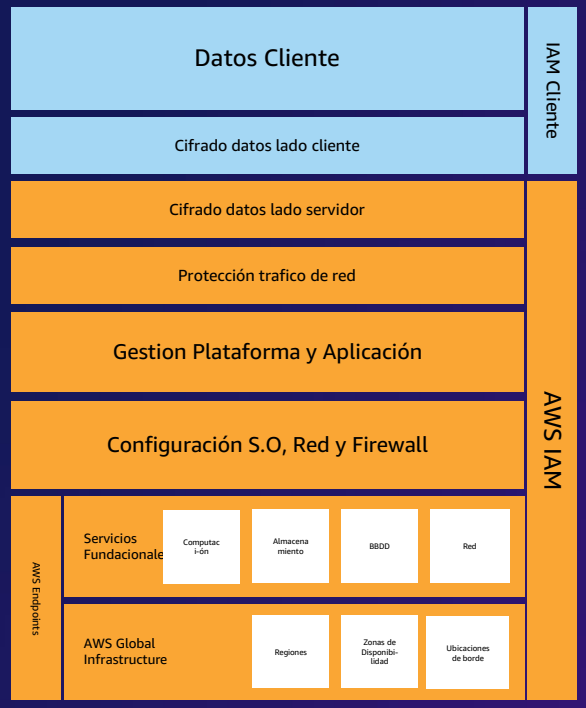
Amazon EC2

2 Servicios gestionado



Amazon RDS

3 Servicios serverless



Amazon S3

Más info: https://aws.amazon.com/es/compliance/shared-responsibility-model/

El diseño de la región de AWS

26 Regiones lanzadas y 8 anunciadas
84 Zonas de Disponibilidad (AZ)
17 zonas locales y 32 anunciadas
245 países y territorios atendidos

Cada región de AWS es una ubicación física en el mundo y tiene al menos tres zonas de disponibilidad (AZ=Availability Zone) para conseguir alta disponibilidad, alta escalabilidad y alta tolerancia a fallos.

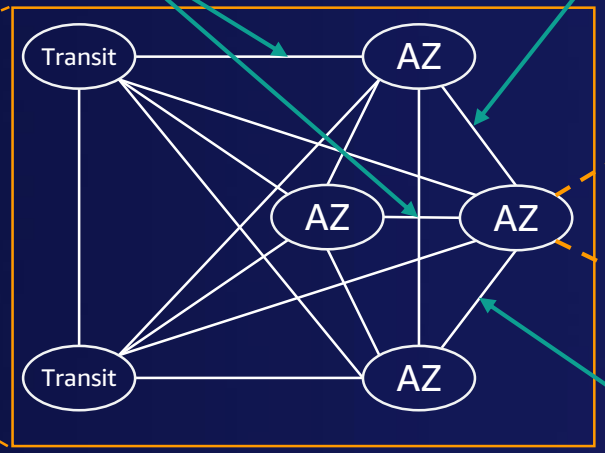
Los clientes mantienen siempre el control total de sus datos: En que región se almacenan, donde se procesan y quien tiene acceso a sus datos.

La red troncal o red interna de AWS, es propiedad de AWS. No utiliza a otros proveedores.

AWS **cifra datos** en la **capa física** de forma **automática**

La distancia asegura la **alta disponibilidad**

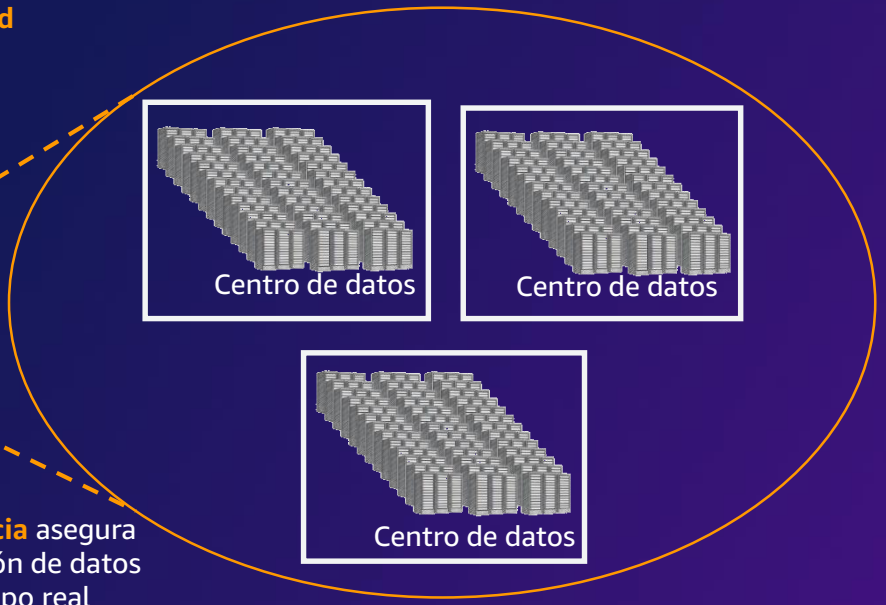
Región AWS



Baja latencia asegura la replicación de datos en tiempo real

Las AZ se crean en lugares donde no haya Fallas sísmicas, ni llanuras de inundación y donde existan redundancia de redes de comunicaciones y eléctricas para así reducir fallos simultáneos

Zonas de Disponibilidad (AZ) de AWS



Cada Zona de Disponibilidad tiene uno o mas centro de datos independientes, cada uno con su fuente de energía, red y conectividad redundante, alojados en instalaciones independientes

Más info: https://aws.amazon.com/about-aws/global-infrastructure/

¿Como protege el cliente la CIA de sus datos en AWS?

Medidas técnicas

Medidas operacionales

Medidas contractuales

Medidas Tecnicas

AWS Key Management Service (KMS)

AWS Certificate Manager

AWS Private Certificate Authority

AWS CloudHSM

AWS Nitro

AWS Identity & Access Management (IAM) y IAM access advisor

AWS Secrets Manager

AWS Certificate Manager

AWS Private Certificate Authority

AWS Signer

Amazon Macie

AWS Config

AWS CloudTrail

Amazon CloudWatch

Más info: https://docs.aws.amazon.com/whitepapers/latest/logical-separation/welcome.html
https://docs.aws.amazon.com/es_es/kms/latest/developerguide/concepts.html#key-mgmt

Medidas operacionales

Procesos y mejores practicas que nos va ayudar a mejorar nuestra postura de seguridad organizativa y a reducir los riesgos para así aumentar la efectividad en la protección de datos, los sistemas y sus recursos

Gestión de Identidad y Acceso

- Identity Mgmt. at scale
- Federation
- Access rights
- Access limitations
- Password policies
- Account level access security (ie: root)
- Local account level authentication
- Role based access control
- Account Hierarchy

Detección

- Org & Account level visibility
- Service level visibility
- Node level visibility
- Retention requirements
- Centralized log Ingestion (SIEM Integration)
- Traffic log collection
- Build foundation for automation

Protección de Infraestructura

- VPC patterns
- Hybrid Connectivity; Direct Connect/VPN
- Network security (Security Groups, NACLs, etc.)
- DDoS mitigation
- Web App Firewalls
- Configuration Mgmt. (ie: AMI Bakery)
- Designing for security, elasticity & availability

Protección del dato

- Encryption strategy
- KMS Playbooks & Runbooks
- Key & secrets management
- Encryption at rest
- Encryption in transit
- Integrity validation

Respuesta a incidente

- Alerting
- Investigations
- Cloud IR Procedures & Playbooks
- Preparation (IAM, AMI's, etc..)
- Automated response & remediation
- Containment
- Forensics
- Simulations

Controla los accesos	Gana visibilidad	Protégé tu infraestructura	Cifra tus Datos	Respuesta inmediata

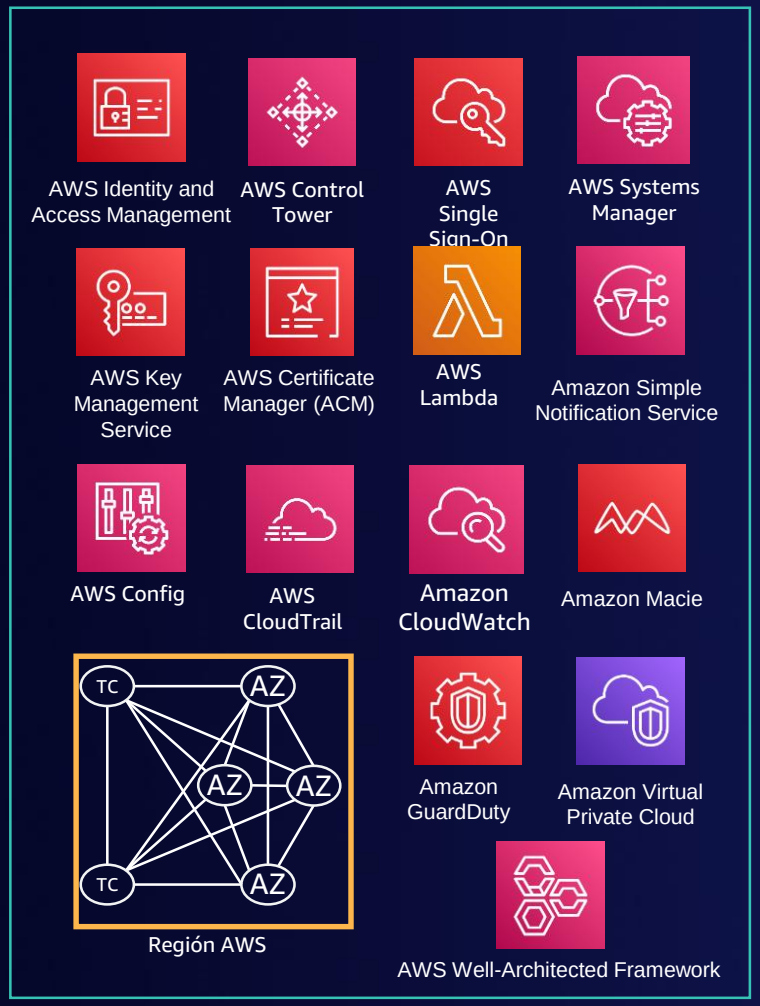
Más info: https://aws.amazon.com/es/architecture/well-architected

¿En que me puedo apoyar?

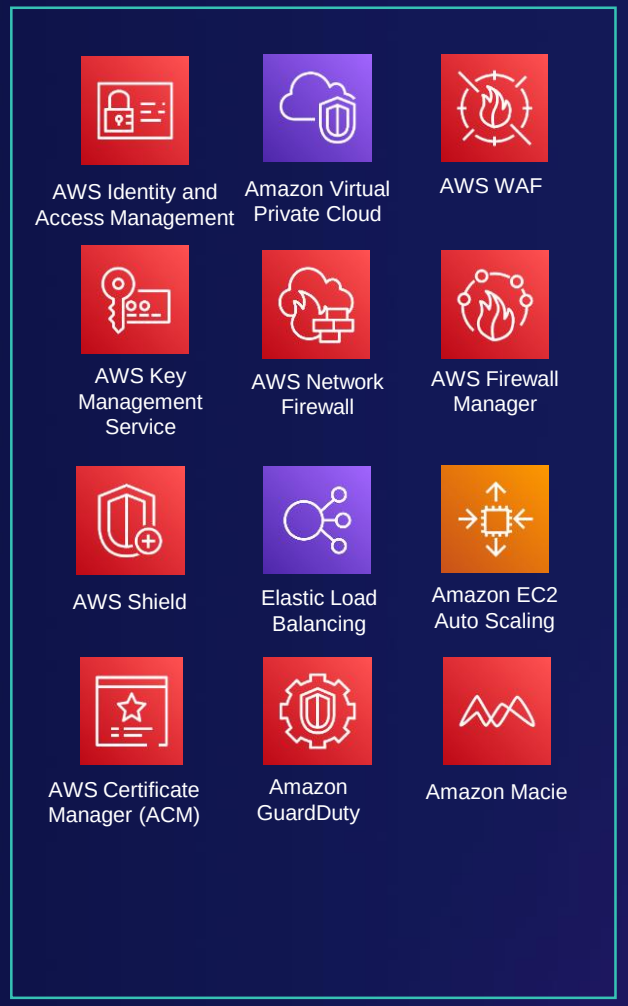
Guías CCN STIC para AWS +

Guía de configuración segura para AWS (CCN-STIC 887A)

Marco Operacional



Medidas de Protección

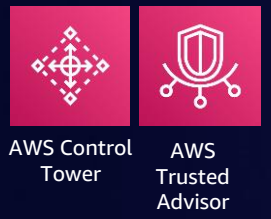


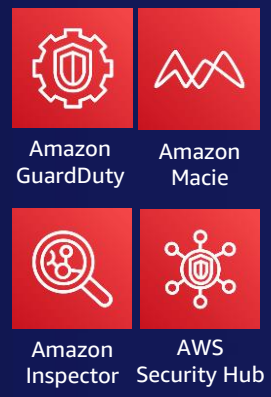
Pagina de inicio del CCN en AWS

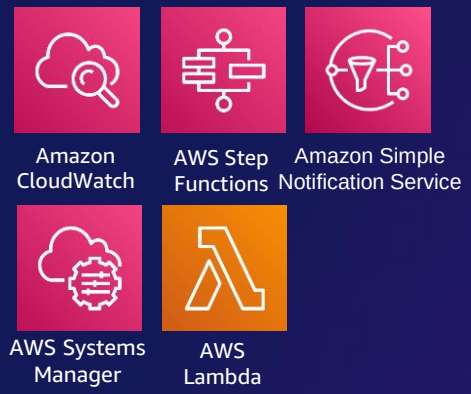
https://aws.amazon.com/es/compliance/esquema-nacional-de-seguridad/

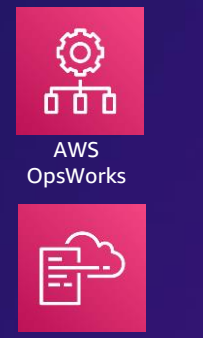
Medidas operacionales

Crear gobernanza del dato y la infraestructura lo mas automatizado posible, reduciendo la intervención humana

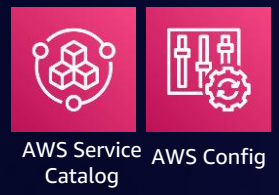




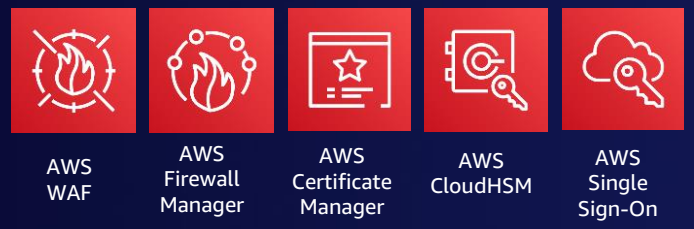




Identifica



Protege



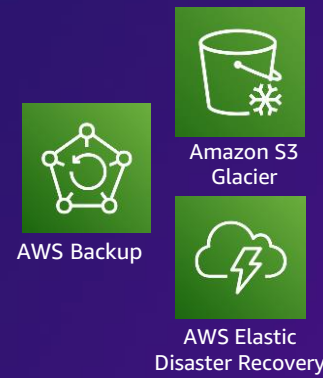
Detecta

Responde

Automatiza

Investiga

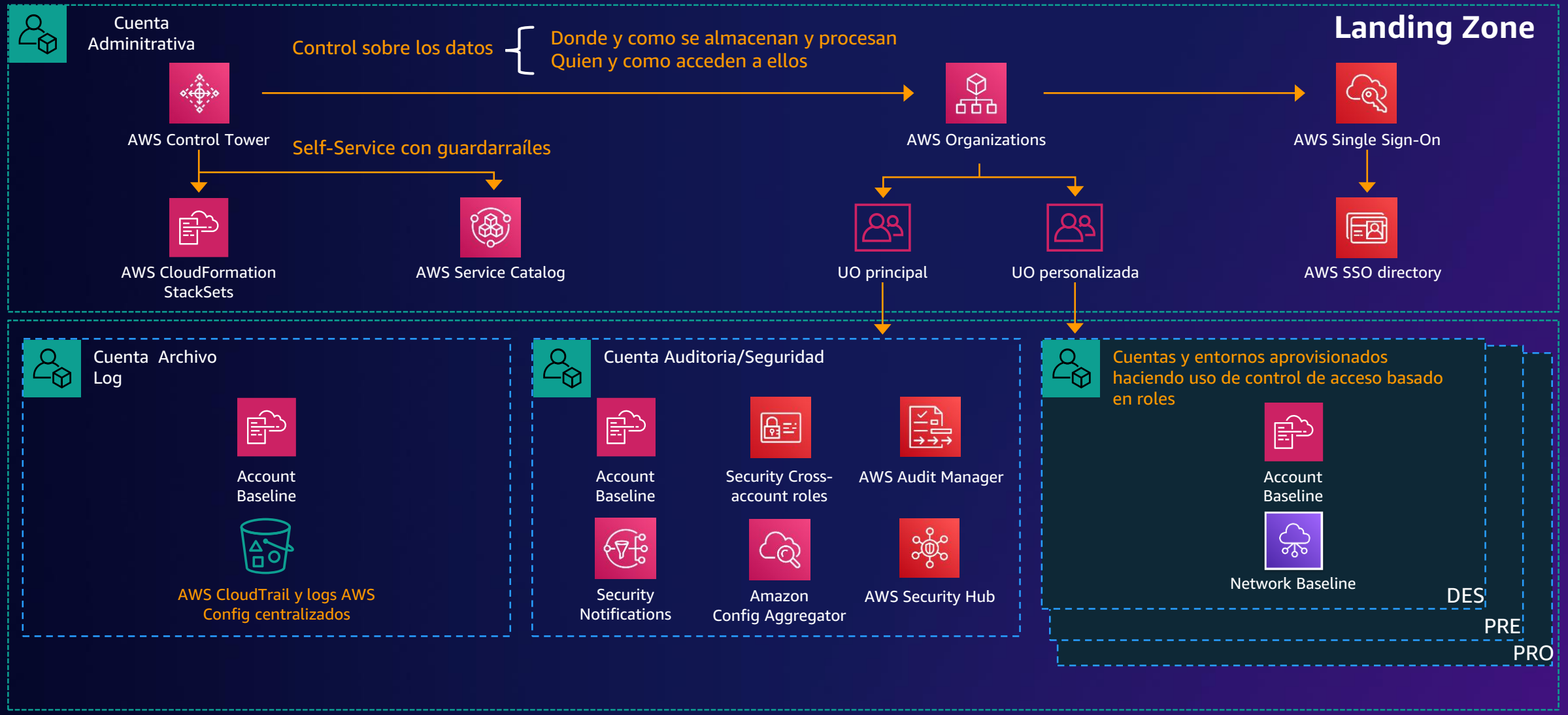
Recupera



Más info: https://aws.amazon.com/es/disaster-recovery/ransomware-recovery/

Como resultado, mediante estas medidas técnicas y operacionales

Vais a poder crear entornos de multi-cuenta seguros por defecto y cumpliendo con vuestra normativa corporativa



Más info: https://aws.amazon.com/es/controltower
https://aws.amazon.com/es/organizations/

Medidas Contractuales

Contrato de AWS con el cliente: Este contrato rige el uso que usted hace de nuestros servicios.

Términos de servicio de AWS: Estos términos adicionales rigen el uso que usted hace de determinados servicios. Incluye:

- Anexo de tratamiento de datos del RGPD de AWS (ATD)
- Anexo suplementario de AWS al ATD que incluye las recomendaciones del Comité Europeo de Protección de Datos para mantener la efectividad de las clausulas contractuales estándar tipo

Contratos de nivel de servicio de AWS: Estos contratos de nivel de servicio rigen el uso que usted hace de determinados servicios.

Política de uso aceptable de AWS: Esta política describe usos prohibidos de nuestros servicios.

Recomendaciones para marcas registradas de AWS: Esta página describe las recomendaciones a la hora de usar determinadas marcas registradas y otras designaciones.

Términos del sitio de AWS: Estos términos rigen el uso que usted hace del sitio web de AWS

Aviso de privacidad: Este aviso describe cómo se utiliza y se comparte la información sobre su persona

Ayuda sobre impuestos de AWS: Esta página ofrece información acerca de los impuestos que se aplican a sus servicios

AWS Europa: Esta página ofrece información acerca de AWS Europa

Más info: https://aws.amazon.com/es/legal/
https://aws.amazon.com/service-terms/?nc1=h_ls
https://aws.amazon.com/es/compliance/data-privacy/

Que encontramos en estas medidas contractuales?

- **Términos y condiciones en lenguaje claro y directo** para que sean transparentes y ayuden a entender la protección de la privacidad de los datos que ofrecemos
- **Obligaciones, rendimiento de cuentas, derechos, garantías, limites**, procesamiento de datos, confidencialidad de los datos, seguridad en el procesamiento de lo datos, medidas de seguridad sobre los datos, solicitud judicial sobre los datos del cliente, SLA de los servicios, notificación de incidentes, etc
- **Compromiso con el cumplimiento regulatorio vía contrato y sus adendum**, por ejemplo, el RGPD donde ofrecemos garantía de la propiedad y control de los datos del cliente por el mismo, incluyendo el almacenamiento y procesamiento
- **Transparencia** (listado de Subcontratatistas, Informes trimestral de solicitudes de información recibidas para la aplicación de la ley, opt-out en transferencia de datos, etc)
- **Certificaciones de seguridad y privacidad** obtenidas por AWS y el acceso al informe de auditoria.

Más info: https://aws.amazon.com/es/compliance/gdpr-center/ y https://aws.amazon.com/es/compliance/privacy-features/
https://aws.amazon.com/es/compliance/sub-processors/?nc1=h_ls
https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF&language=es_US

AWS Artifact

AWS respalda los más altos estándares de privacidad y certificaciones de conformidad para satisfacer los requisitos de nuestros clientes en todo el mundo

Nivel Alto

SOC 1

SOC 2

SOC 3

G-Cloud

FedRAMP

SEC Rule 17a-4(f)

CJIS

VPAT Section 508

My Number Act

GxP

FERPA

MPAA

AWS heredada todos los requisitos globales y nacionales que exigen gobiernos y clientes y da cumplimiento a ellos por auditores independientes de más de **98** programas de cumplimiento normativo en IT donde damos cumplimiento a **certificaciones, homologaciones, acreditaciones, regulaciones** y **leyes** de **Privacidad** en más de **190** países

Más info: https://aws.amazon.com/es/compliance/programs/ y https://aws.amazon.com/es/compliance/cispe/
https://aws.amazon.com/artifact/ y https://aws.amazon.com/es/compliance/esquema-nacional-de-seguridad/
https://oc.ccn.cni.es/catalogo-productos-stic/listado-productos-cualificados/780-aws-key-management-service-kms