PÚBLICO

Guias para a Utilização Segura de Ambientes Cloud

Guia para utilização Segura do ambiente cloud da AWS

Novembro 2025

“

No atual panorama digital em rápida evolução, a integração de serviços de cloud robustos é fundamental. Este guia constitui uma ferramenta útil para as organizações que pretendem tirar partido do potencial da computação em cloud sem prescindir dos mais elevados padrões de segurança no tratamento de informação classificada, na marca NACIONAL e no grau de RESERVADO. Por outro lado, procura apresentar de forma clara as responsabilidades partilhadas inerentes à adoção da cloud, distinguindo os papéis do fornecedor de serviços e das organizações clientes.

São abordados aspetos essenciais da segurança e proteção dos serviços cloud, como o inventário de ativos, a gestão de identidades e acessos, a segurança de redes, a proteção de dados, a segurança de aplicações e a resposta a incidentes, procurando garantir uma abordagem abrangente à segurança da informação classificada. O guia sublinha ainda a importância de as organizações adotarem configurações seguras e de seguirem as melhores práticas, para protegerem de forma eficaz os seus ativos digitais.

”

-- Gabinete Nacional de Segurança - Portugal

Aviso

O presente documento detalha um guia geral para a utilização segura de ambientes cloud públicos certificados pelo Gabinete Nacional de Segurança (GNS) em cenários avançados de utilização que operem com dados classificados com a marca **NACIONAL RESERVADO**.

O presente documento foi construído com o suporte técnico da AWS, que forneceu a orientação necessária para o melhor ajuste dos requisitos de segurança do GNS aos ambientes de cloud públicos. O trabalho realizado foi supervisionado pelo GNS, que forneceu o suporte necessário para o desenvolvimento deste guia.

Índice

Introdução e Conceitos Chave

adyta

Introdução

O objetivo deste documento é especificar os requisitos para a utilização de sistemas cloud, de acordo com o esquema de certificação do Gabinete Nacional de Segurança, GNS. Uma vez que se trata de uma orientação geral, o foco principal é enumerar os requisitos que uma organização deve seguir para garantir a proteção de informações classificadas em sistemas cloud.

Os requisitos apresentados neste documento fornecem reforço de segurança adicional nos seguintes itens:

- Inventário de ativos e gestão de recursos
- Controlo de identidade e acesso
- Segurança de rede
- Segurança de armazenamento
- Criptografia e proteção de dados
- Segurança de aplicações
- Recuperação e resiliência
- Monitorização de eventos de segurança
- Formação de colaboradores

Para cada item de segurança, são definidos requisitos para a configuração segura e utilização de cargas de trabalho envolvendo qualquer tipo de material, incluindo informações classificadas (NACIONAL, RESERVADO), conforme definido pelo GNS.

Antes de apresentar os requisitos de segurança, este documento começa com um conjunto de conceitos básicos, úteis para o leitor. Estes conceitos básicos incluem a distribuição de responsabilidades, que indicam as responsabilidades do fornecedor de serviços em cloud e as responsabilidades da organização cliente como consumidora de recursos em cloud. Além disso, os conceitos básicos também incluirão uma descrição dos tipos de serviços fornecidos pelo ambiente em cloud e algumas considerações ao migrar de servidores locais para a cloud.

Conceitos Chave

A *cloud* refere-se aos servidores acedidos através da Internet e ao software e bases de dados que funcionam nesses servidores [1]. A principal diferença entre a computação em cloud e a computação tradicional é que a gestão da infraestrutura física é totalmente feita pelo fornecedor da cloud.

A adoção de recursos em cloud como mecanismo de suporte parcial ou total para as necessidades de TI de uma organização traz muitas vantagens, como redução de custos, flexibilidade e ausência de recursos ou componentes adicionais.

Considerações

A adoção de serviços em cloud também traz algumas ressalvas, associadas à soberania e ao controlo sobre a localização dos dados, bem como problemas relacionados com a conformidade com as regulamentações de proteção de dados e segurança da informação. Ao utilizar um serviço em cloud, é preciso ter em mente o seguinte:

- **Modelo de responsabilidade partilhada**
  Os fornecedores de serviços cloud e os clientes partilham a responsabilidade de proteger o acesso aos dados e garantir a segurança do seu processamento. O modelo de responsabilidade partilhada especifica, para cada tipo de serviço, quais são as responsabilidades atribuídas ao fornecedor de serviços e quais são as responsabilidades atribuídas ao cliente. O modelo de responsabilidade partilhada é discutido em mais detalhes neste documento.
- **Controlo Reduzido**
  A transferência de dados para um fornecedor de serviços cloud implica um controlo reduzido sobre os dados, que agora estão armazenados numa infraestrutura fora do controlo da organização cliente. Os fornecedores de serviços em cloud certificados pela GNS demonstraram que dispõem de mecanismos e procedimentos para maximizar a soberania dos dados dos clientes.
- **Localização dos Dados**
  Devido à natureza global destes tipos de fornecedores, os dados podem ser armazenados em regiões que não estão sujeitas aos requisitos legais impostos pelo país de origem. Deve ser acordado com o fornecedor que qualquer processamento, incluindo armazenamento, deve ser realizado em zonas sujeitas

aos requisitos legais impostos pelo país de origem. Os fornecedores cloud certificados pela GNS demonstraram que possuem mecanismos para restringir as regiões que irão armazenar ou processar os dados dos clientes. O cliente é obrigado a selecionar uma região na qual deseja executar os recursos cloud provisionados pelo cliente.

- **Conformidade com regulamentos**

  O processamento de dados deve ser realizado de acordo com os regulamentos para garantir a segurança e a integridade dos dados. Os fornecedores cloud certificados pelo GNS comprovaram que os regulamentos europeus de proteção e privacidade de dados são cumpridos.

- **Isolamento de dados**

  Os fornecedores de serviços cloud prestam serviços a muitos clientes, sejam eles indivíduos ou organizações, cujos dados são armazenados na mesma infraestrutura física, o que levanta questões sobre o isolamento dos dados entre os clientes. Os fornecedores de serviços cloud certificados pela GNS demonstraram possuir mecanismos e procedimentos robustos para garantir o isolamento entre os dados dos clientes.

- **Portabilidade e gestão de dados**

  Os fornecedores de serviços cloud podem aplicar programação proprietária às informações transferidas para eles, o que pode tornar a migração futura para outro fornecedor de serviços cloud difícil ou mesmo impossível. Os fornecedores de serviços cloud certificados pela GNS demonstraram a capacidade de importar e exportar recursos entre outros fornecedores de serviços cloud.

- **Acesso Privilegiado**

  Os administradores/utilizadores root dos portais na cloud têm acesso ilimitado, a partir de qualquer lugar, desde às configurações até aos dados armazenados, aumentando o risco de um ataque a esses utilizadores, como por exemplo:

  - Sem uma segregação adequada de contas e gestão de controlo de acesso, há um risco maior de violações de dados, comprometimento de contas e uso indevido de privilégios de contas de administrador/root.
  - A segregação inadequada de contas e o controlo de acesso/gestão de identidades podem resultar num aumento da superfície de ataque para comprometer contas de administrador. Se um atacante for bem-sucedido neste tipo de ataques, ele poderá realizar o leak de todos os dados

disponíveis, realizar movimentos laterais e explorar vulnerabilidades em toda a organização.

Os fornecedores de cloud certificados pela GNS demonstraram mecanismos robustos de controlo de identidade e acesso que minimizam a exposição e o uso de contas root.

O objetivo deste guia é apresentar os requisitos que as organizações devem seguir para melhorar a segurança ao utilizar serviços cloud, introduzindo diretrizes de configuração de serviços seguros que correspondem aos controlos associados à matriz de certificação cloud da GNS.

Tipos de Serviços

Os serviços em cloud variam em termos de nível de controlo e funcionalidades oferecidas. Alguns serviços podem exigir mais personalização por parte do utilizador e, como efeito colateral, atribuir-lhe mais responsabilidades. Os serviços em cloud são frequentemente categorizados da seguinte forma:

- ***Infrastructure-as-a-Service (IaaS)***

  Fornecimento de serviços de infraestrutura, como máquinas virtuais, armazenamento e conectividade, sem qualquer processamento adicional de dados. A organização cliente é responsável pela configuração completa desses serviços, bem como pela manutenção da sua segurança.

  Exemplo de IaaS: Máquinas Virtuais

- ***Platform-as-a-Service (PaaS)***

  Fornecimento de serviços de plataforma, em que o fornecedor de serviços cloud disponibiliza acesso a um componente de software, como uma base de dados, em que a organização cliente tenha de configurar a infraestrutura, sistema operativo, redes ou armazenamento. A organização cliente é responsável pela configuração parcial do serviço de plataforma.

  Exemplo de PaaS: Serviços de base de dados fornecidos pelo fornecedor de serviços em cloud.

- ***Software-as-a-Service (SaaS)***

Fornecimento de serviços de software em que, normalmente, a organização cliente insere dados e obtém alguma resposta, sem ter de realizar configurações de infraestrutura ou instalação/configuração de software. A organização cliente é responsável por gerir o acesso aos serviços e aos dados gerados.

Exemplo de SaaS: Serviços como armazenamento de blobs ou ficheiros fornecidos pela cloud.

Distribuição de Responsabilidades

O uso de sistemas cloud envolve o envio, processamento ou manutenção de informações potencialmente confidenciais para sistemas fora das instalações da organização, onde elas ficarão, pelo menos momentaneamente, fora do controlo da organização que gera os dados. Para melhorar a segurança dos dados e informações transmitidos entre ambientes cloud e tradicionais, foram criados modelos de distribuição de responsabilidades nos quais o provedor cloud e seus clientes estabelecem que responsabilidades são atribuídas aos provedores cloud e aos clientes desses recursos.

O nível de responsabilidades atribuídos ao cliente, o mesmo depende do recurso fornecido, pelo que, no caso de recursos relacionados com a infraestrutura, os fornecedores de serviços cloud assumem um número menor de responsabilidades quando comparado com os recursos de software, em que o fornecedor de serviços em cloud assume mais responsabilidades.

Para facilitar a distribuição de responsabilidades, estas são atribuídas com base no tipo de recurso utilizado.

Para cada um dos tipos de recursos identificados, é estabelecido um modelo de partilha de responsabilidades. O modelo de responsabilidades pode variar ligeiramente entre os fornecedores de serviços em cloud, mas deve ser semelhante ao identificado na Tabela 1.

	On-Premises[1]	IaaS	PaaS	SaaS
Dados e informações				
Acesso e autenticação				
Segurança de aplicações				
Segurança de rede				
Sistema operativo				
Backups e réplicas				
Virtualização				
Redes físicas				
Armazenamento físico				
Servidores físicos				

- *Cloud* Provider - Organização Cliente

Tabela 1 – Distribuição de Responsabilidades

Em ambientes locais, o controlo dos sistemas de informação e dos dados transferidos é total, sendo a organização responsável pela manutenção dos sistemas físicos, software de virtualização e atualização/configuração segura dos sistemas operativos, mecanismos de autenticação e firewalls, bem como pela manutenção da disponibilidade do acesso aos dados (por exemplo, cópias de segurança, réplicas, etc.).

Nos serviços IaaS, os sistemas cloud são responsáveis pela manutenção e configuração segura do hardware que sustenta os recursos fornecidos, tais como servidores, redes físicas, hardware de armazenamento e software de virtualização. Os sistemas cloud também devem fornecer sistemas de backup e replicação em várias zonas, que o cliente é responsável por ativar. A manutenção do sistema operativo, das aplicações instaladas, das regras de firewall e das políticas de acesso aos dados são da responsabilidade da organização que utiliza os recursos em cloud.

[1] ***On-Premises*** – Sistemas de informação que residem na infraestrutura interna da organização

Nos serviços PaaS, os sistemas cloud são responsáveis por preparar a plataforma que a organização deseja utilizar, desde a configuração da aplicação, sistema operativo e regras de segurança iniciais, mas a organização pode alterar essas configurações, pelo que é da responsabilidade da organização manter a segurança das configurações. É também da responsabilidade do cliente configurar corretamente as políticas de acesso.

Nos serviços SaaS, os sistemas em cloud assumem a maior parte da responsabilidade, e cabe apenas ao cliente configurar as políticas de acesso adequadas.

A organização cliente é sempre responsável pelos dados armazenados pelos sistemas em cloud, pois pode sempre escolher quais dados enviar e como processá-los. Qualquer exposição de dados resultante de uma configuração incorreta dos serviços em cloud ou de uma compreensão incorreta do modelo de distribuição de responsabilidades é da responsabilidade do cliente.

Requisitos de Segurança

adyta

Requisitos de Segurança

Esta secção contém uma lista de requisitos que a organização deverá seguir, subdividido de acordo com cada controlo de segurança. Para cada controlo, é apresentado um código (exemplo: OP.INV.1), que permite referenciar controlos individuais ao longo do documento.

[OP.INV] Inventário de Ativos

À medida que as organizações crescem, os requisitos da infraestrutura aumentam, e com isso a complexidade de gestão. Uma infraestrutura altamente complexa sobrecarrega a gestão dos recursos, o que pode aumentar custos e em alguns casos despoletar à fuga de informações. A inventariação dos ativos permite que uma organização acompanhe os recursos em uso na *cloud*, facilitando a gestão da mesma.

Na AWS, a inventariação de ativos pode ser efetuada a partir da utilização dos seguintes serviços:

- **AWS Config:** AWS Config é um serviço de histórico e configuração de recursos que permite a avaliação e auditoria das configurações dos recursos. O AWS Config rastreia os recursos configurados na conta em questão.
  Mais Informações: AWS - Config

Além deste serviço, os inventários dos ativos também podem ser realizados com o seguinte serviço:

- **AWS Resource Explorer:** AWS Resource Explorer permite pesquisas rápidas dos recursos configurados na conta e em todas as regiões de AWS.
  Mais Informações: AWS - Resource Explorer

[OP.INV.1] Inventários de recursos *cloud*

De um modo regular, deverá ser elaborada uma lista dos recursos *cloud* que se encontram atualmente em operação. Para cada recurso, deverá ser indicada uma descrição do seu objetivo e se contém/faz uso de informação classificada.

O principal objetivo deste requisito é permitir sempre uma visão geral e atualizada dos recursos provisionados na AWS, de forma a ser possível indicar a sua criticidade e possível exposição. Os recursos que lidam com informações classificadas “Nacional Reservado” devem ser sempre monitorizados e atualizados devidamente.

De modo a cumprir com este requisito, a organização deve:

- Regularmente efetuar e atualizar listas de recursos atualmente provisionados na(s) conta(s) de AWS. Esta listagem pode ser realizada através do AWS Config a partir do seguinte guia: AWS - Looking Up Discovered Resources.

[OP.INV.2] Gestão de Recursos

A existência de uma lista de recursos permite que as organizações compreendam quais os recursos que estão a ser utilizados, permitindo manter melhor controlo dos recursos existentes e, a limitação do número de recursos que acedem ou processam dados classificados.

O principal objetivo deste controlo é a redução de exposição de dados classificados em recursos que não são necessários ou que não apresentam justificação de negócio valida para as necessidades atuais da organização.

De modo a cumprir com este requisito, a organização deve:

- Enumerar os objetivos relacionados com a necessidade de armazenar ou processar informações classificadas e associar esses objetivos aos recursos provisionados.
- Se não existir necessidade de manter um recurso, o mesmo deverá ser removido.
- Remover recursos não utilizados da(s) conta(s) AWS que lidam com informações classificadas.

[OP.IAM] Controlo de identidade e acessos

O controlo adequado de identidade e de acessos é um dos pilares mais importantes numa organização. Os fornecedores *cloud*, tal como a AWS, fazem a integração dos seus serviços com ferramentas de gestão de identidade e de acesso, permitindo que as organizações criem controlos de acessos resilientes e protejam o acesso a recursos e dados.

Na AWS, o controlo de identidade e de acessos pode ser efetuado a partir dos seguintes serviços:

- **AWS IAM:** Serviço da AWS que lida com a gestão de identidade e de acessos para a conta de AWS. A partir deste serviço é possível criar e gerir utilizadores, criar e

atribuir funções e criar políticas. O AWS IAM também suporta a ligação a fornecedores de identidade externas.
Mais Informações: AWS - IAM

- **AWS IAM policy simulator:** Ferramenta da AWS que permite testar e resolver problemas de políticas e permissões do IAM. Útil para testar acessos antes dos utilizadores.
Mais Informações: AWS - Policy Simulator

[OP.IAM.1] Segurança do Utilizador Root

Na AWS, um *root user* são contas que apresentam o nível mais elevado de permissões na AWS. Após a criação da conta, o *root user* apenas deverá ser utilizado para situações que necessitem explicitamente do seu uso.

É recomendado que seja criado um agrupamento de utilizadores e que os mesmos sejam alocados responsabilidade distintas, tal como, a gestão administrativa, de faturação, identidade, entre outros.

O principal objetivo deste controlo é a implementação de uma camada de segurança robusta para o *root user* e promover a minimização da utilização da mesma.

De modo a cumprir com este requisito, a organização deve:

- Configurar uma palavra-passe para a conta root com, pelo menos, os requisitos de segurança definidos em [OP.IAM.3.1] (AWS - Welcome First Time Users).
- Definir autenticação MFA para o utilizador root da AWS, conforme definido em [OP.IAM.3.2].
- Impedir o uso da conta root, optando por usar utilizadores com funções definidas e permissões limitadas.

[OP.IAM.2] Gestão Segura de Utilizadores

Como as contas root possuem o nível mais alto de permissões disponíveis na AWS, o seu acesso deve ser reduzido a situações de necessidade ou emergência, seguindo a abordagem de privilégios mínimos. A gestão de utilizadores na AWS pode ser feita utilizando o *AWS Identity Center* ou provedores de identidade externos, como o *Active Directory*.

O principal objetivo deste requisito é reforçar a segregação de privilégios, de modo a limitar o impacto de um comprometimento da conta.

Para cumprir com este requisito, a organização deverá:

- Criar funções distintas para cada função de trabalho distinta, minimizando o uso da conta root. Para cada função, deve ser definido um conjunto mínimo de permissões, utilizando o princípio do privilégio mínimo. A gestão de utilizadores pode ser feita a partir do AWS Identity Center (AWS - Permission Sets, AWS - Single Sign On).
- Opcionalmente, o simulador de políticas da AWS pode ser usado para testar se as configurações realizadas correspondem aos requisitos de privilégio mínimo (AWS - IAM Testing Policies).

[OP.IAM.3] Autenticação de Utilizador Segura

Associados a controlos de acesso adequados, os procedimentos seguros de autenticação de utilizadores garantem que o utilizador correto está a aceder ao recurso na cloud. A autenticação segura deve ser realizada utilizando canais de comunicação seguros e fazendo uso de vários autenticadores seguros. Este controlo é subdividido em subcontrolos que regulam a segurança das palavras-passe e a utilização múltipla de autenticadores seguros. Para cumprir este controlo, uma organização deve estar em conformidade com [OP.IAM.3.1] e [OP.IAM.3.2].

[OP.IAM.3.1] Passwords Seguras

As palavras-passe são o principal método de proteção do acesso à conta. As palavras-passe devem ser robustas contra ataques de força bruta e distintas de outras palavras-passe para evitar ataques de preenchimento de credenciais.

O objetivo deste requisito é definir requisitos para a força da palavra-passe, tornando as credenciais mais robustas.

Para cumprir com este requisito, uma organização deve configurar uma política de palavras-passe que imponha os seguintes princípios:

- Comprimento superior a 12 caracteres (exemplo para utilizadores IAM: AWS - Password Policies)

- Contém letras minúsculas e maiúsculas.
- Contém números.
- Contém símbolos.
- A palavra-passe deve ser diferente de outras palavras-passe.
- A palavra-passe não deve conter informações publicamente conhecidas (por exemplo: nome da organização).
- As palavras-passe não devem conter informações pessoais (por exemplo: nomes de família, cães, locais e datas)

[OP.IAM.3.2] Multifactor Authentication (MFA)

A autenticação por palavra-passe pode ser comprometida por meio de força bruta ou engenharia social, concedendo ao atacante acesso ao ambiente cloud. A autenticação MFA requer o uso de outros autenticadores juntamente com a palavra-passe para uma autenticação bem-sucedida. Os *tokens* MFA geralmente têm vida útil curta, reduzindo a possibilidade de ataques de captura e repetição.

O principal objetivo deste requisito é impor o uso da autenticação MFA no acesso do utilizador à infraestrutura cloud da AWS.

Para cumprir com este requisito, uma organização deve:

- Para contas de utilizador em IAM configurar MFA, utilizando aplicações autenticadoras e/ou chaves de segurança como MFA (AWS - MFA ID Credentials)
- Para contas raiz da AWS, configurar a MFA, utilizando aplicações autenticadoras e/ou chaves de segurança como MFA (AWS - Root Account MFA).
- Para utilizadores do IAM Identity Center, configurar avisos de MFA (AWS - Getting Started With MFA), alterando o seguinte:
    - Solicitar MFA em cada início de sessão
    - Permitir aplicações autenticadoras e chaves de segurança como MFA
    - Solicitar ao utilizador que registe um dispositivo MFA se a conta não tiver MFA configurada.
- Para utilizadores de fornecedores de identidade externos, configurar a autenticação multifator utilizando aplicações autenticadoras e/ou chaves de segurança.

[OP.IAM.4] Autenticação Segura de API

As APIs da AWS exigem autenticação a partir de *tokens* de API. Um *token* de API é um par de identificador e segredo usado para autenticar chamadas de API.

Os tokens da API podem ser chamados utilizando chaves de acesso ou credenciais de segurança temporárias. As chaves de acesso são credenciais de longa duração que requerem provisionamento e manutenção manual, enquanto que as credenciais de segurança temporárias permitem a emissão automática de chaves de acesso temporárias que são limitadas à função à qual foi vinculado a solicitação. As credenciais de segurança temporárias são a forma recomendada de autenticar chamadas da API.

O principal objetivo destes requisitos é melhorar a segurança da autenticação da API.

Para cumprir com este requisito, uma organização deve:

- Sempre que possível, utilizar funções IAM e credenciais de segurança temporária (AWS - IAM Temporary Credentials)
- Se forem necessárias chaves de acesso, deve ser criado um utilizador IAM com o número mínimo de permissões/funções atribuídas de modo a reduzir a exposição das funcionalidades através da chave de acesso.
- Se forem necessárias chaves de acesso, as mesmas devem ser armazenadas como variáveis de ambiente e não devem estar *hard-coded* no código usado para a chamada da API.
- A emissão da chave de acesso deve ser limitada à necessidade de uso.
- As chaves de acesso devem ser renovadas a cada 6 meses.
- As chaves de acesso e o utilizador IAM associado, devem ser eliminados assim que o objetivo de utilização já não seja válido.

[OP.NET] Segurança de Redes

Nos sistemas em cloud, a segurança de rede diz respeito às medidas destinadas a proteger os dados em trânsito e a infraestrutura associada. De acordo com o modelo de responsabilidade partilhada referido acima, cabe à organização proteger o fluxo de informação, garantir a resiliência das operações e minimizar a superfície de exposição dos recursos na nuvem que forem disponibilizados.

Na AWS, segurança de rede pode ser aplicado utilizando uma combinação dos seguintes serviços:

- **AWS Security Groups**: Atua como uma firewall ao nível da instância, controlando o tráfego permitido com base em uma ou mais *stacks* (uma instância ou conjunto de instâncias).
  Mais Informações: AWS - Security Groups
- **AWS Network Access Control Lists**: Atua como uma firewall ao nível da rede, que permite filtrar tráfego ao nível da rede.
  Mais Informações: *AWS - VPC Network ACLs*
- **AWS Network Firewall**: Serviço *stateful* e gerenciável que permite definir e aplicar políticas de rede ao tráfego de perímetro.
  Mais Informações: AWS - Network Firewall

Além destes serviços, a segurança da rede pode ser aprimorada e/ou simplificada utilizando os seguintes serviços:

- **AWS Control Tower**: Serviço gerenciável utilizado para provisionar um *AWS Landing Zone*. Control Tower pode ser utilizado para configurar um ponto de partida multi-conta compatível e seguro no contexto da AWS. AWS Landing Zone Accelerator pode ser utilizado em vez de Control Tower para implementações e arquiteturas mais avançadas.
  Mais Informações: AWS - Control Tower
- **AWS VPN**: O serviço VPN permite estabelecer ligações ponto-a-ponto seguras e encriptadas, quer entre um cliente da organização e recursos na AWS ou entre diferentes recursos na AWS (através do *AWS Client VPN* ou *AWS Site-to-Site VPN*).
  Mais Informações: AWS - VPN
- **AWS Web Application Firewall**: O *Web Application Firewall* é um serviço que protege aplicações web contra ataques e explorações comuns. Este serviço necessita de políticas de segurança que antecipam e mitigam vulnerabilidades — estas políticas podem ser definidas pela própria organização ou implementadas diretamente da AWS.
  Mais Informações: *AWS - WAF*
- **AWS Certificate Manager & AWS Private CA**: O *Certificate Manager* é um serviço utilizado para disponibilizar certificados SSL/TLS para uso com serviços e recursos

AWS. Pode ser usado em conjunto com o *AWS Private Certificate Authority (CA)*, permitindo que as organizações criem e gerem a sua própria autoridade certificadora privada, em vez de dependerem da autoridade padrão da AWS.
Mais Informações: AWS - Certificate Manager, AWS - Private CA

- **AWS Firewall Manager**: O *Firewall Manager* é um serviço gerenciável que permite configurar e administrar, de forma centralizada, diversos serviços e capacidades de segurança de rede (como *AWS Network Firewall*, *Security Groups*, *firewalls* de terceiros, instâncias do *Web Application Firewall*, entre outros).
Mais Informações: AWS - Firewall Manager

Abaixo são apresentados os requisitos de segurança de rede relativos aos serviços da AWS.

[OP.NET.1] Configuração Segura de Firewall

Configurar uma firewall de forma segura implica seguir o princípio do menor privilégio ao definir as regras de tráfego. As regras de rede devem ser construídas com base neste princípio, garantindo que cada recurso recebe apenas o nível mínimo de acesso necessário.

O principal objetivo deste requisito é estabelecer um controlo de acesso seguro aos recursos disponibilizados pela organização, permitindo a sua utilização de forma protegida e reduzindo o risco de atividades maliciosas. Tal como referido anteriormente, uma configuração segura deve respeitar o princípio do menor privilégio (por exemplo: definição de Security Groups, Access Control Lists, Network Policies, etc.) e adotar um modelo de segurança em múltiplas camadas.

Para garantir uma configuração de firewall segura, a organização deve, no mínimo:

- Aplicar *Security Groups* (regras de permissão) ao nível das instâncias (AWS - VPC Security Groups);
    - Definir regras restritivas de entrada (*inbound*) e saída (*outbound*) de acordo com o recurso. O acesso por cada porta deve ser limitado às origens e destinos estritamente necessários.
    - Evitar permitir tráfego de entrada com intervalos de IP excessivamente permissivos, como 0.0.0.0/0 (IPv4) ou ::/ (IPv6).
    - Criar *Security Groups* claros e específicos por recurso, de modo a reduzir erros de configuração.
- Aplicar Network Access Control Lists (regras de permissão e negação) ao nível das sub-redes (AWS - VPC Network ACLs).

- Definir listas de controlo de acesso para gerir o tráfego de entrada e saída ao nível da rede.

Para implementações mais avançadas (com custos variáveis), uma organização poderá:

- Ativar o *AWS Network Firewall* (https://docs.aws.amazon.com/network-firewall/latest/developerguide/what-is-aws-network-firewall.html)
  - Definir políticas de rede com base em regras *stateless* e *stateful*.
  - Evitar regras demasiado permissivas.
  - Garantir que existem ações adequadas definidas para todos os casos de exceção previstos nas políticas (enforcement *stateless* vs *stateful*).
- Para ativos web expostos publicamente, ativar o Web Application Firewall (AWS - WAF).
  - Consoante o tipo de recurso usado para expor os serviços web, poderão ser necessários recursos adicionais para integrar a WAF. Por exemplo, se forem utilizadas instâncias EC2 para disponibilizar serviços web, deverá ser configurado um *AWS Application Load Balancer* (AWS - ELB Create Application, AWS - WAF Chapter).
  - Definir políticas com base no comportamento dos ativos subjacentes para prevenir atividades maliciosas (ex.: tentativas de acesso não autorizado em páginas de login, exploração de vulnerabilidades, etc.).
  - Definir regras de filtragem de tráfego web, quando aplicável e necessário.

Como boas práticas, deverá também ser considerado o seguinte:

- Aplicar, por predefinição, ações de negação de tráfego de rede, seguindo o princípio "negar tudo, permitir apenas o necessário".
- Evitar sempre regras excessivamente permissivas.

[OP.NET.2] Encriptação em Trânsito

Aplicar encriptação de dados em trânsito implica garantir os requisitos e características necessários à sua disponibilidade, bem como avaliar os protocolos utilizados para a transferência desses dados. Com a encriptação em trânsito (e transferências seguras de dados), a organização assegura a confidencialidade, a integridade e a disponibilidade das informações trocadas entre os seus recursos e serviços.

O principal objetivo deste requisito é garantir que não são utilizados meios inseguros para comunicar com os recursos e serviços da organização. Para cumprir este requisito, a organização deverá:

- Impor o uso de protocolos encriptados, de acordo com a estratégia de implementação adotada (https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/encrypt-data-in-transit.html)
    - Configurar ligações site-to-site, ativando uma VPC e uma VPN da AWS, bem como túneis site-to-site e/ou baseados em cliente, sempre que aplicável (https://aws.amazon.com/vpn/)
    - Utilizar endpoints AWS API com SSL/TLS, garantindo comunicações encriptadas sempre que possível;
    - Ativar o AWS Certificate Manager, para emitir certificados e estabelecer transporte encriptado entre serviços ou ativos organizacionais (AWS - Certificate Manager)
    - Usar o AWS Private Certificate Authority em conjunto com o Certificate Manager, de modo a emitir certificados assinados pela raiz de confiança da organização. Esta Autoridade de Certificação Privada deve ser configurada como subordinada à raiz de confiança da organização (por exemplo, como uma sub-CA da CA principal da organização);
    - Para ativos públicos, como aplicações web, garantir a utilização de protocolos seguros (por exemplo, HTTPS). A aplicação obrigatória de HTTPS pode ser configurada através do AWS CloudFront (AWS - CloudFront Usage HTTPS);

[OP.STO] Armazenamento

Armazenamento, no sentido lato, é o processo de guardar, manter e gerir dados de forma persistente e que permita a sua recuperação posterior. Este processo envolve definir como os dados devem estar disponíveis (disponibilidade), onde devem residir, ser processados e/ou permanecer acessíveis (localização), e ainda quando e a quem esses dados devem ser enviados.

Na AWS, o armazenamento pode ser realizado através de uma combinação dos seguintes serviços:

- **AWS S3**: Serviço de armazenamento de objetos que disponibiliza várias classes de armazenamento económicas e funcionalidades de gestão. Permite guardar e proteger qualquer volume de dados.

  Mais informações: AWS - S3

- **AWS Elastic Block Store (EBS)**: Serviço de armazenamento em blocos concebido para a AWS Elastic Compute Cloud (EC2), baseado em tipos de volumes pré-definidos.

  Mais informações: AWS - EBS

- **AWS Elastic File System (EFS)**: Serviço de armazenamento que fornece um sistema de ficheiros que pode ser montado em instâncias EC2, noutros serviços da AWS e/ou em servidores locais.

  Mais informações: *AWS - EFS*

[OP.STO.1] Replicação e Redundância

Replicação consiste em manter várias cópias ativas dos dados, enquanto a redundância diz respeito à existência e manutenção de cópias de segurança que garantam a disponibilidade contínua dos dados ao longo do ciclo de vida da organização. Assim, a estratégia adotada deve estar alinhada com os indicadores de **R**ecuperação de **P**onto (**RPO**) e **R**ecuperação de **T**empo (**RTO**) definidos pela organização, independentemente de onde ou como esses critérios são aplicados (dentro ou fora do contexto AWS). A aplicação destes indicadores permite conceber um plano de recuperação de dados adequado, refletido no serviço — ou conjunto de serviços — utilizado, o que, por sua vez, terá impacto direto no custo global.

O principal objetivo deste critério é assegurar a conformidade com as capacidades de replicação e redundância enquanto propriedades do sistema (sendo que a redundância pode ser alcançada através da replicação). Cabe ao leitor avaliar qual o serviço mais adequado para cumprir este critério. Ainda assim, no mínimo, para garantir a

conformidade, deve existir pelo menos uma cópia completa dos dados num ponto de armazenamento distinto localizado na União Europeia, seja em Zonas de Disponibilidade da AWS, em Regiões diferentes da AWS, ou na mesma Região AWS. Caso os indicadores **RPO** e **RTO** tenham sido previamente calculados e avaliados, estes devem ser refletidos na estratégia de implementação do armazenamento definida pela organização.

Para cumprir com os requisitos de replicação e redundância de armazenamento, a organização deve:

- Para cada recurso de armazenamento que contenha dados críticos da organização provisionado na AWS, aplicar replicação multi-regional, garantindo pelo menos uma cópia completa dos dados originais. Na AWS, isto pode ser feito, por exemplo, através do serviço S3 Live Replication (AWS - S3 Replication).
- As cópias multi-regionais dos dados devem estar sincronizadas de modo a permitir failover caso uma das regiões falhe.
- Tanto os dados originais como as suas cópias devem ser versionados. No caso do S3, o versionamento pode ser configurada da seguinte forma: AWS - S3 Versioning.

Opcionalmente, se a organização necessitar de tempos de transferência previsíveis, pode utilizar, por exemplo, o serviço S3 Replication Time Control, que é suportado por um Acordo de Nível de Serviço (Service Level Agreement (*SLA*)) entre a organização e a AWS.

[OP.CRI] Criptografia e Proteção de Dados

Processo de proteção e transmissão de informação de forma a que apenas as partes autorizadas a possam compreender. Este processo envolve o uso de algoritmos de encriptação criptograficamente robustos, a gestão de chaves criptográficas e a garantia da confidencialidade, integridade e autenticidade dos dados, tanto em trânsito como em repouso.

Na AWS, os procedimentos de proteção criptográfica de dados podem ser realizados através da combinação dos seguintes serviços:

- **AWS Key Management Service (KMS):** Serviço gerido utilizado para criar e gerir chaves criptográficas em aplicações organizacionais e serviços AWS. *Mais informações*: AWS - KMS

AWS CloudHSM: Serviço que permite o controlo de módulos de segurança de hardware (HSMs) dedicados, utilizados para gerar, utilizar e armazenar chaves de encriptação.
Mais informações: AWS - Cloud HSMs

Adicionalmente, consoante o esquema de proteção de dados pretendido, estes procedimentos podem ser reforçados (com custos variáveis) através de serviços como:

- **AWS Nitro:** Funcionalidade do AWS EC2 que permite criar ambientes de execução isolados (enclaves) a partir de instâncias EC2.
  Mais informações: AWS - Nitro Enclaves

- **AWS S3 Storage Lens:** Ferramenta de análise do AWS S3 que permite obter uma visão global da utilização e atividade do armazenamento de objetos, bem como da percentagem de dados encriptados.
  Mais informações: AWS - S3 Using Encryption Guide

[OP.CRI.1] Key Management

A gestão de chaves diz respeito à capacidade de criar e administrar chaves criptográficas utilizadas para encriptar dados (em repouso e/ou em trânsito). O AWS KMS funciona como um fornecedor de serviços criptográficos, onde as operações de criptografia são executadas através de uma rede distribuída de módulos de segurança de hardware (HSM do AWS KMS).

De forma conceptual, existem dois modelos principais de encriptação que podem ser aplicados: encriptação do lado do servidor e encriptação do lado do cliente.

O principal objetivo deste requisito é garantir a aplicação de estratégias de encriptação adequadas, de forma a assegurar que os dados — tanto em trânsito como em repouso — estão protegidos ao longo de todo o seu ciclo de vida.

Os dados em trânsito podem ser protegidos através de SSL/TLS (Secure Socket Layer / Transport Layer Security) ou por encriptação no lado do cliente, enquanto os dados em repouso podem ser protegidos por encriptação no lado do servidor ou no lado do cliente.

Para cumprir este requisito, a organização deve garantir que os dados estão protegidos tanto durante a sua transferência como quando armazenados, independentemente do ponto de origem ou destino. Esta proteção pode ser assegurada através de encriptação do lado do servidor ou do lado do cliente. Assim, é importante que as organizações tenham em atenção os seguintes aspetos:

- Encriptação do lado do servidor: garante a confidencialidade da informação ao realizar a encriptação com chaves armazenadas no servidor. A AWS permite que os seus clientes encriptem dados em trânsito ou em repouso utilizando as suas próprias soluções. As chaves utilizadas são geridas no AWS KMS, onde o cliente pode controlá-las facilmente. Por predefinição, para encriptação simétrica, o AWS KMS utiliza chaves AES-GCM de 256 bits, e para encriptação assimétrica, chaves RSA com tamanho igual ou superior a 2048 bits.
- Encriptação do lado do cliente: pode ser utilizada para proteger dados tanto em trânsito como em repouso, mas neste caso a responsabilidade pela gestão do processo de encriptação, das chaves e das ferramentas associadas recai sobre a organização.

Quando é utilizada a encriptação do lado do servidor, devem também ser consideradas as seguintes recomendações:

- A criação de uma chave KMS requer permissões específicas, configuradas através de uma política IAM no AWS IAM (AWS - KMS Key Permissions).
- Ao criar uma chave KMS, não incluir informações pessoais identificáveis no alias, descrição ou etiquetas (*tags*), uma vez que estes dados podem aparecer em texto simples nos registos de auditoria e outros relatórios ().
- Apenas são permitidas Customer Managed Keys ao utilizar o AWS KMS (AWS - KMS Customer Managed Keys)
- Se forem utilizadas chaves assimétricas RSA, deve verificar-se que o tamanho dos dados a encriptar não excede o comprimento máximo de texto simples (*plaintext*) permitido em bytes. Além disso, o algoritmo SHA-256 deve ser preferido em detrimento do SHA-1 (AWS - KMS Key Specs RSA).
- Deve ser definida uma política de chaves KMS que estabeleça e limite quem pode usar a chave e de que forma (). O acesso às chaves deve seguir o princípio de mínimo privilégio.

- Por fim, é necessário configurar os recursos AWS para utilizarem as chaves definidas no KMS, sendo que essa configuração varia consoante o serviço que está a ser provisionado.

[OP.CRI.2] Encriptação em Repouso

A encriptação em repouso refere-se ao mecanismo de encriptar dados que não estão a ser utilizados — ou seja, que se encontram armazenados, quer num serviço da AWS, quer numa unidade de armazenamento externa.

O principal objetivo deste requisito é garantir que os dados armazenados permanecem encriptados. No mínimo, e para cumprir este controlo, as organizações devem considerar que tipo de chave é necessária, qual a sua finalidade e qual o nível de disponibilidade pretendido para os dados em repouso. Na AWS, através do AWS KMS, a encriptação simétrica utiliza por defeito a chave AES-256-GCM.

Para cumprir com o requisito de encriptação em repouso, a organização deve:

- Garantir que as capacidades de encriptação em repouso são aplicadas através do AWS KMS e/ou de mecanismos de encriptação do lado do cliente. Isto pode ser feito utilizando as chaves geradas por defeito (AES-256-GCM), importando material de chave personalizado (BYOK – Bring Your Own Key) ou implementando encriptação e desencriptação no lado do cliente (AWS - KMS Key Creation e AWS - KMS Key Imports).
- Todos os serviços de armazenamento de dados que contenham informação classificada devem ter a encriptação em repouso ativada através do AWS KMS. Por exemplo, no Amazon S3, a encriptação em repouso pode ser configurada da seguinte forma: AWS - S3 Using Encryption.
- Podem ser considerados outros mecanismos de encriptação, desde que cumpram os requisitos mínimos de segurança e não comprometam a disponibilidade ou a usabilidade dos dados pela organização.

[OP.CRI.3] Encriptação em Trânsito

A encriptação em trânsito refere-se ao mecanismo que garante a encriptação dos dados enquanto estes estão a ser transmitidos, seja dentro dos limites da AWS ou nas comunicações para e/ou a partir dos serviços AWS. Dependendo da arquitetura global dos

ativos da organização, esta é responsável por avaliar quais os algoritmos e primitivas criptográficas necessários para assegurar que os dados são devidamente encriptados durante o seu trânsito.

O principal objetivo deste requisito é garantir que existem capacidades de encriptação (e desencriptação) sempre que há transferência de dados, independentemente da origem ou do destino. No mínimo, e para cumprir este controlo, as organizações devem assegurar que não são utilizados protocolos de comunicação inseguros.

Consoante o cenário, este requisito pode ser cumprido através da utilização de:

- **HTTPS**: Extensão segura do protocolo HTTP, que cifra o tráfego utilizando o Transport Layer Security (TLS). Na AWS, o HTTPS pode ser imposto para garantir a privacidade e integridade dos dados enquanto estão em trânsito. Isto pode ser feito ao permitir ligações HTTPS de entrada e configurando o HTTPS para utilizar o certificado previamente gerado. Devem ser aplicadas políticas de segurança de comunicação que limitem as *cipher suites* e os protocolos permitidos. A organização deve desativar os protocolos TLSv1.0, TLSv1.1 e SSLv3 (ou anteriores), e apenas considerar cipher suites com chaves de encriptação de, no mínimo, 128 bits. A encriptação assimétrica deve usar RSA com chave superior a 2048 bits ou EC com chave superior a 256 bits. Os algoritmos de *hash* devem ser restringidos a SHA-256 ou superior.
  Mais informações: AWS - ELB Security Policy Table, AWS - Describe SSL Policies e AWS - CloudHSM SSL Traffic
- **DTLS / TLS**: Em cenários onde são utilizadas comunicações UDP/TCP e o protocolo não implementa encriptação própria, pode ser usada DTLS (para UDP) ou TLS (para TCP). A versão do TLS deve ser igual ou superior à 1.2. Devem ser utilizadas apenas cipher suites com chaves de encriptação de pelo menos 128 bits. A encriptação assimétrica deve usar RSA > 2048 bits ou EC > 256 bits, e os algoritmos de hash devem ser SHA-256 ou superiores.
- **SSH**: O SSH é um protocolo de *shell* remoto seguro, utilizado para gerir remotamente máquinas virtuais ou outras instâncias computacionais que o suportem. O SSH cifra todas as comunicações, podendo ser usado para enviar/receber ficheiros e aceder a serviços TCP expostos pela instância. As

versões do servidor e cliente SSH devem ser as mais recentes disponibilizadas pelo fornecedor.

Mais Informações: AWS - EC2 Connect Methods

- **Systems Manager**: Serviço totalmente gerido que permite aos utilizadores administrar instâncias Amazon EC2, dispositivos de *edge*, servidores locais e máquinas virtuais através de uma shell interativa. Proporciona uma forma segura e auditável de gestão de nós, sem necessidade de abrir portas de entrada, manter *bastion nodes* ou gerir chaves SSH. O controlo de acesso aos nós geridos é feito através de políticas IAM, permitindo definir condições de acesso para utilizadores e grupos.

  Mais Informações: AWS - Systems Manager

- **VPN**: Uma VPN (Virtual Private Network) é um protocolo de comunicação seguro que permite a um cliente remoto ligar-se a uma rede privada (não exposta publicamente). As VPNs podem ser utilizadas para trocar informação com hosts dentro da rede privada. A AWS disponibiliza o serviço AWS VPN, que permite a clientes remotos ligarem-se a uma rede VPC configurada na conta AWS.

  Mais Informações: *AWS - VPN*

[OP.CAT] Categorização de Dados

A categorização de dados é o processo de distribuir a informação por diferentes níveis de classificação. Cada nível pode ter procedimentos e requisitos de segurança próprios, permitindo que as organizações adotem diferentes graus de proteção consoante a categoria dos dados.

De acordo com a Norma Técnica – E01 do GNS, a classificação de informação com o rótulo NACIONAL é dividida em cinco níveis, apresentados abaixo por ordem crescente de confidencialidade:

- **Não Classificado** (**NCL**): Dados que, do ponto de vista da segurança da informação, não requerem classificação. A sua divulgação pública é permitida.

- **Restrito** (**R**): Dados cuja divulgação é desfavorável aos interesses do Estado Português. A distribuição é restrita.
- **Confidencial** (**C**): Dados cuja divulgação é prejudicial aos interesses do Estado Português. A distribuição é restrita.
- **Secreto** (**S**): Dados cuja divulgação teria consequências graves para os interesses do Estado Português. A distribuição é restrita.
- **Muito Secreto** (**MS**): Dados cuja divulgação teria consequências excecionalmente graves para os interesses do Estado Português. A distribuição é restrita.

Apenas as entidades identificadas na Norma Técnica – E01 do GNS têm competência para determinar a classificação da informação. **Os serviços de AWS Cloud apenas podem ser utilizados para armazenar informação classificada como Restrito ou inferior (R e NCL).**

Assim sendo e para o propósito desta guideline apenas serão considerados dois tipos de classificação: Não Classificado e Restrito. O foco estará nos procedimentos de segregação entre dados classificados e não classificados, não abordando o processo de classificação em si. Para mais informações sobre a classificação ou categorização de dados, deverá ser contactado o GNS.

Embora a classificação de dados não esteja incluída no âmbito deste documento, a AWS disponibiliza serviços que permitem detetar automaticamente dados incorretamente armazenados, por exemplo, dados classificados guardados em contentores não classificados:

- **AWS Macie:** Serviço automatizado de deteção de dados sensíveis, baseado em *machine learning* e reconhecimento de padrões, que pode ser configurado para identificar informação sensível em *buckets* S3.

Adicionalmente, a AWS permite configurar controlo de acesso baseado em atributos (Attribute-Based Access Control), através do qual os recursos são "marcados" com pares chave-valor, possibilitando a restrição de acesso com base nos atributos definidos para cada recurso.

[OP.CAT.1] Isolamento de dados baseado em classificação

Dados classificados, devido à sua própria natureza, têm requisitos específicos no que diz respeito à sua disponibilidade pública e ao acesso restrito. Assim, torna-se mais fácil

cumprir esses requisitos quando os dados com diferentes classificações são armazenados e processados de forma isolada uns dos outros.

A GNS exige que a informação classificada seja recebida, processada e armazenada num ambiente separado daquele utilizado para informação não classificada ou pública.

O principal objetivo deste requisito é fornecer orientações sobre a separação entre informação classificada e não classificada, de acordo com as exigências da GNS.

Para cumprir este requisito, uma organização deve:

- Criar pelo menos duas contas AWS distintas: uma dedicada a informação classificada e outra para informação não classificada.

- Caso sejam utilizadas AWS Organizations, garantir que **nenhum** utilizador AWS **tem acesso simultâneo** às contas de informação classificada e não classificada.

[OP.APP] Segurança Aplicacional

Muitas vezes, aplicações personalizadas são lançadas em ambientes na cloud para oferecer funcionalidades a clientes ou cidadãos. No entanto, estas aplicações podem conter vulnerabilidades que resultam em fugas de informação.

A segurança das aplicações pode ser avaliada através de testes automatizados — como os testes de segurança estáticos e dinâmicos (SAST/DAST) — e de exercícios periódicos de pentesting. Para além da análise de código e dos testes de penetração, é recomendável adotar uma metodologia de defesa em camadas, onde várias linhas de defesa são aplicadas sobre a aplicação para reforçar a proteção.

Embora se trate de uma área complexa, a AWS disponibiliza um conjunto de serviços que ajudam a garantir um desenvolvimento mais seguro e a implementar a defesa em camadas. Entre esses serviços destacam-se:

- **AWS CodeGuru Security**: uma ferramenta SAST baseada em aprendizagem automática que deteta vulnerabilidades no código antes de este ser executado ou publicado. O CodeGuru também fornece recomendações de correção e permite acompanhar os esforços de mitigação de vulnerabilidades.

- **AWS WAF**: o Web Application Firewall da AWS é um mecanismo de defesa em profundidade que impede que ataques web comuns atinjam a aplicação subjacente. Além disso, ajuda a evitar o consumo excessivo de recursos.
- **AWS Systems Manager Patch Manager**: esta ferramenta da AWS automatiza a implementação de patches em grande escala, garantindo que as instâncias de computação recebem as atualizações de segurança de forma rápida e consistente.

[OP.APP.1] Atualizações e Patches

Recomenda-se que as organizações verifiquem e apliquem atualizações e correções de forma regular, reforçando assim a segurança dos seus sistemas. Um sistema atualizado apresenta uma superfície de ataque reduzida, o que o torna menos vulnerável a ameaças.

O principal objetivo deste requisito é implementar políticas e metodologias de atualização e correção que aumentem a segurança da infraestrutura.

Para cumprir este requisito, a organização deve:

- Se estiver a utilizar o EC2, criar uma política de correções no AWS Systems Manager (AWS - Patch Management Policies, AWS - Update Management).
    - Definir a política para "Scan and Install" e agendar a execução pelo menos uma vez por semana.

[OP.APP.2] Web Application Firewall (WAF)

Um Firewall de Aplicações Web (WAF) é uma solução de segurança concebida para proteger aplicações web contra várias ameaças e ataques online. Funciona como uma barreira entre a aplicação web e a Internet, monitorizando, filtrando e controlando o tráfego web de entrada e saída com base num conjunto de regras de segurança predefinidas.

O principal objetivo de um WAF é reforçar a segurança das aplicações web, identificando e mitigando vulnerabilidades e ataques comuns.

Para cumprir este requisito, a organização deve:

- Criar um WAF para cada aplicação que disponibilize um website ou API na Internet (AWS - WAF Getting Started).

- Configurar, pelo menos, os seguintes grupos de regras geridas gerais:
  - Proteções de administrador
  - Conjunto de regras base (*core rule set*)
  - Entradas maliciosas (*bad inputs*)
- Configurar, pelo menos, as regras geridas que correspondam ao servidor/aplicação implementado pela organização:
  - Regras de Aplicação Web (i.e. Wordpress, PHP, SQL)
  - Regras do Sistema Operativo (ex.: Windows, POSIX, Linux)
- Opcionalmente, recomenda-se também a configuração dos seguintes conjuntos de regras. No entanto, estas podem implicar custos adicionais:
  - Proteção contra roubo de contas (*Account Takeover Protection*)
  - Proteção contra bots (*Bot Protection*)
- Configurar regras adicionais definidas pela organização (AWS - WAF Rules)

[OP.APP.3] Análise de Código

Análise de código de segurança de aplicações, também conhecida como análise estática de código ou teste estático de segurança de aplicações (SAST), é uma técnica utilizada para analisar o código-fonte de uma aplicação de software em busca de vulnerabilidades e fragilidades de segurança. O principal objetivo desta análise é identificar e corrigir problemas de segurança nas fases iniciais do ciclo de desenvolvimento de software, contribuindo para a criação de aplicações mais seguras e robustas. Este processo é um elemento essencial da segurança das aplicações, garantindo que potenciais vulnerabilidades sejam detetadas e resolvidas antes da implementação da aplicação.

O objetivo principal deste requisito é assegurar que, sempre que seja desenvolvido software personalizado, a análise de segurança do código seja integrada no ciclo de desenvolvimento.

Para cumprir este requisito opcional, a organização deve:

- Quando o código é confirmado (committed), realizar, pelo menos, uma análise estática de código. Esta análise pode ser efetuada na infraestrutura da própria organização, utilizando ferramentas específicas, ou através do CodeGuru Security da AWS (AWS - Code Guru Security).

- As vulnerabilidades detetadas durante os testes SAST devem ser mitigadas antes da publicação da aplicação.

[OP.REC] Recuperação e Resiliência

A resiliência refere-se à capacidade dos sistemas e aplicações de resistirem e recuperarem de interrupções inesperadas, mantendo um nível de serviço aceitável. Neste contexto, recuperação diz respeito ao(s) processo(s) de restauro de um sistema, dados e/ou aplicações para o seu último estado funcional. De forma abrangente, a recuperação e a resiliência podem ser definidas através de métricas específicas, como os Objetivos de Ponto de Recuperação (RPO) e os Objetivos de Tempo de Recuperação (RTO). O RPO representa o período máximo tolerável durante o qual dados podem ser perdidos — ou seja, a quantidade máxima de perda de dados que uma organização pode suportar. Já o RTO indica o tempo máximo aceitável necessário para restaurar dados e sistemas ao funcionamento normal após uma interrupção.

A AWS disponibiliza vários serviços que podem ser utilizados para garantir capacidades de recuperação e resiliência em todos os sistemas, dados e/ou aplicações da organização. Entre esses serviços destacam-se:

- **AWS Backup:** Serviço de cópias de segurança totalmente gerido, que centraliza e automatiza o processo de backup de dados em serviços de armazenamento, bases de dados e computação da AWS. O AWS Backup também permite realizar testes de restauro dos recursos para os quais foram criados pontos de recuperação.
  Mais Informações: AWS - Backup e AWS - Backup Restore and Testing.
- **AWS S3**: Serviço de armazenamento de uso geral, que pode ser integrado com várias funcionalidades para armazenamento, cópias de segurança, arquivo e replicação de dados.
  Mais Informações:
- **AWS Elastic Block Store (EBS)**: Fornece recursos de armazenamento em blocos escaláveis e de elevado desempenho, que podem ser utilizados por instâncias AWS EC2. Com o AWS EBS é possível gerir os seguintes recursos:
  - **AWS EBS volumes** - volumes de armazenamento que podem ser associados individualmente a instâncias AWS EC2.

- **AWS EBS snapshots** - cópias de segurança em momentos específicos, que permanecem disponíveis de forma independente do volume original.

Mais Informações: AWS - EBS

De acordo com a Norma Técnica – E01 da GNS, a etiqueta de classificação da informação NACIONAL está dividida em cinco níveis, sendo que apenas os dois primeiros podem ser considerados para implementações em nuvem: **NCL** (**Não Classificado**) e **R** (**Restrito**). Assim, as estratégias de backup e recuperação devem ser definidas tendo em conta esta classificação, as métricas RTO e RPO previamente estabelecidas (conforme definido na norma NIST 800-53), as decisões de negócio ou organizacionais em vigor, bem como a natureza e a frequência de utilização dos dados.

[OP.REC.1] Backups

As cópias de segurança referem-se ao processo de criação e manutenção de duplicados de dados ou informações, garantindo a sua disponibilidade e recuperação em caso de perda, corrupção, eliminação acidental ou outros incidentes imprevistos. O principal objetivo das cópias de segurança é proteger contra a perda de dados e permitir a restauração da informação para um estado anterior.

Para cumprir este controlo, as organizações devem:

- Assegurar cópias de segurança periódicas dos serviços de armazenamento, bases de dados e/ou computação que sejam críticos para as operações da respetiva organização. Conforme referido em OP.REC, vários serviços da AWS podem ser utilizados para garantir capacidades de backup, dependendo das necessidades e operações da organização.
- Definir a periodicidade dos backups, avaliando o intervalo mais adequado, o tipo de cópia e outras limitações e/ou considerações relevantes (OP.REC.1.1).
- Sempre que possível, utilizar o serviço totalmente gerido AWS Backup, uma vez que este permite automatizar testes de recuperação de backups para diversos serviços da AWS. Quando viável, deve ser elaborado um plano de testes de recuperação de cópias de segurança para todos os recursos de armazenamento, computação e base de dados da organização que sejam compatíveis com o AWS Backup. Ao desenvolver este plano, o período em que os pontos de recuperação estão disponíveis para restauro (ou seja, a definição de utilizador no plano de testes de

restauro do AWS Backup: AWS - Backup Restore and Testing) deve estar alinhado com a métrica RPO da organização, garantindo que os recursos estão prontos para restauro antes de atingir o limite definido pelo RPO (ou seja, assegurar o restauro antes da perda de dados).

[OP.REC.1.1] Frequência

A frequência nas cópias de segurança refere-se à periodicidade com que os dados são copiados e armazenados no âmbito de um processo de backup. A definição dessa frequência é um elemento essencial de qualquer estratégia de backup e depende de vários fatores, como a natureza dos dados, a taxa de alteração da informação, a sua classificação e ainda as métricas RPO (Recovery Point Objective) e RTO (Recovery Time Objective) estabelecidas pela organização. O plano de frequência de cópias de segurança deve ser elaborado tendo em conta estes fatores, de forma a garantir o alinhamento com as expectativas e requisitos da organização.

e acordo com o controlo CP-9 do FedRAMP – Cloud Security Information System Backup, uma organização deve, no mínimo, e para estar em conformidade com este controlo, definir operações de backup **incremental diário** e backup **completo semanal** para dados ao nível do utilizador, do sistema e de outros sistemas de informação relevantes (FedRAMP - CP9 Information System Backup).

Para cumprir este requisito, as organizações devem garantir a periodicidade das cópias de segurança através da criação de um plano de backup com o AWS Backup. Ao definir o plano, devem ser consideradas as seguintes configurações:

- Especificar a frequência de backup para criar cópias **completas semanais**.
- Ativar as cópias de segurança contínuas e a recuperação point-in-time para cada recurso suportado, implementando uma estratégia de backup **incremental** por recurso.
- Alinhar as métricas RPO e RTO da organização com a janela de backup (tempo disponível para início e conclusão do processo) e com o ciclo de vida do backup (período total de retenção e eventual armazenamento em cold storage).

Para mais informações, consulte a documentação do serviço AWS Backup:

- AWS - Create a Backup Plan

- AWS - Point in Time Recovery

[OP.REC.1.2] Backlog

Neste contexto, o termo *backlog* refere-se às tarefas de cópia de segurança que ainda não foram executadas ou concluídas. Isto pode incluir trabalhos de backup pendentes, conjuntos de dados à espera de serem copiados, ou quaisquer outras atividades relacionadas com cópias de segurança que permaneçam por realizar.

Para cumprir este controlo, as organizações devem:

- Reconhecer o tempo necessário para realizar cópias de segurança completas dos seus sistemas, dados e/ou aplicações, de forma a garantir que o volume de tarefas em atraso seja o mínimo possível. Para esse efeito, as cópias de segurança incrementais e/ou diferenciais podem ser consideradas como estratégias para poupar tempo e espaço de armazenamento.

Para mais informações, consulte as fontes online da AWS, de modo a avaliar se e quando devem ser realizadas cópias de segurança incrementais e/ou diferenciais, em comparação com as cópias completas, tendo em conta as necessidades do negócio da organização.

Mais Informações: AWS - Difference between incremental and differential backups

[OP.REC.2] Replicação e Resiliência

A replicação de cópias de segurança consiste no processo de duplicar e manter cópias de dados, normalmente em tempo real ou quase em tempo real, em vários locais. O principal objetivo da replicação, no contexto das cópias de segurança, é aumentar a resiliência, a disponibilidade e a capacidade de recuperação em caso de desastre. Garantir que as cópias de segurança são resistentes a sobrecargas ou ataques é essencial para manter a integridade, disponibilidade e recuperabilidade dos dados perante possíveis interrupções.

Para cumprir este controlo, as organizações devem assegurar que as capacidades de replicação e resiliência estão alinhadas com os requisitos inerentes aos dados, a sua classificação e as métricas de ponto de recuperação previamente definidas. Para dados, sistemas e/ou aplicações com um RPO reduzido — ou seja, um período de tempo muito curto em que é admissível perda de dados — a replicação deverá ser frequente e a

resiliência elevada, o que pode ser alcançado através de mecanismos de elevada redundância.

[OP.REC.2.1] Versionamento e Rollback

A versionagem consiste no processo de criação e manutenção de diferentes versões de um objeto de dados, seguindo uma estrutura baseada em identificadores de versão desses mesmos objetos. Já o rollback refere-se ao processo de controlo do estado dos objetos de dados utilizando os identificadores de versão previamente definidos, ou seja, restaurar um objeto de dados para uma versão anterior identificada por um identificador único de versão.

O principal objetivo deste requisito é permitir, no mínimo, que as organizações mantenham o armazenamento de forma persistente com base em versões, garantindo a capacidade de controlar o estado dos dados através da correspondência entre os estados de armazenamento e os respetivos identificadores únicos de versão.

Para cumprir os requisitos de versionagem e rollback, a organização deve:

- Ativar a funcionalidade de versionamento/criação de instantâneos (snapshotting) em todos os recursos de armazenamento que lidem com dados (ex: S3: AWS - S3 Versioning, EBS: AWS - EBS Snapshots).
- Se for utilizada a classe de armazenamento AWS S3:
    - Ativar o versionamento e o rollback por item, em cada bucket.
- Se for utilizado o AWS EBS:
    - Ativar o versionamento e o rollback, permitindo que os instantâneos (snapshots) sejam tratados como versões distintas; o rollback pode então ser realizado substituindo os instantâneos.
- Se for utilizado o AWS EFS:
    - Ativar o versionamento e o rollback, baseando as versões no sistema de ficheiros como um todo ou ao nível de cada item (dentro do sistema de ficheiros). O rollback pode ser efetuado com base nos "pontos de recuperação" previamente definidos.

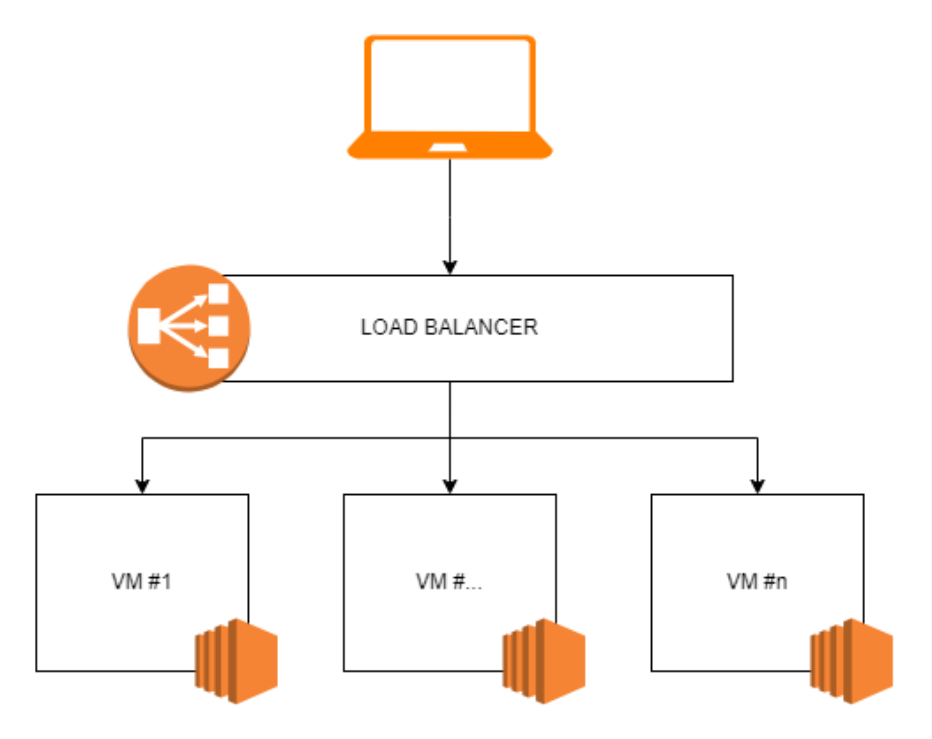
[OP.REC.3] Alta Disponibilidade

A alta disponibilidade refere-se à capacidade de um sistema, componente ou aplicação funcionar de forma contínua, sem interrupções ou falhas, durante um determinado período de tempo. É um aspeto fundamental para garantir que os sistemas e aplicações informáticas se mantenham operacionais e acessíveis aos utilizadores, mesmo em caso de falha de componentes ou outras perturbações.

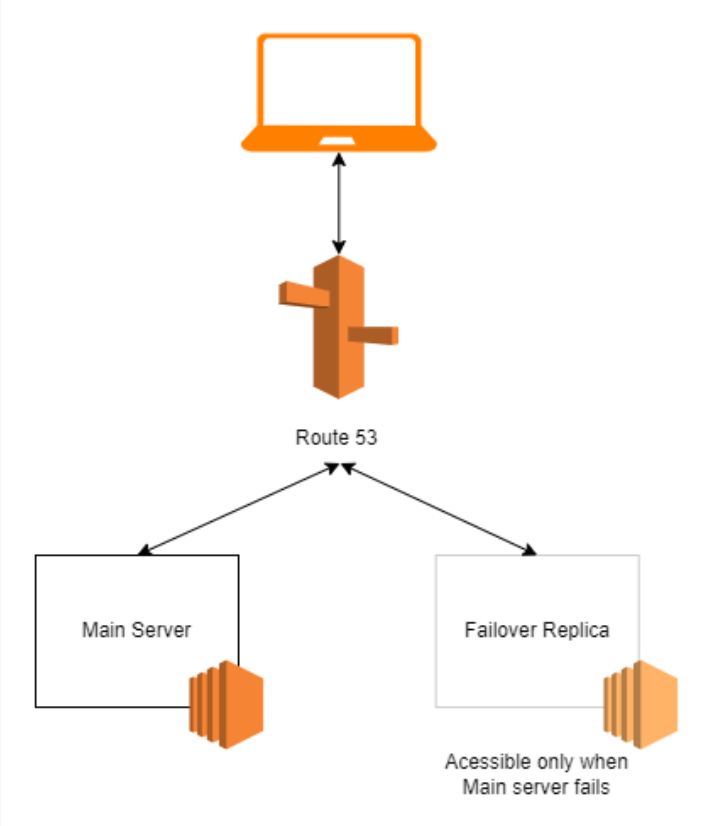
Embora a AWS tenha sido concebida para oferecer elevada disponibilidade, a arquitetura da aplicação deve ser projetada para resistir à falha de uma região (ou seja, implementações multi-regionais), de uma zona de disponibilidade ou de uma máquina virtual. Assim, as organizações podem adotar diferentes modelos arquitetónicos para cumprir os requisitos de RTO (Recovery Time Objective), RPO (Recovery Point Objective) e operacionais.

O principal objetivo de um design de alta disponibilidade é evitar Pontos Únicos de Falha (Single Points of Failure – SPOF). Para eliminar SPOF, podem ser utilizados dois blocos de construção principais:

- **Load Balancing (N+1):** Consiste em ter várias réplicas ativas que partilham a carga entre si. Quando uma réplica falha, as restantes continuam a responder aos pedidos. (Fig.1)



- **Failover (2N):** Consiste em ter uma réplica ativa do recurso a proteger, de modo que, quando o recurso principal falha, a réplica assume automaticamente o seu papel. (Fig.2)



Cabe à organização desenvolver o seu próprio modelo de alta disponibilidade, com base nos blocos de construção referidos e de acordo com os RTO e RPO exigidos.
Na maioria dos casos, e para aumentar a disponibilidade e eficácia destas abordagens, é recomendável separar as funções de computação e armazenamento. Desta forma, todas as réplicas têm acesso à mesma informação e, em caso de falha de uma réplica, a disponibilidade dos dados não é afetada nem ocorre perda adicional de informação.Estas estratégias de implementação podem ser aplicadas por região ou zona de disponibilidade, originando diferentes níveis de disponibilidade. As arquiteturas multi-regionais devem ser implementadas nas seguintes situações:

- Quando a organização possui requisitos rigorosos de alta disponibilidade e continuidade operacional para as suas cargas de trabalho mais críticas e considera que esses requisitos não podem ser cumpridos numa única região.
- Quando é necessário cumprir requisitos de soberania dos dados, como leis, regulamentos ou normas de conformidade que obrigam à operação dentro de uma determinada jurisdição.
- Quando se pretende melhorar o desempenho e a experiência do utilizador, executando as cargas de trabalho em locais mais próximos dos utilizadores finais.

O objetivo principal deste requisito é demonstrar os vários mecanismos que podem ser utilizados para promover a alta disponibilidade e as implementações multi-regionais, quando necessário.
Para cumprir este requisito, a organização deve:

- Conceber e aplicar modelos de alta disponibilidade para sistemas que tratem dados críticos para o negócio, incluindo recursos de armazenamento e computação.
- Conceber e aplicar modelos de alta disponibilidade para sistemas que tratem informação confidencial, incluindo recursos de armazenamento e computação.
- Ter em conta a localização geográfica para decidir entre implementações numa única região ou multi-regionais. Caso seja adotada uma infraestrutura multi-regional, devem ser utilizadas pelo menos duas regiões distintas.

Mais Informações:

- AWS - Resiliency Patterns and Trade Offs
- AWS - Resiliency
- AWS Whitpaper - AWS Multi Region Fundamentals

[OP.MON] Monitorização

De forma geral, a monitorização refere-se à observação, medição e registo contínuos ou periódicos de atividades, processos ou sistemas, com o objetivo de avaliar o seu desempenho, estado ou integridade. Este processo envolve a recolha e análise sistemática de dados para garantir que um sistema está a funcionar conforme o esperado, identificar problemas ou desvios e apoiar uma tomada de decisão informada.

Na AWS, a monitorização pode ser realizada através da combinação dos seguintes serviços:

- **AWS CloudWatch:** O CloudWatch é um serviço de monitorização abrangente que recolhe e acompanha métricas e registos (logs) de recursos e aplicações AWS. Pode ser utilizado para monitorizar cargas de servidores, utilização de CPU e largura de banda. O CloudWatch permite ainda configurar respostas automáticas a determinados eventos e integrar-se com serviços de notificação para o envio de alertas.
  Mais Informações: *AWS - CloudWatch*
- **AWS CloudTrail:** O CloudTrail regista a atividade dentro do ambiente AWS, incluindo todas as chamadas de API, a atividade dos utilizadores e os pedidos efetuados aos serviços AWS. Pode também ser integrado com o CloudWatch.
  Mais Informações: *AWS - CloudTrail*
- **AWS Config:** O AWS Config é um serviço que acompanha alterações na configuração dos recursos (por exemplo, alterações nas definições de um serviço AWS).
  Mais Informações: AWS - Config
- **AWS Simple Notification Service (SNS):** O AWS SNS é um serviço de notificações baseado no modelo *publish–subscribe*, que pode ser integrado com outros serviços AWS para enviar notificações através de vários canais, incluindo e-mail e pedidos HTTP.
  Mais Informações: *AWS - SNS*

- **AWS EventBridge:** O AWS EventBridge (anteriormente conhecido como CloudWatch Events) é uma plataforma de gestão de eventos que permite associar eventos — como registos, eventos de gestão ou outros eventos AWS — a regras que podem acionar outros serviços AWS, como o AWS Lambda ou o AWS SNS, proporcionando uma gestão de eventos totalmente personalizável.
  Mais Informações: *AWS - EventBridge*

Além disso, a monitorização e deteção de eventos podem ser reforçadas com ferramentas de deteção automática de ameaças, como:

- **AWS GuardDuty**: O AWS GuardDuty é um serviço de segurança que identifica automaticamente potenciais ameaças, analisando registos de fluxo de VPC, eventos do CloudTrail, registos DNS, entre outros dados. Pode ser integrado com o EventBridge para gerar notificações ou executar ações automáticas.
  Mais Informações: AWS - Guard Duty
- **AWS Inspector**: O AWS Inspector é um serviço de segurança que utiliza um agente instalado nas instâncias EC2 para detetar vulnerabilidades (CVE) ou outras falhas no software em execução. Também compara o estado da instância com referenciais de segurança, como o CIS.
  Mais Informações: AWS - Inspector
- **AWS Security Hub**: O Security Hub centraliza eventos de segurança e executa verificações automáticas, produzindo pontuações baseadas em normas de segurança como o CIS. Permite obter uma visão geral do estado de segurança da organização.

[OP.MON.1] Captura de Eventos

A captura de eventos consiste na recolha, armazenamento e análise sistemática dos dados de registo (logs) gerados por diferentes sistemas, aplicações e serviços. Estes registos contêm informações valiosas sobre eventos, transações, erros e outras atividades, sendo, por isso, fundamentais para a resolução de problemas, análise de segurança e otimização de desempenho.

O principal objetivo deste requisito é garantir a recolha de todos os eventos relevantes para manter a segurança dos dados e a disponibilidade dos serviços prestados pela

organização. A captura de eventos permite detetar anomalias e assegurar uma resposta mais rápida.

Para cumprir o requisito de captura de registos, a organização deve:

- Ativar o CloudTrail
    - Ativar o registo de logs no CloudWatch Logs.
    - Garantir o registo de pelo menos, os Management Events.
    - Se a recolha de Data Events estiver ativa, incluir pelo menos todos os serviços que tratem informação classificada na secção correspondente.
- Ativar as AWS Config Rules para monitorizar alterações nas definições dos serviços AWS (AWS - Config Getting Started)
    - Selecionar a configuração manual.
    - Garantir que a Gravação Contínua (Continuous Recording) está ativa.
- Ativar o registo de eventos em todos os recursos AWS que suportem logging (por exemplo: AWS - Lamdba CloudWatch Logs).

[OP.MON.2] Armazenamento de Logs

A monitorização do armazenamento de registos envolve supervisionar os processos relacionados com a recolha, retenção e gestão de dados de log. O objetivo é garantir que os sistemas de armazenamento de registos funcionam de forma eficiente, que os logs estão acessíveis sempre que necessário e que quaisquer problemas ou anomalias são rapidamente identificados e resolvidos.

O principal objetivo deste requisito é assegurar o armazenamento seguro dos dados de log, que podem ser úteis em tarefas de análise forense ou para manter um registo das ações realizadas.

Para cumprir o requisito de armazenamento de logs, a organização deve:

- Criar uma conta adicional na AWS e configurar um bucket privado no S3.
- Configurar o AWS Config e o AWS CloudTrail para enviar os logs para o bucket S3 criado anteriormente.
- Impedir que utilizadores humanos tenham permissões de escrita sobre os logs.
- Restringir o acesso de leitura dos logs apenas a quem realmente necessite. Isto pode ser feito através da aplicação de políticas de acesso (bucket policies) no S3.

[OP.MON.2.1] Duração de Armazenamento de Logs

O tamanho do armazenamento dos registos aumenta consoante o número de dias em que estes são guardados e disponibilizados à organização, o que tem um impacto direto nos custos de armazenamento. Para controlar esses custos, é necessário definir períodos de retenção em todos os serviços da AWS utilizados para recolha de registos.

O principal objetivo deste requisito é estabelecer períodos mínimos para a conservação dos dados de registo. Os períodos mínimos definidos representam um bom equilíbrio entre o custo de manter registos por longos períodos e as exigências impostas pela GNS.

Para cumprir o requisito relativo à duração do armazenamento dos registos, a organização deve:

- Manter os registos relacionados com serviços que utilizem informação confidencial armazenados durante, pelo menos, 3 anos.

[OP.MON.3] Consumo de Recursos

Monitorizar o consumo de recursos e definir quotas é essencial para acompanhar a utilização e manter os custos sob controlo. Um consumo elevado de recursos pode ser um sinal de um serviço mal configurado ou até de uma tentativa de ataque de negação de serviço (DoS).

Para cumprir o requisito de consumo de recursos e quotas, a organização deve:

- Instalar e ativar o Cloud Agent em todas as instâncias EC2 (AWS - CloudWatch Agents)
- Ativar a monitorização da utilização de recursos em todas as instâncias de computação (por exemplo: CPU, memória RAM, armazenamento e rede)
- Monitorizar a utilização da API através do CloudWatch (AWS - CloudWatch API Usage Metrics)

[OP.MON.4] Alarmes

É útil que as organizações sejam notificadas sempre que ocorra um consumo anormal de recursos, alterações nas configurações de um serviço ou acessos invulgares à conta AWS da organização. Os alarmes permitem emitir notificações sempre que é detetado um comportamento anómalo (por exemplo: utilização de CPU/RAM acima de 80% ou início de

sessão com a conta root da AWS), possibilitando uma resposta rápida da organização para analisar e resolver eventuais problemas.

Para cumprir os requisitos relativos aos alarmes, a organização deve:

- Gerar um alarme sempre que a conta root seja acedida (AWS - Receive Notifications).
- Criar um alarme quando a utilização de recursos ultrapassar um determinado limite (por exemplo: CPU acima de 80% de utilização) (AWS - CloudWatch Create An Alarm)
- Gerar alarmes quando as quotas de recursos atingirem um limite definido (por exemplo: 80% da quota utilizada).
- Criar um alarme para alterações no IAM (AWS - IAM Alerts)
- Criar um alarme para alterações nas configurações de serviços AWS críticos para monitorização ou que armazenem dados confidenciais e que possam afetar a confidencialidade, integridade, disponibilidade ou controlos organizacionais existentes, como por exemplo:
    - Alterações ao CloudTrail e ao Config
    - Alterações ao acesso ao armazenamento (ex.: bucket S3 tornado público)
    - Alterações na exposição de serviços (ex.: AWS RDS acessível a partir da internet pública)
    - Alterações às regras de firewall do EC2
    - Alterações nas configurações de criptografia (ex.: alteração de chaves)

[OP.TRA] Treino

Formação refere-se ao processo de implementação de programas e atividades educativas dirigidas a indivíduos e/ou organizações, com o objetivo de melhorar as suas capacidades gerais de acordo com o âmbito definido do processo de formação. Os planos de formação são normalmente elaborados em função das competências e conhecimentos que os participantes devem adquirir, de modo a desempenharem de forma mais eficaz as suas funções como membros profissionais da organização.

[OP.TRA.1] Treino de Cibersegurança

A formação em cibersegurança diz respeito a programas e atividades educativas concebidos para dotar os participantes dos conhecimentos, competências e

sensibilização necessários para compreender, prevenir, detetar e responder a ameaças de cibersegurança. O principal objetivo da formação em cibersegurança é reforçar a postura global de segurança de indivíduos e organizações, capacitando-os para proteger ativos digitais, informações sensíveis e sistemas contra ameaças e ataques informáticos.

As infraestruturas em nuvem diferem das infraestruturas tradicionais, introduzindo novos desafios de segurança que afetam a proteção da informação nesse ambiente. O pessoal responsável pelo desenho e implementação da infraestrutura da organização na nuvem deve estar familiarizado com os desafios de segurança específicos deste tipo de infraestrutura.

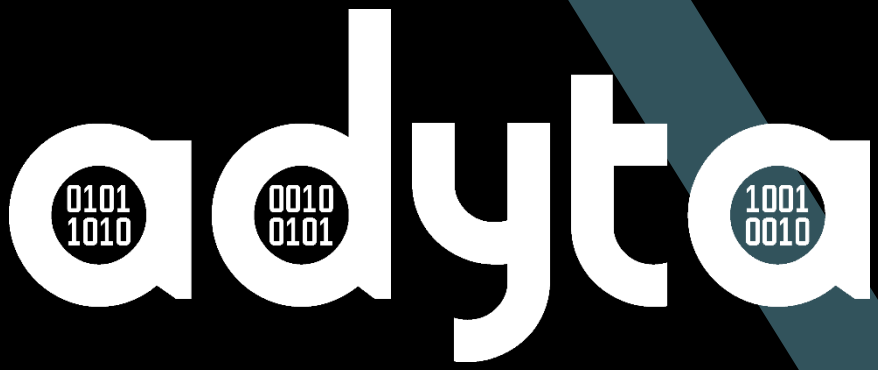
Para cumprir com os requisitos da formação em cibersegurança, a organização deve:

- Garantir a formação do pessoal em temas de cibersegurança, com especial enfoque na segurança em ambiente de nuvem (por exemplo, através do AWS Security Learning Plan);
- Garantir a formação do pessoal em gestão de informação classificada (por exemplo: NAU - Curso de Introdução à Segurança da Informação Classificada);
- As ações de formação em cibersegurança devem ser realizadas pelo menos uma vez por ano.

Referencias

Referencias

[1] - https://www.cloudflare.com/learning/cloud/what-is-the-cloud/



Obrigado por confiar em nós

---

*Este documento está classificado como **PÚBLICO**, o que significa que a informação nele contida pode ser partilhada com qualquer pessoa sem causar qualquer prejuízo à organização*

www.adyta.pt

U.PORTO Spin-off