Guía de Seguridad de las TIC
CCN-STIC 887
Anexo A

Landing Zone Accelerator en AWS para ENS categoría ALTA

DICIEMBRE 2024

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.12.04 09:39:32 +01'00'

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: diciembre de 2024

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. DESCRIPCIÓN GENERAL

La solución Landing Zone Accelerator de AWS (LZA) implementa un conjunto esencial de capacidades diseñadas para alinearse con las mejores prácticas de AWS y múltiples marcos de cumplimiento globales. Con esta solución, es posible administrar y controlar de manera más efectiva un entorno multi-cuenta en AWS que alberga cargas de trabajo altamente reguladas y requisitos de cumplimiento complejos.

Landing Zone Accelerator para ENS (LZA para ENS), es una implementación especial de Landing Zone Accelerator de AWS construida para acelerar el cumplimiento del Esquema Nacional de Seguridad en aquellas organizaciones que lo necesiten. **Landing Zone Accelerator para ENS, por sí misma, no hace que un entorno cumpla el Esquema Nacional de Seguridad en cualquiera de sus niveles, pero proporciona la infraestructura base que permita mantener una configuración segura alineada con el ENS y su monitorización de forma continua**. Landing Zone Acelerator para ENS permite el despliegue de una Landing Zone con y sin Control Tower basada en las buenas prácticas de AWS. Sobre dicho despliegue implementa controles adicionales publicados en la Guía de configuración de seguridad de AWS CCN-STIC-887A y despliega la solución open source Prowler que proporciona un marco de respuesta a incidentes y monitorización continua para el ENS en AWS.

El uso de Landing Zone Accelerator para ENS automatiza la implementación de los controles de refuerzo de ENS categoría ALTA en un entorno multi-cuenta en AWS y reduce el esfuerzo que deben realizar las organizaciones para configurar y operar cargas de trabajo seguras alineadas con la política del Esquema Nacional de Seguridad. Los principales beneficios de usar esta solución son:

- **Acelerar el cumplimiento de ENS**: el entorno de referencia incluye una estructura de organización preconfigurada, políticas de seguridad, configuración de red y otros servicios de seguridad de AWS para acelerar los procesos de cumplimiento generales, puesto que se basa en el código abierto predeterminado *lza-sample-config*. Adicionalmente Landing Zone Accelerator para ENS implementa controles específicos de AWS alineados con la última versión del ENS regulada en el Real Decreto 311/2022 que establece los estándares de seguridad que aplican a agencias gubernamentales y organismos públicos en España. Para más información sobre los controles implementados consulte la Guía de configuración de seguridad de AWS CCN-STIC-887A.
- **Acelerar la implementación de Landing Zone en la región de AWS de España**: implementa el entorno en la región "*eu-south-2*" (España), lo que aplica un refuerzo adicional alineado con la línea base de ENS publicada. Landing Zone Accelerator para ENS se despliega de forma preferencial en España, utilizando solamente servicios y funcionalidades soportadas en dicha región.
- **Mejora de la postura de seguridad y monitorización continua:** Landing Zone Acelerator para ENS despliega Prowler en la cuenta de auditoría de su Landing Zone para ayudarle en la tarea de evaluación continua del cumplimiento de las políticas de ENS y en la posible respuesta a incidentes o análisis forenses. Los controles de seguridad de Prowler se ejecutan a diario, enviando informes de cumplimiento a AWS Security Hub y almacenándolos en un bucket de S3.

2. CONTROLES DE SEGURIDAD DE LANDING ZONE ACELERATOR PARA ENS

Landing Zone Accelerator para ENS implementa una serie de controles de seguridad alineados y despliega herramientas para ayudar a las organizaciones a acelerar el cumplimiento de Esquema Nacional de Seguridad, incluyendo el nivel alto, siguiendo las recomendaciones plasmadas en la Guía de configuración de seguridad de AWS CCN-STIC-887A y en la matriz de controles adjunta al código de la solución.

De entre todos estos controles, a continuación, se detallan una serie de controles específicos que requieren una consideración especial.

2.1 USO DE IMDSv2

Amazon Elastic Compute Cloud (EC2) permite acceder a los metadatos de las instancias en ejecución mediante Instance Metadata Service (IMDS). IMDSv2 ofrece conexiones orientadas a la sesión que ofrecen medidas seguridad más estrictas que la versión predecesora. De cara reforzar los mecanismos de acceso a la información, Landing Zone Accelerator para ENS fuerza el uso de IMDSv2 en instancias EC2. Al activar IMDSv2, desactiva la posibilidad de usar IMDSv1, lo cual podría causar problemas con cualquiera de sus instancias existentes si están usando IMDSv1. Aunque a recomendación general de AWS de cara a mejorar su postura de seguridad y cumplir el ENS en su nivel alto es migrar sus instancias a IMDSv2, si desea desactivarlo, excluya enforce-imdsv2.json de la sección `serviceControlPolicies` en `organization-config.yaml` y comente la acción de corrección para `EC2_IMDSV2_CHECK`.

2.2 EVITE EL USO DE SERVICIOS Y REGIONES QUE NO CUMPLAN CON ENS NIVEL ALTO

AWS sigue un proceso de auditoría externo para validar que sus servicios y regiones cumplen con las condiciones marcadas en el ENS. En la actualidar, hay 31 regiones de AWS y 172 servicios de AWS que cumplen con ENS en su versión RD 311/2022, todos ellos de categoría ALTA.

Para evitar el uso de regiones y servicios que no se incluyen en esta lista, Landing Zone Accelerator para ENS implementa una política a nivel organizacional (SCP) que limita el uso de regiones y servicios para evitar el uso, por defecto, del uso de regiones o servicios no certificados para el ENS nivel alto. Esto podría generar que tuviera que modificar dicha política si quisiera incluir servicios no certificados.

2.3 ACCESO SEGURO A LOS SERVICIOS DE AWS

Un VPC Endpoint permite a los clientes conectarse de forma privada a servicios de AWS compatibles con la tecnología de AWS PrivateLink. Los VPC endpoints son dispositivos virtuales. Son componentes escalables horizontalmente, redundantes y que proporcionan alta disponibilidad. Permiten la comunicación entre instancias en una Amazon VPC y servicios sin imponer riesgos de disponibilidad ni restricciones de ancho de banda en el tráfico de red.

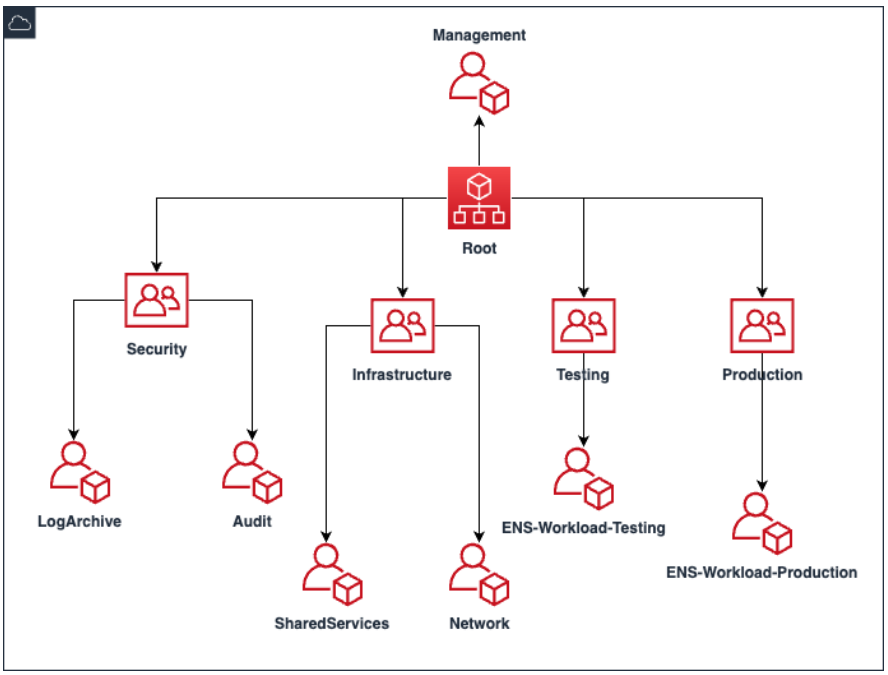
Landing Zone Accelerator para ENS crea automáticamente una colección básica de endpoints para los servicios más populares de AWS. Para evitar que el tráfico con otros servicios de AWS se fuera de su VPC, la recomendación es activar más VCP Endpoints. Podrá hacerlo en la sección `interfaceEndpoints` en la configuración de VPC en el fichero `network-config.yaml`, donde encontrará más ejemplos.

2.4 POLÍTICAS DE ETIQUETADO

Siguiendo los requisitos de ENS, los datos deben etiquetarse correctamente para crear inventarios de los datos y sistemas en diferentes dimensiones. Landing Zone Accelerator para ENS incluye una configuración de políticas de etiquetado base, basada en dimensiones de ejemplo, como centro de costos, tipo de entorno o confidencialidad de datos. Defina sus propias políticas de etiquetado para adaptarlas a los requisitos de su organización.

2.5 ESTRUCTURA DE LA ORGANIZACIÓN Y LA CUENTA

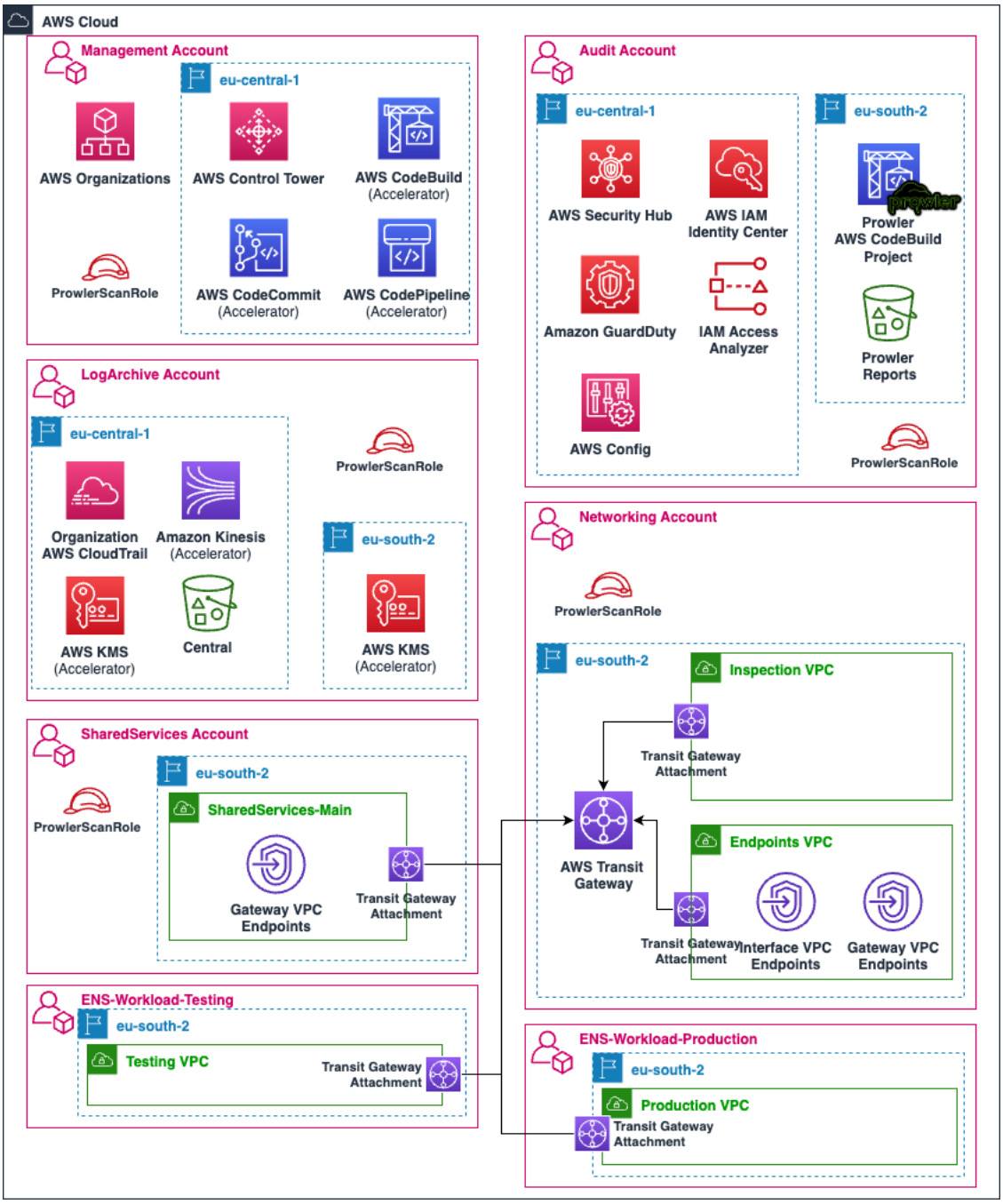
La organización y las cuentas se organizan de la siguiente manera:



Organización de LZA par ENS

Esta estructura es un ejemplo de una configuración básica, sin embargo, usted es libre de cambiar la estructura organizativa, las unidades organizativas (OU) y las cuentas para satisfacer sus necesidades específicas.

2.6 DIAGRAMA DE ARQUITECTURA



Arquitectura global de LZA para ENS

3. ANTES DE DESPLEGAR LANDING ZONE ACCELERATOR PARA ENS

Esta plantilla se ha probado y validado con LZA v1.10.0.

Si va a desplegar LZA para ENS en España, tenga en cuenta que esta es una región que no está activada por defecto en su cuenta de AWS y requerirá su activación previa. Adicionalmente, debe tener también en cuenta las consideraciones especiales para usar regiones opcionales.

Actualice su LZA a una versión soportada por esta configuración antes de desplegar LZA para ENS.

LZA para ENS requiere las siguientes unidades organizativas en su organización, y deben crearse antes de comenzar la implementación:

- Pruebas: unidad organizativa para cargas de trabajo de prueba.
- Producción: unidad organizativa para cargas de trabajo de producción.

Verifique los archivos de configuración y complételos con sus propios datos:

I. global-config.yaml

Modifique `enabledRegions` para incluir más regiones si es necesario. Incluya direcciones de correo electrónico para las notificaciones de AWS Security Hub y AWS Budget sustituyendo el texto `# <YOUR_EMAIL_ADDRESS>`.

Use el parámetro `controlTower` para desplegar la Landing Zone con AWS Control Tower. Tenga en cuenta que la implementación de Control Tower solo es compatible con la región de origen de LZA y que esta región debe ser compatible con AWS IAM Identity Center.

II. organization-config.yaml

Incluya las regiones adicionales incluidas anteriormente en la configuración de backup AWS Organizations (`backup-policies/backup-plan.json`). Tenga en cuenta que las regiones de 'opt-in' (entre las que está incluida `eu-south-2`) no admiten la función de administración de backup a nivel de Organización y debe configurar su plan de respaldo manualmente en estas regiones.

III. security-config.yaml

LZA para ENS incluye controles de seguridad específicos, así como la configuración de seguridad de las mejores prácticas de AWS. Sin embargo, algunas de las reglas de AWS Config especificadas para las buenas prácticas de AWS no son compatibles con `eu-south-2`, por lo que LZA para ENS no las incluye por defecto. Téngalo en cuenta a la hora de implementar su estrategia de cumplimiento.

IV. network-config.yaml

De manera predeterminada, los servicios de cuenta de red se implementan en `eu-south-2`. Cambie la variable `&HOME_REGION` para implementarlos en otra región. Tenga en cuenta que la configuración de las VPC se proporciona a modo de ejemplo. Dichas VPC están vacías y se crean para mostrar diferentes tipos de configuración. Cree su configuración de red antes de implementarla y considere seguir las recomendaciones de la Arquitectura de referencia de seguridad para diseñar su red:

https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/network.html

V. customizations-config.yaml

Este archivo controla la implementación de Prowler. Agregue su dirección de correo electrónico en `# <YOUR_EMAIL_ADDRESS>` para recibir notificaciones de informes de Prowler. También puede cambiar la variable `&HOME_REGION` para implementar Prowler en otra región.

4. INSTRUCCIONES

Siga los siguientes pasos para el despliegue de la solución Landing Zone Accelerator para ENS. En este documento se mencionan los pasos básicos, para obtener instrucciones detalladas, siga los vínculos de cada paso.

4.1 PASO 1. INICIE LA PILA

https://docs.aws.amazon.com/solutions/latest/landing-zone-accelerator-on-aws/step-1.-launch-the-stack.html

1. Inicie la plantilla de AWS CloudFormation en su cuenta de AWS.
2. Revise los parámetros de las plantillas e ingrese o ajuste los valores predeterminados según sea necesario.

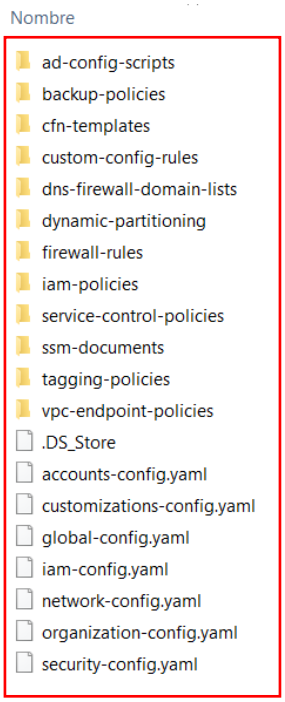
4.2 PASO 2. ESPERE EL DESPLIEGUE INICIAL DEL ENTORNO

https://docs.aws.amazon.com/solutions/latest/landing-zone-accelerator-on-aws/step-2.-await-initial-environment-deployment.html

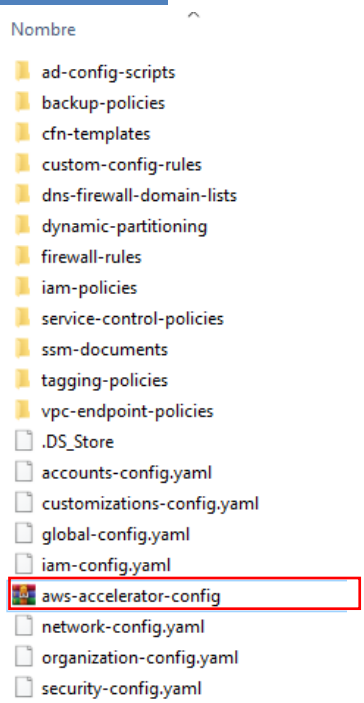
Espere que finalice el pipeline `AWSAccelerator-Pipeline` de forma correcta. Tardará unos 45 minutos en completarse.

4.3 PASO 3. COPIE LOS ARCHIVOS DE CONFIGURACIÓN DE LZA PARA ENS

Descargue y descomprima el template de LZA para ENS https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7262-ccn-stic-887-anexo-a-ens-lza-zip/file.html



Comprima todos los ficheros y renombralos a “aws-accelerator-config”



Estos archivos se deben subir a su repositorio de `CodeCommit`, `bucket S3`, o en un repositorio personalizado usando `AWS CodeConnections` dependiendo de los parámetros seleccionados durante el despliegue. Si no estás seguro, puede comprobar el `Configuration Repository Location` parámetro de su `AWSAccelerator-Installer`.

Se deben de sustituir los ficheros de aws-accelerator-config.zip, por los ficheros del LZA ENS.

https://docs.aws.amazon.com/solutions/latest/landing-zone-accelerator-on-aws/step-3.-update-the-configuration-files.html

4.4 PASO 4. DESPLIEGUE DE LZA PARA ENS

Una vez se han subido y sustituido los ficheros de configuración, debe acceder al servicio de CodePipeline – AWSAccelerator-Pipeline y haga clic en “Release changes” para realizar los cambios de template en el Landing Zone.

Posteriormente, se debe realizar la aprobación manual del Pipeline

Ten en cuenta que puedes encontrar algunos problemas durante el desarrollo. Comprueba si el problema es uno de los casos explicados en [Problemas conocidos y limitaciones.

Cualquier ejecución de la secuencia completa tarda alrededor de 45 minutos. Considere usar las opciones *"Retry Stage"* y *"Retry failed shares"* en CodePipeline para acelerar la implementación.

5. GLOSARIO

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía.

Término	Definición
ABAC	Attribute Based Access Control (control de acceso basado en atributos)
ACL	Access Control List (lista de control de acceso)
AI	Artificial Intelligence (Inteligencia Artificial)
API	Application Programming Interface (Interfaz de programación de aplicaciones)
Bucket	Contenedor para almacenar objetos pertenecientes al servicio S3
CCN	Centro Criptográfico Nacional
CloudTrail	Servicio de AWS que registra las llamadas a la API de AWS de la cuenta y proporciona archivos de registro.
CloudWatch	Servicio de AWS que permite monitorizar y administrar diversas métricas- así como configurar acciones de alarma en función de los datos de esas métricas
CMK	Customer Master Key (clave maestra del cliente)
Config	Servicio de AWS que ofrece un inventario de recurso de AWS- así como el historial de configuración y las notificaciones de los cambios en la configuración.
Control Tower	Servicio que ofrece una forma sencilla de configurar y gobernar un entorno de varias cuentas.
EBS	Elastic Block Storage (almacenamiento de bloques elástico)
EC2	Servicio web para lanzar y administrar instancias Linux/UNIX y Windows Server en los centros de datos de Amazon
ELB	Elastic LoadBalancer (balanceador de carga elástico)
ENS	Esquema Nacional de Seguridad
IAM	Identity and Access Management (gestión de accesos e identidades)
KMS	Key Management Service. Servicio gestionado de AWS que simplifica la creación y el control de las claves de cifrado que se utilizan para cifrar los datos.

Término	Definición
Lambda	Servicio web que permite ejecutar código sin aprovisionar ni administrar servidores. Puede ejecutar código para prácticamente cualquier tipo de aplicación o servicio back-end- sin necesidad de de administración
Landing Zone	Es una solución que ayuda a los clientes a configurar un entorno de AWS seguro y para varias cuentas, basado en las prácticas recomendadas de AWS.
Macie	Servicio de privacidad y seguridad de datos administrado que utiliza el aprendizaje automático y la correspondencia de patrones para descubrir y proteger datos confidenciales en AWS.
MFA	Multi-Factor Authentication (Autenticación de múltiples factores)
Prowler	Herramienta de software libre que se puede integrar con AWS que ayuda en la evaluación de la seguridad, auditoría, reducción de vulnerabilidades y respuesta a incidentes
S3	Servicio de almacenamiento para Internet. Se puede usar para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la Web.
Security Hub	Servicio que proporciona una vista integral del estado de seguridad de los recursos de AWS
SNS	Simple Notification Service (servicio de notificaciones simples)
Tags	Etiquetas
VPC	Virtual Private Cloud (nube privada virtual)
WAF	Web Application Firewall (cortafuegos de aplicaciones web)

6. GLOSARIO DE SERVICIOS AWS

A continuación, se reúnen los diferentes servicios mencionados a lo largo de esta guía incluyendo enlaces a la documentación concreta de cada uno de ellos. Como complemento de estos documentos se recomienda el uso del siguiente recurso enfocado a los aspectos de seguridad de cada uno de ellos: https://docs.aws.amazon.com/security/

Servicio	URL de documentación del servicio
Amazon CloudTrail	https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
Amazon CloudWatch	https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html
Amazon EC2	https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html
Amazon EFS	https://docs.aws.amazon.com/es_es/efs/latest/ug/whatisefs.html
Amazon Identity & Access Management (IAM)	https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/introduction.html
Amazon Macie	https://docs.aws.amazon.com/es_es/macie/latest/userguide/what-is-macie.html
Amazon S3	https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/Welcome.html
Amazon SNS	https://docs.aws.amazon.com/es_es/sns/latest/dg/welcome.html
Amazon VPC	https://docs.aws.amazon.com/es_es/vpc/latest/userguide/what-is-amazon-vpc.html
AWS Config	https://docs.aws.amazon.com/es_es/config/latest/developerguide/WhatIsConfig.html
AWS Control Tower	https://docs.aws.amazon.com/es_es/controltower/latest/userguide/what-is-control-tower.html
AWS Key Management Service (KMS)	https://aws.amazon.com/es/kms/
AWS Lambda	https://docs.aws.amazon.com/es_es/lambda/latest/dg/welcome.html
AWS Security Hub	https://docs.aws.amazon.com/es_es/securityhub/latest/userguide/what-is-securityhub.html

Servicio	URL de documentación del servicio
AWS VPN	https://docs.aws.amazon.com/es_es/vpn/latest/s2svpn/VPC_VPN.html
AWS WAF	https://docs.aws.amazon.com/es_es/waf/latest/developerguide/what-is-aws-waf.html