

# Guía de seguridad de las TIC CCN-STIC 887A

## Guía de configuración segura para AWS



Septiembre 2023





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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid  
© Centro Criptológico Nacional, 2023  
NIPO: 083-20-214-3

Fecha de Edición: septiembre de 2023

#### 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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## ÍNDICE

<b>1.</b>	<b>GUÍA DE CONFIGURACIÓN SEGURA PARA AWS</b>	<b>6</b>
1.1.	DESCRIPCIÓN DEL USO DE ESTA GUÍA	6
1.2.	DEFINICIÓN DEL SERVICIO	7
1.3.	MODELO DE RESPONSABILIDAD COMPARTIDA	7
1.4.	FUNCIONALIDADES DEL SERVICIO DE AWS	10
<b>2.</b>	<b>DESPLIEGUE SEGURO PARA AWS</b>	<b>11</b>
2.1	INFORMACIÓN PRECISA DE CUENTA	11
2.2	MÉTODOS DE PAGO	12
2.3	ETIQUETADO DE RECURSOS	12
2.4	INFRAESTRUCTURA COMO CÓDIGO	12
<b>3.</b>	<b>CONFIGURACIÓN SEGURA PARA AWS</b>	<b>13</b>
3.1	MARCO OPERACIONAL [OP]	13
	ARQUITECTURA DE SEGURIDAD [OP.PL.2]	13
	<i>Tecnologías de referencia en AWS</i>	13
	<i>Recomendaciones</i>	13
	DIMENSIONAMIENTO / GESTIÓN DE LA CAPACIDAD [OP.PL.4]	13
	<i>Tecnologías de referencia en AWS</i>	13
	<i>Requisitos y elementos de configuración</i>	14
	CONTROL DE ACCESO [OP.ACC]	16
	<i>Tecnologías de referencia en AWS</i>	16
	IDENTIFICACIÓN [OP.ACC.1]	20
	<i>Requisitos y elementos de configuración</i>	20
	<i>Recomendaciones</i>	21
	REQUISITOS DE ACCESO [OP.ACC.2]	21
	<i>Requisitos y elementos de configuración</i>	21
	<i>Recomendaciones</i>	21
	SEGREGACIÓN DE FUNCIONES Y TAREAS [OP.ACC.3]	22
	<i>Requisitos y elementos de configuración</i>	22
	<i>Recomendaciones</i>	22
	PROCESO DE GESTIÓN DE DERECHOS DE ACCESO [OP.ACC.4]	23
	<i>Requisitos y elementos de configuración</i>	23
	<i>Recomendaciones</i>	23
	MECANISMO DE AUTENTICACIÓN (USUARIOS DE LA ORGANIZACIÓN) [OP.ACC.6]	24
	<i>Requisitos y elementos de configuración</i>	24
	INVENTARIO DE ACTIVOS [OP.EXP.1]	28
	<i>Tecnologías de referencia en AWS</i>	28
	<i>Requisitos y elementos de configuración</i>	29
	<i>Recomendaciones</i>	29
	GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD [OP.EXP.3]	30
	<i>Tecnologías de referencia en AWS</i>	30
	<i>Recomendaciones</i>	30
	MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD [OP.EXP.4]	31
	<i>Tecnologías de referencia en AWS</i>	31
	<i>Requisitos y elementos de configuración</i>	32
	<i>Recomendaciones</i>	32
	GESTIÓN DE CAMBIOS [OP.EXP.5]	33
	<i>Tecnologías de referencia en AWS</i>	33
	<i>Recomendaciones</i>	33
	PROTECCIÓN FRENTE A CÓDIGO DAÑINO [OP.EXP.6]	34
	<i>Tecnologías de referencia en AWS</i>	34

Requisitos y elementos de configuración .....	34
Recomendaciones.....	34
GESTIÓN DE INCIDENTES [OP.EXP.7] .....	35
Requisitos y elementos de configuración .....	35
Recomendaciones.....	36
REGISTRO DE LA ACTIVIDAD [OP.EXP.8] .....	37
Tecnologías de referencia en AWS .....	37
Requisitos y elementos de configuración .....	37
Recomendaciones.....	38
REGISTRO DE LA GESTIÓN DE INCIDENTES [OP.EXP.9] .....	39
Tecnologías de referencia en AWS .....	39
Recomendaciones.....	39
PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS [OP.EXP.10] .....	40
Tecnologías de referencia en AWS .....	40
Requisitos y elementos de configuración .....	41
Recomendaciones.....	42
CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO [OP.EXT.1] .....	42
Requisitos y elementos de configuración .....	42
GESTIÓN DIARIA [OP.EXT.2].....	43
Recomendaciones.....	43
PLAN DE CONTINUIDAD [OP.CONT.2].....	43
Tecnologías de referencia en AWS .....	43
Requisitos y elementos de configuración .....	43
Recomendaciones.....	45
PRUEBAS PERIÓDICAS [OP.CONT.3] .....	46
Tecnologías de referencia en AWS .....	46
Recomendaciones.....	46
MEDIOS ALTERNATIVOS [OP.CONT.4] .....	46
Tecnologías de referencia en AWS .....	46
Recomendaciones.....	47
DETECCIÓN DE INTRUSIÓN [OP.MON.1] .....	48
Tecnologías de referencia en AWS .....	48
Requisitos y elementos de configuración .....	48
Recomendaciones.....	48
SISTEMA DE MÉTRICAS [OP.MON.2] .....	49
Tecnologías de referencia en AWS .....	49
Recomendaciones.....	49
VIGILANCIA [OP.MON.3] .....	50
Tecnologías de referencia en AWS .....	50
Requisitos y elementos de configuración .....	50
<b>3.1 MEDIDAS DE PROTECCIÓN [MP] .....</b>	<b>52</b>
PROTECCIÓN DE LAS COMUNICACIONES [MP.COM] .....	52
Tecnologías de referencia en AWS .....	52
PERÍMETRO SEGURO [MP.COM.1] .....	53
Requisitos y elementos de configuración .....	53
PROTECCIÓN DE LA CONFIDENCIALIDAD [MP.COM.2] .....	54
Requisitos y elementos de configuración .....	54
Recomendaciones.....	55
PROTECCIÓN DE LA INTEGRIDAD Y DE LA AUTENTICIDAD [MP.COM.3] .....	55
Requisitos y elementos de configuración .....	55
Recomendaciones.....	55
SEPARACIÓN DE FLUJOS DE INFORMACIÓN EN LA RED [MP.COM.4] .....	55
Requisitos y elementos de configuración .....	55
CRIPTOGRAFÍA [MP.SI.2].....	57
Tecnologías de referencia en AWS .....	57
Requisitos y elementos de configuración .....	57
Recomendaciones.....	58

ACEPTACIÓN Y PUESTA EN SERVICIO [MP.SW.2] .....	58
<i>Tecnologías de referencia en AWS</i> .....	58
<i>Recomendaciones</i> .....	59
COPIAS DE SEGURIDAD [MP.INFO.6] .....	60
<i>Tecnologías de referencia en AWS</i> .....	60
<i>Recomendaciones</i> .....	62
PROTECCIÓN DEL CORREO ELECTRÓNICO [MP.S.1] .....	63
<i>Tecnologías de referencia en AWS</i> .....	63
<i>Requisitos y elementos de configuración</i> .....	63
PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB [MP.S.2] .....	64
<i>Requisitos y elementos de configuración</i> .....	64
PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO [MP.S.4] .....	64
<i>Tecnologías de referencia en AWS</i> .....	64
<i>Requisitos y elementos de configuración</i> .....	65
<i>Recomendaciones</i> .....	65
<b>4 GLOSARIO DE TÉRMINOS .....</b>	<b>66</b>
<b>5 GLOSARIO DE SERVICIOS AWS .....</b>	<b>68</b>
<b>6 CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD .....</b>	<b>73</b>

## 1. GUÍA DE CONFIGURACIÓN SEGURA PARA AWS

### 1.1. DESCRIPCIÓN DEL USO DE ESTA GUÍA

El contenido de esta guía muestra el despliegue y configuración para cargas de trabajo en la nube pública de Amazon Web Services (AWS) siguiendo las exigencias del Esquema Nacional de Seguridad (ENS).

Siguiendo los pasos de configuración descritos en esta guía se pueden validar los siguientes principios de seguridad:

- Implementación de una base de identidades solidas.
- Trazabilidad.
- Seguridad en todas las capas.
- Automatización de las buenas prácticas de seguridad.
- Protección de los datos en tránsito y en reposo.
- Automatización en el procesamiento de datos.
- Gestión de eventos de seguridad.

La principal utilidad de esta guía es explicar y referir a los servicios ofrecidos por AWS para cumplir con las diferentes medidas de seguridad del ENS. Algunos de estos servicios y su nomenclatura pueden ser nuevos para el lector, por lo que se ha incluido un glosario de términos como anexo al documento, así como referencias a la documentación oficial del fabricante de modo que se facilite la lectura y comprensión por parte del usuario de esta guía.

Por cada una de las medidas de seguridad del ENS se han descrito, según el caso, todos o algunos de los siguientes apartados:

- Tecnologías de referencia en AWS: Descripción de las herramientas y servicios disponibles en AWS para el cumplimiento de los controles o familia de controles.
- Requisitos y elementos de configuración: Explicación prescriptiva sobre cómo usar las herramientas y servicios de AWS para el cumplimiento de las medidas de seguridad del ENS.
- Recomendaciones: Explicaciones adicionales de carácter voluntario para una mejor seguridad en el entorno de AWS y/o cumplimiento del ENS.

La aplicabilidad de las diferentes medidas de seguridad en ENS queda definida en la guía **CCN-STIC 887 Perfil de cumplimiento específico para AWS Servicio de Cloud Corporativo**, en el que se ofrece el detalle de qué medidas del ENS son de aplicación al ámbito de AWS y deberán implementarse para acogerse al perfil de cumplimiento, así como criterios interpretativos para su correcta adopción. Quedan fuera de la presente guía aquellas medidas de seguridad que se encuentran fuera del ámbito de AWS bien por ser de carácter organizativo o procedimental o bien por requerir una operativa manual ajena a AWS para su cumplimiento.

Muchas de las configuraciones incluidas en este documento tienen la posibilidad técnica de ser validadas de manera automática durante su planificación en el tiempo

(programática). Para todas estas medidas se incluye una referencia a un identificador que corresponde a un chequeo de Prowler.

Prowler es una herramienta de software libre que permite analizar múltiples servicios y recursos desplegados en AWS de forma manual o automática. Tanto la documentación como el código de la herramienta se encuentra en la siguiente dirección web.

### Documentación Prowler

Prowler se puede integrar con AWS Security Hub, un conjunto de herramientas que tiene el cometido de proporcionar una visión completa del estado de seguridad de una infraestructura en AWS y permite comprobar el entorno comparándolo con los estándares y las prácticas recomendadas por las diferentes entidades del sector de la seguridad incluyendo, entre éstas, el ENS.

La sección 6 consolida la lista completa de medidas de seguridad y recomendaciones, incluyendo los chequeos automatizables de manera programática, así como una referencia de inicio rápido a la herramienta Prowler.

## 1.2. DEFINICIÓN DEL SERVICIO

Amazon Web Services (AWS) es un servicio de infraestructura y plataforma de nube completa que puede alojar aplicaciones, simplificar el desarrollo de nuevas soluciones e incluso mejorar los sistemas locales. Amazon Web Services ofrece un amplio conjunto de servicios globales basados en la nube, incluidos recursos para cómputo, almacenamiento, bases de datos, análisis, redes, herramientas para desarrolladores, herramientas de administración, IoT, seguridad y aplicaciones empresariales, entre otros. Estos servicios ayudan a las organizaciones, tanto públicas como privadas, a avanzar con mayor rapidez, reducir los costos de TI permitiéndole ser elástica y escalable.

AWS cuenta con la confianza de las mayores compañías y las empresas emergentes más innovadoras para respaldar una amplia variedad de cargas de trabajo, como las aplicaciones web y móviles, el desarrollo de juegos, el almacenamiento y procesamiento de datos, el almacenamiento en general o el archivado, entre muchas otras. Para el sector público, los servicios en la nube de AWS facilitan un soporte para mejorar la eficacia, la escalabilidad y la seguridad de las operaciones y, en definitiva, prestar mejores servicios a los ciudadanos. Además, los servicios de AWS están alineados con los mayores estándares de seguridad tanto nacionales como internacionales, incluido el ENS.

## 1.3. MODELO DE RESPONSABILIDAD COMPARTIDA

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS y el cliente. Este modelo compartido puede aliviar la carga operativa del cliente, ya que AWS opera, administra y controla los componentes del sistema operativo host y la capa de virtualización hasta la seguridad física de las

instalaciones en las que funcionan los servicios. El cliente asume la responsabilidad y la administración del sistema operativo que utiliza cada instancia (incluidas las actualizaciones y los parches de seguridad), de cualquier otro software de aplicaciones asociado y de la configuración del firewall del grupo de seguridad que ofrece AWS.

Los clientes deben pensar detenidamente en los servicios que eligen, ya que las responsabilidades varían en función de los servicios que utilicen, de la integración de estos en su entorno de TI y de la legislación y los reglamentos correspondientes.

En el caso de que se vayan a utilizar soluciones de terceros que formen parte de la arquitectura de seguridad del sistema, estas deben cumplir con el ENS, preferiblemente provistas por partners de AWS o adquiridas a través del Marketplace de AWS.

La naturaleza de esta responsabilidad compartida también ofrece la flexibilidad y el control por parte del cliente que permite concretar la implementación. Como se muestra a continuación. La diferenciación de responsabilidades se conoce normalmente como seguridad "de" la nube y seguridad "en" la nube.

**Responsabilidad de AWS en relación con la "seguridad de la nube":** AWS es responsable de proteger la infraestructura que ejecuta todos los servicios provistos en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

**Responsabilidad del cliente en relación con la "seguridad en la nube":** la responsabilidad del cliente estará determinada por los servicios de la nube de AWS que el cliente seleccione. Esto determina el alcance del trabajo de configuración a cargo del cliente como parte de sus responsabilidades de seguridad. Es importante tener en cuenta que el cliente de los servicios de AWS no queda exento de esta responsabilidad, aunque cuente con los servicios de un partner de AWS o de un tercero que se encargue de la operación o configuración de su entorno AWS.

Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se clasifica como servicios de Infraestructura y, como tal, requiere que el cliente realice todas las tareas de administración y configuración de seguridad necesarias, incluyendo el ya mencionado firewall del grupo de seguridad.

Amazon EC2 es una solución de virtualización similar a los servicios que ofrecen las herramientas de tipo Hypervisor (al menos en lo que a nivel operacional se refiere) en la que un servidor actúa de huésped alojando máquinas virtuales (en este caso, denominadas instancias) e interconectándolas. Los sistemas y servicios instalados en dichas máquinas virtuales y las comunicaciones y permisos entre ellas, así como la protección de datos contenidos y seguridad en dichas comunicaciones, no son gestionados por AWS sino por el cliente.

Los clientes que implementan una instancia de Amazon EC2, por tanto, son responsables de la administración del sistema operativo que usen en la misma (incluidos los parches de seguridad y las actualizaciones), de cualquier utilidad o software de aplicaciones que el cliente haya instalado en las instancias y de la configuración del firewall provisto por AWS (llamado grupo de seguridad) en cada instancia.



En el caso de los servicios gestionados por AWS, como Amazon Simple Storage Service (Amazon S3, servicios de almacenamiento gestionados) y Amazon DynamoDB (servicios de base de datos gestionados), AWS maneja la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes acceden a los puntos de enlace para recuperar y almacenar los datos. Los clientes son responsables de administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y utilizar las herramientas de AWS Identity and Access Management (AWS IAM) para solicitar los permisos correspondientes.

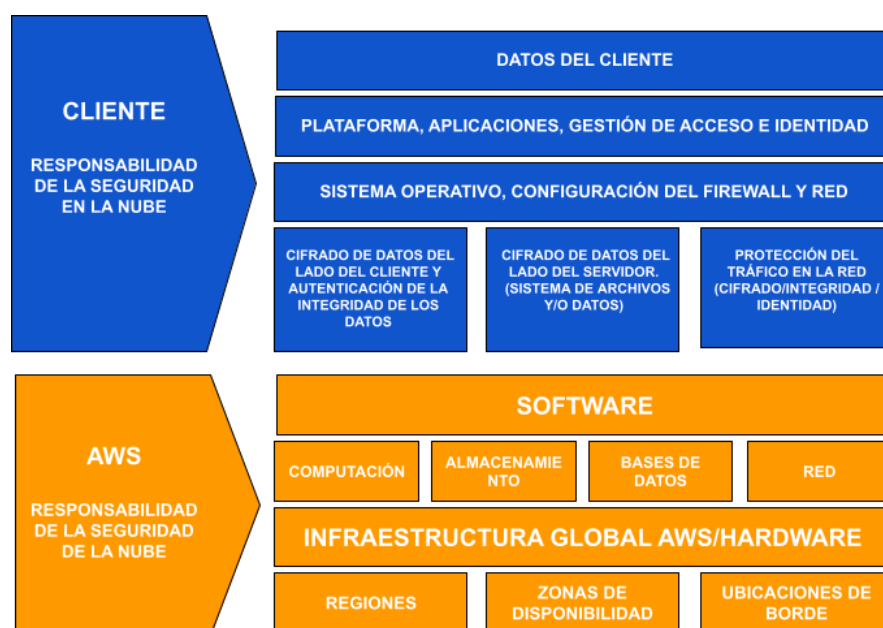


Fig. 1 - Representación del modelo de responsabilidad compartida en AWS

El modelo de responsabilidad compartida entre AWS y sus clientes, abarca también los controles de TI. Del mismo modo que comparten la responsabilidad del entorno, también comparten la administración, el funcionamiento y la verificación de los controles de TI. En este sentido, la presente guía es un recurso para el cliente de AWS referente al ámbito de la responsabilidad del cliente en cuanto a la seguridad de infraestructura y datos según el tipo de servicios utilizados.

Así mismo, los clientes pueden hacer uso de la documentación de conformidad y control disponible en AWS, así como sus procedimientos de verificación y evaluación de los controles.

A continuación, se enumeran varios ejemplos de controles y se especifica a qué entidad corresponde la responsabilidad según el tipo de control:

- **Controles heredados:** Los controles heredados son aquellos que un cliente hereda de AWS en su totalidad. Son aquellos controles sobre los que el cliente no tiene ningún tipo de acceso, como los controles físicos y de entorno.
- **Controles compartidos:** Aplican tanto a la capa de infraestructura como a las capas de clientes. En un control compartido, el encargado de suministrar los

requisitos para la infraestructura recae en AWS y la responsabilidad de configuración de aplicaciones, bases de datos y sistemas operativos de las instancias (de los huéspedes). Por ejemplo, la administración de parches, la corrección de imperfecciones o la administración de las configuraciones, serían responsabilidad de AWS en lo que se refiere a los elementos internos de la infraestructura (hosts y servicios gestionados). Sin embargo, el cliente será responsable de configurar sus aplicaciones, bases de datos y sistemas operativos huésped.

- **Controles específicos del cliente:** Aquellos elementos que son de absoluta responsabilidad del cliente incluirían la seguridad de zonas, protección de comunicaciones y servicios. El direccionamiento y el aislamiento para la protección de la información deberá ser definido por el cliente.

## 1.4. FUNCIONALIDADES DEL SERVICIO DE AWS

La plataforma AWS ofrece diferentes servicios de infraestructura y de plataforma definidos como herramientas estandarizadas y automatizadas. Se puede diferenciar en esta oferta de servicios entre:

- **Infraestructura**, que incluye recursos de infraestructura como computación, redes y almacenamiento. Ejemplos de estos servicios son:
  - Amazon VPC (Virtual Private Cloud): Red privada virtual en la nube (redes virtuales gestionadas por el cliente).
  - Amazon EC2 (Elastic Computing): Servicio de instancias gestionadas por el cliente (instancias de Linux y Windows Server).
  - Amazon EBS (Elastic Block Store): Volúmenes de almacenamiento persistente en bloques (almacenamiento virtual gestionado por el cliente).
- **Plataforma**, que ofrece aplicaciones, bases de datos y funciones, todas ellas como servicios gestionados por AWS. La diferencia radica en que el cliente configura parámetros del servicio, pero no el propio servicio. Por ejemplo, el cliente añade instancias y alimenta una base de datos, pero no gestiona el servidor que contiene dicha base de datos. Ejemplos de estos servicios son
  - Amazon RDS (Relational Database Service). AWS Gestiona servicios de bases de datos relacionales (soporta diferentes tipos de bases de datos) encargándose del mantenimiento, la seguridad y la disponibilidad.
  - Amazon S3 (Simple Cloud Storage). AWS gestiona servicios de almacenamiento encargándose del mantenimiento, la seguridad y la disponibilidad.
  - AWS Lambda. Servicio de ejecución de código que soporta diferentes lenguajes y permite lanzar instrucciones mediante scripting a elementos gestionados por AWS.
- **Software**, que se ofrece bajo demanda de forma totalmente gestionada. Ejemplos de estos servicios son:
  - Amazon Workspaces. Aprovisionamiento de escritorios virtuales (Windows y Linux) completamente gestionados por AWS.
  - Amazon Workmail. Servicio de correo totalmente gestionado por AWS.

- Amazon Workdocs. Servicio de creación de contenido, almacenamiento y colaboración gestionado completamente por AWS.

Todos estos recursos son escalables y elásticos en el tiempo y son medibles por uso. El servicio AWS incluye interfaces de autoservicio que están directamente disponibles para el usuario en forma de interfaces web (UI) y APIs para consumo de manera programática.

La plataforma de nube AWS cumple con las medidas de seguridad exigidas que permiten conseguir la certificación de conformidad del Esquema Nacional de Seguridad en su categoría ALTA.

Para obtener más detalles de la conformidad de AWS en cuanto a sus responsabilidades de seguridad para el ENS, es posible consultar el siguiente documento del fabricante:

[Esquema Nacional de Seguridad \(categoría Alta\)](#)

Es posible comprobar los productos y servicios que son aprobados para su uso dentro del ENS por medio del siguiente enlace:

[Servicios de AWS en el ámbito del programa de conformidad](#)

## 2. DESPLIEGUE SEGURO PARA AWS

Una cuenta de AWS es un contenedor de todos sus recursos de AWS. Puede crear y administrar sus recursos de AWS en una cuenta de AWS, y esta cuenta proporcionará capacidades administrativas de acceso y facturación. Desde la cuenta de AWS también permite administrar aspectos como la facturación, la seguridad y los permisos de acceso. Es preciso no confundir la cuenta de AWS con los usuarios de AWS Identity and Access Management (IAM), que son recursos de AWS IAM con credenciales y permisos asociados que representan a una persona o a una aplicación que utiliza sus credenciales para realizar solicitudes de AWS.

En el ámbito de la seguridad es preciso tener en cuenta una serie de aspectos generales que garanticen la continuidad y confidencialidad de los servicios.

Se detallan a continuación los aspectos necesarios para una correcta configuración de una nueva cuenta:

### 2.1 INFORMACIÓN PRECISA DE CUENTA

El correo electrónico principal que será proporcionado al dar de alta los servicios en AWS, y al cual quedará asociado el correo electrónico del usuario root de la cuenta deberá ser siempre un correo con el dominio de la empresa de modo que su recuperación sea independiente de la permanencia de determinados empleados en la empresa. Ya que, en caso de necesidad, debe ser posible la recuperación de dicha cuenta de correo o su asignación a otro usuario. En este sentido se recomienda el uso de una lista de distribución cuyo acceso esté correctamente protegido. Esta cuenta root

deberá configurarse siguiendo las recomendaciones del apartado [Control de acceso \[op.acc\]](#) y evitar completamente su uso para tareas habituales.

## 2.2 MÉTODOS DE PAGO

El método de pago tiene impacto en cuanto a que la disponibilidad del servicio estará sujeta a la disponibilidad del método de pago. Se recomienda en este aspecto el uso depago por IBAN o de facturación a través de un partner de AWS en lugar de tarjeta de crédito, que siempre podrá sufrir problemas de limitaciones o incluso caducidades no controladas.

Puede consultar más detalles sobre el proceso de activación de una cuenta en el siguiente documento:

[Proceso de creación y activación de una cuenta AWS](#)

## 2.3 ETIQUETADO DE RECURSOS

El etiquetado en AWS consiste en la asignación de metadatos en forma de etiquetas (*tags*) a los diferentes recursos. Cada etiqueta consta de una clave y un valor definidos por el usuario y sirven para ayudar a la entidad usuaria a administrar, identificar, organizar, buscar y filtrar recursos con base en diferentes criterios como pueden ser la finalidad, la propiedad o la criticidad del recurso en cuestión.

Más allá de los requisitos de etiquetado contenidos en el cuerpo de esta guía (por ejemplo, para la identificación de los responsables de los activos en la medida de seguridad Inventario de activos [op.exp.1]), para llevar a cabo una adecuada gestión de la configuración de la seguridad en AWS es importante que sean etiquetados todos los recursos pertenecientes a la misma pila applicativa o sistema sobre el que se quiera implementar las medidas de seguridad. De este modo, se podrá delimitar el alcance sobre el que se quieren aplicar las medidas de seguridad y, en su caso, certificar el Esquema Nacional de Seguridad.

Para llevar a cabo un adecuado seguimiento de la configuración de seguridad es importante que sean etiquetados todos los recursos pertenecientes a la misma pila applicativa y poder así delimitar el alcance de las evaluaciones de seguridad automatizadas. En caso contrario, la herramienta de análisis automatizado incluirá todos los recursos pertenecientes a una misma cuenta, independientemente de su función o valor.

En la documentación de AWS encontrará información detallada sobre la implementación y la aplicación de una estrategia de etiquetado.

[Etiquetado de los recursos de AWS](#)

## 2.4 INFRAESTRUCTURA COMO CÓDIGO

En la nube de AWS se permite el aprovisionamiento de la infraestructura a través de código, lo cual es una práctica altamente recomendada. Para ello, el servicio AWS

Cloud Formation permite modelar, aprovisionar y administrar los recursos de AWS a partir del tratamiento de código. Se pueden crear plantillas que describan todos los recursos de AWS necesarios (como por ejemplo instancias Amazon EC2 o de bases de datos Amazon RDS) y sus configuraciones, sin que sea necesario crear y configurar individualmente los recursos ni averiguar las dependencias entre ellos.

Esta modalidad de despliegue no solamente simplifica el despliegue de la infraestructura, sino también su escalado, la automatización y pruebas y, además, constituye una buena práctica de seguridad en tanto en cuanto permite la vuelta de los recursos a un estado definido en el código simplemente ejecutando éste, sin necesidad de llevar a cabo toda la operativa de configuración manual.

### 3. CONFIGURACIÓN SEGURA PARA AWS

En las secciones siguientes se presentan las tecnologías de referencia en AWS y las medidas de aplicación comprendidas en los ámbitos Marco Operacional y Medidas de Protección del Esquema Nacional de Seguridad.

#### 3.1 MARCO OPERACIONAL [op]

Este conjunto de medidas de seguridad del marco operacional está formado por las medidas a tomar en cuenta para proteger la operación del sistema como un conjunto integral de componentes para un fin.

##### Arquitectura de Seguridad [op.pl.2]

#### Tecnologías de referencia en AWS

##### *Well-Architected Framework*

AWS Well-Architected Framework proporciona una serie de prácticas recomendadas de arquitectura segura dividida en seis pilares fundamentales para diseñar y operar sistemas confiables, seguros, eficientes, rentables y sostenibles en la nube que permitirán al usuario centrarse en mayor medida en los requisitos funcionales de cada servicio. Adicionalmente, sirve para garantizar la aplicación de buenas prácticas de arquitectura e identificar áreas de mejora de negocio.

#### Recomendaciones

Para cumplir con las exigencias del Esquema Nacional de Seguridad e identificar buenas prácticas en el despliegue de una arquitectura de seguridad en AWS, es recomendable que la entidad usuaria se apoye en el marco de trabajo AWS Well-Architected Framework.

##### Dimensionamiento / gestión de la capacidad [op.pl.4]

#### Tecnologías de referencia en AWS

### *Amazon CloudWatch Logs*

Amazon CloudWatch Logs es un servicio que permite monitorear, almacenar y acceder a los archivos de registro de instancias de Amazon Elastic Compute Cloud (Amazon EC2), AWS CloudTrail, Amazon Route 53 y otras fuentes. Mediante el uso de otros servicios asociados como AWS CloudTrail es posible generar alarmas en Amazon CloudWatch, recibir notificaciones de diferentes eventos; y utilizar esa notificación para solucionar problemas o dimensionar la capacidad de servicios concretos, alertando al usuario del momento en el que se acerca al umbral de uso contratado.

Más información sobre este servicio en el siguiente enlace.

[CloudWatch Logs - AWS CloudWatch.](#)

### *Service Quotas*

Las Cuotas de Servicio, anteriormente denominadas límites de servicio de AWS, son los valores máximos de recursos, acciones y elementos asignados a una cuenta o región de AWS. Para cada servicio contratado se definen una serie de cuotas a las cuales se les asigna un valor inicial por defecto, que podrá ser revisado y modificado en función de las necesidades del negocio. Haciendo uso de otras soluciones de AWS como Quota Monitor o Amazon CloudWatch el usuario puede hacer un seguimiento proactivo del uso de los recursos mediante métricas y enviar notificaciones de alerta cuando este se acerque al valor establecido para cada cuota.

Más información sobre las cuotas de servicio en el siguiente enlace.

[Cuotas de servicio - Service Quotas.](#)

## **Requisitos y elementos de configuración**

Para cumplir con el requisito base de [op.pl.4], la entidad usuaria deberá llevar a cabo el estudio de capacidades al que hace referencia la medida de seguridad, si bien, en el ámbito de AWS, se deberá tener especialmente en cuenta:

- Las necesidades de capacidad de procesamiento, almacenamiento y comunicaciones de las instancias desplegadas en AWS.
- Las cuotas de los servicios a utilizar. En particular, deberá tener en cuenta si las cuotas predeterminadas de los servicios a utilizar son suficientes para la satisfacción de las necesidades del sistema o se requerirá solicitar una ampliación.

Además, para el cumplimiento del refuerzo para la Mejora continua de la gestión de la capacidad [op.pl.4.r1], en caso de no disponer de herramientas de terceros, se deberán utilizar las herramientas de monitorización de la capacidad indicadas para monitorizar las capacidades de la infraestructura y el grado de consumo de los servicios en función de las cuotas disponibles.

Para la creación de alarmas en materia de capacidad de las instancias se deben

seguir los siguientes pasos.

1. Permitir el envío de mails automáticos a la dirección de correo seleccionada.

#### [Configurar una notificación mediante Amazon SNS](#)

2. Configurar las alarmas correspondientes a las diferentes capacidades, por ejemplo:

#### [Creación de una alarma basada en el uso de la CPU superior al 70% de una instancia vía AWS CLI<sup>1</sup>:](#)

```
aws cloudwatch put-metric-alarm --alarm-name cpu-mon --  
alarm-description "Alarm when CPU exceeds 70%" --metric-  
name CPUUtilization --namespace AWS/EC2 --statistic  
Average --period 300 --threshold 70 --comparison-operator  
GreaterThanThreshold --dimensions  
Name=InstanceId,Value=i-12345678 --evaluation-periods 2 --  
alarm-actions arn:aws:sns:us-east-1:111122223333:my-  
topic --unit Percent
```

#### [Creación de una alarma de capacidad de almacenamiento superior al 100MB de un volumen Amazon EBS vía AWS CLI:](#)

```
aws cloudwatch put-metric-alarm --alarm-name ebs-mon --  
alarm-description "Alarm when EBS volume exceeds 100MB  
throughput" --metric-name VolumeReadBytes --namespace  
AWS/EBS --statistic Average --period 300 --threshold  
100000000 --comparison-operator GreaterThanThreshold --  
dimensions Name=VolumeId,Value=my-volume-id --  
evaluation-periods 3 --alarm-actions arn:aws:sns:us-  
east-1:111122223333:my-alarm-topic --insufficient-data-  
actions arn:aws:sns:us-east-1:111122223333:my-  
insufficient-data-topic
```

#### [Creación de una alarma de latencia superior a 100 segundos de un balanceador de carga vía AWS CLI:](#)

```
aws cloudwatch put-metric-alarm --alarm-name lb-mon --  
alarm-description "Alarm when Latency exceeds 100s" --  
metric-name Latency --namespace AWS/ELB --statistic  
Average --period 60 --threshold 100 --comparison-  
operator GreaterThanThreshold --dimensions  
Name=LoadBalancerName,Value=my-server --evaluation-  
periods 3 --alarm-actions arn:aws:sns:us-east-  
1:111122223333:my-topic --unit Seconds
```

<sup>1</sup> Las diferentes alarmas también pueden ser creadas a través del Panel de Administración.

En cuanto a la monitorización y la generación de alertas sobre el grado de consumo de las cuotas de servicios, bien se puede utilizar la solución nativa [Quota Monitor](#) o bien se pueden visualizar las cuotas de servicio y configurar las alarmas a través de la integración de Service Quotas con Amazon CloudWatch.

Para [visualizar una cuota de servicio en Amazon CloudWatch](#):

1. Desde la consola de administración de Amazon CloudWatch, acceder al panel de Métricas.
2. Activar la casilla situada junto a una de las métricas.
3. Elegir la pestaña *Graphed metrics*.
4. Elegir *Add Math* y luego *Start with an empty expression*. En el nuevo registro, bajo el título *Details*, ingresar `SERVICE_QUOTA(m1)`.
5. Para ver el uso actual como porcentaje de cuota, añadir una nueva expresión o cambiar la expresión `SERVICE_QUOTA` por `m1/SERVICEQUOTA(m1)*100`.

Para configurar una alarma que notifique si se acerca a la cuota del servicio:

1. En la fila con `m1/SERVICEQUOTA(m1) *100`, elegir el ícono de alarma, aparecerá la página de creación de alarmas.
2. En *Conditions*, hay que asegurar que *Threshold type* es *Static* y *Whenever Expression1* se establece en *Greater* (que) y escribir 80 (por ejemplo). Esto creará una alarma cuando el uso supere el 80% de la cuota.
3. En la página siguiente, seleccionar un tema de SNS o crear uno nuevo (se recomienda utilizar el mismo que para la monitorización de las capacidades de las instancias).
4. Escribir un nombre y una descripción de la alarma y seleccionar *Next*.

## Control de Acceso [op.acc]

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción. El control de acceso que se implante en un sistema real será un punto de equilibrio entre la usabilidad y la protección de la información.

## Tecnologías de referencia en AWS

Para la gestión de los controles de acceso en AWS deberán tenerse en cuenta las siguientes tecnologías y funciones:



## *AWS Organizations*

AWS Organizations es un servicio de gestión de cuentas que le permite consolidar varias cuentas de AWS en una organización que cree y administre de forma centralizada. AWS Organizations incluye todas las prestaciones de facturación unificada y posibilidades de administración de cuentas para que pueda satisfacer mejor las necesidades presupuestarias, de seguridad y de conformidad de su negocio. Como administrador de su organización, puede crear cuentas e invitar a cuentas existentes a unirse a la organización. Puede encontrar más información de este servicio en el enlace.

También puede consultar la guía ***STIC CCN-STIC 887D Guía de configuración segura para entornos multi-cuenta en AWS***.

## *AWS Identity and Access Management (IAM)*

En AWS el control de accesos está principalmente gobernado por el servicio AWS IAM. Con AWS IAM se puede administrar de forma centralizada los usuarios, las credenciales de seguridad y los permisos que controlan qué pueden hacer los [usuarios, roles y grupos](#) sobre los recursos de AWS y el grado de acceso a éstos.

La correcta configuración de AWS IAM garantizará que sólo aquellos usuarios y componentes autenticados y autorizados (grupos, roles y cuentas de servicio) podrán acceder a los recursos.

### *Proveedores de identidad externos*

Un Proveedor de Identidad o IdP es una herramienta que permite crear, mantener y administrar la información relativa a la identidad de los usuarios al tiempo que proporciona servicios de autenticación a las aplicaciones.

Si la entidad administra identidades fuera de AWS, [puede utilizar los proveedores de identidades \(IdP\) en lugar de hacer uso del servicio AWS IAM](#) para crear atributos, usuarios o grupos en la cuenta de AWS y administrar permisos para el uso de los recursos de AWS<sup>2</sup>. Para ello el usuario deberá autenticarse vía IdP para obtener las claves de acceso temporal al servicio de AWS. Estas claves las genera y distribuye el servicio [Amazon Security Token Service](#).

### *Credenciales y claves de acceso*

En función de cómo se accede a AWS, los usuarios requieren diferentes tipos de mecanismos de seguridad: credenciales y claves de acceso.

Por una parte, las credenciales son la información de autenticación necesaria para iniciar sesión en la Consola de Administración de AWS (la interfaz web que permite crear y administrar los recursos de AWS). La forma de iniciar sesión en la Consola dependerá del tipo de usuario de AWS:

<sup>2</sup> Tal y como se expondrá más adelante, para mejorar la seguridad en el ámbito del control de acceso, se recomienda gestionar las identidades de manera centralizada desde un proveedor de identidades externo, en vez de hacer uso de IAM para ello.

- El usuario raíz (usuario que se crea cuando se crea la cuenta de AWS) accede con la dirección de correo electrónico y la contraseña que se utilizaron para la creación de la cuenta.
- Los usuarios de AWS IAM, que son creados por el usuario raíz o un administrador de AWS IAM, acceden con el alias o el ID de la cuenta, el nombre de usuario de AWS IAM y la contraseña de usuario de AWS IAM.

Por otra parte, las claves de acceso son utilizadas por los usuarios AWS IAM y el usuario raíz de la cuenta de AWS para firmar llamadas mediante programación a la AWS CLI o a la API de AWS. Estas claves de acceso se componen de un ID de clave de acceso y una clave de acceso secreta, que se utilizan juntas. El periodo de validez de las claves de acceso varía en función del tipo de usuario:

- Las claves de acceso asociadas con los usuarios AWS IAM y el usuario raíz de la cuenta son claves a largo plazo, es decir, son válidas hasta que se revoken manualmente. Por lo tanto, las claves de acceso de estos usuarios no caducarán automáticamente.
- Sin embargo, las claves obtenidas a través de funciones AWS IAM y otras características del Security Token Service caducan después de un periodo de tiempo. Es importante destacar que los usuarios autenticados vía proveedor de identidades externo recibirán sus claves de acceso a través del Security Token Service (una vez autenticados en dicho proveedor y siempre y cuando así lo tengan asignado). Por lo tanto, las claves de estos usuarios son temporales.

### Identities

Hay dos tipos de identidades que se deben administrar al abordar cargas de trabajo de AWS seguras y operativas.

- **Identities humanas:** los administradores, desarrolladores, operadores y consumidores de las aplicaciones necesitan una identidad para acceder a las entornos y aplicaciones de AWS. Estos pueden ser miembros de la organización o usuarios externos que interactúan con los recursos de AWS a través de un navegador web, una aplicación cliente, una aplicación móvil o herramientas interactivas de línea de comandos.
- **Identities de la máquina:** Las aplicaciones de carga de trabajo, herramientas operativas y componentes requieren una identidad para realizar solicitudes a los servicios de AWS, por ejemplo, para leer datos. Estas identidades incluyen máquinas que se ejecutan en su entorno de AWS, como instancias de Amazon EC2 o funciones de AWS Lambda. También se puede administrar las identidades de las máquinas para las partes externas que necesitan acceso y además es posible que también tenga máquinas fuera de AWS que necesiten acceso al entorno de AWS.

### Roles AWS IAM

Un [rol de AWS IAM](#) es una identidad de AWS IAM con permisos específicos que se

puede crear en la cuenta de AWS. Un rol de AWS IAM es similar a un usuario de AWS IAM, ya que se trata de una identidad de AWS con políticas de permisos que determinan lo que la identidad puede hacer o no en AWS. Sin embargo, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol.

### *Políticas AWS IAM*

Una [política AWS IAM](#) es un objeto de AWS que, cuando es asociada a una entidad o recurso, define sus permisos para una acción en AWS independientemente del método que se utilice para realizar dicha acción. AWS IAM ofrece las herramientas para crear y administrar todos los [tipos de políticas](#) (administradas por AWS, administradas por el usuario del servicio, o insertadas a un usuario o rol).

### *Amazon Policy Simulator*

[Amazon Policy Simulator](#) es un servicio que permite al usuario probar y solucionar problemas de políticas basadas en identidad, asignación y límites de permisos AWS IAM, políticas de control de servicios de AWS Organizations y políticas basadas en recursos. El simulador evalúa las políticas seleccionadas y determina los permisos en vigor para cada una de las acciones que se especifiquen. El simulador utiliza el mismo motor de evaluación de políticas que se utiliza durante las solicitudes reales realizadas a los servicios de AWS. Sin embargo, difiere del entorno real de AWS en cuanto a que no utiliza solicitudes reales, al igual que tampoco las ejecuta, devolviendo únicamente un valor que otorga o deniega la acción solicitada.

### *IAM Access Analyzer*

[IAM Access Analyzer](#) es un servicio que ayuda a identificar los recursos de la organización y cuentas, las compartidas con una entidad externa, así como validar las políticas de IAM contra políticas y buenas prácticas o generar políticas de AWS IAM en función de la actividad de accesos registrada por AWS CloudTrail. De esta forma, se facilita la identificación de accesos no deseados a recursos y datos del usuario.

IAM Access Analyzer genera un resultado para cada instancia que incluye información sobre el acceso y la entidad externa a la que ha sido concedido, ayudando a identificar si este ha sido intencionado y seguro o bien supone un riesgo para la seguridad.

### *AWS Tags*

[Las etiquetas](#) o AWS Tags son pares de clave y valor que actúan como metadatos para organizar los recursos de AWS. AWS Tags gestiona las etiquetas asignadas a los recursos tanto en el momento de creación, como la modificación posterior y facilita el sistema de consultas de recursos. Con el servicio AWS Tags se podrá, en función de las etiquetas, aplicar claves de condición que poder usar en su política de permisos de AWS IAM.

Las etiquetas de AWS se pueden usar para muchos propósitos, como son la asignación de costes, la automatización, la compatibilidad de operaciones, la gestión de riesgos y el control de acceso. AWS ofrece una guía de buenas prácticas de etiquetado que puede consultar en el siguiente enlace:

[Prácticas recomendadas sobre el etiquetado - AWS Tags.](#)

### *AWS Systems Manager Automation*

AWS Systems Manager es un conjunto de capacidades que ayudan a administrar las aplicaciones y la infraestructura que se ejecutan en la nube de AWS, proporcionando una interfaz de usuario unificada para ver los datos operativos de varios servicios de AWS.

Su utilidad [Automation](#) permite definir tareas de automatización en las instancias administradas a través de documentos de automatización que contienen los pasos necesarios para realizar las tareas. AWS Systems Manager Automation se puede utilizar para llevar a cabo tareas de implementación y mantenimiento comunes como, por ejemplo, crear o actualizar una imagen de máquina de Amazon (AMI).

### *MFA*

[MFA](#) (Multi Factor Authentication) aporta seguridad adicional, ya que exige a los usuarios que proporcionen una autenticación exclusiva obtenida de un mecanismo de MFA admitido por AWS, además de sus credenciales de inicio de sesión habituales, para obtener acceso a los sitios web o servicios de AWS. MFA se puede implementar a través de dispositivos virtuales (aplicaciones software que se ejecutan en un teléfono u otro dispositivo y generan un código de seis dígitos), llaves de seguridad U2F (dispositivos que se conectan al puerto USB del equipo) y dispositivos físicos (que generan un código de seis dígitos basándose en un algoritmo de contraseña de uso único y sincronización en el tiempo).

## **Identificación [op.acc.1]**

### **Requisitos y elementos de configuración**

Para cumplir con los requisitos de la medida de seguridad Identificación [op.acc.1], se deberán seguir las siguientes prácticas:

- Deberán utilizarse los grupos y roles, en lugar de los usuarios individuales, para controlar el acceso. Esto permitirá implementar un conjunto de permisos en lugar de actualizar muchas políticas individuales cuando el acceso de un usuario necesita cambiar.
- Los identificadores de usuario deberán ser asignados en el proveedor de identidades (o en AWS IAM) de modo que se permita singularizar a la persona asociada a cada identificador y cumplir con el resto de los requisitos del control Identificación [op.acc.1] relativas a la gestión de los usuarios.

## Recomendaciones

Para realizar la identificación de los usuarios según las exigencias del Esquema Nacional de Seguridad es muy recomendable la utilización de un proveedor de identidades que permita administrar las identidades en un lugar centralizado, en vez de utilizar AWS IAM para ello [op.acc.1.aws.iam.1].

A medida que aumenta el número de usuarios y roles que se administra, deben determinarse formas de organizarlos para poder administrarlos a escala. Deben asociarse los usuarios con requisitos de seguridad comunes en grupos definidos por el proveedor de identidad y establecerse mecanismos para garantizar que los atributos de usuario que pueden usarse para el control de acceso (por ejemplo, departamento o ubicación) sean correctos y estén actualizados.

En caso de que la organización no disponga de un proveedor de identidades, se deberán generar las identidades de los usuarios directamente en AWS IAM teniendo en cuenta, del mismo modo, las exigencias del Esquema Nacional de Seguridad.

En cualquier caso, es recomendable disponer de un usuario AWS IAM de seguridad (usuario “breakglass”), que no se encuentre sincronizado con el proveedor de identidades externo y que permita la recuperación de emergencia del acceso a AWS en caso de imposibilidad de autenticar a los usuarios a través del proveedor de identidades.

## Requisitos de acceso [op.acc.2]

### Requisitos y elementos de configuración

Para cumplir con esta medida de seguridad, se deberá hacer uso de las políticas AWS IAM para la asignación de privilegios de acceso. Deberán administrarse permisos para controlar el acceso de las identidades de personas y máquinas y sus cargas de trabajo. Los permisos para identidades humanas y de máquinas específicas se deberán establecer para otorgar acceso a acciones de servicio específicas en recursos específicos y evitando la asunción de roles para cualquier cuenta. Además, deberán especificarse las condiciones que se deben cumplir para que se otorgue el acceso. Por ejemplo, se puede permitir que los desarrolladores creen nuevas funciones de Lambda, pero solo en una región específica.

## Recomendaciones

En lo referente a la protección de las credenciales de los usuarios es importante tener en cuenta que, en caso de utilizar el servicio [IMDS](#) (metadatos de instancia y datos del usuario) se recomienda encarecidamente el uso de la versión 2 del servicio, lanzada a finales de 2019, en lugar de la versión original, siempre y cuando la arquitectura de la aplicación así lo permita [op.acc.2.aws.imds.1]. Encontrará más información sobre la configuración de instancias Amazon EC2 para requerir el uso de IMDSv2 en el siguiente [enlace](#). El abuso del servicio IMDSv1 por parte de un atacante podría permitir el descubrimiento, a través de los metadatos de la instancia, de información sobre los privilegios, roles y credenciales de AWS IAM. IMDSv2 refuerza la protección al proteger

todas las solicitudes con autenticación de la sesión, devolviendo al software que ejecuta la instancia un token secreto que sirve como contraseña para realizar la solicitud. A diferencia de las contraseñas tradicionales, el token de sesión nunca es almacenado por IMDSv2 y nunca puede ser recuperado por llamadas posteriores, siendo efectivamente destruido conforme la sesión termina.

Para más información sobre seguridad en el servicio IMDS, puede consultar el siguiente [enlace](#).

### Segregación de funciones y tareas [op.acc.3]

#### Requisitos y elementos de configuración

La segregación de funciones y tareas en AWS se lleva a cabo tradicionalmente a través de un modelo *Role Based Access Control* (RBAC). En AWS IAM se implementa RBAC creando diferentes políticas para diferentes funciones de trabajo. Las políticas se asocian a identidades de usuarios de AWS IAM, grupos de usuarios o roles de AWS IAM, concediendo los permisos mínimos necesarios para la función de trabajo. Para ello, deben enumerarse los recursos específicos a los que puede obtener acceso una función de trabajo.

La desventaja de utilizar el modelo RBAC tradicional es que cuando los empleados añaden nuevos recursos, se deberán actualizar las políticas para permitir el acceso a dichos recursos. Para suplir esta carencia se puede utilizar una estrategia de autorización que defina permisos basados en atributos (*Attribute Based Access Control* – ABAC). En AWS estos atributos se denominan etiquetas (tags). Las etiquetas se pueden asociar a entidades principales de AWS IAM (usuarios o roles) y a recursos de AWS, diseñando las políticas AWS IAM para que permitan operaciones únicamente cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. La estrategia ABAC es especialmente útil en entornos que están creciendo rápidamente y ayuda con situaciones en las que la administración de políticas resulta engorrosa.

Atendiendo a las exigencias del Esquema Nacional de Seguridad y, en función de la estrategia de control de accesos se deben seguir las siguientes prácticas:

- Emplear correctamente el uso de RBAC/ABAC para separar las funciones de desarrollo y operación.
- Emplear correctamente el uso de RBAC/ABAC para separar las funciones de autorización y control de uso.
- Las políticas IAM deberán estar asociadas sólo a grupos o roles.

Además, en caso de ser de aplicación el refuerzo R1 – Segregación rigurosa [op.acc.3.r1], la segregación deberá tener en cuenta la separación de las funciones de configuración y mantenimiento y de auditoría de cualquier otra [op.acc.3.r1.aws.iam.1].

#### Recomendaciones

En caso de aplicar los refuerzos R2 – Privilegios de auditoría y R3 – Acceso a la información de seguridad (opcionales) que exigen la existencia de cuentas con

privilegios de auditoría estrictamente controladas [op.acc.3.r2.aws.iam.1] y la restricción del acceso a la información de seguridad del sistema únicamente a los administradores de seguridad o del sistema, respectivamente, esto se puede lograr, del mismo modo, a través del uso de las políticas AWS IAM para la asignación de permisos y la aplicación de los modelos RBAC o ABAC para la separación de estas funciones.

## Proceso de gestión de derechos de acceso [op.acc.4]

### Requisitos y elementos de configuración

En atención a estos principios de seguridad contemplados en el control Proceso de gestión de los derechos de acceso [op.acc.4], se deben seguir las siguientes prácticas:

- Las políticas AWS IAM deben permitir sólo los privilegios necesarios para cada rol. Se recomienda comenzar con el mínimo nivel de permisos e ir añadiendo permisos adicionales según vaya surgiendo la necesidad en lugar de comenzar con permisos administrativos [op.acc.4.aws.iam.1].
- Las políticas AWS IAM únicamente deben poder asignarse por el usuario que tenga la función de control de accesos expresamente atribuida.
- No utilizar la cuenta raíz salvo necesidad expresa. Cuando se crea una cuenta en AWS, se debe crear un usuarios, grupos o roles con privilegios administrativos para realizar las tareas de administración y utilizar éstos, dejando sin uso el usuario raíz. Esta configuración debe entenderse como un mecanismo para impedir que el trabajo directo con privilegios de administrador repercuta negativamente en la seguridad, al acometer todas las acciones con el máximo privilegio cuando éste no es siempre requerido.
- Evitar políticas con comodines (wildcards) en su definición, que pueden otorgar privilegios administrativos completos [op.acc.4.aws.iam.2].

### Recomendaciones

Para una correcta implementación de la estrategia de políticas de acceso, se recomienda, en primer lugar, utilizar la herramienta Policy Simulator para probar y solucionar posibles problemas en la asignación de políticas. A medida que se van implementando las políticas se puede utilizar Access Analyzer para identificar recursos y cuentas, validar las políticas contra las prácticas recomendadas y generar políticas con base en la actividad de acceso de registros de AWS CloudTrail.

En cuanto a los accesos a las instancias alojadas en AWS se recomienda emplear mecanismos para mantener a las personas alejadas de los datos. Es decir, limitar al máximo el acceso directo a los datos por parte de los usuarios. Para ello, con AWS Systems Manager Automation pueden utilizarse documentos de automatización y diseñar flujos de trabajo para la administración de cambios o la ejecución de operaciones estándar para administrar las instancias Amazon EC2 (p. ej., actualizar los sistemas operativos), en lugar de permitir el acceso directo [op.acc.4.aws.iam.3].



## Mecanismo de autenticación (usuarios de la organización)<sup>3</sup> [op.acc.6]

### Requisitos y elementos de configuración

Para cumplir con el requisito base de la medida de seguridad Mecanismo de autenticación (usuarios de la organización) [op.acc.6], deberán tenerse en cuenta las siguientes prácticas:

- Evitar el uso de múltiples claves de acceso para un mismo usuario IAM [op.acc.6.aws.iam.1]. Mantener más de una clave incrementa el riesgo de accesos no autorizados y el compromiso de las credenciales.

En la mayoría de los casos, no son necesarias claves a largo plazo que nunca caduquen (como son las de los usuarios AWS IAM). En su lugar, es posible crear roles de AWS IAM y generar credenciales de seguridad temporales, o bien utilizar las claves de seguridad temporales obtenidas a través de AWS Security Token Service. Además,

- Las claves de acceso de los usuarios AWS IAM deberán rotarse cada 90 días o menos [op.acc.6.aws.iam.2].
- Deberá habilitarse el vencimiento de las credenciales de los usuarios. (Bien a través de la política de contraseñas de AWS IAM o del proveedor de identidades federado) [op.acc.6.aws.iam.3].
- Se deberá evitar la asignación por defecto de claves de acceso para todos los usuarios que tengan acceso a la consola. Para cumplir con este requisito, se recomienda revisar qué usuarios se encuentran dados de alta en la cuenta de AWS y disponen de acceso a la consola de administración y evitar la asignación de claves de acceso cuando no son necesarias [op.acc.6.aws.iam.4]. Cuando un usuario requiera claves de acceso, se deberán enviar por correo electrónico.

El resto de los requisitos del requisito base (como o la muestra al usuario de la información mínima imprescindible antes de autorizar el acceso [op.acc.6.7] o el establecimiento de un número máximo de intentos de acceso permitidos [op.acc.6.8]) se deben cubrir desde el proveedor de identidades.

En cuanto al refuerzo R1 – Contraseñas [op.acc.6.r1] y en atención a la definición de “Área controlada” realizada por el ENS<sup>4</sup>, es importante tener en cuenta que al ser AWS un servicio cloud accesible por el usuario final a través de Internet, deberá entenderse que los accesos se realizan atravesando zonas no controladas. Por lo tanto, con carácter general, no podrá ser utilizada únicamente una contraseña (R1) como mecanismo de autenticación.

No obstante, el servicio AWS Direct Connect ofrece el establecimiento de una conexión de red dedicada entre la red de las instalaciones y AWS, manteniendo el tráfico

<sup>3</sup> La medida de seguridad del ENS Mecanismo de autenticación (usuarios externos) [op.acc.5] referente al acceso de usuarios que no son usuarios de la organización (en particular, los ciudadanos administrados) no es de aplicación en el ámbito de esta guía, dado que no es previsible que usuarios ajenos a la organización accedan a la configuración de servicios de AWS (sin perjuicio de los accesos que puedan realizar a las aplicaciones o sistemas soportados por la infraestructura de AWS, en cuyo ámbito sí que serán de aplicación las exigencias de la citada medida de seguridad).

<sup>4</sup> “Zona o área en la que la organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella”.



en la red global de AWS y separándolo del Internet público. Por ello, cuando el tráfico de red hacia AWS se canalice a través de este servicio y siempre y cuando tenga origen en zonas controladas, se podrá hacer uso únicamente de la contraseña como mecanismo de autenticación.

En estos casos, las contraseñas de los usuarios deberán seguir las siguientes normas de complejidad mínima y robustez [op.acc.6.r1.aws.iam.1]:

- Longitud mínima de 12 caracteres.
- Al menos, una minúscula.
- Al menos, una mayúscula.
- Al menos, un número.
- Al menos, un carácter especial.

Además, se debe configurar la política de contraseñas para que se prohíba la utilización de contraseñas antiguas y se debe permitir a los usuarios cambiar sus propias contraseñas.

Por otro lado, también se debe seleccionar la opción *reset password* cuando se crean usuarios para que se obligue al cambio de contraseña en el primer acceso.

Para configurar las normas de las contraseñas de los usuarios AWS IAM, se deberán contar con los permisos necesarios para establecer una política de contraseñas. Más información en: [Configuración de una política de contraseñas de la cuenta para usuarios de AWS IAM](#).

En caso de optar por el refuerzo R2 – Contraseña + otro factor de autenticación [op.acc.6.r2], MFA deberá estar habilitado para todas las cuentas que tengan contraseña para acceder a la consola, incluyendo el usuario root [op.acc.6.r2.aws.iam.1].,

Para configurar y habilitar un dispositivo MFA virtual para usarlo con el usuario root(console) se deben seguir los siguientes pasos en la consola de configuración:

1. Iniciar sesión en Consola de administración de AWS.
2. En la parte derecha de la barra de navegación, se debe de elegir un nombre de cuenta y seleccionar My Security Credentials (Mis credenciales de seguridad). Si es necesario, pulsar sobre Continue to Security Credentials (Continuar a credenciales de seguridad). A continuación, ampliar la sección Multi-Factor Authentication (MFA) (Autenticación multifactor [MFA]) en la página.

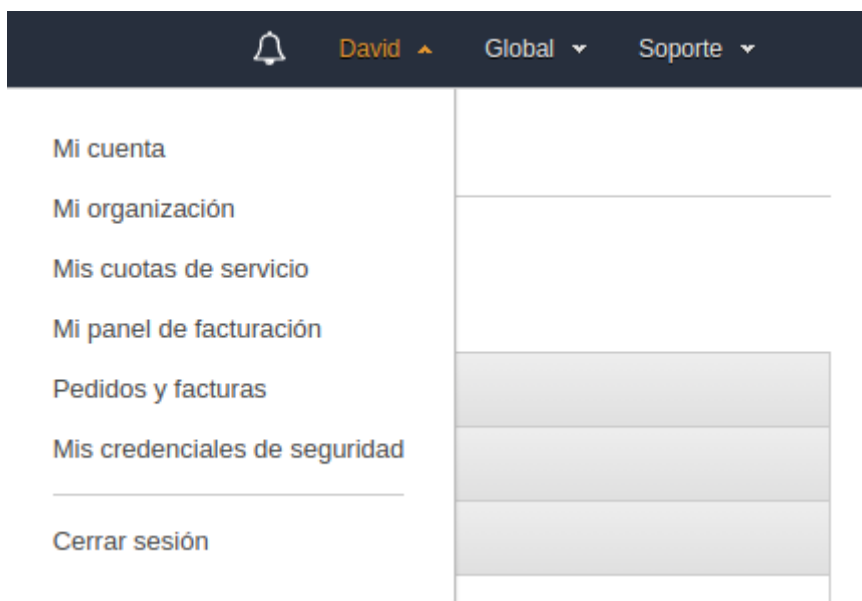


Fig. 2 - Menú de opciones de cuenta en la consola de AWS

Además, se recomienda que la organización determine qué llamadas a la API deben también contar con seguridad reforzada a través de un doble factor de autenticación. Con las políticas AWS IAM se puede exigir a los usuarios que se autenticuen mediante la autenticación multifactorial para permitirles llevar a cabo acciones especialmente sensibles. Para más información sobre el establecimiento del doble factor de autenticación en las llamadas a la API, consultar:

#### [Configuración del acceso a una API protegido por MFA](#)

Si se opta por la aplicación del refuerzo R3 – Certificados, se deberá utilizar el servicio AWS IAM Roles Anywhere para crear un ancla de confianza en la que se haga referencia al servicio AWS Certificate Manager Private CA o registrar sus propias autoridades de certificación (CA), permitiendo usar el certificado emitido por la misma para obtener credenciales temporales para el acceso al entorno AWS. Estos certificados deberán estar protegidos por un segundo factor.

Por el contrario, si se opta por la utilización de un certificado en dispositivo físico como mecanismo de autenticación, en aplicación del refuerzo R4 – Certificados en dispositivo físico [op.acc.6.r4], deberán habilitarse los dispositivos MFA físicos para todos los usuarios IAM mediante la consola, línea de comandos o la propia API de IAM. Del mismo modo, el uso de estos certificados deberá estar protegido por un segundo factor de tipo PIN o biométrico [op.acc.6.r4.aws.iam.1].

Además de estos refuerzos, los siguientes son aplicables desde el nivel medio de las dimensiones de seguridad confidencialidad, integridad, trazabilidad y autenticidad:

El Refuerzo R5 – Registro, indica que se deben registrar los accesos con éxito y los fallidos e informar al usuario del último acceso efectuado con su identidad. Para registrar los intentos de acceso, se deberá habilitar AWS CloudTrail en todas las regiones y activar el registro de acceso de usuarios [op.acc.6.r5.aws.iam.1]. Los eventos de inicio de sesión de AWS CloudTrail permiten registrar los inicios de sesión del usuario raíz, los

usuarios de AWS IAM y los usuarios federados, indicando, por ejemplo, si se trata de inicios de sesión exitosos o fallidos o si se ha utilizado MFA.

La información al usuario sobre el último acceso efectuado con su identidad se deberá cubrir desde el proveedor de identidades, si bien, la información de último acceso está disponible tanto en la consola como en AWS CLI y su recopilación está activada por defecto al usar IAM. Esta información puede ser no visible para el usuario final dependiendo de sus permisos en AWS IAM, pero un usuario con permisos sobre AWS IAM pueden generar reportes que la reflejen. Encontrará más información en el [enlace](#).

Por otro lado, tal y como se ha expuesto anteriormente, con carácter general el acceso a AWS se realizará a través de zonas no controladas. Por ello, y salvo las excepciones mencionadas, para cumplir con R8 – Doble factor para acceso desde o a través de zonas no controladas [op.acc.6.r8] se deberán emplear, al menos los mecanismos de autenticación a los que se refieren R2, R3 y R4 [op.acc.6.r8.aws.iam.1].

En cuanto a las exigencias del refuerzo R9 – Acceso remoto, muchas de ellas tienen carácter organizativo o quedan cubiertas por otras medidas de seguridad, salvo las siguientes:

- Cifrado de tráfico: Si bien todas las APIs tienen capacidad HTTPS, algunas también funcionan con HTTP. Por lo tanto, deberá asegurarse que se está haciendo uso de HTTPS en todas las llamadas a API. Esto se puede lograr, en el caso de S3 con políticas de recurso ([bucket policies](#)). También es importante conocer si el API endpoint de los servicios utilizados utiliza HTTP o HTTPS, lo cual se puede consultar en el siguiente [enlace](#).
- En caso de que las llamadas a las APIs no se produzcan de manera constante, se recomienda condicionar su realización a aquellas franjas horarias en las que sean necesarias. Esto se puede conseguir haciendo uso del elemento Condition y los operadores de condición de tipo fecha y hora en las políticas de AWS IAM. Los operadores de condición de fecha y hora permiten construir elementos de condición que restringen el acceso basándose en la comparación de una clave con un valor de fecha/hora. Puede ampliar más información sobre cómo hacerlo en el [enlace](#).

Por último, son aplicables en el nivel alto de las dimensiones citadas los dos siguientes refuerzos:

- R6 – Limitación de la ventana de acceso [op.acc.6.r6]. Este refuerzo exige la definición de puntos en los que el sistema requiere renovar la autenticación del usuario mediante una identificación singular adicional a la sesión establecida. Dado que la administración de AWS funciona a través de llamadas API con claves de acceso (que son válidas una vez autenticado el usuario) y no a través de sesiones, este control deberá implementarse únicamente en el ámbito del sistema de información soportado por la infraestructura de AWS.
- R7 – Suspensión por no utilización [op.acc.6.r7], se deberá activar la inhabilitación de las credenciales de los usuarios AWS IAM que no hayan sido

empleadas durante un periodo de tiempo (o bien, se deberá establecer la inhabilitación en el proveedor de identidades) [op.acc.6.r7.aws.iam.1]. Se recomienda que el periodo de no utilización para la inhabilitación no sea superior a 90 días [op.acc.6.r7.aws.iam.2].

### Inventario de activos [op.exp.1]

#### Tecnologías de referencia en AWS

##### AWS Config

Antes de comenzar a utilizar AWS Config debe crear un rol que permita el acceso al servicio de AWS Config. Encontrará como crear el rol en el siguiente [enlace](#).

AWS Config proporciona una vista detallada de la configuración de los recursos de AWS en la cuenta de AWS, incluyendo cómo se relacionan los recursos entre sí cómo se han configurado en el pasado. Además, por medio de AWS Config rules es posible añadir condiciones a la configuración del entorno para el uso de etiquetas (mediante el atributo [Required Tags](#)).

Se recomienda seleccionar los recursos de AWS que quieran ser analizados. Puede obtener más información sobre dichos recursos en el [enlace](#).

Así mismo, y en función de las necesidades del usuario, recomendamos definir reglas para la evaluación de los recursos. Estas deben ser una combinación de reglas administradas por AWS (AWS managed rules), reglas propias del usuario y reglas propias para AWS Lambda. Encontrará más información sobre las reglas de AWS Config en el [enlace](#).

##### AWS Systems Manager Inventory

[AWS Systems Manager Inventory](#) ofrece visibilidad del entorno recopilando metadatos de las instancias administradas. Estos metadatos se pueden almacenar en un bucket de Amazon S3 central y, a continuación, utilizar las herramientas integradas para consultar los datos y determinar rápidamente qué instancias ejecutan el software y las configuraciones requeridas por la política de software, así como las instancias que deben actualizarse.

Es posible activar AWS Config para que también pueda ver el seguimiento de cambios y el historial de instancias a través de AWS Systems Manager. Para ello deben habilitar los siguientes recursos en AWS Config:

```
SSM:ManagedInstanceInventory
```

```
SSM:PatchCompliance
```

```
SSM:AssociationCompliance SSM:FileData (SSM: Datos de  
archivo)
```

## Requisitos y elementos de configuración

Para cumplir con Inventario de activos [op.exp.1], deberán tenerse en cuenta las siguientes prácticas:

Por un lado, en lo referente al inventariado de los recursos de AWS (entidades que creadas y administradas en AWS como Amazon VPCs, volúmenes Amazon EBS, grupos de seguridad, instancias Amazon EC2), etc., se debe asegurar que AWS Config está habilitado en todas las regiones y utilizar la herramienta para obtener una vista de los recursos existentes en las cuentas de AWS [op.exp.1.aws.cfg.1]. Además, para la correcta identificación del responsable se deberá asociar etiquetas con esta información para todos los activos [op.exp.1.aws.tag.1]. Para facilitar el cumplimiento de este aspecto, se puede configurar una regla de AWS Config Rules que alerte sobre el despliegue de recursos sin las etiquetas correspondientes asociadas [op.exp.1.aws.cfg.2].

Por otro lado, en el ámbito del software desplegado en las instancias de Amazon EC2 se deberá habilitar AWS System Manager Inventory en caso de no utilizar otra herramienta de terceros [op.exp.1.aws.sys.1]. Entre los tipos de datos de las instancias que se pueden recopilar con AWS Systems Manager Inventory se encuentran el nombre y las versiones de los sistemas operativos, la pertenencia a un dominio o grupo de trabajo, o los roles de Windows. Además, se deben asignar metadatos personalizados a cada nodo administrado con información sobre el responsable del activo [op.exp.1.aws.sys.2].

## Recomendaciones

Para dar cumplimiento al refuerzo R1 – Inventario de etiquetado (opcional), del mismo modo, se recomienda hacer uso de AWS Config para la identificación de los equivalentes virtuales al equipamiento tales como los puntos de enlace de la Amazon VPC, los Gateway virtuales, las interfaces de red o los grupos de seguridad, siempre teniendo en cuenta la [lista de recursos admitidos por AWSConfig](#).

Por su parte, el refuerzo R2 – Identificación periódica de activos (opcional), exige disponer de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, servidores y dispositivos de red y comunicaciones. Este requisito estaría satisfecho por defecto al utilizar las herramientas descritas, particularmente AWS Config, en tanto en cuanto actualiza automáticamente el estado de los recursos identificados.

Asimismo, sería recomendable la asignación de etiquetas que permitan categorizar los activos que se consideran críticos según el contexto y los riesgos de la organización mediante AWS tags, dando así cumplimiento al refuerzo R3 – Identificación de activos críticos (opcional).

Además del inventario relativo a los recursos propios de AWS, también se recomienda disponer de una relación actualizada de los componentes software de terceros utilizados en el despliegue del sistema, tal y como se describe en el refuerzo R4 – Lista de componentes software (opcional). Si bien, para listar cualquier elemento que

se instale sobre terceros se puede utilizar AWS System Manager Inventory, sería recomendable mantener un registro actualizado de las librerías utilizadas por los desarrolladores en sus tareas, y tratarlas como un activo más.

Adicionalmente, se recomienda el uso de AWS Resource Explorer para la exploración de recursos como instancias Amazon RDS, Amazon buckets S3 o tablas de Amazon DynamoDB [op.exp.1.aws.re.1]. Esta herramienta permite la búsqueda de recursos en todas las regiones de la cuenta utilizando metadatos como nombres, tags o IDs.

## Gestión de la configuración de seguridad [op.exp.3]

### Tecnologías de referencia en AWS

#### *AWS Config Rules y Conformance Packs*

[AWS Config Rules](#) es un conjunto de funciones de gobernanza que permiten definir directrices de aprovisionamiento y configuración de recursos de AWS y supervisar la conformidad con esas directrices. Para ello, el servicio permite elegir entre un conjunto de reglas basadas en las prácticas recomendadas por AWS, o bien reglas personalizadas establecidas por el propio usuario.

Por su parte, los [AWS Conformance Packs](#) son colecciones de reglas de detección de AWS Config que se pueden implementar fácilmente como una sola entidad en una cuenta, región u organización en AWS Organizations.

### Recomendaciones

Si bien, los requisitos de la medida de seguridad Gestión de la configuración [op.exp.3] deberán satisfacerse principalmente a través de procedimientos organizativos de autorización y gestión en el ámbito del software, en lo referente a las configuraciones de los recursos de AWS, el cumplimiento de los requisitos se puede apoyar en la utilización de los servicios AWS Config, AWS Config Rules y Conformance Packs [op.exp.3.aws.cfg.1]. Con estos servicios, los administradores de seguridad pueden identificar líneas base de configuración para evaluar si los recursos de AWS se ajustan a las prácticas autorizadas por la organización.

En cuanto al requisito base [op.exp.3.6] y el refuerzo R2 – Responsabilidad de la configuración [op.exp.3.r2.1], relativos a la existencia de un número limitado y autorizado de administradores del sistema, se puede utilizar la asignación de políticas AWS IAM para lograr este resultado.

En cuanto a la realización de copias de seguridad de las configuraciones exigidas por R3 – Copias de seguridad [op.exp.r3.1], la entidad puede consultar el histórico de configuraciones de recursos en AWS Config [op.exp.3.r3.aws.cfg.1]. No obstante, al ser un servicio de registro, no es posible realizar una captura de la configuración y aplicarla o replicarla desde esta herramienta, por lo que la reconstrucción del sistema deberá llevarse a cabo según sus procesos operacionales habituales.

Tal y como se ha adelantado en el apartado 2.4 Infraestructura como Código, el despliegue de la infraestructura a través de código permitiría satisfacer este refuerzo, dado que puede conservar como copias de seguridad de las configuraciones el propio código utilizado para el despliegue.

Para el cumplimiento del refuerzo R4 – Aplicación de la configuración (opcional), si bien AWS no dispone de un procedimiento que permita la instalación manual de versiones y actualizaciones del sistema, se recomienda hacer uso de los servicios AWS Systems Manager Explorer y Patch Manager como solución para mantener actualizada la configuración de seguridad del S.O., tal y como se describe en el apartado [Mantenimiento y actualizaciones de seguridad \[op.exp.4\]](#) de este mismo documento [op.exp.3.r4.aws.smexp.1] [op.exp.3.r4.aws.patch.1].

Por último, para dar cumplimiento al refuerzo R5 – Control del estado de seguridad de la Configuración (opcional), referente al conocimiento del estado de la configuración de los dispositivos de red, AWS Config, tal y como se ha adelantado en el apartado [Inventario de activos \[op.exp.1\]](#), permite el registro de los detalles de la configuración de diferentes dispositivos de red virtuales y elementos de la Amazon VPC.

AWS pone a disposición de sus usuarios distintas herramientas para la remediación de la configuración, citaremos en esta guía algunos ejemplos.

- Puede preconfigurar las plantillas de AWS Systems Manager para llevar a cabo auto-remediasiones. Encontrará más información en este [enlace](#).
- También puede configurar las acciones de AWS Systems Manager para las remediaciones manuales.
- Además. Puede configurar las acciones para los recursos de AWS con un estado de no cumplimiento(non-compliant). Puede ampliar información en el [enlace](#).

## Mantenimiento y actualizaciones de seguridad [op.exp.4]

### Tecnologías de referencia en AWS

#### *AWS Systems Manager Explorer*

[Explorer](#) es una funcionalidad de AWS Systems Manager consistente en un panel de operaciones personalizable que transmite información sobre los recursos de AWS. Explorer muestra una vista agregada de los datos de operaciones de las cuentas de AWS en todas las regiones, incluyendo metadatos sobre las instancias Amazon EC2 y detalles de conformidad de parches.

#### *AWS Systems Manager Patch Manager*

AWS Systems Manager también ofrece la solución [Patch Manager](#) para facilitar el mantenimiento y la aplicación de actualizaciones relacionadas con la seguridad y nuevas versiones de software y sistema operativo. Este servicio también permite analizar



instancias y generar informes de los parches que faltan, o bien analizar e instalar automáticamente todos los parches que faltan.

### Requisitos y elementos de configuración

Para cumplir con el requisito base de la medida de seguridad Mantenimiento y actualizaciones de seguridad [op.exp.4], deberán tenerse en cuenta las siguientes prácticas:

- Activar AWS Systems Manager y gestionar la conformidad de los parches a través de la solución Explorer [op.exp.4.aws.sys.1]. Adicionalmente se instalará el agente AWS Systems Manager Agent (SSM Agent), que es el software de Amazon que se ejecuta en instancias de Amazon Elastic Compute Cloud (Amazon EC2), dispositivos periféricos, servidores en las instalaciones o máquinas virtuales (VM). SSM Agent permite que AWS Systems Manager actualice, administre y configure estos recursos. Encontrará más información sobre SSM Agent en el [enlace](#).
- Utilizar AWS Systems Manager Patch Manager para planificar y gestionar la aplicación de parches minimizando los riesgos asociados a tener instancias con software desactualizado y expuesto a vulnerabilidades conocidas [op.exp.4.aws.sys.2].

### Recomendaciones

En cuanto al requisito base de la medida, una forma eficiente de garantizar la instalación de las versiones actualizadas y aprobadas del software de los sistemas es la utilización de Golden AMIs. Las Golden AMIs son AMIs estandarizadas que, a través de la configuración, el parcheado de seguridad y el bastionado garantizan que incluyen las últimas actualizaciones de seguridad.

El cumplimiento de los refuerzos de esta medida de seguridad puede apoyarse en los servicios de AWS. En primer lugar, para el cumplimiento del refuerzo R1 – Pruebas en preproducción [op.exp.4.r1.1], la entidad usuaria puede utilizar el entorno de la nube de AWS para la realización de sus pruebas en preproducción con carácter general. En segundo lugar, para el cumplimiento del refuerzo R2 – Prevención de fallos [op.exp.4.r2.1], se puede utilizar la solución AWS Systems Manager Automation para automatizar las tareas de corrección en servicios de AWS como Amazon EC2 y Amazon RDS [op.exp.4.r2.aws.sys.1].

Por último, el refuerzo R4 – Monitorización continua (opcional), exige el despliegue a nivel de sistema de una estrategia de monitorización continua de amenazas y vulnerabilidades. Por un lado, en cuanto a la monitorización de amenazas, se puede comprobar la configuración de los recursos a analizar para ver si estos son o no vulnerables. Tanto Amazon GuardDuty como AWS Security Hub permiten realizar este análisis. AWS Security Hub ingesta datos desde AWS Config y Amazon GuardDuty informa de la actividad en el momento; tal y como se describe en el apartado [\[op.mon.3\]](#) [Vigilancia](#) de este mismo documento [op.exp.4.r4.aws.shub.1] [op.exp.4.r4.aws.gd.1].



Por otro lado, en cuanto a la monitorización de vulnerabilidades, el servicio Amazon Inspector permite, gracias a su monitorización continua, la revisión regular de las vulnerabilidades del sistema [op.exp.4.r4.aws.insp.1].

## Gestión de cambios [op.exp.5]

### Tecnologías de referencia en AWS

#### *AWS Systems Change Manager*

[AWS Systems Change Manager](#) es un marco de gestión de cambios empresariales que sirve para solicitar, aprobar, implementar y generar informes sobre cambios operativos en la infraestructura y la configuración de aplicaciones, permitiendo administrar los cambios tanto en los recursos de AWS como en los recursos locales.

A través de su integración con AWS Systems Change Calendar, se pueden configurar intervalos de fecha y hora para realizar o no acciones específicas sobre una cuenta de AWS. De esta manera, se pueden implementar de manera segura los cambios evitando conflictos entre eventos.

### Recomendaciones

Para cumplir con el requisito base de la medida de seguridad Gestión de cambios [op.exp.5] en las instancias Amazon EC2, la entidad usuaria puede hacer uso de la utilidad AWS Systems Change Manager para mantener un registro actualizado de las plantillas y peticiones de cambio en las que se incluya información en detalle sobre estos. Además, se puede configurar la herramienta para la notificación del cambio a los responsables y utilizar AWS Systems Change Calendar para establecer ventanas temporales en la que realizar los cambios y las pruebas de preproducción exigidas por el ENS sin riesgo a que éstas afecten a la continuidad del servicio prestado.

Más allá del ámbito de Amazon EC2, tanto la gestión de los cambios referida en [op.exp.5] como el Refuerzo R1 – Prevención de fallos [op.exp.5.r1], contienen exigencias de carácter operacional, sin que existan, por lo tanto, configuraciones concretas en AWS para su cumplimiento. No obstante, algunas consideraciones generales para tener en cuenta para la gestión de los cambios y la prevención de fallos son:

- La definición de diferentes ambientes operacionales y procesos que los soportan.
- La adopción de un modelo de [DevOps](#) que utilice políticas de conformidad, controles minuciosos y técnicas de administración de la configuración.
- Utilizar prácticas como son la [integración](#) y [entrega](#) continua para comprobar que los cambios realizados en el sistema sean funcionales y seguros.
- Hacer uso del marco de trabajo [AWS Well-Architected Framework](#) para identificar las mejores prácticas en cuanto a despliegue de arquitectura segura en AWS.

## Protección frente a código dañino [op.exp.6]

### Tecnologías de referencia en AWS

#### *Amazon GuardDuty*

[Amazon GuardDuty](#) es un servicio de detección de amenazas que monitoriza continuamente el entorno AWS y utiliza inteligencia y aprendizaje automático para identificar actividades maliciosas, anomalías y comportamientos no autorizados con el fin de proteger datos, cargas de trabajo y cuentas de AWS almacenados en Amazon S3, además de enviar hallazgos detectados para su visibilidad y resolución.

#### *Amazon GuardDuty Malware Protection*

[Protección contra malware de Amazon GuardDuty](#) es una mejora del servicio AWS Amazon GuardDuty que identifica los recursos de una organización que hayan sido comprometidos por malware o aquellos recursos que estén en riesgo. También permite la realización de escaneos de recursos seleccionados.

### Requisitos y elementos de configuración

Para cumplir con el requisito base de la medida de seguridad Protección frente a código dañino [op.exp.6] se deberá activar la protección contra software malintencionado de Amazon GuardDuty en todas las regiones [op.exp.6.aws.gd.1]. Esto permitirá detectar el compromiso con malware de, por ejemplo, instancias Amazon EC2 o cargas de trabajo que se ejecuten en contenedores. No obstante, las actuaciones reactivas destinadas a la eliminación del código malicioso o la mitigación de sus efectos deben ser ejecutadas en el ámbito de los recursos desplegados a nivel de software.

### Recomendaciones

Algunas de las herramientas y servicios de AWS pueden ayudar asimismo al cumplimiento de los refuerzos de esta medida de seguridad, por ejemplo:

- AWS Systems Manager Inventory permite la gestión del software y la identificación del software autorizado por la organización, pudiendo así definir la lista blanca de aplicaciones a la que se refiere el refuerzo R3 – Lista blanca [op.exp.6.r3]. Y si bien, a través de su integración con AWS Config se permite el lanzamiento de alertas para la detección de la instalación de software no autorizado, es importante tener en cuenta que AWS System Manager no puede actuar borrando software o bloqueando su instalación o ejecución.
- Las operaciones estándar que llevar a cabo para la respuesta en caso de incidente se pueden automatizar a través de AWS Systems Manager.

## Gestión de incidentes [op.exp.7]

### Requisitos y elementos de configuración

Si bien el detalle sobre el uso de las herramientas para la gestión de incidentes en AWS puede encontrarse en la guía **CCN-STIC 887F Guía de Respuesta a incidentes de seguridad en AWS**, para el cumplimiento de los requisitos básicos de la medida Gestión de incidentes [op.exp.7], deberán seguirse las siguientes prácticas:

- Habilitar Amazon GuardDuty para la detección de incidentes de seguridad [op.exp.7.aws.gd.1].
- Habilitar AWS Security Hub [op.exp.7.aws.sh.1].

Para habilitar Security Hub se deben seguir los siguientes pasos:

- Disponer de una identidad AWS IAM (usuario, rol o grupo) con los permisos necesarios. Si se habilita la integración con AWS Organizations, las cuentas disponen de AWS Security Hub habilitado automáticamente. En caso contrario, se debe asignar manualmente la política administrada AWSSecurityHubFullAccess a una identidad.
- Habilitar AWS Security Hub desde la consola, desde la API de AWS Security Hub o desde la CLI de AWS.
- Activar AWS Config en todas las cuentas que AWS Security Hub vaya a monitorizar y configurar sus reglas para evitar errores de comprobación que dependan de AWS Config.

Al habilitar el servicio se asigna un rol vinculado llamado `AWSServiceRoleForSecurityHub`, que incluye los permisos y la política que Security Hub requiere para detectar y agregar los hallazgos de otras herramientas y configurar la infraestructura de AWS Config necesaria para ejecutar las comprobaciones de seguridad de los estándares admitidos.

Asimismo, para el cumplimiento de esta medida de seguridad, es preciso habilitar los logs de acceso de Amazon CloudFront [op.exp.7.aws.cf.1].

Por otra parte, para que el soporte técnico de AWS pueda ponerse en contacto fácilmente con los responsables de la cuenta en caso de problemas de seguridad o facturación, deberá proveerse la información relacionada de contactos alternativos (de facturación, operaciones y seguridad) con correos que no dependan de la misma persona. Deberá comprobarse regularmente que estas cuentas funcionan correctamente y mantener listas de correo para asegurar la recepción de avisos por personal disponible en cada momento [op.exp.7.aws.iam.1].

## ▼ Contactos alternativos

[Editar](#)

Para mantener a las personas adecuadas al tanto, puede agregar un contacto alternativo para las comunicaciones de Facturación, Operaciones y Seguridad. Para especificar un contacto alternativo, haga clic en el botón Editar.

Tenga en cuenta que, como titular de la cuenta principal, todavía recibirá todas las comunicaciones por correo electrónico. Como práctica recomendada, no incluya información confidencial en los campos Cargo o Nombre completo, ya que se pueden utilizar en las comunicaciones por correo electrónico dirigidas a usted.

**Facturación** ⓘ

Contacto: Ninguno

**Operaciones** ⓘ

Contacto: Ninguno

**Seguridad** ⓘ

Contacto: Ninguno

Fig. 3 – Información relacionada con contactos alternativos

Además, deberán establecerse preguntas de desafío de seguridad y respuestas para el caso de que sea necesario autenticarse como propietario de la cuenta para ponerse en contacto con el soporte de AWS. Para la configuración o cambio de preguntas de desafío de seguridad se deben seguir los pasos que se establecen en el siguiente [enlace](#).

## Recomendaciones

Se recomienda activar en AWS Security Hub, AWS Foundational Security Best Practices v1.0.0 y CIS AWS Foundations Benchmark v1.2.0. AWS Foundational Security Best Practices v1.0.0 es un conjunto de controles que detectan cuándo sus cuentas de AWS y sus recursos se desvían de las prácticas recomendadas de seguridad. Encontrará más información en el [enlace](#). CIS AWS Foundations Benchmark v1.2.0 sirve como un conjunto de mejores prácticas de configuración de seguridad para AWS. Estas mejores prácticas aceptadas por la industria le proporcionan procedimientos claros de step-by-step implementación y evaluación. Más información sobre estas prácticas en el [enlace](#).

En el caso de que su organización vaya a manejar información para almacenar, procesar o transmitir datos del titular de tarjetas de pago, le recomendamos activar [PCI DSS V3.2.1](#). Este estándar de seguridad de datos del sector de pagos con tarjeta (PCI DSS) de Security Hub proporciona un conjunto de prácticas recomendadas de AWS seguridad para el manejo de los datos de los titulares de tarjetas.

En cuanto a la posibilidad de disponer herramientas de automatización de los procesos de prevención y respuesta mediante detección de anomalías, segmentación dinámica de red y aislamiento de dispositivos críticos, tal y como se expone en el refuerzo R4 – Prevención y respuesta automática (opcional), si bien AWS no dispone de una herramienta concreta para dar cumplimiento al contenido del refuerzo, pone a disposición de los usuarios un [ejemplo](#) que sirve como orientación para ello [*op.exp.7.r4.aws.gd.1*].

En él se muestra una solución para la detección de eventos de seguridad relacionados con una instancia de Amazon EC2 a través de Amazon GuardDuty mediante el aislamiento de la instancia, realización de snapshot de volumen de disco, revisión e informe final.

Aunque se disponga de soluciones accesibles ya creadas, es responsabilidad de la entidad usuaria hacer uso de ellas como orientación para aproximar una posible solución que se ajuste a las necesidades y arquitectura de su organización.

## Registro de la actividad [op.exp.8]

### Tecnologías de referencia en AWS

#### *AWS CloudTrail*

[AWS CloudTrail](#) es un servicio de monitorización que ayuda al usuario a habilitar la gestión, el cumplimiento, el funcionamiento y el análisis de operaciones y riesgo en su cuenta de AWS. Las medidas que adopta un usuario, rol o un servicio de AWS se registran como eventos en AWS CloudTrail. Los eventos incluyen las acciones llevadas a cabo en la Consola de administración de AWS y AWS CLI, así como las AP o los SDK de AWS.

### Requisitos y elementos de configuración

Para cumplir con el requisito base de la medida de seguridad Registro de actividad [op.exp.8], se deben seguir las siguientes prácticas:

- Habilitar la herramienta AWS CloudTrail en todas las regiones. Este servicio está habilitado por defecto cuando se crea una nueva cuenta, pero es posible deshabilitarlo [op.exp.8.aws.ct.1].
- Establecer un filtro de métricas desde Amazon CloudWatch para detectar cambios en las configuraciones de AWS CloudTrail [op.exp.8.aws.ct.2]. Se debe configurar la retención de métricas según las necesidades de latencia, en función de los intereses del usuario. Más información sobre las métricas de Amazon CloudWatch en el [enlace](#).
- Crear trails para los registros de auditoría y habilitar la validación de archivos en todos los trails, evitando así que estos se vean modificados o eliminados [op.exp.8.aws.ct.3].
- Habilitar la entrega continua de eventos de AWS CloudTrail a un bucket Amazon S3 dedicado con el fin de unificar los archivos de registro [op.exp.8.aws.ct.4].

Para el cumplimiento del refuerzo R1 – Revisión de los registros [op.exp.8.r1.1], se debe:

- Utilizar el servicio Amazon CloudWatch, para centralizar y revisar los registros de todos los sistemas independientemente de su origen.
- Registrar los eventos de escritura y lectura de datos [op.exp.8.r1.aws.ct.3].

En cuanto al Refuerzo R2 – Sincronización del reloj del sistema, para disponer de una referencia de tiempo para facilitar las funciones de registro de eventos y auditoría, cabe destacar que AWS dispone del servicio Amazon Time Sync Service presente de forma nativa en todos los servicios que proporciona. De este modo, en el entorno de AWS, este refuerzo se encuentra satisfecho por defecto. No obstante, en máquinas o servidores de las instancias de EC2 es posible modificar la fuente de tiempo, lo cual, con carácter general, no es recomendable dado que se podrían producir discrepancias entre la fuente seleccionada y la fuente nativa de AWS, especialmente si se utilizan fuentes de

tiempo poco fiables.

Por otra parte, para activar la retención de los registros de acuerdo con lo exigido en el refuerzo R3 – Retención de registros, se debe ejecutar la acción *PutRetentionPolicy* de Amazon CloudWatch, permitiendo así establecer la retención del grupo de registros especificado y configurar el número de días durante los cuales se conservarán los eventos de registro en el grupo seleccionado de acuerdo con el documento de seguridad correspondiente.

Para garantizar un control de acceso adecuado según R4 – Control de acceso [op.exp.8.r4.1], se debe:

- Asignar correctamente las políticas AWS IAM para el acceso y borrado de los registros y sus copias de seguridad haciendo uso del principio de mínimo privilegio [op.exp.8.r4.aws.ct.1].
- Utilizar únicamente usuarios AWS IAM a los que se les haya sido asignada la política *AWSCloudTrail\_FullAccess* para las tareas de administración (no pudiendo eliminar en ningún momento el depósito de Amazon S3).
- Utilizar una política de bucket para restringir el acceso de forma pública e imponer restricciones sobre cuáles de los usuarios pueden eliminar objetos de Amazon S3 [op.exp.8.r4.aws.ct.2].
- Activar el acceso por MFA al registro de actividad almacenado en los buckets de Amazon S3 dedicados para AWS CloudTrail [op.exp.8.r4.aws.ct.3].

## Recomendaciones

Para garantizar un mayor control se recomienda configurar los archivos de logs de AWS CloudTrail para aprovechar el cifrado del lado del servidor (SSE-Server Side Encryption) y las claves maestras creadas por el cliente (CMK de AWS KMS) [op.exp.8.r4.aws.ct.4].

Así mismo, se recomienda habilitar notificaciones mediante Amazon SNS para los siguientes eventos [op.exp.8.aws.ct.5]:

- Llamadas no permitidas a la API.
- Accesos no permitidos a la consola.
- Todos los intentos de acceso sin el correcto uso de MFA.
- Toda la actividad realizada sobre y por la cuenta root.
- Cualquier cambio en las políticas AWS IAM.

Además, puede configurar las notificaciones mediante otros servicios como por ejemplo Amazon CloudWatch.

Se recomienda crear CloudTrail lakes.

Otra recomendación adicional que puede implementar es la de utilizar la función AWS CloudTrail lakes para generar diferentes data lakes para la retención y consulta de registros de actividad. Al crearse se le activaran de forma predeterminada la opción Management Events (Eventos de administración), pudiendo activar también la opción de Data Events (Eventos de datos). No obstante, ha de tener en cuenta que esta segunda opción conlleva una gran cantidad de datos a almacenar y un incremento importante en los costos.

Paralelamente, se recomienda definir un periodo de retención para los datos almacenados en AWS CloudTrail Lakes [op.exp.8.r3.aws.cw.1].

### Registro de la gestión de incidentes [op.exp.9]

#### Tecnologías de referencia en AWS

##### *AWS Systems Manager Incident Manager*

[AWS Systems Manager Incident Manager](#) es una consola de administración de incidentes diseñada para ayudar a los usuarios en las tareas de mitigación y recuperación ante incidentes que afecten a las aplicaciones alojadas en AWS (entendiendo por incidente cualquier interrupción no planificada o reducción de calidad de un servicio).

Este servicio puede apoyarse en otros como Amazon CloudWatch Alarms, Amazon CloudWatch Metrics o AWS CloudTrail.

Este servicio permite:

- Creación y automatización de planes de respuesta. Iniciados por Amazon CloudWatch Alarms o AWS Event Bridge.
- Automatización de runbooks.
- Participación y escalado en el flujo de comunicación de incidentes.
- Colaboración activa con los equipos de respuesta ante incidentes. Mediante la integración del AWS Chatbot.
- Seguimiento de incidentes.

#### Recomendaciones

Si bien, los requisitos de la medida de seguridad Registro de la gestión de incidentes [op.exp.9] deberán satisfacerse principalmente a través de procedimientos organizativos, AWS dispone de la capacidad para cumplir con esta medida de seguridad haciendo uso de diferentes servicios de su catálogo.

Mediante el uso de servicios como AWS Incident Manager o AWS CloudTrail es posible mantener un registro de las actuaciones y modificaciones realizadas en y sobre el sistema, de manera que estas puedan ser recogidas para ser reflejadas

posteriormente en los informes exigidos por la medida de seguridad; siendo estos informes previos, intermedios y finales de:

- Incidentes de seguridad.
- Actuaciones de emergencia.
- Modificaciones del sistema derivadas de un incidente.

Estos servicios no aportan el informe de forma automática, pero pueden servir como herramienta para generar contenido prescriptivo de los mismos; por ello, se recomienda habilitar AWS CloudTrail en todas las regiones y hacer uso de AWS Incident Manager [op.exp.9.aws.img.1] [op.exp.9.aws.ct.1].

Además de ello, la organización puede hacer uso del servicio AWS Security Hub que reúne toda la información proveniente de diferentes alertas y fuentes en un solo lugar, brindando una vista completa del estado general de seguridad y cumplimiento con las medidas de seguridad.

### Protección de claves criptográficas [op.exp.10]

#### Tecnologías de referencia en AWS

##### *AWS Key Management Service (AWS KMS)*

Es importante recordar que el cliente tenga en cuenta las recomendaciones de la [guía CCN STIC 807 - Criptología de empleo en el Esquema Nacional de Seguridad](#). AWS KMS es un servicio cualificado en el Catálogo de Productos y Servicios de las Tecnologías de la Información y la Comunicación (CPSTIC) y que cumple con los requisitos de dicha guía.

[AWS Key Management Service - AWS KMS](#) es un servicio administrado que facilita la creación y el control claves maestras de cliente (CMKs - Customer Managed Keys), las claves de cifrado utilizadas para cifrar los datos. Las AWS KMS CMKs están protegidos por módulos de seguridad de hardware (HSM - Hardware Security Module) validados por el Programa de validación del módulo criptográfico FIPS 140-2, actualizado a nivel de seguridad 3.

Es importante diferenciar las diferentes opciones de CMK:



Tipo de CMK	Puede ver los metadatos de CMK	Puede administrar CMK	Usada solo para mi cuenta de AWS	Rotación automática
CMK administrada por el cliente	Sí	Sí	Sí	Opcional. Cada 365 días (1 año).
CMK administrado por AWS	Sí	No	Sí	Obligatorio. Cada 365 días (1 año).
CMK propiedad de AWS	No	No	No	Varía

AWS KMS está integrado con la mayoría de los servicios de AWS que cifran los datos. Adicionalmente, [Almacén de claves externas \(XKS\)](#), una característica para los clientes que quieren proteger sus datos con claves de cifrado almacenadas en un sistema externo de administración de claves bajo su control. Esta capacidad ofrece una nueva flexibilidad para que los clientes cifren o descifren datos con claves criptográficas, autorización independiente y auditoría en un sistema externo de administración de claves fuera de AWS.

AWS KMS también está integrado con AWS CloudTrail para registrar el uso de CMKs para las necesidades de auditoría, normativas y cumplimiento.

### Requisitos y elementos de configuración

La utilización de AWS Key Management Service permite la protección de las claves criptográficas de acuerdo con el ENS, siempre y cuando se apliquen las siguientes configuraciones en cada una de las fases del ciclo de vida de las claves:

En lo que respecta a la generación de claves:

- Los usuarios o roles con privilegios para la creación de claves deben ser diferentes a los que van a utilizar las claves para operaciones de cifrado [*op.exp.10.aws.cmk.1*].

En cuanto a la utilización de las claves, se debe:

- Priorizar claves gestionadas por los clientes (CMK) en los servicios de AWS dónde esté disponible [*op.exp.10.aws.cmk.2*].
- Utilizar el principio de mínimos privilegios tanto para las políticas asociadas a las claves KMS (key politics), como para las políticas asociadas a los usuarios AWS IAM.
- Activar la rotación de las CMK. La rotación de claves de cifrado ayuda a reducir

el impacto potencial de una clave comprometida, ya que no se puede acceder a los datos cifrados con una nueva clave por medio de una clave anterior que puede haber estado expuesta [op.exp.10.aws.cmk.3]. Puede ampliar la información sobre la rotación de CMK en el [enlace](#).

Para el archivo posterior a la explotación y la destrucción de las claves, se debe:

- Deshabilitar todas las CMK que no estén en uso. Cuando se deshabilita una CMK, se vuelve inutilizable y no se puede usar para cifrar o descifrar datos [op.exp.10.aws.cmk.4]. Puede encontrar más información sobre cómo deshabilitar las CMK en el siguiente [enlace](#).
- Eliminar las claves deshabilitadas que no estén en uso y no mantengan ningún objeto o recurso cifrado, completando el ciclo de vida de la clave. Tener en cuenta que este proceso es irreversible, por lo que, en caso de no estar seguro, se recomienda únicamente realizar la acción de deshabilitar [op.exp.10.aws.cmk.5]. Encontrará más información sobre cómo eliminar las claves en el [enlace](#).

Para la correcta implantación del servicio de AWS KMS puede consultar la documentación del fabricante en el siguiente [enlace](#).

- Es importante recordar que, para la creación, visualización y utilización de las claves, [los usuarios deben tener asignada las correspondientes políticas AWS IAM](#), de manera que se defina un conjunto mínimo de permisos que permita a un usuario con un rol específico trabajar con los recursos de AWS KMS.

Además, para el cumplimiento de R1 – Algoritmos autorizados [op.exp.10.r1] en las categorías MEDIA y ALTA se debe tener en cuenta que, para la selección de los tipos de clave y su tamaño, se debe cumplir con los requisitos especificados en la guía de ***Seguridad de las TIC CCN-STIC-807 Criptología de Empleo en el Esquema Nacional de Seguridad***.

## Recomendaciones

Se recomienda utilizar [tags](#) y alias para una mejor gestión y administración de las claves [op.exp.10.aws.tag.1], siguiendo con las mejores prácticas sobre [etiquetado de recursos de AWS](#).

Además de ello, para dar cumplimiento al refuerzo R2 – Protección avanzada de claves criptográficas (opcional), se debe hacer uso de la guía [CCN-STIC 807 Criptología de empleo en el ENS](#) para seleccionar cifradores que cumplan con los requisitos establecidos.

## Contratación y acuerdos de nivel de servicio [op.ext.1]

### Requisitos y elementos de configuración

El cumplimiento de esta medida de seguridad implica que la organización deba tener en cuenta y establecer contractualmente los niveles de servicio ofrecidos por los

proveedores. En el caso de AWS, para diseñar una arquitectura en función de los niveles de servicio necesarios, se deberán consultar los acuerdos de nivel de servicio disponibles en el siguiente enlace: [nivel de servicios \(SLA\) de AWS](#).

## Gestión diaria [op.ext.2]

### Recomendaciones

Para poder llevar a cabo la medición del cumplimiento de las obligaciones de servicio a la que se refiere el ENS, en el ámbito de AWS es importante tener en cuenta que deberá existir algún usuario, grupo o rol que tenga asociada la política AWSSupportAccess [op.ext.2.aws.iam.1]. Esta política es la que permite a los usuarios gestionar los incidentes con el soporte técnico de AWS. Puede encontrar más información sobre esta política en el [enlace](#).

## Plan de continuidad [op.cont.2]

### Tecnologías de referencia en AWS

#### *Regiones, Zonas de Disponibilidad y zonas locales*

Las regiones son ubicaciones físicas donde AWS agrupa los centros de datos. Las zonas de disponibilidad (AZ) son grupos de centros de datos físicos en ubicaciones aisladas y separadas en un rango de 100 km de distancia dentro de cada región, interconectadas con redes de alta velocidad y baja latencia a través de fibra redundada cuyo tráfico está cifrado. Hay un mínimo de tres AZs por región. Además, las zonas locales son extensiones de una región de AWS en las que se ubican el cómputo, el almacenamiento, las bases de datos y otros servicios selectos de AWS, ofreciendo la capacidad de colocar estos recursos más cerca de los usuarios finales.

Más información sobre las regiones, zonas de disponibilidad y zonas locales en: [Regiones, zonas de disponibilidad y zonas locales](#)

### Requisitos y elementos de configuración

En el ámbito de AWS, deberá implementarse correctamente la distribución de servicios según regiones y zonas de disponibilidad para limitar al máximo los riesgos asociados a una única ubicación.

Los niveles de disponibilidad de los servicios se pueden modular en función de la utilización de varias zonas de disponibilidad y una o más regiones. La siguiente arquitectura cuenta con un SLA de 99.95% utilizando varias zonas de disponibilidad dentro de una región de AWS:

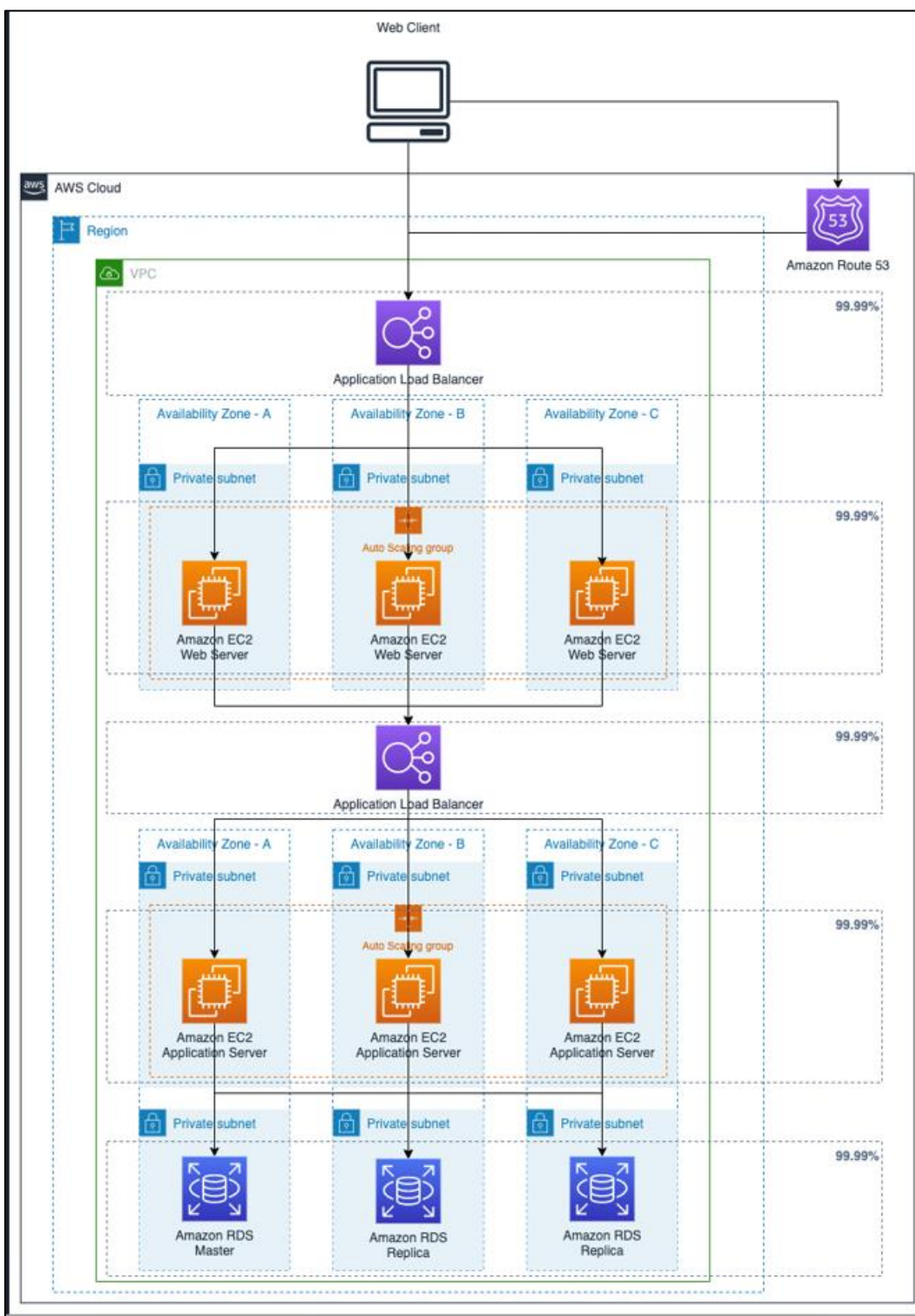


Fig. 4 - Arquitectura utilizando varias zonas de disponibilidad dentro de una región de AWS

Implementando esta arquitectura en dos regiones podemos obtener el siguiente SLA:

- Porcentaje de no disponibilidad de la aplicación en una región:  $100\% - 99.05\% = 0.05\%$  (hasta 4.38 horas por año).

- Porcentaje de no disponibilidad de la aplicación en dos regiones combinadas:  
 $0.05\% * 0.05\% = 0.000025\%$  (Hasta 7.884 segundos por año)
- SLA total utilizando ambas regiones =  $100\% - 0.000025\% = 99.999975\%$

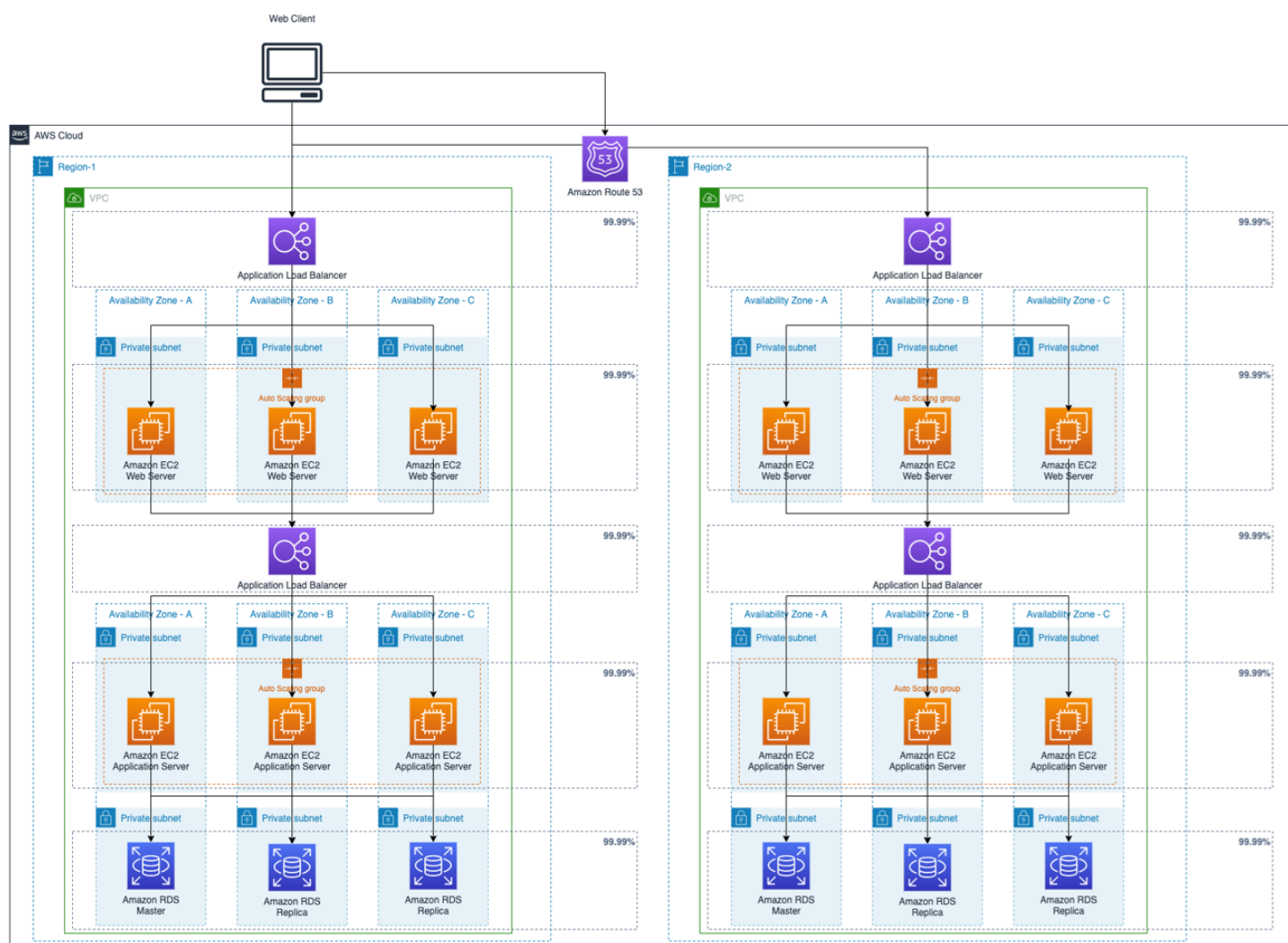


Fig. 5 - Arquitectura utilizando dos regiones y varias zonas de disponibilidad en cada región

## Recomendaciones

El refuerzo R2 – Comprobación de integridad (opcional) exige comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración. Si bien la comprobación de la integración del firmware será una responsabilidad de AWS en el ámbito de la seguridad de los elementos físicos de los sistemas, para la comprobación de los sistemas operativos y los ficheros de configuración de aquellas máquinas virtuales cuyo S.O. esté gestionado por la entidad usuaria, se recomienda hacer uso de los snapshots a través del servicio AWS Backup, tal y como se describe en el apartado [\[mp.info.6\] Copias de seguridad](#) de este mismo documento.

## Pruebas periódicas [op.cont.3]

### Tecnologías de referencia en AWS

#### *AWS Elastic Disaster Recovery*

[AWS Elastic Disaster Recovery \(AWS DRS\)](#) es un servicio que minimiza el tiempo de inactividad y la pérdida de datos con una recuperación rápida y confiable de aplicaciones locales y basadas en la nube mediante almacenamiento asequible, informática mínima y recuperación a un momento dado. AWS DRS permite la replicación de aplicaciones y datos mediante instancias de recuperación utilizadas por los procesos de conmutación por error, en caso de desastre, y conmutación por recuperación una vez mitigado el desastre.

#### Recomendaciones

Para realizar las pruebas periódicas que exige la medida de seguridad en el entorno AWS, la organización puede hacer uso del servicio AWS Elastic Disaster Recovery, programando y ejecutando pruebas no disruptivas (simulacros que no afectan ni al servidor de origen ni a la replicación de datos en curso) que prueben el correcto funcionamiento de las recuperaciones del plan de continuidad [op.cont.3.aws.drs.1].

La herramienta permite lanzar simulacros simultáneos en varios servidores de origen e informará, al finalizar el simulacro, del éxito o fracaso del lanzamiento de las instancias de simulacro, incluyendo si se ha logrado el primer arranque. Más información sobre la realización de simulacros en:

[Preparación para la conmutación por error - AWS DRS](#)

## Medios alternativos [op.cont.4]

### Tecnologías de referencia en AWS

#### *AWS Application Migration Service*

AWS Application Migration Service (AWS MGN) es una solución de elevación y cambio (rehost) altamente automatizada que simplifica, agiliza y reduce el costo de migrar aplicaciones a AWS. Permite a las empresas levantar y cambiar una gran cantidad de servidores físicos, virtuales o en la nube sin problemas de compatibilidad, interrupción del rendimiento o ventanas de cambio prolongadas. AWS MGN replica los servidores de origen en su cuenta de AWS. Cuando esté listo, convierte y lanza automáticamente sus servidores en AWS para que pueda beneficiarse rápidamente del ahorro de costos, la productividad, la resiliencia y la agilidad de la nube. Una vez que sus aplicaciones se ejecutan en AWS, puede aprovechar los servicios y las capacidades de AWS para cambiar de plataforma o refactorizar esas aplicaciones de forma rápida y sencilla, lo que hace que el sistema de elevación y cambio sea una ruta rápida hacia la modernización.



## *AWS Database Migration Service*

[AWS Database Migration Service](#) (AWS DMS) es un servicio en la nube que facilita la migración de bases de datos relacionales, almacenes de datos, bases de datos NoSQL y otros tipos de almacenes de datos entre entornos locales y la nube. Este servicio permite realizar migraciones únicas y replicar los cambios continuos para mantener sincronizados tanto el origen como el destino.

### **Recomendaciones**

Las herramientas de AWS referidas ofrecen capacidades para la replicación de recursos locales hacia la nube que pueden ayudar a cumplir los requerimientos de la medida de seguridad Medios alternativos [op.cont.4].

En el caso de los servidores, se cuenta con AWS Application Migration Service (AWS MGN). En el siguiente [documento](#) se puede consultar información como los requisitos de las máquinas virtuales a replicar, los sistemas operativos compatibles, los tipos de volúmenes y sistemas de archivos admitidos y otro tipo de información relevante. Para usar AWS Application Migration Service (AWS MGN), primero se debe inicializar el servicio para cualquier región de AWS en la que planea usar AWS MGN.

Puede inicializar el servicio a través de la consola o mediante la API.

Durante el proceso de inicialización:

- Se crearán las funciones y políticas de IAM requeridas.
- Las plantillas requeridas están configuradas.

En cuanto a las bases de datos, se pueden replicar utilizando AWS Database Migration Service para la creación de servidores de replicación y la ejecución de tareas de migración.

Adicionalmente, para cumplir con el refuerzo R1 – Automatización de la transición a medios alternativos (opcional), si bien no existe un servicio que realice de manera automática la transferencia de los servicios a los medios alternativos, se recomienda hacer uso de AWS Backup como medio para transferir la última configuración (snapshot), pudiendo ser replicada en dichos medios alternativos.

También puede utilizar Amazon Data Lifecycle Manager para automatizar la creación, retención y eliminación de instantáneas de EBS y las AMI respaldadas por EBS. Cuando automatiza la administración de instantáneas y la AMI, lo ayuda a:

- Proteger datos valiosos aplicando una programación periódica de copias de seguridad.
- Cree las AMI estandarizadas que se puedan actualizar a intervalos regulares.
- Conservar las copias de seguridad de acuerdo con los requisitos de los auditores o las políticas internas de conformidad



- Reducir los costos de almacenamiento al eliminar las copias de seguridad obsoletas
- Cree políticas de copia de seguridad de recuperación ante desastres que respalden los datos en cuentas aisladas.

## Detección de intrusión [op.mon.1]

### Tecnologías de referencia en AWS

#### *Amazon VPCFlowlogs*

Amazon [VPC FlowLogs](#) es una característica de Amazon VPC que permite capturar información acerca del tráfico IP que entra y sale de las interfaces de red en la VPC. Los datos del registro de flujo se pueden publicar en Amazon CloudWatch Logs o Amazon S3. Los datos de registro de flujo se recopilan fuera de la ruta del tráfico de red y, por lo tanto, no afectan al rendimiento ni a la latencia de la red, permitiendo crear o eliminar registros de flujo sin ningún riesgo de impacto. Los Amazon VPC FlowLogs pueden ayudar en una serie de tareas, tales como:

- Diagnosticar reglas de grupo de seguridad muy restrictivas
- Supervisar el tráfico que llega a su instancia
- Determinar la dirección del tráfico hacia y desde las interfaces de red

### Requisitos y elementos de configuración

Para cumplir con el requisito base de la medida de seguridad Detección de intrusión [op.mon.1] se deberán seguir las siguientes prácticas:

- Utilizar Amazon GuardDuty (o herramientas de terceros con funcionalidades equivalentes) para la detección de amenazas e intrusiones. [op.mon.1.aws.gd.1].
- Activar el servicio de eventos AWS CloudTrail para todas las regiones [op.mon.1.aws.ct.1].

### Recomendaciones

Para el que el sistema ejecute acciones automáticas de respuesta ante alertas generadas tal y como exige el refuerzo R3 – Detección de intrusión (opcional), se recomienda habilitar los servicios Amazon GuardDuty y AWS System Manager. Amazon GuardDuty permite la detección de las alertas, mientras que System Manager pone a disposición de la entidad usuaria herramientas para generar y ejecutar scripts de respuesta para esas alertas. En cualquier caso, es responsabilidad de la entidad usuaria, no solo el diseño de la respuesta específica (script), sino también detallar aquellas alertas que quieran ser monitorizadas.

También se recomienda activar el servicio Amazon VPC FlowLogs

[op.mon.1.aws.flow.1] para analizar con herramientas adicionales el tráfico que soportan aquellos servicios críticos bajo el alcance del ENS.

## Sistema de métricas [op.mon.2]

### Tecnologías de referencia en AWS

#### *Amazon Security Hub*

[Amazon Security Hub](#) es un servicio que proporciona una vista integral del estado de seguridad de los recursos en AWS recopilando datos de seguridad en las cuentas y servicios de AWS y permitiendo el análisis de tendencias para identificar y priorizar los problemas de seguridad en el entorno AWS.

#### *AWS Budgets*

El servicio [AWS Budgets](#) permite realizar un seguimiento de los costes y del uso de AWS y tomar decisiones al respecto. Por ejemplo, se pueden establecer presupuestos de costes mensuales con un importe objetivo fijo para realizar un seguimiento de todos los costes o elegir que se generen avisos sobre los gastos reales y los gastos previstos.

#### *AWS Cost Explorer*

AWS Cost Explorer puede explorar el uso y los costos usando el gráfico principal, los informes de uso y costos de AWS Cost Explorer o los informes de instancias reservadas de AWS Cost Explorer. Puede ver los datos de los últimos 12 meses, pronosticar la cantidad que probablemente gastará durante los 12 meses siguientes y obtener recomendaciones de qué instancias reservadas adquirir. Puede utilizar AWS Cost Explorer para identificar aspectos que deben estudiarse más a fondo y consultar tendencias que puede usar para comprender los costos.

### Recomendaciones

Si bien el requisito base de la medida Sistema de métricas [op.mon.2] exige la recopilación de la información para conocer el grado de implantación de las medidas de seguridad con carácter general, en el ámbito de AWS se debe utilizar AWS Security Hub para obtener una vista consolidada de los hallazgos de seguridad en los servicios de AWS habilitados [op.mon.2.aws.sh.1].

Por su parte, AWS Budgets puede ayudar a la recopilación de los datos sobre recursos consumidos a los que se refiere el Refuerzo 2 – Eficiencia del sistema de gestión de la seguridad [op.mon.2.r2]. No obstante, se debe tener en cuenta que este servicio muestra la información sobre costes de una cuenta agregados, sin especificar qué costes específicos se refieren a servicios de seguridad. También puede analizar tendencias y hacer previsiones con el uso de AWS Cost Explorer. Encontrará más información en el [enlace](#).

## Vigilancia [op.mon.3]

### Tecnologías de referencia en AWS

#### *Amazon Inspector*

[Amazon Inspector](#) es un servicio de administración de vulnerabilidades que analiza continuamente las cargas de trabajo de AWS. Amazon Inspector detecta y analiza automáticamente las instancias de Amazon EC2, las imágenes de los contenedores que residen en Amazon ECR y las funciones de AWS Lambda en busca de vulnerabilidades de software y/o exposición no deseada de la red.

Cuando una vulnerabilidad es detectada (hallazgo), Amazon Inspector crea una búsqueda que describe la vulnerabilidad, identifica el recurso afectado y califica la gravedad de ésta. El servicio proporciona, además, orientación para la corrección de estos hallazgos.

Más información sobre la descripción de los resultados de Amazon Inspector en:

[Descripción de los resultados - Amazon Inspector](#)

### Requisitos y elementos de configuración

Como requisito básico para el cumplimiento del control Vigilancia [op.mon.3], deberá asegurarse que todos los servicios que se utilicen en la arquitectura de la aplicación desplegada en AWS estén generando logs. Aunque muchos de los servicios provistos por AWS tienen habilitado por defecto la generación de logs, hay algunos servicios en los que es preciso habilitarla. En los siguientes enlaces se puede encontrar información para la habilitación de logs en los servicios de cómputo, contenedores y tecnología sin servidor, y para los servicios de bases de datos, gestión y gobernanza, redes y entrega de contenido y almacenamiento.

Para acceder a los registros de los diferentes servicios de AWS de forma centralizada, se deberá utilizar el servicio Amazon CloudWatch Logs [op.mon.3.aws.cwl.1], que permite la identificación, la búsqueda de códigos de error o patrones específicos, así como el filtrado en función de campos específicos.

Para el almacenamiento a largo plazo de los datos de registro, es recomendable que éstos se exporten a Amazon S3, definiendo previamente el ciclo de vida de los logs e identificando qué se necesita almacenar en frío. Para hacer la exportación se deberá utilizar un usuario AWS IAM con acceso completo a los registros de Amazon S3 y Amazon CloudWatch Logs y seguir el procedimiento que se detalla en los siguientes documentos, según se desee realizar la operación utilizando la [consola](#) o la [CLI de AWS](#).

El refuerzo R1 – Correlación de eventos [op.mon.3.r1.1], aplicable a los sistemas desde la categoría media, exige no únicamente la recolección de los eventos, sino la disposición de un sistema que permita la correlación de los mismos, lo cual se puede lograr a través de las herramientas Amazon GuardDuty, AWS Security Hub, o bien a través de un SIEM externo a AWS [op.mon.3.r1.aws.gd.1] [op.mon.3.r1.aws.sh.1].

En cuanto a las soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración a las que se refiere el refuerzo R2 – Análisis dinámico [op.mon.3.r2.1], se deberá, en primer lugar, utilizar la herramienta Inspector para la detección de posibles vulnerabilidades de las instancias Amazon EC2, las funciones AWS Lambda y las imágenes de contenedor [op.mon.3.r2.aws.insp.1]. Para analizar las vulnerabilidades de las instancias Amazon EC2, Amazon Inspector requiere la instalación del agente de AWS Systems Manager en las mismas que, si bien está preinstalado en muchas instancias Amazon EC2, es posible que se deba habilitar manualmente. En segundo lugar, en lo relativo a las deficiencias de configuración, se deben utilizar las herramientas AWS Config y AWS Security Hub (ya explicadas en otros apartados de la presente guía) [op.mon.3.r2.aws.cfg.1] [op.mon.3.r2.aws.sh.1]. Adicionalmente, se puede utilizar el servicio AWS [Trusted Advisor](#), que inspecciona el entorno AWS y ofrece recomendaciones para mejorar el rendimiento y la disponibilidad del sistema, así como para ayudar a corregir deficiencias de configuración [op.mon.3.r2.aws.adv.1].

El refuerzo R3 – Ciberamenazas avanzadas [op.mon.3.r3.1] y [op.mon.3.r3.2] queda cubierto con la activación de Amazon GuardDuty, dado que este servicio analiza diversas fuentes, entre otras, el tráfico de red, para la detección de anomalías y amenazas persistentes avanzadas [op.mon.3.r3.aws.gd.1].

Por otro lado, la aplicación de medidas de prevención, detección y reacción frente a los intentos de minería de datos a la que se refiere el refuerzo R5 – Minería de datos [op.mon.r5.2] se puede cubrir a través de diferentes soluciones entre otras:

- La característica Amazon [S3 Protection](#) de Amazon GuardDuty habilita la monitorización de operaciones en Amazon S3 tales como el listado o la eliminación de buckets.
- [AWS Network Firewall](#) se puede configurar, con las reglas adecuadas, para la protección contra el malware de minería de criptomonedas.
- El hallazgo [CryptoCurrency:EC2/BitcoinTool.B!DNS](#) de Amazon GuardDuty indica que una instancia Amazon EC2 en el entorno AWS está consultando un nombre de dominio que se encuentra asociado a una actividad relacionada con las criptomonedas, como el minado.

Por último, en cuanto al refuerzo R6 – Inspecciones de seguridad [op.mon.4.r6], tanto la verificación de la configuración [op.mon.3.r6.1] como los análisis de vulnerabilidades [op.mon.3.r6.2] a efectuar tras los incidentes que hayan desvelado vulnerabilidades del sistema, ambos aspectos quedarían cubiertos, respectivamente, a través de AWS Config Rules, que verifica la configuración de forma continua, y de Amazon Inspector [op.mon.3.r6.aws.cfg.1] [op.mon.3.r6.aws.insp.1], que también efectúa los análisis de vulnerabilidades de forma continua. El último aspecto de este refuerzo, la ejecución de pruebas de penetración [op.mon.3.r6.3] deberá ejecutarse manualmente por parte del usuario. En este aspecto, es importante tener en cuenta las [reglas que rigen las pruebas de intrusión en AWS y las listas de servicios permitidos y actividades prohibidas](#) para que dichas pruebas no afecten a los sistemas propios del proveedor.

### 3.1 MEDIDAS DE PROTECCIÓN [mp]

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

#### Protección de las comunicaciones [mp.com]

##### Tecnologías de referencia en AWS

###### *Amazon Virtual Private Clouds (VPCs)*

Una [red privada virtual \(Amazon VPC\)](#) es una red virtual dedicada en la cuenta de AWS y lógicamente aislada de otras redes virtuales en la nube de AWS. La Amazon VPC predeterminada de cada región se configura de manera que se pueda comenzar a lanzar instancias Amazon EC2 y conectarse a ellas de inmediato.

###### *AWS WAF*

[AWS WAF](#) es un firewall de aplicaciones web que permite monitorizar las solicitudes HTTP y HTTPS que se reenvían a los recursos de aplicaciones web protegidas y controlar el acceso al contenido de los recursos de usuario de AWS en función de una serie de criterios especificados, como las direcciones de IP de origen de las solicitudes o valores de las cadenas de consultas.

###### *AWS Network Firewall*

[AWS Network Firewall](#) es un servicio administrado que facilita la implementación de protecciones de a nivel de Amazon VPCs, creando y aplicando políticas basadas en reglas y filtrando el tráfico de acuerdo a dichas reglas.

###### *AWS Firewall Manager*

[AWS Firewall Manager](#) ayuda con las tareas de administración y mantenimiento centralizado de las reglas de seguridad de red (de AWS WAF, AWS Shield y grupos de seguridad) en varias cuentas y recursos de AWS, aplicando automáticamente las reglas y otras protecciones de seguridad en todas las cuentas y recursos, incluso cuando estos sean nuevos.

###### *Listas de control de acceso (ACL) de red*

Las [Listas de control de acceso](#) de red actúan como firewall sin información de estado (*stateless*) para las subredes asociadas y controlan el tráfico entrante y saliente en el ámbito de la subred. Las VPCs incluyen automáticamente una ACL de red predeterminada y modificable que permite todo el tráfico IPv4 e IPv6 entrante y saliente. Una misma ACL se puede asociar a varias subredes, pero una subred sólo puede asociarse a una ACL a la vez.

## Security Groups

Los grupos de seguridad ([Security Groups](#)) actúan como firewall virtual con información de estado (*stateful*) a nivel de instancia Amazon EC2, a las que se asocian para controlar el tráfico entrante y saliente. Cuando se crea una instancia, puede asociarse a uno o varios grupos de seguridad. Si no se especifica ningún grupo de seguridad, la instancia se asocia al grupo de seguridad predeterminado de la Amazon VPC que, por defecto, implementa unas reglas consistentes en permitir el tráfico entrante de las interfaces de red de instancias asignadas al mismo grupo de seguridad y permitir todo el tráfico saliente.

## AWS Gateway Load Balancer

Los [AWS Gateway Load Balancer](#) permiten implementar, escalar y administrar dispositivos virtuales de terceros como firewalls, sistemas de detección y prevención de intrusiones y sistemas de inspección profunda de paquetes, escuchando todos los paquetes en todos los puertos y reenviando el tráfico al grupo objetivo que se especifica en la regla. El tráfico de los Gateway Load Balancer se configura mediante tablas de enrutamiento y fluye desde la Amazon VPC del consumidor de servicios a través del endpoint del Gateway Load Balancer hasta el Gateway Load Balancer en la Amazon VPC del proveedor de servicios para luego regresar a la VPC del consumidor.

## VPN Site-to-Site

De forma predeterminada, las instancias que se lanzan en una Amazon VPC de AWS no pueden comunicarse con la red de la entidad usuaria (remota). [AWS VPN Site-to-Site](#) permite habilitar el acceso a la red remota desde la VPC y la configuración del enrutamiento para que el tráfico pase a través de la conexión VPN.

## Perímetro Seguro [mp.com.1]

### Requisitos y elementos de configuración

Para una adecuada protección del perímetro de la red en AWS deberán seguirse las siguientes prácticas:

- Asegurar que el Security Group por defecto restrinja todo el tráfico. Para ello, se deberán agregar las reglas del Security Group que se aplica por defecto cuando se crea una Amazon VPC. Salvo modificación, cualquier Amazon VPC recién creada contendrá un grupo de seguridad predeterminado que necesitará corrección [mp.com.1.aws.sg.1].
- Evitar la existencia de grupos de seguridad que dejen abierto todo el tráfico entrante [mp.com.1.aws.sg.2].
- Evitar tener un repositorio de security groups que no estén siendo usados. Es necesario disponer de un proceso regular de revisión y limpieza manual para la eliminación de los security groups que no estén siendo usados. [mp.com.1.aws.sg.3].

- Filtrar todo el tráfico entrante y saliente de la Amazon VPC [mp.com.1.aws.nfw.1] para dejar pasar únicamente el tráfico previamente autorizado y estrictamente necesario para la correcta utilización de los servicios.
- Asimismo, con security groups deberá evitarse una configuración de acceso que permita llegar desde internet a los servicios que no lo precisen como los siguientes [mp.com.1.aws.sg.4]:
  - SSH (TCP/22),
  - RDP (TCP/3389),
  - Oracle (TCP/1521 y TCP/2483),
  - MySQL (TCP/3306),
  - Postgres (TCP/5432),
  - Redis (TCP/6379),
  - MongoDB (TCP/27017 y TCP/27018),
  - Cassandra (TCP/7199, TCP/8888 y TCP/9160),
  - Memcached (TCP/11211).

## Protección de la confidencialidad [mp.com.2]

### Requisitos y elementos de configuración

Dado que en el servicio cloud de AWS el tráfico siempre va a discurrir por la red externa al propio dominio, para el cumplimiento del requisito base de la medida de seguridad Protección de la confidencialidad [mp.com.2] se debe garantizar que las conexiones entre la Amazon VPC y la red local (remota) se canalizan a través de VPN Site-to-Site o bien a través de AWS Direct Connect.

Además, los algoritmos y parámetros utilizados en la conexión VPN deberán atender a los requisitos especificados en la guía **CCN-STIC-807 Criptología de Empleo en el Esquema Nacional de Seguridad** en el caso de aplicar el refuerzo R1 – Algoritmos y parámetros autorizados.

Si es de aplicación el Refuerzo R2 – Dispositivos Hardware [mp.com.2.r2] y se necesita el empleo de dispositivos hardware en el establecimiento de la VPN, deberá tenerse en cuenta que AWS únicamente facilitará al usuario los archivos de configuración que deberán aplicarse en el dispositivo, que será en todo caso responsabilidad del cliente.

Por último, para el cumplimiento del refuerzo R3 – Productos certificados [mp.com.2.r3], se deberá emplear para el establecimiento de la VPN un producto o servicio que cumpla con los requisitos de la medida de seguridad Componentes



certificados [op.pl.5].

## Recomendaciones

Para dar cumplimiento al refuerzo R4 – Cifradores (opcional), se recomienda usar como apoyo la guía [CCN-STIC 807 Criptología de empleo en el ENS](#) para seleccionar cifradores que cumplan con los requisitos establecidos.

Por su parte, el refuerzo R5 – Cifrado de información especialmente sensible (opcional) exige el cifrado de toda la información transmitida. El cifrado de la información en tránsito, recomendado, en cualquier caso, depende notablemente de los servicios utilizados, pero todos los servicios de AWS disponen de herramientas de cifrado que permiten satisfacer este requisito.

## Protección de la integridad y de la autenticidad [mp.com.3]

### Requisitos y elementos de configuración

Para el cumplimiento de los requisitos base de la medida de seguridad Protección de la integridad y de la autenticidad [mp.com.3] se deberán seguir las siguientes prácticas:

- Habilitar TLS en los balanceadores de carga ELB. Puede consultarse los detalles sobre la configuración de los *listeners* de ELB en el siguiente documento: [Configuración de Listeners para Classic Load Balancers - ELB \[mp.com.3.aws.elb.1\]](#)
- Evitar el uso de protocolos de cifrado inseguros en la conexión TLS entre clientes y balanceadores de carga. Esto podría dejar la conexión TLS entre balanceadores y clientes vulnerable a ser explotada. En particular, se deberá evitar el uso de TLS 1.1 y anteriores [\[mp.com.3.aws.elb.2\]](#).
- Asegurar que los Buckets de almacenamiento Amazon S3 apliquen cifrado para la transferencia de datos empleando TLS [\[mp.com.3.aws.s3.1\]](#).
- Asegurar que la distribución entre frontales Amazon CloudFront y sus orígenes únicamente emplee tráfico HTTPS [\[mp.com.3.aws.cf.1\]](#).

## Recomendaciones

Del mismo modo que para el Refuerzo R5 de [\[mp.com.2\] Protección de la confidencialidad](#), se deben seleccionar cifradores que cumplan los requisitos, pudiendo utilizar como apoyo la guía [CCN-STIC 807 Criptología de empleo en el ENS](#).

## Separación de flujos de información en la red [mp.com.4]

### Requisitos y elementos de configuración

Para cumplir con este requisito base de la medida de seguridad Separación de flujos

de información en la red [op.com.4] en AWS, los flujos de información de red se deben separar a través de la utilización de diferentes subnets [mp.com.4.aws.vpc.1].

Además, se debe evitar el uso de subnets con la opción de asignación automática de IPs públicas (auto-assign Public IP) [mp.com.4.aws.vpc.2], para lo cual deberá desmarcarse la siguiente casilla. No obstante, conviene aclarar que esto sólo aplica en subredes que tienen asociado un internet Gateway.

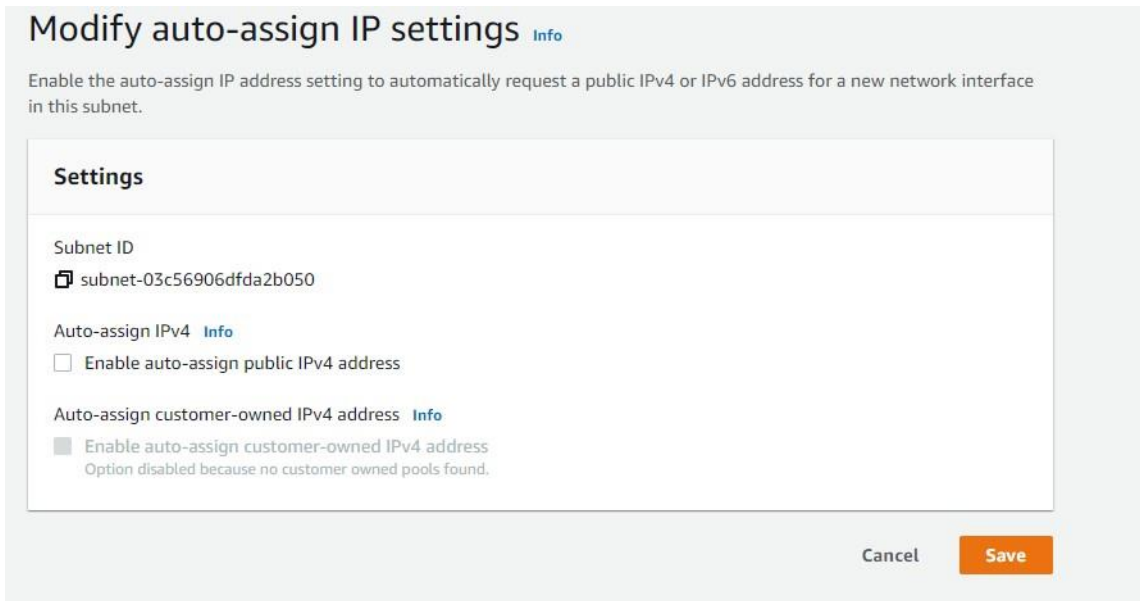


Fig. 6 - Opciones disponibles en una subnet para la asignación automática de IPs

O bien configurar esta opción desde la CLI, pudiendo ajustar este atributo en el momento de creación de la subnet o en subredes ya existentes:

```
-aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --no-map-public-ip-on-launch
```

En cuanto a los diferentes refuerzos opcionales de esta medida de seguridad, deberá implementarse la segmentación seleccionando entre alguna de tecnologías disponibles en AWS:

- Para el caso de R1 – Segmentación lógica básica [mp.com.4.r1], se deberá implementar a través de la utilización de diferentes Amazon VPCs [mp.com.4.r1.aws.vpc.1].
- Para el caso de R2 – Segmentación lógica avanzada [mp.com.4.r2], se deberá implementar a través de la utilización de diferentes Amazon VPCs que, en caso de necesitar ser conectadas entre ellas, se deberá utilizar VPC Peering o Transist GW.
- Para el caso de R3 – Segmentación física [mp.com.4.r3], se deberá implementar

a través de diferentes Amazon VPCs situadas en diferentes regiones de AWS [*mp.com.4.r3.aws.vpc.1*].

## Criptografía [mp.si.2]

### Tecnologías de referencia en AWS

El cifrado de la información en los soportes de almacenamiento de AWS está principalmente cubierto por el servicio *AWS KMS (Key Management Service)* descrito en el apartado [Tecnologías de referencia en AWS del capítulo Protección de claves criptográficas \[op.exp.10\]](#). Se añaden en esta sección algunos aspectos adicionales para la aplicación del cifrado a la información en reposo.

Para la aplicación de esta medida de seguridad en el ámbito de AWS se entenderá que será necesario aplicar mecanismos criptográficos sobre los recursos que almacenen información.

### Requisitos y elementos de configuración

Para el cumplimiento del requisito base de la medida de seguridad Criptografía [mp.si.2], deben de aplicarse el cifrado sobre:

- El almacenamiento de las instancias en todos sus volúmenes de datos. En el siguiente documento se muestra el proceso de cifrado de volúmenes Amazon EBS: [Cifrado de recursos – EBS. \[mp.si.2.aws.kms.1\]](#)
- Los distintos buckets de Amazon S3, de los cuáles se debe asegurar que tengan activado en cifrado en reposo [*mp.si.2.aws.s3.1*].

Adicionalmente, se deben tener en cuenta los siguientes requerimientos, pero deberá tener en cuenta la repercusión que tienen en su organización, con respecto tanto a los costes del servicio como al consumo de cuotas y en base a el análisis de riesgos correspondiente.

- Las colas de mensajes de AWS (Amazon SQS). Las colas de mensajes pueden llegar a almacenar importantes cantidades de información sensible hasta el momento en el que vaya a ser tratada por una aplicación [*mp.si.2.aws.sqs.1*].
- Los datos en Amazon RDS [*mp.si.2.aws.rds.1*].
- Las bases de datos Amazon Dynamo DB, que deben implementar cifrado seguro mediante el uso de claves de cliente (AWS KMS) [*mp.si.2.aws.dydb.1*].
- Todos los dominios del servicio Amazon Elasticsearch Service (ES). En caso de que se utilice este servicio, deberá asegurarse la activación de la opción de cifrado en reposo [*mp.si.2.aws.es.1*].

Adicionalmente, es importante tener en cuenta que el Refuerzo R1 – Productos

certificados [mp.si.2.r1] exige la utilización de productos certificados conforme a [op.pl.5], si bien AWS KMS es un producto certificado cuyo uso satisface la exigencia de este control.

Por último, para el cumplimiento de R2 – Copias de seguridad [mp.si.2.r2] que exige el cifrado de las copias de seguridad con algoritmos y parámetros autorizados por el CCN, se deberá asegurar el cifrado de las copias de seguridad ([snapshots](#)) de Amazon EBS [mp.si.2.r2.aws.ebs.1].

## Recomendaciones

Para el mejor cumplimiento de esta medida de seguridad y asegurar que no se crean nuevos volúmenes de almacenamiento sin cifrar, se recomienda dejar activada la opción de cifrado por defecto para nuevos volúmenes, tal y como se describe en el siguiente documento [mp.si.2.aws.ebs.1]:

### [Activar el cifrado automático de nuevos volúmenes y copias instantáneas de Amazon EBS - EBS.](#)

Para realizar tareas de monitorización referentes a la detección de actividades relacionadas con el servicio de AWS KMS, se recomienda integrar este junto con las funcionalidades de Amazon Cloudwatch [mp.si.2.aws.cw.1], de manera que se puedan recopilar y procesar datos del uso de claves y sus cambios, pudiendo generar alertas para eventos de seguridad como: Fecha de vencimiento, alerta de uso de una clave con estado “pendiente de eliminación”, rotación automática o eliminación. AWS KMS predefine las métricas de Amazon CloudWatch para facilitar el monitoreo de los datos críticos y la creación de alarmas. Estas métricas se pueden consultar a través de la Consola de AWS o la propia API de Amazon CloudWatch. Más información en: [Monitoreo de con Amazon CloudWatch - AWS Key Management Service](#)

## Aceptación y puesta en servicio [mp.sw.2]

### Tecnologías de referencia en AWS

#### *Amazon CodeGuru*

[Amazon CodeGuru](#) es una herramienta para desarrolladores que proporciona recomendaciones inteligentes para la mejora de la calidad del código fuente que permite identificar las líneas de código más costosas en una aplicación. El servicio Amazon CodeGuru, pone a disposición del usuario la biblioteca de detectores de Amazon CodeGuru, que es un recurso que contiene información detallada sobre los detectores de seguridad y calidad de código para ayudar a los desarrolladores a crear aplicaciones seguras y eficientes en AWS. Amazon CodeGuru está compuesto por dos componentes principales:

- [Amazon CodeGuru Reviewer](#), que utiliza el machine learning y el razonamiento automatizado para identificar problemas críticos y errores difíciles de detectar a simple vista durante el desarrollo de la aplicación para mejorar la calidad del código.

- [Amazon CodeGuru Profiler](#), que optimiza el rendimiento de las aplicaciones que se ejecutan en la fase de producción e identifica las líneas de código más costosas, reduciendo así los costos operativos de forma significativa.

### AWS CodeBuild

[AWS CodeBuild](#) es un servicio de integración continua completamente administrado en la nube. AWS CodeBuild compila código fuente, ejecuta pruebas y produce paquetes de software listos para su implementación. Además de ello, elimina la necesidad aprovisionar, administrar y escalar los propios servicios de compilación, pagando por cada minuto de uso. En la siguiente imagen se muestra un diagrama de lo que ocurre cuando se ejecuta una compilación con AWS CodeBuild:

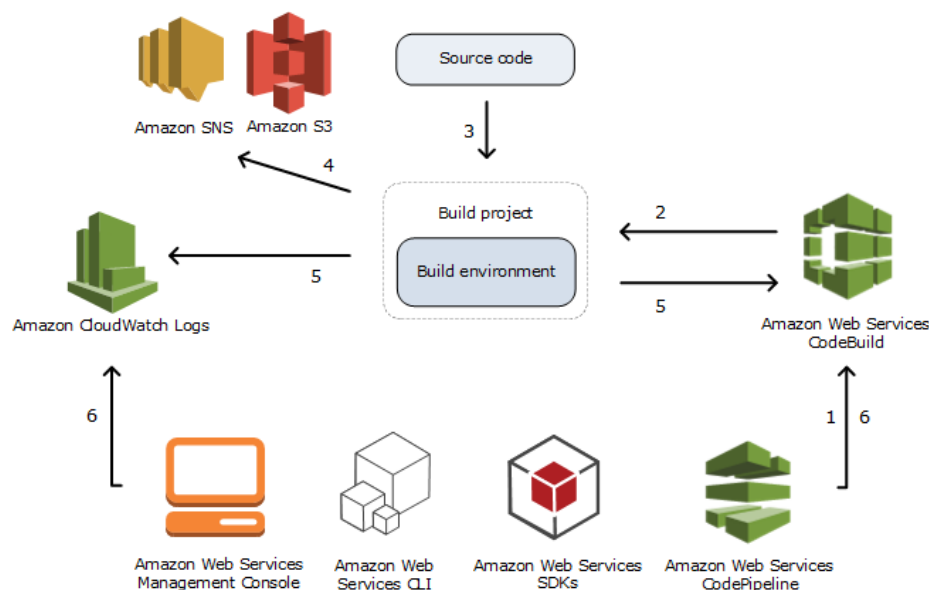


Fig. 7 – Diagrama de ejecución de compilación con Amazon CodeBuild.

### AWS CloudFormation Guard

[AWS CloudFormation Guard \(cfn-guard\)](#) es una interfaz de línea de comandos de código abierto (CLI) que ayuda a las organizaciones a lograr que sus recursos de infraestructura y aplicaciones de AWS cumplan con las directrices definidas en la política de la compañía. Cfn-guard ofrece a los administradores de cumplimiento un lenguaje sencillo de política como código que permite definir reglas capaces de comprobar las diferentes configuraciones de los recursos, diferenciando entre permitidas y prohibidas y validar sus plantillas de AWS CloudFormation mediante dichas reglas.

### Recomendaciones

Para cumplir con el requisito base de la medida de seguridad Aceptación y puesta en servicio [mp.sw.2], se debe cumplir con los criterios de aceptación en materia de seguridad, así como garantizar que no se deteriora la seguridad de los componentes del servicio. Si bien AWS no dispone de un servicio u herramienta específica que garantice el cumplimiento de la medida de seguridad, la organización puede apoyarse en AWS para cumplir con los refuerzos de esta.

Para cumplir con el refuerzo R1 – Pruebas, la organización puede hacer uso del

servicio Amazon CodeBuild como solución para realizar pruebas en un entorno aislado. Amazon CodeBuild permite ejecutar su versión en entornos aislados del resto de usuarios y descarta cada entorno de compilación una vez ha finalizado este proceso; esto proporciona seguridad y separación en los niveles de infraestructura y ejecución. Además de ello, permite realizar informes sobre las pruebas realizadas dentro del entorno y especificar claves almacenadas en AWS KMS para cifrar los artefactos utilizados, así como controlar el acceso a los proyectos de compilación mediante los permisos de nivel de recursos definidos en las políticas AWS IAM [mp.sw.2.r1.aws.acb.1]. Además, en entornos multi-cuenta, el entorno aislado de pruebas se puede lograr a través de la implementación de diferentes unidades organizativas con AWS Control Tower, destinando una de ellas a funcionar como entorno de pruebas en preproducción<sup>5</sup>.

En cuanto a la auditoría de código fuente a la que se refiere el refuerzo R2 – Inspección del código fuente (opcional), la organización puede hacer uso del servicio Amazon CodeGuru para la detección de problemas y solución de vulnerabilidades en el código fuente previa entrada a operación. Los desarrolladores confirman el código en GitHub y agregan Amazon CodeGuru Reviewer como uno de los revisores de código principales, permitiendo centrar el esfuerzo en la mejora de la calidad del código fuente y en la aplicación de las prácticas recomendadas de seguridad específicas para aplicaciones y arquitectura. Amazon CodeGuru publica automáticamente recomendaciones orientadas a cambios en el código y admite el análisis completo del repositorio o de la base de código para el mantenimiento periódico del mismo. Más información sobre el funcionamiento de Amazon CodeGuru Reviewer en:

### [¿Cómo funciona Amazon CodeGuru Reviewer?](#)

De forma paralela, los desarrolladores pueden apoyarse en AWS CloudFormation Guard ([cfn-guard-rulegen](#)) para extraer de fuentes de código abierto reglas de plantillas de AWS CloudFormation compatibles y ya existentes, de forma que no tengan que ser creadas de cero, y usarlas de forma local mientras editan plantillas o bien de forma automática, para impedir que se implementen recursos no conformes con la organización, acción que proporciona información a los desarrolladores a la hora de la identificación.

Para la realización de auditorías de código fuente, tal y como se describe en el refuerzo R2 – Inspección del código fuente (opcional), se recomienda hacer uso del servicio Amazon CodeGuru, anteriormente descrito.

### Copias de seguridad [mp.info.6]

#### Tecnologías de referencia en AWS

<sup>5</sup> Ver Guía **CCN-STIC 887D – Guía de Configuración Segura para entornos multi-cuenta en AWS**, apartado Control Tower – recomendaciones para la arquitectura de seguridad – AWS Control Tower.

### *AWS Backup*

AWS Backup es un servicio administrado que facilita la centralización y automatización de la protección de información y datos en servicios de AWS, nube e instalaciones. Mediante el uso de este servicio, se pueden configurar políticas de copias de seguridad (conocidas como planes de copias de seguridad) y monitorear la actividad de los recursos de AWS de forma centralizada. Además de ello, permite automatizar tareas de backup, eliminando la necesidad de creación de scripts o procesos manuales.

El despliegue de recursos en AWS implica que la normativa interna de la organización sobre copias de seguridad exigida en esta medida de seguridad deba aplicarse no únicamente sobre los recursos locales (como pueden ser máquinas virtuales ejecutada en instalaciones propias), sino también sobre los recursos desplegados en AWS.

### *Amazon Dynamo DB*

Amazon Dynamo DB es un servicio de base de datos NoSQL totalmente administrado que ofrece un rendimiento rápido, así como una perfecta escalabilidad. Amazon Dynamo DB permite delegar las cargas administrativas que supone tener que utilizar y escalar bases de datos distribuidas y ofrece también soluciones de cifrado en reposo, lo que elimina carga y complejidad operativa derivada de la protección de información confidencial.

Amazon Dynamo DB permite crear tablas de bases de datos capaces de almacenar y recuperar cualquier cantidad de contenido, así como atender cualquier nivel de tráfico de solicitudes al poder escalar la capacidad del rendimiento de estas tablas en cada momento.

Este servicio proporciona, además, capacidad para crear backup en diferido y habilitar la recuperación a un momento dado en las tablas de bases de datos, protegiendo las mismas de operaciones accidentales de escritura o eliminación.

### *Amazon S3*

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento. Amazon S3 permite el almacenamiento y protección de datos de cualquier tamaño y origen (lagos de datos, sitios web, aplicaciones móviles, copias de seguridad y restauración, archivado, aplicaciones empresariales, dispositivos IoT o big data) y proporciona funciones de gestión para optimizar, organizar y configurar el acceso a los datos para satisfacer los requisitos organizativos y de conformidad específicos.

Más información en: [Amazon S3 - Amazon Simple Storage Service](#)

### *Amazon EFS*

Amazon Elastic File System (Amazon EFS) es un sistema de archivos elástico, simple y sin servidor que facilita la configuración, escalado y optimización de costos de almacenamiento de archivos en AWS. Amazon EFS permite crear sistemas de archivos



accesibles para instancias de Amazon Elastic Compute Cloud (Amazon EC2), servicios de contenedores de Amazon Elastic Container Service (Amazon ECS), Amazon Kubernetes Service (EKS) y AWS Fargate, así como funciones de AWS Lambda mediante una interfaz de sistema de archivos. Los sistemas de Amazon EFS pueden escalarse automáticamente desde gigabytes hasta petabytes de datos sin necesidad de aprovisionar almacenamiento. Este servicio está diseñado para ofrecer alta disponibilidad y durabilidad, permitiendo el acceso simultáneo de decenas, cientos y hasta miles de instancias a un sistema de archivos de Amazon EFS.

Más información en: [Amazon Elastic File System \(EFS\)](#)

### *Amazon RDS*

Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, operación y escala de una base de datos relacional en la nube de AWS. Este servicio proporciona una capacidad rentable y redimensionable para una base de datos relacional estándar, ocupándose además de las tareas de administración de bases de datos comunes. Amazon RDS puede realizar copias de seguridad automáticas de las bases de datos y actualizar el software de base de datos a la última versión.

Más información en: [Amazon Relational Database Service \(Amazon RDS\)](#)

### **Recomendaciones**

Para los procedimientos de respaldo de cualquiera de los dos entornos (local y nube) y siempre y cuando se utilicen recursos compatibles en el entorno local, la entidad puede hacer uso de AWS Backup, que permite elaboración de planes de respaldo y la definición de reglas de frecuencia, ciclo de vida, lugar de almacenamiento y etiquetado de las copias de seguridad [mp.info.6.aws.bcku.1]. Para seguir las buenas prácticas recomendadas por AWS en el servicio AWS Backup, se puede utilizar el siguiente

#### [Conformance Pack de AWS Config.](#)

Además, los planes de respaldo se pueden integrar con AWS tags, acotando con base en las etiquetas de los recursos el alcance de cada proceso de copiado [mp.info.6.aws.tag.1]. En caso de utilizar estas tecnologías, se deberá activar la opción de versionado, que permite la elección del punto de restauración y copiar la totalidad de los datos.

En cuanto a los controles de acceso de las copias de respaldo, la organización puede hacer uso de roles y políticas para la definición y la asignación de permisos necesarios para llevar a cabo las copias de seguridad. En los siguientes documentos se aportan [ejemplos de políticas AWS IAM](#) para denegar el acceso a tipos de recursos, a almacenes y para denegar la eliminación de puntos de recuperación en almacenes; y [recomendaciones](#) para asegurar los datos y las operaciones de AWS Backup a través de políticas de control de servicios (SCP).

En cuanto a R1 – Pruebas de recuperación [mp.info.6.r1], si se utiliza AWS backup, esta herramienta permite llevar a cabo pruebas de restauración sin que se destruyan o sustituyan los recursos originales ni afectar a las cargas de trabajo. No obstante, es

importante tener en cuenta que, en caso de querer ejecutar restauraciones automatizadas, únicamente se podrán efectuar sobre aquellos recursos que hayan sido copiados con la propia herramienta.

Asimismo, la entidad usuaria también puede apoyarse en AWS para el cumplimiento de R2 – Protección de las copias de seguridad [mp.info.6.r2], que exige que al menos una de las copias de seguridad se almacene en un lugar diferente. Para ello, además de poder utilizar la nube de AWS como ubicación diferente para el almacenamiento de las copias de seguridad separadas de los datos copiados desde otro entorno, dentro de la propia nube se pueden almacenar los backups en diferentes regiones o en diferentes cuentas dentro de la organización, tal y como se indica entre las buenas prácticas de este [documento](#) y en la guía **CCN-STIC 887D Guía de configuración segura para entornos multi-cuenta en AWS**. Asimismo, es importante tener en cuenta que todas las funcionalidades de snapshots replican los datos automáticamente en tres zonas de disponibilidad diferentes.

## Protección del correo electrónico [mp.s.1]

### Tecnologías de referencia en AWS

#### *Amazon Workmail*

[Amazon WorkMail](#) es un servicio de calendario y correo electrónico administrado compatible con clientes de correo electrónico Microsoft Outlook para el móvil y equipos de sobremesa. Amazon Workmail se puede integrar con los directorios corporativos y controlar las claves que cifran los datos y la ubicación en que estos se almacenan.

#### *Amazon Simple Email Service (SES)*

Amazon Simple Email Service - SES es una plataforma de correo electrónico que ofrece un método de enviar y recibir correos electrónicos a través de los propios dominios y direcciones de correo de la entidad usuaria. Amazon SES se integra con otros productos de AWS lo que, entre otras funcionalidades, permite añadir capacidades de envíos de correo a cualquier aplicación, configurar Amazon SNS para recibir notificaciones de los correos electrónicos rebotados, controlar el acceso de los usuarios a su envío de correo electrónico o almacenar los mensajes que se reciban en un Amazon S3.

Esta medida de seguridad será aplicable en AWS cuando la entidad usuaria utilice los servicios AWS Workmail o Amazon Email Service.

### Requisitos y elementos de configuración

Para una correcta configuración de los servicios de correo electrónico, en primer lugar, se deberá hacer uso del cifrado de la información contenida en los correos electrónicos. Amazon Workmail implementa de forma nativa el cifrado con claves AWS KMS, cifrando todos los mensajes de correo antes de que se escriban en el disco y descifrándolos cuando el usuario obtiene acceso a ellos. En Amazon SES, se [debe hacer uso de la opción que permite a los usuarios enviar correo electrónico cifrado con S/MIME](#).

En cuanto a la protección contra el spam y el código dañino, si bien está implementado de forma nativa, se deberá [habilitar el registro de eventos](#) de Amazon Workmail en AmazonCloudWatch para realizar el seguimiento de mensajes con spam. Entre los eventos que Amazon Workmail registra en Amazon CloudWatch, se encuentra el evento ORGANIZATION\_EMAIL\_RECEIVED, que se genera cuando la organización recibe un mensaje de correo electrónico y que, entre otros, incluye los campos spamVerdict (indica si Amazon SES ha marcado el mensaje como spam) y spamVerdict (indica si se ha superado la comprobación de SPF).

## Protección de servicios y aplicaciones web [mp.s.2]

### Requisitos y elementos de configuración

Los sistemas dedicados a la publicación de información no deberán ser publicados sin estar antes protegidos frente a las amenazas propias de los servicios web, por lo que para cumplir con el requisito base de esta medida de seguridad debe configurar lo siguiente:

- Todas las aplicaciones web distribuidas por el servicio Amazon CloudFront deben estar integradas con el servicio de firewall de aplicaciones web AWS WAF [mp.s.2.aws.waf.1].
- Los API Gateway utilizados deben tener un ACL WAF asociado [mp.s.2.aws.waf.2].
- Todo el tráfico hacia los balanceadores de aplicación debe pasar antes a través de un firewall de aplicación web para quedar protegidos ante ataques en la capa de aplicación. [mp.s.2.aws.waf.3].

## Protección frente a la denegación de servicio [mp.s.4]

### Tecnologías de referencia en AWS

#### *AWS Shield Standard y AWS Shield Advanced*

[AWS Shield](#) es un servicio de protección administrado contra ataques de denegación de servicio distribuido (DDoS) que protege las aplicaciones ejecutadas en AWS. Proporciona detección dinámica y mitigaciones en línea automáticas que minimizan el tiempo de inactividad y la latencia de la aplicación. Su modalidad Standard proporciona monitoreo del flujo de red de funcionamiento continuo que inspecciona el tráfico entrante en los servicios de AWS y aplica una combinación de firmas de tráfico, algoritmos de anomalías y otras técnicas de análisis para detectar el tráfico malicioso en tiempo real. Su modalidad Advanced ofrece un nivel de protección superior contra ataques dirigidos a aplicaciones que se ejecuten en recursos de Amazon EC2, ELB, Amazon CloudFront, AWS Global Accelerator o Amazon Route 53. Además de la protección en la capa básica de transporte, proporciona detección y mitigación adicionales contra ataques DDoS sofisticados y a gran escala, visibilidad de los ataques

casi en tiempo real e integración con servicios como AWS WAF.

### *AWS Auto Scaling*

[AWS Auto Scaling](#) es un servicio de AWS que integra múltiples funcionalidades para el escalado dinámico y predictivo de los recursos, permitiendo la creación de planes de escalado que automatizan la manera en que diferentes recursos responden ante los cambios que se producen en la demanda pudiendo así optimizar la disponibilidad, los costos, o lograr un equilibrio entre ambos. Se pueden utilizar etiquetas para agrupar los recursos a escalar en diferentes planes de escalado.

### **Requisitos y elementos de configuración**

Para cumplir con el requisito base de esta medida de seguridad dotando a los sistemas de la capacidad suficiente para atender la carga prevista con holgura y desplegar tecnologías para la prevención de ataques conocidos, se debe diseñar las aplicaciones soportadas por los servicios de AWS de modo que, en todos aquellos servicios que no dispongan de soluciones de auto escalado nativas, se active el servicio AWS Auto Scaling [mp.s.4.aws.as.1]. Concretamente, AWS Auto Scaling permite la definición de planes de escalado para los servicios y recursos de Amazon Aurora, Amazon EC2, Amazon Elastic Container Service, Amazon DynamoDB y Spot Fleet.

Con el fin de disponer de una herramienta de prevención, detección y mitigación de ataques de denegación de servicio que haga cumplir con el refuerzo R1, se debe hacer uso del servicio AWS Shield Advanced [mp.s.4.r1.aws.shieldadv.1]. Con AWS Shield Advanced es posible, además de aplicar las protecciones comunes de la capa de transporte y red, disponer de una herramienta de detección y mitigación adicionales contra ataques de tipo DoS o DDoS sofisticados y a gran escala, visibilidad de los ataques en tiempo real e integración con otras herramientas como AWS WAF.

### **Recomendaciones**

En cuanto al refuerzo R2 – Ataques propios (opcional), se recomienda habilitar y activar el servicio Amazon GuardDuty como ayuda a la hora de detectar volumen de tráfico inusual, pudiendo notificar del lanzamiento de ataques desde propias instalaciones.

## 4 GLOSARIO DE TÉRMINOS

Término	Definición
<b>ABAC</b>	Attribute Based Access Control (Control de Acceso Basado en Atributos)
<b>ACL</b>	Access Control List (Lista de Control de Acceso)
<b>ACM</b>	AWS Certificate Manager (Gestor de Certificados de AWS)
<b>AMI</b>	Amazon Machine Images (Imágenes de Máquinas de Amazon)
<b>API</b>	Application Programming Interface (Interfaz de Programación de Aplicaciones)
<b>APT</b>	Advanced Persistent Threat (Amenaza Persistente Avanzada)
<b>Área controlada</b>	Zona o área en la que la organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.
<b>Área no controlada</b>	Zona o área en la que la organización considera que no se cumplen las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.
<b>Autenticación multifactor</b>	Exigencia de dos o más factores de autenticación para ratificar una autenticación como válida.
<b>AZ</b>	Availability Zone (Zona de disponibilidad)
<b>Back-end</b>	Conjunto del desarrollo que se encarga de que una página web funcione correctamente, conocida como parte trasera de la web.
<b>Bucket</b>	Contenedor para almacenar objetos (archivos) pertenecientes al servicio S3
<b>CA</b>	Autoridades de Certificación
<b>Caché</b>	Capa de almacenamiento de datos de alta velocidad que almacena un subconjunto de datos, normalmente transitorios, de modo que las solicitudes futuras de dichos datos se atienden con mayor rapidez que si se debe acceder a los datos desde la ubicación de almacenamiento principal.
<b>Categoría de seguridad de un sistema</b>	Grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de servicio.
<b>CCN</b>	Centro Criptológico Nacional
<b>Certificado cualificado</b>	Un certificado electrónico cualificado es un documento electrónico que vincula a una persona física o jurídica con una clave pública y una clave privada y confirma su identidad.
<b>CLI</b>	Command Line Interface (Interfaz de Línea de Comandos)
<b>CMK</b>	Customer Master Key (Clave Maestra de Cliente)
<b>Confidencialidad</b>	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
<b>DDoS</b>	Distributed Denial of Service (Denegación de Servicio Distribuido)
<b>DoS</b>	Denial of Service (Denegación de Servicio)
<b>EDR</b>	Endpoint Detection and Response (Detección y Respuesta de Endpoint)
<b>ELB</b>	Elastic Load Balancer (Balanceador de Carga Elástico)

<b>Endpoint</b>	Cualquier dispositivo que sea físicamente la parte final de una red.
<b>HSM</b>	Hardware Security Module (Módulo de Seguridad en formato Hardware)
<b>HTTP</b>	Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto)
<b>HTTPS</b>	Hypertext Transfer Protocol Secure (Protocolo de Transferencia de Hipertexto Seguro)
<b>IaaS</b>	Infraestructura As A Service (Infraestructura como servicio)
<b>Incidente de seguridad</b>	Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.
<b>Instancia</b>	Servidor virtual en la nube de AWS.
<b>Integridad</b>	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
<b>IoT</b>	Internet of Things (Internet de las cosas)
<b>IPSec</b>	Internet Protocol Security (Protocolo de Seguridad en Internet)
<b>Medidas de seguridad</b>	Conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción o de recuperación.
<b>Mínimo privilegio</b>	Principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.
<b>OIDC</b>	Open ID Connect. Protocolo de identidad simple y de estándar abierto basado en el protocolo OAuth 2.0 que permite a las aplicaciones cliente confiar en la autenticación realizada por un proveedor de OpenID Connect para verificar la identidad de un usuario.
<b>PaaS</b>	Platform As A Service (Plataforma como Servicio)
<b>Partner</b>	Aquellas personas, organizaciones o instituciones con las que se está involucrado a nivel de negocio.
<b>Prowler</b>	Herramienta de seguridad para comprobar los sistemas de AWS con respecto al punto de referencia CIS relacionado. Esta prueba comparativa proporciona un conjunto de prácticas recomendadas para AWS. El uso principal de esta herramienta es el endurecimiento del sistema y la comprobación del cumplimiento.
<b>Proxy</b>	Tecnología que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (Internet).
<b>RBAC</b>	Role Based Access Control (Control de Acceso Basado en Roles)
<b>SaaS</b>	Software As A Service (Software como Servicio)
<b>SAML</b>	Security Assertion Markup Language. Estándar de código abierto basado en XML que permite el intercambio de información de autenticación y autorización.
<b>SDK</b>	Software Development Kit (Kit de Desarrollo de Software)
<b>SSE</b>	Server Sent Events (Envío de Eventos de Servidor)
<b>SSH</b>	Secure Shell-Protocol (Protocolo de acceso seguro servidores)
<b>Subnet</b>	Subdivisión de una red.
<b>Tags</b>	Etiquetas
<b>TCP</b>	Transfer Control Protocol (Protocolo de Control de Transferencia)

<b>TI</b>	Tecnología de la Información
<b>TIC</b>	Tecnologías de la Información y la Comunicación
<b>TLS</b>	Transport Layer Security (Seguridad en Capas de Transporte)
<b>Token</b>	Tipo de identificador que permite que los permisos de una concesión surtan efecto inmediatamente.
<b>Trazabilidad</b>	Propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.
<b>U2F</b>	Universal Second Factor (Segundo Factor Universal)
<b>UI</b>	User Interface (Interfaz de Usuario)
<b>Usuario Breakglass</b>	Cuenta que se utiliza con fines de emergencia para obtener acceso a un sistema o servicio al que no se puede acceder bajo los controles normales.
<b>Usuario Root</b>	Cuenta de administrador.
<b>Usuarios de la organización</b>	Personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.
<b>Usuarios externos</b>	Usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.
<b>VLAN</b>	Virtual Local Area Network (Red de Área Local Virtual)
<b>VPC</b>	Virtual Private Cloud (Nube Privada Virtual)
<b>WAF</b>	Web Application Firewall (Cortafuegos de Aplicaciones Web)
<b>Wildcard</b>	Comodines de búsqueda.

## 5 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
<b>Acuerdos a nivel de servicios (SLA)</b>	<a href="#">Acuerdos de nivel de servicios (SLA) de AWS</a>
<b>Amazon API Gateway</b>	<a href="#">Amazon API Gateway</a>
<b>Amazon Aurora</b>	<a href="#">Amazon Aurora</a>
<b>Amazon CloudWatch</b>	<a href="#">Amazon CloudWatch</a>
<b>Amazon CloudWatch Logs</b>	<a href="#">CloudWatch Logs - AWS CloudWatch</a>
<b>Amazon CodeBuild</b>	<a href="#">Amazon CodeBuild</a>
<b>Amazon CodeGuru</b>	<a href="#">Amazon CodeGuru</a>



Servicio	URL de documentación del servicio
Amazon CodeGuru Profiler	<a href="#">Amazon CodeGuru Profiler</a>
Amazon CodeGuru Reviewer	<a href="#">Amazon CodeGuru Reviewer</a>
Amazon Dynamo DB	<a href="#">Amazon DynamoDB</a>
Amazon Elastic Computer Cloud (EC2)	<a href="#">Amazon Elastic Computer Cloud (EC2)</a>
Amazon Elastic File System (EFS)	<a href="#">Amazon Elastic File System - AWS EFS</a>
Amazon GuardDuty	<a href="#">Amazon GuardDuty</a>
Amazon GuardDuty Malware Protection	<a href="#">Protección contra malware en Amazon GuardDuty - Amazon GuardDuty</a>
Amazon Inspector	<a href="#">Amazon Inspector</a>
Amazon Relational Database Service (RDS)	<a href="#">Amazon Relational Database Service</a>
Amazon S3	<a href="#">Amazon Simple Storage Service - Amazon S3</a>
Amazon S3 Protection	<a href="#">Protección de datos en Amazon S3 - Amazon S3 Protection</a>
Amazon Simple Email Service (SES)	<a href="#">Amazon Simple Email Service - SES</a>
	<a href="#">Habilitación del correo electrónico firmado o cifrado - SES</a>
	<a href="#">Activación del registro de eventos - SES</a>
Amazon Simple Queue Service (SQS)	<a href="#">Amazon Simple Queue Service - AWS SQS</a>
Amazon Systems Manager Incident Manager	<a href="#">AWS Systems Manager Incident Manager</a>
Amazon Workdocs	<a href="#">Amazon WorkDocs</a>
Amazon WorkMail	<a href="#">Amazon WorkMail</a>
Amazon Workspaces	<a href="#">Amazon WorkSpaces</a>
Autenticación Multifactor (MFA)	<a href="#">Uso de autenticación multifactor (MFA) en AWS - AWS IAM</a>
	<a href="#">Configuración del acceso a una API protegido por MFA</a>
AWS Auto Scaling	<a href="#">AWS Auto Scaling</a>
AWS Backup	<a href="#">Copia de seguridad centralizada en la nube - AWS Backup</a>
AWS Budgets	<a href="#">Administración de costes - AWS Budgets</a>
AWS Certificate Manager	<a href="#">AWS Certificate Manager</a>
AWS Change Manager	<a href="#">AWS Change Manager</a>
AWS Cloud Formation	<a href="#">AWS Cloud Formation</a>
AWS CloudFormation Guard	<a href="#">AWS CloudFormation Guard</a>
AWS CloudFront	<a href="#">Amazon CloudFront</a>

Servicio	URL de documentación del servicio
AWS CloudTrail	<a href="#">AWS CloudTrail</a>
AWS Config	<a href="#">Documentación de AWS Config - AWS Config</a> <a href="#">Tipos de recursos admitidos en AWS Config - AWS Config</a> <a href="#">Required Tags - AWS Config</a>
AWS Config Rules	<a href="#">AWS Config Rules - AWS Config</a>
AWS Database Migration Service	<a href="#">AWS Database Migration Service</a>
AWS Direct Connect	<a href="#">AWS Direct Connect</a>
AWS Firewall Manager	<a href="#">AWS Firewall Manager</a>
AWS Gateway Load Balancer	<a href="#">AWS Gateway Load Balancer</a>
AWS Identity & Access Manager (IAM)	<a href="#">Identities de IAM (usuarios, grupos de usuarios y roles) - AWS IAM</a>
AWS Key Management Service (KMS)	<a href="#">AWS Key Management Service - AWS KMS</a> <a href="#">Políticas de claves - AWS KMS</a>
AWS Lambda	<a href="#">AWS Lambda</a>
AWS Network Firewall	<a href="#">AWS Network Firewall</a>
AWS Security Hub	<a href="#">Amazon Security Hub</a>
AWS Security Token Service (STS)	<a href="#">Amazon Security Token Service - AWS STS</a>
AWS Server Migration Service	<a href="#">AWS Server Migration Service</a> <a href="#">Requisitos para AWS Server Migration Service - AWS Server Migration Service</a>
AWS Shield	<a href="#">Protección administrada contra DDoS - AWS Shield</a>
AWS Shield Advanced	<a href="#">AWS Shield Advanced</a>
AWS System Manager Automation	<a href="#">AWS Systems Manager Automation</a>
AWS Systems Manager Explorer	<a href="#">AWS Systems Manager Explorer</a>
AWS Systems Manager Inventory	<a href="#">AWS Systems Manager Inventory</a>
AWS Systems Patch Manager	<a href="#">AWS Systems Manager Patch Manager</a>
AWS Tags	<a href="#">Etiquetado de recursos en AWS - AWS Tags</a> <a href="#">Prácticas recomendadas sobre el etiquetado - AWS Tags</a>
AWS Trusted Advisor	<a href="#">AWS Trusted Advisor</a>

Servicio	URL de documentación del servicio
AWS Virtual Private Cloud (VPC)	<a href="#">AWS Virtual Private Cloud - AWS VPC</a>
AWS Web Application Firewall (WAF)	<a href="#">AWS Web Application Firewall - AWS WAF</a>
Conformance Packs	<a href="#">AWS Conformance Packs - AWS Config</a>
Elastic Block Store (EBS)	<a href="#">Cifrado de recursos - EBS</a>  <a href="#">Activar el cifrado automático de nuevos volúmenes y copias instantáneas de Amazon EBS - EBS</a>  <a href="#">Instantáneas de Amazon EBS - EBS</a>
Elastic Disaster Recovery (DRS)	<a href="#">AWS Elastic Disaster Recovery - AWS DRS</a>  <a href="#">Preparación para la conmutación por error - AWS DRS</a>
Elastic Load Balancing (ELB)	<a href="#">Configuración de Listeners para Classic Load Balancers - ELB</a>
IAM Access Analyzer	<a href="#">IAM Access Analyzer</a>
Listas de control de acceso (Access Control List – ACL)	<a href="#">Access Control List - ACL</a>
Policy Simulator	<a href="#">Prueba de políticas IAM con simulador - AWS Policy Simulator</a>
Políticas IAM	<a href="#">Tipos de políticas IAM - AWS IAM</a>  <a href="#">Políticas IAM - AWS IAM</a>  <a href="#">Configuración de una política de contraseñas de la cuenta para usuarios de IAM - AWS IAM</a>
Proceso de creación y activación de una nueva cuenta en AWS	<a href="#">Proceso de creación y activación de una cuenta AWS</a>
Proveedores de identidad externos - Identity Provider (IdP)	<a href="#">Acceso mediante proveedores de identidad (IdP) a servicios AWS - AWS IdP</a>
Regiones, zonas de disponibilidad y zonas locales	<a href="#">Regiones, zonas de disponibilidad y zonas locales</a>
Roles IAM	<a href="#">Roles de IAM - AWS IAM</a>
Security Groups	<a href="#">Security Groups</a>
Service Quotas	<a href="#">Cuotas de servicio - Service Quotas</a>  <a href="#">Service Quotas y Amazon CloudWatch alarms - Service Quotas</a>
Servicios de AWS en el ámbito del programa de conformidad	<a href="#">Servicios de AWS en el ámbito del programa de conformidad</a>
VPC FlowLogs	<a href="#">Registro del tráfico IP - VPC FlowLogs</a>

Servicio	URL de documentación del servicio
VPN Site-to-Site	<a href="#">AWS VPN Site-to-Site</a>
Well-Architected Framework	<a href="#">AWS Well-Architected Framework</a>

## 6 CUADRO RESUMEN DE MEDIDAS DE SEGURIDAD

Se facilita a continuación un cuadro resumen de configuraciones a aplicar para la protección del servicio. Estas medidas sirven para valorar el nivel de cumplimiento de la organización.

Para entender la herramienta Prowler y su activación para evaluación de cumplimiento con el Esquema Nacional de Seguridad consulte la Guía **CCN-STIC 887B Guía Rápida de Prowler**.

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
[op.pl.2]	Arquitectura de Seguridad	Es recomendable que la entidad usuaria se apoye en el marco de trabajo AWS Well-Architected Framework.		
[op.pl.4]	Necesidades de procesamiento	La entidad usuaria deberá llevar a cabo el estudio de capacidades a las que hace referencia la medida de seguridad, si bien (...) deberá tener especialmente en cuenta:  * Las capacidades de procesamiento, almacenamiento y comunicaciones de las instancias desplegadas en AWS.  * Las cuotas de los servicios a utilizar.		
[op.pl.4.r1]	Mejora continua de la gestión de la capacidad	En caso de no disponer de herramientas de terceros, se deberán utilizar las herramientas de monitorización de la capacidad indicadas para monitorizar las capacidades de la infraestructura y el grado de consumo de los servicios en función de las cuotas disponibles. (Amazon CloudWatch)		
		Para la creación de alarmas en materia de capacidad de las instancias, se debe configurar un tema de Amazon SNS que permita el envío de mails automáticos a la dirección de correo seleccionada.		
		Configurar alarmas correspondientes a las diferentes capacidades (Amazon SNS) como uso de CPU, capacidad de almacenamiento o latencia.		
		En cuanto a la monitorización sobre el grado de consumo, se puede utilizar la solución nativa Quota Monitor, o bien se pueden visualizar las cuotas de servicio y configurar alarmas a través de la integración de AWS Service		

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		Quotas con Amazon CloudWatch.		
[op.acc.1]	Identificación	Utilizar los grupos y roles, en lugar de los usuarios individuales, para controlar el acceso. Esto permitirá implementar un conjunto de permisos en lugar de actualizar muchas políticas individuales cuando el acceso de un usuario necesita cambiar.		
		Los identificadores de usuario deberán ser asignados en el proveedor de identidades (o en AWS IAM) de modo que se permita singularizar a la persona asociada a cada identificador y cumplir con el resto de los requisitos del control Identificación [op.acc.1] relativas a la gestión de los usuarios.		
		Es muy recomendable la utilización de un proveedor de identidades que permita administrar las identidades en un lugar centralizado, en vez de utilizar AWS IAM para ello.	op.acc.1.aws.iam.1	iam_check_saml_providers_sts
		En caso de que la organización no disponga de un proveedor de identidades, se deberán generar las identidades de los usuarios directamente en AWS IAM teniendo en cuenta, del mismo modo, las exigencias del Esquema Nacional de Seguridad.		
		Es recomendable disponer de un usuario AWS IAM de seguridad (usuario "breakglass"), que no se encuentre sincronizado con el proveedor de identidades externo y que permita la recuperación de emergencia del acceso a AWS en caso de imposibilidad de autenticar a los usuarios a través del proveedor de identidades.		
[op.acc.1.r1]	Identificación avanzada	Los identificadores de usuario deberán ser asignados en el proveedor de identidades (o en AWS IAM) de modo que se permita singularizar a la persona asociada a cada identificador y cumplir con el resto de los requisitos del refuerzo.		
[op.acc.2]	Requisitos de acceso	Hacer uso de las políticas AWS IAM para la asignación de privilegios de acceso. Deberán administrarse permisos para controlar el acceso de las identidades de personas y máquinas y sus cargas de trabajo.		

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		En caso de utilizar el servicio IMDS (metadatos de instancia y datos del usuario) se recomienda encarecidamente el uso de la versión 2 del servicio.	op.acc.2.aws.imds.1	ec2_instance_imdsv2_enabled
[op.acc.3]	Segregación de funciones y tareas	Enumerar los recursos específicos a los que puede obtener acceso una función de trabajo.		
		Emplear correctamente el uso de RBAC para separar las funciones de desarrollo y operación.		
		Emplear correctamente el uso de ABAC para separar las funciones de autorización y control de uso.		
		Las políticas AWS IAM deberían estar asociadas solo a grupos y a roles.		
[op.acc.3.r1]	Segregación rigurosa	En caso de ser de aplicación, la segregación deberá tener en cuenta la separación de las funciones de configuración y mantenimiento y de auditoría de cualquier otra.	op.acc.3.r1.aws.iam.1	iam_support_role_created
[op.acc.3.r2]	Privilegios de auditoría	Disponer de cuentas con privilegios de auditoría estrictamente controladas y personalizadas.	op.acc.3.r2.aws.iam.1	iam_securityaudit_managed_policy_attached_to_role
[op.acc.3.r3]	Acceso a la información de seguridad	Limitar el acceso a la información de seguridad del sistema a los administradores de seguridad utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto etc.).		
[op.acc.4]	Proceso de gestión de derechos de acceso	Las políticas AWS IAM deben permitir sólo los privilegios necesarios para cada rol. Se recomienda comenzar con el mínimo nivel de permisos e ir añadiendo permisos adicionales según vaya surgiendo la necesidad en lugar de comenzar con permisos administrativos.	op.acc.4.aws.iam.1	sqs_queues_not_publicly_accessible, s3_bucket_policy_public_write_access, awslambda_function_not_publicly_accessible, iam_no_custom_policy_permissive_role_assumption, cloudwatch_cross_account_sharing_disabled, awslambda_function_url_public, awslambda_function_url_cors_policy,



ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		Las políticas AWS IAM únicamente deben poder asignarse por el usuario que tenga la función de control de accesos expresamente atribuida.		iam_policy_allows_privilege_escalation, iam_policy_no_administrative_privileges
		No utilizar la cuenta raíz salvo necesidad expresa. Cuando se crea una cuenta en AWS, se deben crear usuarios, grupos o roles con privilegios administrativos para realizar las tareas de administración administrador y utilizar éstos, dejando sin uso el usuario raíz. Esta configuración debe entenderse como un mecanismo para impedir que el trabajo directo con privilegios de administrador repercuta negativamente en la seguridad, al acometer todas las acciones con el máximo privilegio cuando éste no es siempre requerido.		
		Evitar políticas con comodines (wildcards) en su definición, que puedan otorgar privilegios administrativos completos.	op.acc.4.aws.iam.2	iam_policy_allows_privilege_escalation, iam_no_custom_policy_permissive_role_assumption, iam_policy_no_administrative_privileges
		Para una correcta implementación de la estrategia de políticas de acceso, se recomienda utilizar la herramienta Policy Simulator para probar y solucionar posibles problemas en la asignación de políticas.		
		Se puede utilizar AWS Acces Analyzer para identificar recursos y cuentas, validar las políticas contra las prácticas recomendadas y generar políticas con base en la actividad de acceso de registros de AWS CloudTrail.		
		En cuanto a los accesos a las instancias alojadas en AWS se recomienda emplear mecanismos para mantener a las personas alejadas de los datos. Es decir, limitar al máximo el acceso directo a los datos por parte de los		

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		usuarios.		
		Con AWS Systems Manager Automation pueden utilizarse documentos de automatización y diseñar flujos de trabajo para la administración de cambios o la ejecución de operaciones estándar para administrar las instancias Amazon EC2 (p. ej., actualizar los sistemas operativos), en lugar de permitir el acceso directo.	op.acc.4.aws.iam.3	ec2_instance_managed_by_ssm
[op.acc.6]	Mecanismo de autenticación (usuarios de la organización)	Evitar el uso permanente de múltiples claves de acceso para un mismo usuario AWS IAM.	op.acc.6.aws.iam.1	iam_user_two_active_access_key
		Las claves de acceso deberán rotarse cada 90 días o menos.	op.acc.6.aws.iam.2	iam_disable_90_days_credentials,iam_rotate_access_key_90_days
		Deberá habilitarse el vencimiento de las credenciales de los usuarios. (Bien a través de la política de contraseñas de AWS IAM o del proveedor de identidades federado).	op.acc.6.aws.iam.3	iam_password_policy_expires_passwords_within_90_days_or_less,iam_disable_90_days_credentials,iam_rotate_access_key_90_days
		Se deberá evitar la asignación por defecto de claves de acceso para todos los usuarios que tengan acceso a la consola. Para cumplir con este requisito, se recomienda revisar qué usuarios se encuentran dados de alta en la cuenta de AWS y disponen de acceso a la consola de administración y evitar la asignación de claves de acceso cuando no son necesarias. Cuando un usuario requiera claves de acceso, se deberán enviar por correo electrónico.	op.acc.6.aws.iam.4	iam_user_no_setup_initial_access_key
[op.acc.6.r1]	Contraseñas	<p>Las contraseñas de los usuarios deberán tener las siguientes normas de complejidad mínima y robustez:</p> <ul style="list-style-type: none"> <li>• Longitud mínima de 12 caracteres.</li> <li>• Al menos, una mayúscula.</li> <li>• Al menos, una minúscula.</li> <li>• Al menos, un número.</li> <li>• Al menos, un carácter especial.</li> </ul>	op.acc.6.r1.aws.iam.1	iam_password_policy_lowercase,iam_password_policy_minimum_length_14,iam_password_policy_number,iam_password_policy_reuse_24,iam_password_policy_symbol,iam_password_policy_uppercase

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		Se debe configurar la política de contraseñas para que se prohíba la utilización de contraseñas antiguas		
		Se debe permitir a los usuarios cambiar sus propias contraseñas.		
		Se debe seleccionar la opción reset password cuando se crean usuarios para que se obligue al cambio de contraseña en el primer acceso.		
		Se debe configurar la política de contraseñas para que se prohíba la creación de contraseñas antiguas.		
		Se debe permitir a los usuarios cambiar sus propias contraseñas.		
[op.acc.6.r2]	Contraseña + otro factor de autenticación	MFA deberá estar habilitado para todas las cuentas que tengan contraseña para acceder a la consola, incluyendo el usuario root. Además, se debe aplicar la MustBeSignedInWithMFA a los usuarios, grupos y roles. Esta política exige que antes de que se ejecute la API se deba haber hecho alguna autenticación multifactorial.	op.acc.6.r2.aws.iam.1	iam_user_mfa_enabled_console_access,iam_administrator_access_with_mfa,iam_root_mfa_enabled
		Se recomienda que la organización determine qué llamadas a la API deben también contar con seguridad reforzada a través de un doble factor de autenticación.		
[op.acc.6.r3]	Certificados	Utilizar el servicio AWS IAM Roles Anywhere para crear un ancla de confianza en la que se haga referencia al servicio AWS Certificate Manager Private CA o registrar sus propias autoridades de certificación (CA), permitiendo usar el certificado emitido por la misma para obtener credenciales temporales para el acceso al entorno AWS. Estos certificados deberán estar protegidos por un segundo factor.		
[op.acc.6.r4]	Certificados en dispositivo físico	Habilitar los dispositivos MFA físicos para todos los usuarios AWS IAM mediante la consola, línea de comandos o la propia API de AWS IAM. Del mismo modo, el uso de estos certificados deberá estar protegido por un segundo factor de tipo PIN o biométrico.	op.acc.6.r4.aws.iam.1	iam_user_mfa_enabled_console_access,iam_root_hardware_mfa_enabled

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
[op.acc.6.r5]	Registro	Para registrar los intentos de acceso, se deberá habilitar AWS CloudTrail en todas las regiones y activar el registro de acceso de usuarios.	op.acc.6.r5.aws.iam.1	cloudtrail_multi_region_enabled
		Habilitar la información de usuario sobre la fecha de último uso de sus claves de acceso.		
[op.acc.6.r7]	Suspensión por no utilización	Activar la inhabilitación de las credenciales de los usuarios AWS IAM que no hayan sido empleadas durante un periodo de tiempo (o bien, se deberá establecer la inhabilitación en el proveedor de identidades).	op.acc.6.r7.aws.iam.1	iam_disable_30_days_credentials
		El periodo de no utilización para la inhabilitación no sea superior a 90 días.	op.acc.6.r7.aws.iam.2	iam_disable_90_days_credentials
[op.acc.6.r8]	Doble factor para acceso desde o a través de zonas no controladas	Se deberá emplear como mecanismo de autenticación o bien una contraseña más otro factor de autenticación, o bien un certificado cualificado (con o sin soporte físico) protegido por un doble factor de autenticación.	op.acc.6.r8.aws.iam.1	iam_user_mfa_enabled_console_access
[op.acc.6.r9]	Acceso remoto (todos los niveles)	Deberá asegurarse que se está haciendo uso de HTTPS en todas las llamadas a API. Esto se puede lograr a través de una política IAM que rechace el tráfico que no sea HTTPS.		
		En caso de que las llamadas a las APIs no se produzcan de manera constante, se recomienda condicionar su realización a aquellas franjas horarias en las que sean necesarias.		
[op.exp.1]	Inventario de activos	En lo referente al inventariado de activos, se debe asegurar que AWS Config está habilitado en todas las regiones y utilizar la herramienta para obtener una vista de los recursos existentes en las cuentas de AWS.	op.exp.1.aws.cfg.1	config_recorder_all_regions_enabled
		Para la correcta identificación del responsable, asociar etiquetas para todos los activos	op.exp.1.aws.tag.1	tags_exist_in_required_resources
		Configurar una regla de AWS Config Rules que alerte sobre el despliegue de recursos sin las etiquetas correspondientes asociadas.	op.exp.1.aws.cfg.2	cloudwatch_log_metric_filter_resource_untagged
		En el ámbito del software desplegado en las instancias de Amazon EC2, habilitar AWS System Manager Inventory para todo el entorno de Amazon EC2 en caso de no utilizar herramientas de terceros.	op.exp.1.aws.sys.1	ec2_instance_managed_by_ssm, ssm_managed_compliant_patching
		Asignar metadatos personalizados a cada nodo administrado con información sobre el responsable del activo.	op.exp.1.aws.sys.2	tags_exist_in_required_resources

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		Se recomienda el uso de AWS Resource Explorer para la exploración de los recursos como instancias RDB, buckets Amazon S3 o tablas de Amazon DynamoDB.	op.exp.1.aws.re.1	resourceexplorer_enabled
[op.exp.1.r1]	Inventario de etiquetado	Hacer uso de AWS Config para la identificación de los equivalentes virtuales del equipamiento tales como puntos de enlace de la VPC, Gateway virtuales, interfaces de red o grupos de seguridad.		
[op.exp.1.r2]	Identificación periódica de activos	Disponer de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular servidores y los dispositivos de red y comunicaciones.		
[op.exp.1.r3]	Identificación de activos críticos	Disponer de herramientas que permitan categorizar los activos críticos por contexto y riesgos de la organización.		
[op.exp.1.r4]	Lista de componentes software	Mantener actualizada una relación de los componentes software de terceros utilizados en el despliegue del sistema. Listado equivalente a lo requerido en mp.sw.1.r5.		
[op.exp.3]	Gestión de la configuración de seguridad	El cumplimiento de los requisitos se puede apoyar en la utilización de los servicios AWS Config, AWS Config Rules y Conformance Packs para identificar líneas base de configuración para evaluar si los recursos de AWS se ajustan a las prácticas autorizadas por la organización.	op.exp.3.aws.cfg.1	config_recorder_all_regions_enabled
[op.exp.3.r2]	Responsabilidad de la configuración	Utilizar la asignación de políticas AWS IAM para lograr una correcta configuración relativa a la existencia de un número limitado y autorizado de administradores del sistema.		
[op.exp.3.r3]	Copias de seguridad	La entidad usuaria puede consultar el histórico de configuraciones de recursos en AWS Config.	op.exp.3.r3.aws.cfg.1	config_recorder_all_regions_enabled
[op.exp.3.r4]	Aplicación de la configuración	Se recomienda hacer uso de los servicios AWS System Manager Explorer y Patch Manager como solución para mantener actualizada la configuración de seguridad del S.O y de las aplicaciones a través de una aplicación o procedimiento manual que permita la instalación de versiones y actualizaciones de seguridad.	op.exp.3.r4.aws.smexp.1	ec2_instance_managed_by_ssm
			op.exp.3.r4.aws.patch.1	ssm_managed_compliant_patching
[op.exp.3.r5]	Control del estado de seguridad de la Configuración	Disponer de herramientas que permitan conocer de forma periódica el estado de seguridad de la configuración de los dispositivos de red y permitir su corrección.		

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
[op.exp.4]	Mantenimiento y actualizaciones de seguridad	Activar AWS Systems manager y gestionar la conformidad de los parches a través de su solución Explorer.	op.exp.4.aws.sys.1	ssm_managed_compliant_patching
		Utilizar AWS Systems Manager Patch Manager para planificar y gestionar la aplicación de parches minimizando los riesgos asociados a tener instancias con software desactualizado y expuesto a vulnerabilidades conocidas.	op.exp.4.aws.sys.2	ec2_instance_managed_by_ssm, ssm_managed_compliant_patching
		Una forma eficiente de garantizar la instalación de las versiones actualizadas y aprobadas del software de los sistemas es la utilización de Golden AMIs.		
[op.exp.4.r1]	Pruebas de preproducción	La entidad usuaria puede utilizar el entorno de la nube de AWS para la realización de sus pruebas en preproducción con carácter general.		
[op.exp.4.r2]	Prevención de fallos	Utilizar la solución AWS Systems Manager Automation para automatizar las tareas de corrección en servicios de AWS como EC2 y Amazon RDS.	op.exp.4.r2.aws.sys.1	ec2_instance_managed_by_ssm
[op.exp.4.r4]	Monitorización continua	Desplegar a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades detallando: indicadores críticos de seguridad, política de aplicación de parches y criterios de revisión regular y excepcional de amenazas del sistema.	op.exp.4.r4.aws.shub.1	securityhub_enabled
			op.exp.4.r4.aws.gd.1	guardduty_is_enabled
			op.exp.4.r4.aws.insp.1	ssm_inspector_findings_exist
[op.exp.5]	Gestión de cambios	La entidad usuaria puede hacer uso de la utilidad AWS Change Manager para mantener un registro actualizado de las plantillas y peticiones de cambio en las que se incluya información en detalle sobre estos.		
		Configurar AWS Systems Manager Change Manager para notificar de los cambios a los responsables.		
		Utilizar AWS Change Calendar para establecer una ventana de tiempo (fecha y hora) en la que realizar los cambios y las pruebas de preproducción en equipos equivalentes a los de producción sin riesgo a que estas afecten a la continuidad del servicio prestado.		
[op.exp.5.r1]	Prevención de fallos	Definir diferentes ambientes operacionales y procesos soportan la gestión de los cambios y la prevención de fallos.		

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		Adoptar un modelo de DevOps que utilice políticas de conformidad, controles minuciosos y técnicas de administración de la configuración.		
		Utilizar prácticas como son la integración y entrega continua para comprobar que los cambios realizados en el sistema sean funcionales y seguros.		
		Hacer uso del marco de trabajo AWS Well-Architected Framework para identificar las mejores prácticas en cuanto a despliegue de arquitectura segura en AWS.		
[op.exp.6]	Protección frente a código dañino	Activar la protección contra software malintencionado de Amazon GuardDuty en todas las regiones.	op.exp.6.aws.gd.1	guardduty_is_enabled
[op.exp.6]	Protección frente a código dañino	Automatizar las operaciones estándar a llevar a cabo para la respuesta en caso de incidente a través de AWS System Manager		
[op.exp.6.r3]	Lista blanca	Hacer uso de AWS System Manager Inventory para definir, a nivel de software, una lista blanca de aplicaciones.		
[op.exp.7]	Gestión de incidentes	Habilitar Amazon GuardDuty para la detección de incidentes de seguridad	op.exp.7.aws.gd.1	guardduty_is_enabled, guardduty_no_high_severity_findings
		Habilitar AWS Security Hub	op.exp.7.aws.sh.1	securityhub_enabled
		Habilitar los logs de acceso de Amazon CloudFront	op.exp.7.aws.cf.1	cloudfront_distributions_logging_enabled
		Deberá proveerse la información relacionada con contactos alternativos (de facturación, operaciones y seguridad), con correos que no dependan de la misma persona. Deberá comprobarse regularmente que estas cuentas funcionan correctamente y mantener listas de correo para asegurar la recepción de avisos por personal disponible en cada momento. Además, deberán establecerse preguntas de desafío de seguridad y respuestas para el caso de que sea necesario autenticarse como propietario de la cuenta para ponerse en contacto con el soporte de AWS.	op.exp.7.aws.iam.1	account_maintain_current_contact_details, account_security_contact_information_is_registered, account_security_questions_are_registered_in_the_aws_account
[op.exp.7.r4]	Prevención y Respuesta	Disponer de herramientas que automaticen los procesos de prevención y respuesta mediante la detección e identificación de anomalías, la	op.exp.7.r4.aws.gd.1	guardduty_no_high_severity_findings, securityhub_enabled



ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
	Automática	segmentación dinámica de red y aislamiento de dispositivos críticos. Se recomienda activar en AWS Security Hub AWS Foundational Security Best Practices v1.0.0 y CIS AWS Foundations Benchmark v1.2.0. En el caso de que su organización vaya a manejar información para almacenar, procesar o transmitir datos del titular de tarjetas de pago, le recomendamos activar PCI DSS V3.2.1		
[op.exp.8]	Registro de actividad	Habilitar la herramienta AWS CloudTrail en todas las regiones. Este servicio está habilitado por defecto cuando se crea una nueva cuenta, pero es posible deshabilitarlo.	op.exp.8.aws.ct.1	cloudtrail_multi_region_enabled
		Establecer un filtro de métricas desde Amazon CloudWatch para detectar cambios en las configuraciones de AWS CloudTrail	op.exp.8.aws.ct.2	cloudwatch_log_metric_filter_and_alarm_for_cloudtrail_configuration_changes_enabled
		Crear trails para los registros de auditoría y habilitar la validación de archivos en todos los trails, evitando así que estos se vean modificados o eliminados.	op.exp.8.aws.ct.3	cloudtrail_log_file_validation_enabled
		Habilitar la entrega continua de eventos de AWS CloudTrail a un bucket Amazon S3 dedicado con el fin de unificar los archivos de registro.	op.exp.8.aws.ct.4	cloudtrail_logs_s3_bucket_is_not_publicly_accessible, cloudtrail_s3_dataevents_write_enabled
		Se recomienda crear CloudTrail lakes.		
		Se recomienda habilitar notificaciones mediante Amazon SNS para los siguientes eventos: <ul style="list-style-type: none"> <li>Llamadas no permitidas a la API.</li> <li>Accesos no permitidos a la consola.</li> <li>Todos los intentos de acceso sin el correcto uso de MFA.</li> <li>Toda la actividad realizada sobre y por la cuenta root.</li> <li>Cualquier cambio en las políticas AWS IAM.</li> </ul> Además, puede configurar las notificaciones mediante otros servicios como por ejemplo Amazon CloudWatch	op.exp.8.aws.ct.5	cloudwatch_log_metric_filter_authorized_api_calls,cloudwatch_log_metric_filter_authentication_failures,cloudwatch_log_metric_filter_sign_in_without_mfa,cloudwatch_log_metric_filter_root_usage,cloudwatch_log_metric_filter_policy_changes

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
[op.exp.8.r1]	Revisión de los registros	Utilizar el servicio Amazon CloudWatch para centralizar y revisar los registros de todos los sistemas independientemente de su origen.		
		Utilizar la función AWS CloudTrail lakes para generar diferentes data lakes para la retención y consulta de registros de actividad. Al crearse se le activaran de forma predeterminada la opción Management Events (Eventos de administración), pudiendo activar también la opción de Data Events (Eventos de datos). No obstante, ha de tener en cuenta que esta segunda opción conlleva una gran cantidad de datos a almacenar y un incremento importante en los costos.		
		Configurar la herramienta AWS CloudTrail de manera que realice el registro de eventos de administración, eventos de datos y eventos anómalos (insights).	op.exp.8.r1.aws.ct.1	cloudwatch_log_metric_filter_and_alarm_for_cloudtrail_configuration_changes_enabled,cloudtrail_s3_dataevents_write_enabled,cloudtrail_s3_dataevents_read_enabled
		Configurar la herramienta AWS CloudTrail de manera que realice el registro de eventos anómalos (insights).	op.exp.8.r1.aws.ct.2	cloudtrail_insights_exist
		Registrar los eventos de lectura y escritura de datos.	op.exp.8.r1.aws.ct.3	cloudtrail_s3_dataevents_write_enabled,cloudtrail_s3_dataevents_read_enabled
[op.exp.8.r2]	Retención de registros	Para disponer de una referencia de tiempo para facilitar las funciones de registro de eventos y auditoría, AWS dispone del servicio Amazon Time Sync Service presente de forma nativa en todos los servicios que proporciona.		
[op.exp.8.r3]	Retención de registros	Ejecutar la acción PutRetentionPolicy de Amazon CloudWatch, permitiendo así establecer la retención del grupo de registros especificado y configurar el número de días durante los cuales se conservarán los eventos de registro en el grupo seleccionado de acuerdo con el documento de seguridad correspondiente. Paralelamente, se recomienda definir un periodo de retención para los datos almacenados en AWS CloudTrail Lakes.	op.exp.8.r3.aws.cw.1	cloudwatch_log_group_retention_policy_specific_days_enabled

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
[op.exp.8.r4]	Control de acceso	Asignar correctamente las políticas AWS IAM para el acceso y borrado de los registros y sus copias de seguridad haciendo uso del principio de mínimo privilegio.	op.exp.8.r4.aws.ct.1	iam_policy_allows_privilege_escalation,iam_policy_no_administrative_privileges,iam_no_custom_policy_permissive_role_assumption,iam_policy_attached_only_to_group_or_roles,iam_role_cross_service_confused_deputy_prevention
		Utilizar únicamente usuarios AWS IAM a los que se les haya sido asignada la política AWSCloudTrail_FullAccess para tareas de administración (no pudiendo eliminar en ningún momento el depósito de Amazon S3).		
		Utilizar una política de bucket para restringir el acceso de forma pública e imponer restricciones sobre cuáles de los usuarios pueden eliminar objetos de Amazon S3.	op.exp.8.r4.aws.ct.2	s3_bucket_public_access,cloudtrail_logs_s3_bucket_is_not_publicly_accessible,s3_bucket_policy_public_write_access
		Activar el acceso por MFA al registro de actividad almacenado en los buckets de Amazon S3 dedicados para AWS CloudTrail.	op.exp.8.r4.aws.ct.3	cloudtrail_bucket_requires_mfa_access
		Configurar los archivos de logs de AWS CloudTrail para aprovechar el cifrado del lado del servidor (SSE – Server Side Encryption) y las claves maestras creadas por el cliente (CMK de KMS).	op.exp.8.r4.aws.ct.4	cloudtrail_kms_encryption_enabled
[op.exp.9]	Registro de la gestión de incidentes	Habilitar AWS Incident Manager y AWS CloudTrail en todas las regiones con el fin de recopilar información para generar contenido prescriptivo para la creación de informes exigidos por la medida de seguridad.	op.exp.9.aws.img.1	ec2_instance_managed_by_ssm,ssm_incident_manager_enabled_with_plans
			op.exp.9.aws.ct.1	cloudtrail_multi_region_enabled
[op.exp.10]	Protección de claves criptográficas	Los usuarios o roles con privilegios para la creación de claves deben ser diferentes a los que van a utilizar las claves para operaciones de cifrado.	op.exp.10.aws.cmk.1	iam_roles_kms_no_full_access,iam_roles_kms_admins_not_users
		Priorizar claves gestionadas por los clientes (CMK) en los servicios de AWS dónde esté disponible.	op.exp.10.aws.cmk.2	kms_cmk_in_use
		Utilizar el principio de mínimos privilegios para las políticas asociadas a claves.		

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		Utilizar las políticas AWS IAM y las concesiones de claves para el acceso a las mismas.		
		Activar la rotación de las claves CMK.	op.exp.10.aws.cmk.3	kms_cmk_rotation_enabled
		Deshabilitar todas las CMK que no estén en uso.	op.exp.10.aws.cmk.4	cloudwatch_log_metric_filter_disable_or_scheduled_deletion_of_kms_cmk
		Eliminar las claves deshabilitadas que no estén en uso y no mantengan ningún objeto o recurso cifrado, completando el ciclo de vida de la clave.	op.exp.10.aws.cmk.5	cloudwatch_log_metric_filter_disable_or_scheduled_deletion_of_kms_cm
		Se recomienda utilizar tags y alias para una mejor gestión y administración de las claves.	op.exp.10.aws.tag.1	tags_exist_in_required_resources
[op.exp.10.r1]	Algoritmos autorizados	Para la elección del tipo de clave y tamaño se debe cumplir con los requisitos especificados en la guía de Seguridad de las TIC CCN-STIC-807 Criptología de Empleo en el Esquema Nacional de Seguridad.		
[op.ext.1]	Contratación y acuerdos a nivel de servicio	Tener en cuenta y establecer contractualmente los niveles de servicio ofrecidos por los proveedores.		
[op.ext.2]	Gestión diaria	Deberá existir algún usuario que tenga asignado el rol iam_support_role.	op.ext.2.aws.iam.1	iam_support_role_created
[op.cont.2]	Plan de continuidad	Deberá implementarse correctamente la distribución de servicios según regiones y zonas de disponibilidad para limitar al máximo los riesgos asociados a una única ubicación.		
[op.cont.2.r2]	Comprobación de integridad	Comprobar la integridad del S.O, firmware y los ficheros de configuración ante una caída o discontinuidad del sistema.		
[op.cont.3]	Pruebas periódicas	La organización puede hacer uso del servicio AWS Elastic Disaster Recovery, programando y ejecutando pruebas no disruptivas (simulacros que no afectan ni al servidor de origen ni a la replicación de datos en curso) que prueben el correcto funcionamiento de las recuperaciones del plan de continuidad.	op.cont.3.aws.drs.1	elasticdisasterrecovery_jobs_exist

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
[op.cont.4]	Medios alternativos	Utilizar el servicio AWS Application Migration Service (AWS MGN) para la migración de servidores.		
		Crear un usuario IAWS AM con la política administrada Server Migration Connector habilitada y la instalación del conector para la configuración de la replicación.		
		Utilizar el servicio AWS Database Migration Service para la migración de bases de datos.		
[op.cont.4.r1]	Automatización de la transición a medios alternativos	Hacer uso de AWS Backup como medio para transferir la última configuración (snapshot), pudiendo ser replicada en los otros medios alternativos. También puede utilizar Amazon Data Lifecycle Manager para automatizar la creación, retención y eliminación de instantáneas de EBS y las AMI respaldadas por EBS,		
[op.mon.1]	Detección de intrusión	Utilizar Amazon GuardDuty (o herramientas de terceros con funcionalidades equivalentes) para la detección de amenazas e intrusiones	op.mon.1.aws.gd.1	guardduty_is_enabled
		Activar el servicio de eventos AWS CloudTrail para todas las regiones.	op.mon.1.aws.ct.1	cloudtrail_multi_region_enabled
		Se recomienda activar el servicio Amazon VPC FlowLogs para analizar con herramientas adicionales el tráfico que soportan aquellos servicios críticos bajo el alcance del ENS.	op.mon.1.aws.flow.1	vpc_flow_logs_enabled
[op.mon.1.r3]	Acciones predeterminadas	Se recomienda habilitar los servicios Amazon GuardDuty y AWS System Manager.		
[op.mon.2]	Sistema de métricas	Utilizar AWS Security Hub para obtener una vista consolidada de los hallazgos de seguridad en los servicios de AWS habilitados.	op.mon.2.aws.sh.1	securityhub_enabled
[op.mon.2.r2]	Eficiencia del sistema de gestión de la seguridad	Administrar los presupuestos y los costes con AWS Budgets. También puede analizar tendencias y hacer previsiones con el uso de AWS Cost Explorer		

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
[op.mon.3]	Vigilancia	Se deberá utilizar el servicio Amazon CloudWatch Logs para acceder a los registros de los diferentes servicios de AWS de forma centralizada	op.mon.3.aws.cwl.1	cloudtrail_cloudwatch_logging_enabled
		Deberá asegurarse que todos los servicios que se utilicen en la arquitectura de la aplicación desplegada en AWS estén generando logs		
		Para el almacenamiento a largo plazo de los datos de registro, es recomendable que estos se exporten a Amazon S3, definiendo previamente el ciclo de vida de los logs e identificando qué se necesita almacenar en frío.		
[op.mon.3.r1]	Correlación de eventos	Activar Amazon GuardDuty y AWS Security Hub o bien disponer de un SIEM externo a AWS	op.mon.3.r1.aws.gd.1	guardduty_is_enabled
			op.mon.3.r1.aws.sh.1	securityhub_enabled
[op.mon.3.r2]	Análisis dinámico	Utilizar la herramienta Inspector para la detección de posibles vulnerabilidades de las instancias Amazon EC2, las funciones Lambda y las imágenes de contenedor	op.mon.3.r2.aws.insp.1	ssm_inspector_findings_exist
		Utilizar las herramientas AWS Config y AWS Security Hub en lo relativo a deficiencias de configuración.	op.mon.3.r2.aws.cfg.1	config_recorder_all_regions_enabled
			op.mon.3.r2.aws.sh.1	securityhub_enabled
		Utilizar el servicio AWS Trusted Advisor para la inspección del entorno de AWS, ya que ofrece recomendaciones para mejorar el rendimiento y la disponibilidad del sistema.	op.mon.3.r2.aws.adv.1	trustedadvisor_errors_and_warnings
[op.mon.3.r3]	Ciber-amenazas avanzadas	Activar Amazon GuardDuty	op.mon.3.r3.aws.gd.1	guardduty_is_enabled
[op.mon.3.r5]	Minería de datos	Se deberá tener en cuenta a la hora de prevenir, detectar y reaccionar frente a intentos de minería de datos:  - La característica S3 Protection de Amazon GuardDuty habilita la monitorización de operaciones en Amazon S3 tales como el listado o eliminación de buckets. - AWS Network Firewall se puede configurar, con las reglas adecuadas, para	op.mon.3.r5.aws.gd.1	guardduty_is_enabled

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		la protección contra el malware de minería de criptomonedas. - El hallazgo CryptoCurrency:EC2/BitcoinTool.BIDNS de GuardDuty indica que una instancia EC2 en el entorno AWS está consultando un nombre de dominio que se encuentra asociado a una actividad relacionada con las criptomonedas, como el minado.		
[op.mon.3.r6]	Inspecciones de seguridad	Utilizar AWS Config Rules y AWS Inspector	op.mon.3.r6.aws.cfg.1	config_recorder_all_regions_enabled
			op.mon.3.r6.aws.insp.1	ssm_inspector_findings_exist
		Ejecutar manualmente las pruebas de penetración tras los incidentes		
[mp.com.1]	Perímetro seguro	Asegurar que el Security Group restrinja todo el tráfico. Para ello, se deberán agregar las reglas del Security Group que se aplica por defecto cuando se crea una VPC.	mp.com.1.aws.sg.1	ec2_securitygroup_default_restrict_traffic, ec2_securitygroup_from_launch_wizard
		Evitar la existencia de Security Groups que dejen abierto todo el tráfico entrante.	mp.com.1.aws.sg.2	ec2_securitygroup_in_use_without_ingress_filtering
		Evitar tener un repositorio de Security Groups que no estén siendo usados.	mp.com.1.aws.sg.3	ec2_securitygroup_not_used
		Filtrar todo el tráfico entrante y saliente de la VPC a través de Firewalls de red.	mp.com.1.aws.nfw.1	networkfirewall_in_all_vpc
		Con Security Groups deberá evitarse una configuración de acceso que permita llegar desde internet a los servicios que no lo precisen como los siguientes: * SSH (TCP/22) * RDP (TCP/3389) * Oracle (TCP/1521 y TCP/2483) * MySQL (TCP/3306) * Postgres (TCP/5432) * Redis (TCP/6379) * MongoDB (TCP/27017 y TCP/27018)	mp.com.1.aws.sg.4	ec2_network_acls_allow_ingress_tcp_port_3389, ec2_network_acls_allow_ingress_tcp_port_22, ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_22, ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_3389, ec2_securitygroup_allow_ingress_from_internet_to_tcp_port_oracle_



ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		* Cassandra (TCP/7199, TCP/8888 y TCP/9160) * Memcached (TCP/11211)		1521_2483, ec2_securitygroup_allow_ingress_f rom_internet_to_tcp_port_mysql_ 3306, ec2_securitygroup_allow_ingress_f rom_internet_to_tcp_port_postgre s_5432, ec2_securitygroup_allow_ingress_f rom_internet_to_tcp_port_redis_6 379, ec2_securitygroup_allow_ingress_f rom_internet_to_port_mongodb_2 7017_27018, ec2_securitygroup_allow_ingress_f rom_internet_to_tcp_port_memca ched_11211, ec2_securitygroup_allow_ingress_f rom_internet_to_tcp_port_cassan dra_7199_9160_8888
[mp.com.2]	Protección de la confidencialidad	Garantizar que las conexiones entre la Amazon VPC y la red local (remota) se canalizan a través de VPN Site-to-Site o bien a través de Direct Connect.		
[mp.com.2.r1]	Algoritmos y parámetros autorizados	Los algoritmos y parámetros utilizados en la conexión VPN deberán atender a los requisitos especificados en la guía de Seguridad de las TIC CCN-STIC-807 Criptología de Empleo en el Esquema Nacional de Seguridad		
[mp.com.2.r2]	Dispositivos hardware	En caso de que se necesite el empleo de dispositivos hardware en el establecimiento de la VPN, se deberá tener en cuenta que AWS únicamente facilitará al usuario los archivos de configuración que deberán aplicarse en el dispositivo, que será en todo caso responsabilidad del cliente.		
[mp.com.2.r3]	Productos certificados	Se deberán utilizar para el establecimiento de la VPN un producto o servicio que cumpla con los requisitos de la medida de seguridad		

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		Componentes certificados [op.pl.5].		
[mp.com.2.r4]	Cifradores	Debe hacerse uso de diferentes cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.		
[mp.com.2.r5]	Cifrado de la información especialmente sensible	Se cifrará toda la información transmitida.		
[mp.com.3]	Protección de la integridad y de la autenticidad	Habilitar TLS en los balanceadores de carga ELB.	mp.com.3.aws.elb.1	elbv2_insecure_ssl_ciphers
		Evitar el uso de protocolos de cifrado inseguros en la conexión TLS entre clientes y balanceadores de carga. En particular, se deberá evitar el uso de TLS 1.1 y anteriores.	mp.com.3.aws.elb.2	elbv2_insecure_ssl_ciphers
		Asegurar que los Buckets de almacenamiento Amazon S3 apliquen cifrado para la transferencia de datos empleando TLS.	mp.com.3.aws.s3.1	s3_bucket_secure_transport_policy
		Asegurar que la distribución entre frontales Amazon CloudFront y sus orígenes únicamente emplee tráfico HTTPS.	mp.com.3.aws.cf.1	cloudfront_distributions_https_enabled
[mp.com.4]	Separación de flujos de información en la red	Los flujos de información de red se deben separar a través de la utilización de diferentes subnets.	mp.com.4.aws.vpc.1	vpc_subnets_separate_private_public
		Evitar el uso de subnets con la opción de asignación automática de IPs públicas (auto-assign Public IP), para lo cual deberá desmarcarse la siguiente casilla.	mp.com.4.aws.vpc.2	ec2_instance_internet_facing_with_instance_profile
[mp.com.4.r1]	Segmentación lógica básica	Implementar la segmentación a través de la utilización de diferentes VPCs.	mp.com.4.r1.aws.vpc.1	vpc_subnets_separate_private_public
[mp.com.4.r2]	Segmentación lógica avanzada	Se deberá implementar a través de la utilización de diferentes Amazon VPCs conectadas entre sí por VPC Peering o Transist GW		
[mp.com.4.r3]	Segmentación física	Implementar la segmentación a través de diferentes VPCs situadas en diferentes ubicaciones.	mp.com.4.r3.aws.vpc.1	vpcs_subnets_different_az
[mp.si.2]	Criptografía	Aplicar cifrado sobre el almacenamiento de las instancias en todos sus volúmenes de datos.	mp.si.2.aws.kms.1	ec2_ebs_volume_encryption

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		Aplicar cifrado sobre los distintos buckets de Amazon S3, de los cuales se debe asegurar que tengan activado el cifrado en reposo.	mp.si.2.aws.s3.1	s3_bucket_default_encryption
		Aplicar cifrado sobre las colas de mensajes de AWS (Amazon SQS).	mp.si.2.aws.sqs.1	sqs_queues_server_side_encryption_enabled
		Aplicar cifrado sobre las bases de datos Amazon RDS.	mp.si.2.aws.rds.1	rds_instance_storage_encrypted
		Aplicar cifrado sobre las bases de datos Amazon DynamoDB, que deben implementar cifrado seguro mediante el uso de claves de cliente (AWS KMS).	mp.si.2.aws.dydb.1	dynamodb_tables_kms_cmek_encryption_enabled
		Aplicar cifrado sobre todos los dominios del servicio Amazon Elasticsearch Service (ES). En caso de usar este servicio, deberá asegurarse la activación del cifrado en reposo.	mp.si.2.aws.es.1	opensearch_service_domains_encryption_at_rest_enabled
		Se recomienda dejar activada la opción de cifrado por defecto para nuevos volúmenes.	mp.si.2.aws.ebs.1	ec2_ebs_snapshots_encrypted
		Para realizar tareas de monitorización referentes a la detección de actividades relacionadas con el servicio de AWS KMS, recomienda integrar este junto con las funcionalidades de Amazon CloudWatch.	mp.si.2.aws.cw.1	cloudwatch_log_group_kms_encryption_enabled
[mp.si.2.r1]	Productos certificados	Utilizar productos certificados conforme a op.pl.5, si bien AWS KMS es un producto certificado cuyo uso satisface la exigencia de este control.		
[mp.si.2.r2]	Copias de seguridad	Se deberá asegurar el cifrado de las copias de seguridad (snapshots) de EBS.	mp.si.2.r2.aws.ebs.1	ec2_ebs_snapshots_encrypted
[mp.sw.2.r1]	Pruebas	Habilitar Amazon CodeBuild para el apoyo de la realización de pruebas en entornos aislados.	mp.sw.2.r1.aws.acb.1	codebuild_project_older_90_days, codebuild_project_user_controlled_buildspec
[mp.sw.2.r2]	Inspección de código fuente	Habilitar Amazon CodeGuru para la realización de pruebas de inspección de código fuente.	mp.sw.2.r2.aws.acg.1	devopsguru_notifications_enabled
		Habilitar Amazon CloudFormation Guard para el apoyo en las tareas de inspección de recursos no conformes implementados en el código fuente.		
[mp.info.6]	Copias de seguridad	Para los procedimientos de respaldo de cualquiera de los dos entornos (local y nube) y siempre y cuando se utilicen recursos compatibles en el entorno local, la entidad puede hacer uso de AWS Backup, que permite	mp.info.6.aws.bcku.1	backup_plans_exist backup_vaults_exist backup_reportplans_exist

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
		elaboración de planes de respaldo y la definición de reglas de frecuencia, ciclo de vida, lugar de almacenamiento y etiquetado de las copias de seguridad.		
		Los planes de respaldo se pueden integrar con AWS tags, acotando con base en las etiquetas de los recursos el alcance de cada proceso de copiado.	mp.info.6.aws.tag.1	tags_exist_in_required_resources
		La organización puede hacer uso de roles y políticas AWS IAM para la definición y asignación de permisos en cuanto a controles de acceso de las copias de respaldo.		
[mp.info.6.r1]	Pruebas de recuperación	Mediante el uso de AWS Backup se pueden llevar a cabo pruebas de restauración sin que se destruyan o sustituyan recursos originales ni se provoque afección sobre las cargas de trabajo.		
[mp.info.6.r2]	Protección de las copias de seguridad	La organización puede hacer uso de la nube de AWS como ubicación diferente para el almacenamiento de la copia de seguridad separada del resto o, incluso, utilizar los servicios de ubicación para separar una copia de seguridad en una ubicación diferente dentro de la propia nube.		
[mp.s.1]	Protección del correo electrónico	Se deberá hacer uso del cifrado de la información contenida en los correos electrónicos.		
		En SES, se debe hacer uso de la opción que permite a los usuarios enviar correo electrónico cifrado con S/MIME		
		Habilitar el registro de eventos de Amazon Workmail en Amazon CloudWatch para realizar el seguimiento de mensajes con spam.		
[mp.s.2]	Protección de servicios y aplicaciones web	Todas las aplicaciones web distribuidas por el servicio de AWS CloudFront deben estar integradas con el servicio de firewall de aplicaciones web AWS WAF.	mp.s.2.aws.waf.1	cloudfront_distributions_using_waf
		Los API gateways deben tener un ACL WAF asociado.	mp.s.2.aws.waf.2	apigateway_waf_acl_attached
		Todo el tráfico hacia los balanceadores de aplicación debe pasar antes a través de un firewall de aplicación web para quedar protegidos ante ataques en la capa de aplicación.	mp.s.2.aws.waf.3	elbv2_waf_acl_attached

ID Control ENS	Nombre control ENS	Descripción control	Identificador chequeo con prowler (si aplica)	Chequeo Prowler v3 automatizado
[mp.s.4]	Protección frente a la denegación de servicio	Activar la solución AWS Auto Scaling para dotar a los sistemas de la capacidad suficiente para atender la carga prevista con holgura y desplegar tecnologías para la prevención de ataques conocidos.	mp.s.4.aws.as.1	autoscaling_group_multiple_az
[mp.s.4.r1]	Detección y reacción	Activar AWS Shield Advanced con el fin de disponer de una herramienta de prevención, detección y mitigación de ataques de denegación de servicio.	mp.s.4.r1.aws.shieldadv.1	shield_advanced_protection_in_associated_elastic_ips, shield_advanced_protection_in_classic_load_balancers, shield_advanced_protection_in_cloudfront_distributions, shield_advanced_protection_in_global_accelerators, shield_advanced_protection_in_internet_facing_load_balancers, shield_advanced_protection_in_route53_hosted_zones
[mp.s.4.r2]	Ataques propios	Detectar y avisar el lanzamiento de ataques desde propias instalaciones perjudicando terceros.		



CCN-STIC 887A



## Guía de configuración segura para AWS

