PÚBLICO

Guias para a Utilização Segura de Ambientes Cloud

Guia geral para utilização segura de ambientes cloud

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 da 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 do local 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 **atribuído** ao cliente 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

A secção atual conterá a lista de requisitos que a organização deve seguir, subdividida em controlos de segurança. Cada controlo tem uma representação de código (ou seja, OP.INV.1) que permite referenciar requisitos individuais em todo o documento.

[OP.INV] Inventário de Ativos

À medida que uma organização cresce, os requisitos de infraestrutura aumentam e, com isso, a complexidade da gestão. Uma infraestrutura altamente complexa, sobrecarrega a gestão de recursos, o que pode aumentar os custos e, em alguns casos, levar ao leak de informações. O inventário de ativos permite que uma organização acompanhe os recursos implantados na cloud, facilitando a gestão da infraestrutura cloud.

[OP.INV.1] Inventário de recursos cloud

Deve ser elaborada regularmente uma lista dos serviços em cloud atualmente em funcionamento. Para cada serviço, deve ser indicada uma descrição da sua finalidade e se contém informações classificadas.

O principal objetivo deste requisito é ter sempre uma visão geral e atualizada dos recursos provisionados num provedor cloud, de modo a indicar a sua criticidade e possível exposição. Os recursos que lidam com informações classificadas como restritas nacionalmente pela GNS devem ser monitorizados e estar sempre atualizados.

Para cumprir este requisito, a organização deve:

- Regularmente realizar listagens dos ativos atualmente provisionados na cloud.

[OP.INV.2] Gestão de Recursos

Ter uma lista de recursos permite que as organizações compreendam quais recursos estão em uso, permitindo-lhes manter um melhor controlo dos recursos existentes e limitar o número de recursos que têm acesso ou processam informações classificadas.

O principal objetivo deste requisito é impor a redução da exposição de dados classificados em recursos que não são exigidos ou necessários para as necessidades atuais da organização:

Para cumprir este requisito, a organização deve:

- Acompanhar os requisitos relacionados com a necessidade de armazenar ou processar informações confidenciais e associar os requisitos aos recursos.
- Quando não houver mais necessidade de manter o recurso, o mesmo deverá ser removido.
- Remover os recursos não utilizados nas contas dos fornecedores cloud que lidam com informações confidenciais.

[OP.IAM] Identidade e Controlo de Acesso

O controlo adequado de identidade e acesso é um dos pilares mais importantes da segurança numa organização. Os fornecedores de serviços na cloud integram os seus serviços com ferramentas de gestão de identidade e acesso que permitem às organizações criar controlos de acesso robustos e proteger o acesso a recursos e dados.

[OP.IAM.1] Segurança do Utilizador Root

"Root User" é o nome atribuído ao utilizador com privilégios mais elevados na conta do fornecedor cloud e é criado quando uma conta do fornecedor cloud é criada. Após a criação da conta do fornecedor cloud, a conta root só deve ser utilizada em situações que exijam especificamente a sua utilização.

Recomenda-se criar um conjunto de utilizadores e atribuí-los às responsabilidades distintas da conta raiz, como faturação, administração, identidade, gestão de acesso, entre outras.

O principal objetivo deste requisito é implementar uma segurança robusta da conta root e promover a minimização da sua utilização.

Para cumprir 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]
- Definir autenticação MFA para o utilizador root, conforme definido em [OP.IAM.3.2]
- Evitar a utilização da conta root, optando por utilizar utilizadores com funções definidas e com permissões limitadas

[OP.IAM.2] Gestão segura de Utilizadores

Como o utilizador root possui o nível mais alto de permissões disponíveis num fornecedor de serviços em cloud, o seu acesso deve ser reduzido a situações de necessidade ou emergência, seguindo a abordagem de privilégios mínimos.

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

Para cumprir este requisito, a organização deve:

- Criar contas para cada função de trabalho distinta, minimizando o uso da conta root. Para cada conta, deve ser definido um conjunto mínimo de permissões, utilizando o princípio do privilégio mínimo.

[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 de MFA.

Para cumprir este controlo, uma organização deve cumprir [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.

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

Para cumprir este requisito, uma organização deve configurar uma política de palavras-passe que imponha o seguinte:

- Comprimento da palavra-passe deverá ser superior a 12 caracteres
- Contém letras minúsculas e maiúsculas.

- Contém números.
- Contém símbolos.
- A palavra-passe deve ser distinta 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 de repetição.

O principal objetivo deste requisito é impor o uso da autenticação MFA no acesso do utilizador ao provedor de cloud.

Para cumprir este requisito, uma organização deve:

- Para contas de utilizador IAM configurar o MFA e utilizar aplicações Authenticator e/ou chaves de segurança como MFA
- Para utilizadores root, configurar o MFA, utilizando aplicações Authenticator e/ou chaves de segurança como MFA.
- Para utilizadores de fornecedores de identidade externos, configure a autenticação multifator utilizando aplicações Authenticator e/ou chaves de segurança

[OP.IAM.4] Autenticação de API Segura

As APIs do provedor de cloud exigem autenticação usando tokens de API. Um token de API é um par de identificador e segredo usado para autenticar chamadas de API.

Os tokens de API podem ser chamados usando chaves de acesso ou credenciais de segurança temporárias. As chaves de acesso são credenciais de longa duração que exigem provisionamento e manutenção manuais, enquanto as credenciais de segurança temporárias permitem a emissão automática de chaves de acesso temporárias limitadas à

função à qual a solicitação estava vinculada. As credenciais de segurança temporárias são a forma recomendada de autenticar chamadas de API.

O principal objetivo deste requisito é melhorar a segurança e robustez da autenticação da API.

Para cumprir este requisito, a organização deve:

- Sempre que possível, e se permitido pelo fornecedor cloud, utilizar credenciais de segurança temporárias

- Se forem necessárias chaves de acesso, deve ser criado um utilizador IAM com o número mínimo de permissões/funções atribuídas para reduzir a exposição da funcionalidade através da chave de acesso.

- Se forem necessárias chaves de acesso, estas devem ser armazenadas como variáveis de ambiente e não devem estar presentes no código usado para a chamada da API.

- A emissão da chave de acesso deve ser limitada apenas à necessidade da sua utilização.

- As chaves de acesso devem ser renovadas pelo menos a cada 6 meses.

- As chaves de acesso e o utilizador IAM associado devem ser eliminados quando o objetivo da chave não for mais válido ou quando houver suspeita de comprometimento.

[OP.NET] Segurança de Redes

Nos sistemas em cloud, a segurança de rede aborda as considerações para proteger os dados em trânsito e a infraestrutura associada. De acordo com o modelo de responsabilidade partilhada detalhado acima, a organização é responsável por proteger o fluxo de informações, garantir a resiliência das operações e minimizar a exposição dos recursos em cloud provisionados.

[OP.NET.1] Configuração Segura de Firewall

Configurar uma firewall de forma segura envolve aderir ao princípio do acesso mínimo ao especificar regras de firewall. As regras de tráfego de rede devem ser elaboradas com base nesse princípio, de modo que apenas o nível mínimo de acesso seja atribuído a um recurso.

O principal objetivo deste requisito é configurar um controlo de acesso seguro aos recursos provisionados pela organização. Assim, os recursos podem ser usados com segurança, sem expô-los à possibilidade de atividades maliciosas. Conforme expresso anteriormente, uma configuração segura seguirá o princípio do acesso mínimo (ou seja: definição de grupos de segurança, listas de controlo de acesso, políticas de rede, etc.) e um esquema de segurança em várias camadas.

Para cumprir com uma configuração segura da firewall, no mínimo, a organização deve:

- Aplicar grupos de segurança (regras de permissão) para operações ao nível da instância
    - Especificar regras restritivas de entrada e saída com base no recurso. O acesso através de cada porta deve ser restrito às fontes e destinos necessários.
    - Evitar permitir tráfego de entrada com intervalos de IP excessivamente permissivos, ou seja: 0.0.0.0/0 (IPv4) e ::/ (IPv6).
    - Definir grupos de segurança concisos e baseados em recursos para reduzir configurações incorretas.
- Aplicar listas de controlo de acesso à rede (regras de permissão/negação) para operações ao nível da sub-rede
    - Definir listas de controlo de acesso para controlar o tráfego de entrada e saída ao nível da sub-rede.

Como boas práticas recomendadas, deverá se considerar o seguinte:

- Aplicar ações de negação, por defeito, para o tráfego de rede, ou seja: “Negar tudo, permitir alguns”.
- Não definir regras excessivamente permissivas.

[OP.NET.2] Encriptação em trânsito

A aplicação de encriptação de dados em trânsito envolve supervisionar os requisitos necessários de disponibilidade de dados, características, bem como avaliar os protocolos subjacentes utilizados para a transferência de dados. Com a encriptação em trânsito (e transferências seguras de dados), uma organização oferece confidencialidade, integridade e disponibilidade de informações de e para os seus recursos.

O principal objetivo deste requisito é garantir que nenhum meio inseguro seja utilizado para comunicação com recursos e serviços organizacionais. Para cumprir este requisito, a organização deve:

- Garantir que todas as comunicações de e para os recursos provisionados no provedor cloud utilizam protocolos de comunicação seguros, como TLS, HTTPS e SSH.
- Garantir que toda a criptografia simétrica seja realizada com AES ou algoritmos mais seguros. O tamanho da chave deve ser de pelo menos 128 bits. (OP.CRI.3)
- Garantir que todas as operações de *hashing* sejam realizadas usando SHA-256 ou superior.
- Garantir que as ligações TLS e HTTPS utilizem TLSv1.2 ou superior.
- Garantir que as ligações TLS/HTTPS utilizem certificados assinados por autoridades de certificação confiáveis.

[OP.STO] Armazenamento

Armazenamento, em sentido amplo, é o processo de armazenar, manter e gerir dados de forma persistente e recuperável. Esse processo envolve definir como esses dados devem estar disponíveis (disponibilidade), onde os dados devem residir, ser processados e/ou estar disponíveis (localidade) e quando e para quem esses dados devem ser enviados.

[OP.STO.1] Replicação e Redundância

A replicação envolve manter várias cópias ativas dos dados, enquanto a redundância consiste em manter e ter cópias de segurança dos dados para garantir uma disponibilidade consistente ao longo do ciclo de vida da organização. Como tal, a organização deve alinhar a estratégia subjacente com as métricas de Objetivo de Ponto de Recuperação (RPO) e Objetivo de Tempo de Recuperação (RTO) da organização, independentemente de onde e

como os critérios são aplicados. A aplicação destas métricas permite à organização conceber um plano de recuperação de dados, refletido no serviço ou combinação de serviços utilizados, o que se refletirá consequentemente no custo global.

O principal objetivo deste controlo é cumprir com a capacidade de replicação e redundância como propriedades (onde a redundância pode ser alcançada devido à replicação). O leitor é responsável por avaliar o melhor serviço para cumprir este controlo. Independentemente disso, no mínimo e para cumprir este critério, o leitor deve ter pelo menos 1 clone completo num ponto de armazenamento de dados distinto dentro da UE, seja nas zonas de disponibilidade do fornecedor de serviços em cloud, em diferentes regiões ou na mesma região. Se as métricas RPO e RTO foram pré-calculadas e avaliadas, então estas devem ser refletidas na estratégia de implementação de armazenamento considerada pela organização.

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

- Para cada recurso de armazenamento que contenha dados críticos para a organização provisionados no provedor de cloud, imponha a replicação multirregional provisionando, no mínimo, 1 clone completo dos dados originais.

- Os clones multirregionais dos dados devem ser sincronizados para permitir o failover caso uma das regiões falhe.

- Tanto os dados originais quanto os clonados devem ser versionados.

[OP.CRI] Criptografia e Proteção de Dados

Processo de proteção e transmissão de informações de forma que apenas as partes autorizadas possam compreender. Isso inclui o uso de algoritmos de criptografia robustos, a gestão de chaves criptográficas e a garantia da confidencialidade, integridade e autenticidade dos dados em trânsito e em repouso.

[OP.CRI.1] Gestão de Chaves

A gestão de chaves consiste na capacidade de criar e gerir chaves criptográficas utilizadas para encriptar dados (em repouso e/ou em trânsito). Os sistemas de gestão de chaves (KMS) funcionam como um fornecedor de serviços criptográficos, em que as operações

criptográficas são solicitadas a um conjunto distribuído de módulos de segurança de hardware ou outros mecanismos fornecidos pelo fornecedor de serviços na cloud. Além disso, a encriptação nos fornecedores de serviços na cloud pode ocorrer de duas formas possíveis: encriptação do lado do servidor e encriptação do lado do cliente.

- A encriptação do lado do servidor protege a confidencialidade das informações trocadas, realizando a encriptação usando chaves armazenadas no lado do servidor.
- A encriptação do lado do cliente protege a confidencialidade das informações trocadas, encriptando os dados no lado da aplicação/cliente. Embora a encriptação do lado do cliente possa ser usada para garantir a proteção dos dados em trânsito e em repouso, a organização será responsável por gerir o processo de encriptação, as chaves e as ferramentas relacionadas.

O principal objetivo deste requisito é aplicar estratégias adequadas de gestão de chaves para uma criação, utilização, gestão e destruição seguras das chaves quando se recorre a um fornecedor de serviços em cloud.

Para cumprir este requisito, uma organização deve:

- Utilizar módulos de segurança de hardware para gerar chaves criptográficas.

- As chaves simétricas devem ter pelo menos 256 bits de comprimento.

- As chaves assimétricas devem ter pelo menos 2048 bits de comprimento para RSA e 256 bits de comprimento para curva elíptica (EC).

- As chaves criptográficas devem ser armazenadas em HSMs e todas as operações criptográficas devem ser realizadas dentro do HSM.

- Garantir que a chave não esteja mais acessível quando uma exclusão de chave for emitida.

[OP.CRI.2] Encriptação em repouso

A encriptação em repouso está relacionada com o mecanismo de encriptação de dados que estão em repouso. Seja num serviço de fornecedor de cloud e/ou numa unidade de armazenamento externa.

O principal objetivo deste requisito é aplicar a encriptação aos dados quando estão em repouso. No mínimo, e para aplicar o requisito de controlo, as organizações devem considerar que tipo de chave é necessária, a sua finalidade e a disponibilidade desejada dos dados em repouso.

Para cumprir com a criptografia em repouso, a organização deve:

- Certificar-se **de que** os recursos de criptografia em repouso sejam aplicados usando os recursos do provedor cloud e/ou mecanismos de criptografia do lado do cliente, seja usando as chaves padrão geradas pelo AES-256-GCM, importando material de chave personalizado (BYOK) ou implementando primitivas de criptografia do lado do cliente, respetivamente.
- Todos os serviços de armazenamento de dados que contenham informações confidenciais devem ativar a encriptação em repouso utilizando o KMS do fornecedor de serviços na cloud.
- Outros mecanismos de encriptação podem ser considerados, mas devem estar alinhados para cumprir os requisitos mínimos de segurança sem comprometer a disponibilidade ou a usabilidade dos dados pela organização.

[OP.CRI.3] Encriptação em trânsito

A encriptação em trânsito está relacionada com o mecanismo de encriptação de dados que estão em trânsito, seja dentro dos limites do fornecedor de serviços na cloud ou de e/ou para serviços na cloud. Dependendo da arquitetura geral dos ativos organizacionais, uma organização é responsável por avaliar quais primitivas criptográficas são necessárias para garantir que os dados sejam encriptados em trânsito.

O principal objetivo deste requisito é garantir que os recursos de criptografia estejam disponíveis sempre que houver transferência de dados, independentemente da origem e/ou destino. No mínimo e para cumprir este controlo, as organizações devem garantir que nenhum protocolo de comunicação inseguro seja usado.

Dependendo do cenário, isso pode ser alcançado utilizando:

- **HTTPS**: Extensão segura do HTTP que encripta o tráfego utilizando Transport Layer Security (TLS). Isto pode ser feito ativando as ligações HTTPS de entrada e configurando o HTTPS para utilizar o certificado gerado anteriormente. Para

comunicações HTTPS, devem ser utilizadas políticas de segurança para limitar os conjuntos de cifras e protocolos permitidos para comunicações. A organização deve desativar os protocolos TLSv1.0, TLSv1.1 e SSLv3 ou anteriores e considerar apenas conjuntos de criptografia com chaves de criptografia de pelo menos 256 bits. A criptografia assimétrica deve usar RSA com uma chave superior a 2048 bits ou EC com uma chave superior a 256 bits. Os algoritmos de hash devem ser restritos a SHA-256 ou superior.

- **DTLS/TLS**: Em cenários em que são utilizadas comunicações UDP/TCP e não há criptografia de comunicação adicional implementada pelo protocolo de comunicação, pode-se utilizar DTLS (para UDP) ou TLS (para TCP). A versão TLS deve ser maior ou igual a 1.2. A organização deve considerar apenas conjuntos de criptografia com chaves de criptografia de pelo menos 256 bits. A criptografia assimétrica deve usar RSA com uma chave superior a 2048 bits ou EC com uma chave superior a 256 bits. Os algoritmos de hash devem ser restritos a SHA-256 ou superior.
- **SSH**: SSH é um protocolo de shell remoto seguro que pode ser usado para gerir remotamente uma máquina virtual ou outras instâncias de computação compatíveis com SSH. O SSH encripta todas as comunicações executadas e pode ser usado para enviar/receber ficheiros e aceder a serviços TCP expostos na instância de computação acedida. As versões do servidor e do cliente SSH devem ser as mais recentes disponíveis pelo fornecedor.
- **VPN**: A Rede Privada Virtual (VPN) é um protocolo de comunicação seguro que permite que um cliente remoto se conecte a uma rede privada (não exposta publicamente). As VPNs podem ser usadas para trocar informações com ativos na rede privada.

[OP.CAT] Categorização de Dados

A categorização de dados é o processo de distribuir informações por diferentes graus de classificação. Cada classificação pode ter procedimentos e padrões de segurança distintos, permitindo que as organizações tenham diferentes níveis de segurança, dependendo da categoria dos dados.

De acordo com a Norma Técnica – E01 da GNS, o rótulo NACIONAL de classificação de informações é dividido em 5 graus, descritos abaixo em ordem crescente de confidencialidade:

- **Não Classificado (NCL):** Dados que, em termos de segurança de dados, não requerem classificação. A distribuição pública pode ser feita.
- **Restrito (R):** Dados cuja divulgação, do ponto de vista da segurança, é desfavorável aos interesses do Estado português. A sua distribuição é restrita.
- **Confidencial (C):** Dados cuja divulgação, do ponto de vista da segurança, prejudica os interesses do Estado português. A sua distribuição é restrita.
- **Secreto (S):** Dados cuja divulgação, do ponto de vista da segurança, tem consequências graves para os interesses do Estado português. A sua distribuição é restrita.
- **Muito Secreto (MS):** Dados cuja divulgação, do ponto de vista da segurança, tem consequências excecionalmente graves para os interesses do Estado português. A sua distribuição é restrita.

Apenas as entidades descritas na Norma Técnica GNS – E01 têm a capacidade de determinar a classificação das informações. **Os serviços cloud só podem ser utilizados para armazenar informações classificadas como Restrito ou inferior (R e NCL).**

Assim sendo, e para efeitos desta diretriz, consideraremos apenas dois tipos de classificação: Não Classificado e Restrito, bem como os procedimentos relativos à segregação entre dados classificados e não classificados, sem abordar a forma como os dados devem ser classificados. Para mais informações sobre classificação ou categorização de dados, contacte a GNS.

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

Os dados classificados, devido à sua classificação, têm requisitos distintos para disponibilidade pública e acesso restrito. Assim, torna-se mais fácil lidar com esses requisitos quando os dados com diferentes classificações são armazenados e processados de forma isolada de outras classificações de dados.

O GNS exige que as informações classificadas sejam recebidas, processadas e armazenadas num locatário isolado de informações não classificadas ou públicas.

O GNS exige que as informações classificadas sejam recebidas, processadas e armazenadas num locatário isolado de informações não classificadas ou públicas.

Para cumprir este requisito, uma organização deve:

- Criar, pelo menos, duas contas distintas na cloud, uma para informações confidenciais e outra para informações não confidenciais.
- Validar que nenhum utilizador possa ter acesso a informações confidenciais e não confidenciais com o mesmo conjunto de credenciais.

[OP.APP] Segurança Aplicacional

Frequentemente, aplicações personalizadas são lançadas em ambientes de cloud para fornecer recursos. Essas aplicações podem ter vulnerabilidades que podem levar a fugas de informação e/ou outros tipos de ataques.

A segurança das aplicações pode ser testada utilizando testadores de segurança de aplicações estáticos e dinâmicos automatizados (SAST/DAST), bem como exercícios periódicos de testes de penetração. Além da análise de código e dos testes de penetração, recomenda-se adotar uma metodologia de defesa em camadas, na qual várias camadas podem ser adicionadas à aplicação para fornecer segurança adicional.

[OP.APP.1] Atualizações e patches

Recomenda-se que as organizações verifiquem e apliquem atualizações e patches regularmente, melhorando a sua segurança. Um sistema com patches tem uma superfície de ataque menor, o que significa que é menos suscetível a ataques.

O principal objetivo deste requisito é implementar políticas e metodologias de atualização e aplicação de patches para melhorar a segurança.

Para cumprir este requisito, uma organização deve:

- Verifique periodicamente as máquinas virtuais e instale atualizações de software para vulnerabilidades e software desatualizado.

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

Uma Web Application Firewall (WAF) é uma solução de segurança concebida para proteger aplicações web contra várias ameaças e ataques online. Ele atua como uma barreira entre

uma aplicação web e a Internet, monitorizando, filtrando e controlando o tráfego web de entrada e saída com base num conjunto de regras de segurança pré-determinadas. O objetivo principal de um WAF é melhorar a postura de segurança das aplicações web, identificando e mitigando vulnerabilidades e ataques comuns a aplicações web.

O principal objetivo deste requisito é ativar o WAF na organização, criando uma camada adicional de segurança e impedindo que ataques mais comuns atinjam os ativos.

Para cumprir este requisito, uma organização deve:

- Implemente um WAF para recursos da Web configurados no ambiente da cloud.
- Configurar e validar a aplicação das regras WAF adequadas para o recurso web que está a ser protegido (crie regras com base no motor do servidor, linguagem de programação e utilização (ou seja, API, página web, CDN, etc.)

[OP.APP.3] Análise de Código

A análise de código de segurança de aplicações, também conhecida como análise de código estático ou teste de segurança de aplicações estático (SAST), é uma técnica utilizada para analisar o código-fonte de uma aplicação de software em busca de vulnerabilidades e pontos fracos de segurança. O objetivo principal da análise de código é identificar e corrigir problemas de segurança nas fases iniciais do ciclo de vida do desenvolvimento de software, ajudando a criar aplicações mais seguras e robustas. Este processo é um componente crucial da segurança de aplicações, garantindo que potenciais vulnerabilidades sejam descobertas e corrigidas antes da implementação da aplicação.

O principal objetivo deste requisito é, sempre que for desenvolvido software personalizado, aplicar a análise de segurança de código no ciclo de vida do desenvolvimento.

Para cumprir este requisito, uma organização deve:

- Ao efetuar uma alteração no código, a organização deve realizar, no mínimo, uma análise estática do código. A análise pode ser feita na infraestrutura da organização, utilizando ferramentas específicas concebidas para esse fim.
- As vulnerabilidades detetadas pelos testes SAST devem ser mitigadas antes da publicação da aplicação.

[OP.REC] Resiliência e Recuperação

Resiliência refere-se à capacidade dos sistemas e aplicações de resistir e recuperar-se de interrupções inesperadas, mantendo um nível aceitável do serviço em questão. Neste contexto, recuperação refere-se ao(s) processo(s) de restaurar um sistema, dados e/ou aplicações ao seu último estado funcional. Em sentido lato, a recuperação e a resiliência podem ser estipuladas utilizando métricas de recuperação, tais como Objetivos de Ponto de Recuperação (RPO) e Objetivos de Tempo de Recuperação (RTO). O RPO refere-se ao período máximo tolerável em que os dados podem ser perdidos, definindo a quantidade máxima aceitável de perda de dados que uma organização pode suportar. O RTO é o tempo máximo aceitável para restaurar os dados e sistemas ao funcionamento normal após uma interrupção.

De acordo com a Norma Técnica – E01 da GNS, o rótulo NACIONAL de classificação de informações é dividido em um total de 5 graus, onde apenas os 2 graus iniciais podem ser considerados para implementações em cloud, **NCL** e/ou R, "**Não Classificado**" e "**Restrito**", respetivamente. Assim, as estratégias de backup e recuperação devem ser elaboradas com base nesta classificação inerente, nas métricas RTO e RPO previamente estipuladas (conforme definido pela NIST 800-53), nas decisões comerciais e/ou organizacionais atuais, bem como na natureza e taxa de utilização dos dados.

[OP.REC.1] Backups

Backups referem-se ao processo de criação e manutenção de cópias de dados ou informações para garantir a sua disponibilidade e recuperação em caso de perda, corrupção, eliminação acidental ou outros incidentes imprevistos. O objetivo principal dos backups é proteger contra a perda de dados e facilitar a restauração das informações para um estado anterior.

Para cumprir este requisito, uma organização deve:

- Garantir backups periódicos dos serviços de armazenamento, base de dados e/ou computação que são críticos para as operações da respetiva organização.
- A periodicidade dos backups deve ser abordada pela organização para avaliar o melhor período viável, o tipo de backup e outras limitações e/ou considerações (**OP.REC.1.1**).
- Os backups devem atender aos objetivos de RPO definidos para a organização.

[OP.REC.1.1] Frequência

A frequência dos backups refere-se à periodicidade com que os dados são copiados e armazenados como parte de um processo de backup. A frequência dos backups é um aspeto crucial de uma estratégia de backup e é influenciada por fatores como a natureza dos dados, a taxa de alteração dos dados, a classificação inerente dos dados e as métricas RPO e RTO, determinadas pela organização. O plano de frequência de backup deve ser elaborado tendo em conta estas considerações, para estar alinhado com as expectativas da organização.

De acordo com o controlo de Backup do Sistema de Informação de Segurança em Cloud (CP-9) da FedRAMP, uma organização deve, no mínimo, e para cumprir com este controlo, definir **operações diárias de backup incremental e semanal completo** para dados relacionados com os utilizadores, ao nível dos sistemas de informação relevantes (https://wayfinder.digital/FedRAMP/CP009-FedRAMP.html).

Para cumprir este controlo, as organizações devem garantir a periodicidade dos backups, elaborando um plano de backup utilizando os recursos do fornecedor de serviços em cloud. As seguintes configurações devem ser consideradas ao elaborar o plano de backup:

- Especificar a frequência de backup para criar backups **completos semanais**.
- Efetuar backups contínuos e restauração pontual para cada recurso utilizado e suportado para integração: estratégia de backup **incremental** por recurso.
- Alinhar as métricas RPO e RTO da organização com a janela de backup: tempo necessário para iniciar e concluir o backup, bem como o ciclo de vida do backup: período total de retenção e se o backup deve ser armazenado como armazenamento frio.

[OP.REC.1.2] Backlog

Backlog neste sentido é relativo às tarefas de backup que ainda não foram executadas ou concluídas. Isso pode incluir trabalhos de backup pendentes, conjuntos de dados aguardando backup ou quaisquer atividades pendentes relacionadas ao backup.

Para cumprir este requisito, uma organização deve:

- Reconhecer a latência necessária para realizar procedimentos completos de backup dos seus sistemas, dados e/ou aplicações, a fim de garantir que seja

previsto um atraso mínimo. Para esse efeito, os backups incrementais e/ou diferenciais podem ser considerados estratégias para economizar tempo e espaço de armazenamento.

[OP.REC.2] Replicação e Resiliência

A replicação de backups refere-se ao 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 dos backups é melhorar a resiliência dos dados, a disponibilidade e as capacidades de recuperação de desastres. Garantir a resiliência dos backups para carregar ataques é crucial para manter a integridade, a disponibilidade e a recuperabilidade dos dados diante de possíveis interrupções.

Para cumprir este controlo, as organizações devem abordar as capacidades de replicação e resiliência com base nos requisitos inerentes aos dados, na classificação dos dados, bem como nas métricas de ponto de recuperação pré-determinadas. Para dados, sistemas e/ou aplicações que se espera que tenham um RPO baixo, ou seja, um pequeno período de tempo em que os dados podem ser perdidos, a replicação terá de ser frequente e a resiliência (como propriedade) terá de ser elevada, o que é possível com capacidades de alta redundância.

[OP.REC.2.1] Versioning e Rollback

O controle de versão envolve o procedimento de criar e manter versões de um objeto, assumindo uma topologia baseada em identificadores de versão para o objeto. Já o rollback pode ser referido como o procedimento de controlar o estado do objeto utilizando os identificadores de versão previamente definidos, ou seja: restaurar um objeto para uma versão anterior identificável por um identificador de versão único.

O principal objetivo deste requisito é, no mínimo, permitir que as organizações mantenham o armazenamento com base em cada versão, com a capacidade de controlar o estado, mantendo uma correspondência entre os estados de armazenamento e os seus identificadores de versão exclusivos correspondentes.

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

- Periodicamente, criar instantâneos e marcar os recursos de armazenamento para permitir a reversão das alterações.

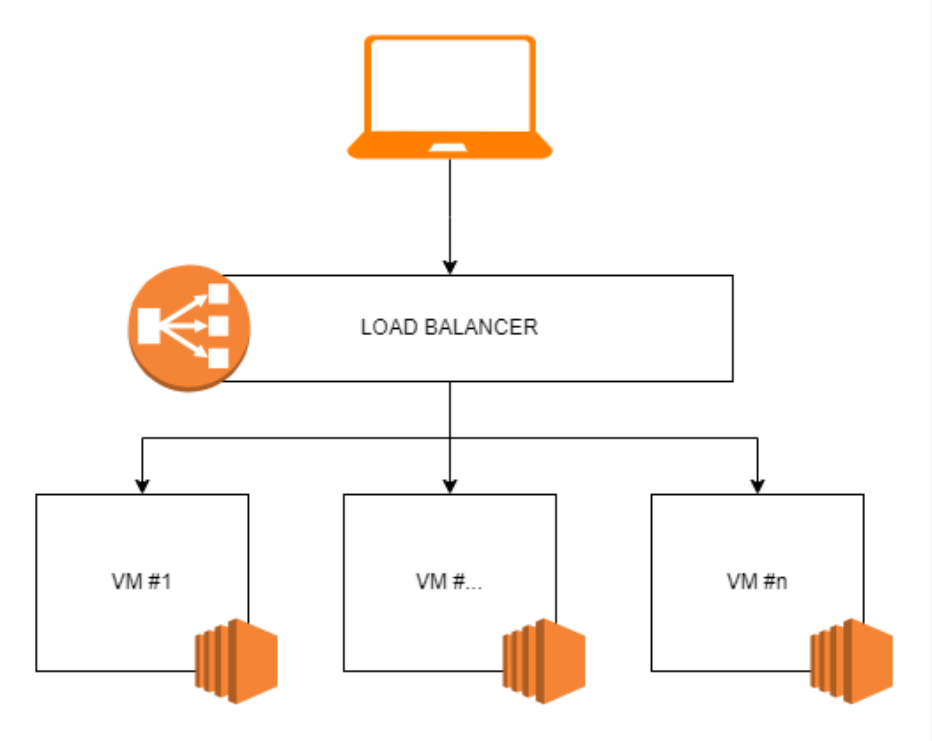
[OP.REC.3] Alta Disponibilidade

Alta disponibilidade refere-se à capacidade de um sistema, componente ou aplicação operar continuamente, sem interrupções ou falhas, durante um período determinado. É um aspeto crítico para garantir que os sistemas e aplicações permaneçam funcionais e acessíveis aos utilizadores, mesmo em caso de falhas de componentes ou outras interrupções.

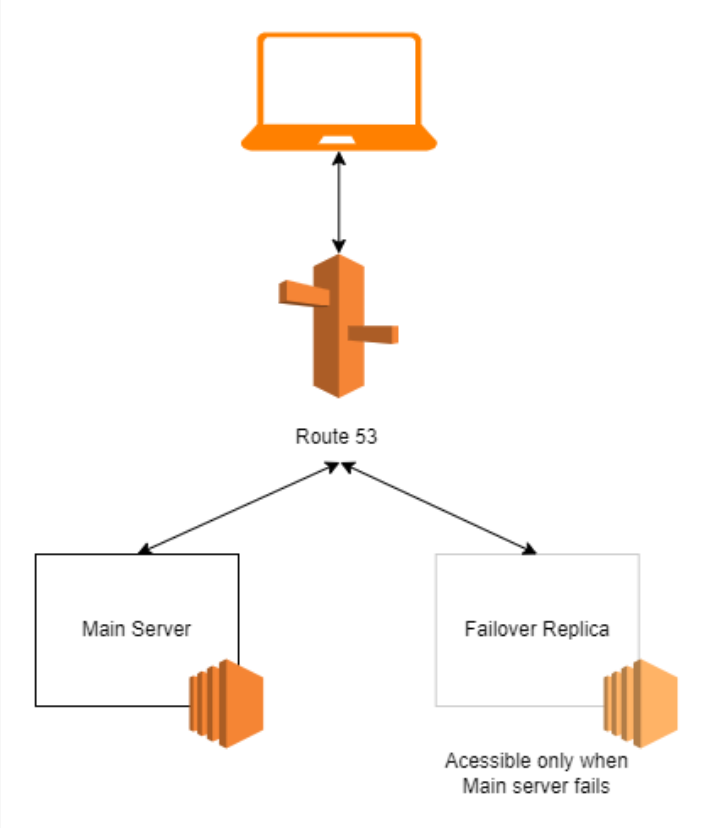
Apesar de os fornecedores de cloud serem projetados para ter alta disponibilidade, a arquitetura da aplicação deve ser projetada para ser capaz de suportar falhas de uma região (ou seja, implementações multirregionais), zona de disponibilidade ou falha de uma máquina virtual. Assim, as organizações podem implementar vários projetos arquitetónicos para atender aos requisitos de RTO, RPO e operacionais.

O principal objetivo de um projeto de alta disponibilidade é evitar pontos únicos de falha (Single Point Of Failure - SPOF). Para evitar SPOF, podem ser usados dois componentes principais:

- **Load Balancing (N+1):** Ter várias réplicas ativas que equilibram a carga entre si. Quando uma réplica falha, as outras réplicas serão capazes de responder às solicitações. (Fig. 1)



- **Failover (2N):** Ter uma réplica ativa do ativo que está a ser protegido, de forma que, quando o ativo falhar, a réplica possa assumir a função do ativo com falha. (Fig. 2)



É da responsabilidade da organização desenvolver o seu próprio projeto de alta disponibilidade, com base nos blocos de construção mencionados acima, de acordo com o RTO e o RPO exigidos. Na maioria dos casos, e para melhorar a disponibilidade e a eficácia dos blocos de construção, as tarefas de computação e armazenamento devem ser desacopladas, dessa forma, cada réplica pode ter acesso às mesmas informações e, no caso de uma falha na réplica, isso não afeta a disponibilidade dos dados nem causa perdas adicionais de dados. Essas estratégias de implementação podem ser implementadas por região ou zona de disponibilidade, levando a recursos de disponibilidade distintos. Arquiteturas multirregionais devem ser implementadas pelos seguintes motivos:

- A organização tem requisitos de alta disponibilidade e continuidade de operações para suas cargas de trabalho de nível mais alto e acredita que essas operações não podem ser atendidas em uma única região.
- A necessidade de satisfazer requisitos de soberania de dados (como adesão a leis, regulamentos e conformidade locais) que exigem que as cargas de trabalho operem dentro de uma determinada jurisdição.
- A necessidade de melhorar o desempenho e a experiência do cliente para as cargas de trabalho, executando-as em locais mais próximos dos utilizadores finais.

O principal objetivo deste requisito é ilustrar os vários mecanismos que podem ser usados para promover alta disponibilidade e implementações multirregionais, se necessário.

Para cumprir este requisito, uma organização deve:

- Projetar e aplicar projetos de alta disponibilidade para sistemas que lidam com dados críticos para os negócios, incluindo recursos de armazenamento e computação.

- Projetar e aplicar projetos de alta disponibilidade para sistemas que lidam com informações confidenciais, incluindo recursos de armazenamento e computação.

- Os projetos de alta disponibilidade devem considerar a localização geográfica para selecionar implementações únicas ou multirregionais. Se for provisionada

uma infraestrutura multirregional, devem ser utilizadas, pelo menos, duas regiões distintas.

[OP.MON] Monitorização

Monitorização, em sentido lato, refere-se à observação, medição e registo contínuos ou periódicos de atividades, processos ou sistemas para avaliar o seu desempenho, estado ou saúde. Envolve a recolha e análise sistemáticas de dados para garantir que um sistema está a funcionar conforme pretendido, para identificar problemas ou desvios e para facilitar a tomada de decisões informadas.

[OP.MON.1] Captura de Eventos

A captura de eventos envolve a recolha, armazenamento e análise sistemáticos de dados de registo gerados por vários sistemas, aplicações e serviços. Os registos contêm informações valiosas sobre eventos, transações, erros e outras atividades, tornando-os cruciais para a resolução de problemas, análise de segurança e otimização de desempenho.

O principal objetivo deste requisito é capturar todos os eventos que são importantes para manter a segurança dos dados e a disponibilidade dos serviços prestados pela organização. A captura de eventos ajudará a detetar anomalias e promoverá uma resposta mais rápida.

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

- Configurar o registo no fornecedor de serviços na cloud. Os registos devem incluir registos de acesso, registos de autenticação e registos de alterações de configuração.

[OP.MON.2] Armazenamento de Logs

A monitorização e armazenamento de registos envolve supervisionar os processos relacionados à recolha, retenção e gestão de dados de registos. Isso garante que os sistemas de armazenamento de registos estejam a funcionar de maneira ideal, que os registos estejam acessíveis quando necessário e que quaisquer problemas ou anomalias potenciais sejam prontamente resolvidos.

O principal objetivo desse requisito é promover o armazenamento seguro de dados de registos que podem ser úteis em tarefas forenses ou para manter um livro-razão das ações realizadas.

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

- Criar uma conta na cloud separada e isolada que será responsável pelo armazenamento dos registos

- Vincular os registos de outras contas na cloud à conta criada anteriormente

- Configurar o controlo de acesso à conta de registos para limitar o acesso aos registos apenas a utilizadores autorizados.

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

O tamanho do armazenamento de registos aumenta com o número de dias em que os registos são armazenados e disponibilizados à organização, o que tem um impacto direto nos custos de armazenamento. Para controlar os custos de armazenamento, os períodos de retenção devem ser configurados em todos os serviços de recolha de registos em uso.

O principal objetivo deste requisito é impor períodos mínimos para o armazenamento de dados de registo. Os períodos mínimos indicados nos requisitos representam um bom equilíbrio entre o custo do armazenamento de dados de registo por longos períodos e os requisitos impostos pela GNS.

Para cumprir o requisito de duração do armazenamento de registos, a organização deve:

- Manter os registos relativos aos serviços que utilizam informações confidenciais armazenadas durante pelo menos 3 anos.

[OP.MON.3] Consumo de Recursos

Monitorizar o consumo de recursos e definir quotas é importante para acompanhar a utilização dos recursos e manter os custos sob controlo. Uma utilização elevada dos recursos pode ser um sintoma de um serviço mal configurado ou de uma tentativa de Denial-Of-Service (DoS).

Para cumprir os requisitos de consumo de recursos e quotas, a organização deve:

- Monitorizar a utilização dos recursos das máquinas virtuais, incluindo a utilização da RAM, da CPU e do armazenamento

[OP.MON.4] Alarmes

É útil que as organizações sejam notificadas quando ocorrer um consumo incomum de recursos, alterações nas configurações de um serviço ou acessos incomuns à conta na cloud da organização. Os alarmes são uma forma de emitir uma notificação sempre que um comportamento incomum é detetado (por exemplo: uso de CPU/RAM acima de 80% ou login na conta root), solicitando uma resposta rápida da organização para analisar e corrigir possíveis problemas.

Para cumprir os requisitos de alarmes, a organização deve:

- Gerar um alarme quando a conta root for acedida
- Criar um alarme quando a utilização de recursos ultrapassar um determinado limite (por exemplo: CPU ultrapassa 80% de utilização)
- Gerar alarmes quando as quotas de recursos atingirem um determinado limite (por exemplo: 80% da quota é utilizada).
- Criar um alarme para alterações no IAM
- Criar um alarme para alterações em monitorização crítica ou configurações de serviços de cloud que armazenam dados confidenciais que afetam a confidencialidade, integridade, disponibilidade ou controlos organizacionais existentes.

[OP.TRA] Treino

Formação refere-se ao processo de implementação de programas e atividades educacionais para indivíduos e/ou organizações, com o objetivo de aprimorar as capacidades gerais dos respetivos sujeitos, de acordo com o escopo definido do processo de formação. Os planos de formação geralmente seguem as capacidades e conhecimentos que o(s) indivíduo(s) em questão deve(m) ter para desempenhar melhor as suas funções como membros profissionais da organização.

[OP.TRA.1] Formação de Cibersegurança

A formação em cibersegurança refere-se aos programas e atividades educacionais concebidos para dotar os indivíduos dos conhecimentos, competências e consciência necessários para compreender, prevenir, detetar e responder a ameaças à cibersegurança.

O objetivo principal da formação em cibersegurança é melhorar a postura geral de segurança dos indivíduos e das organizações, capacitando-os para proteger ativos digitais, informações confidenciais e sistemas contra ameaças e ataques cibernéticos.

As infraestruturas em cloud são diferentes das infraestruturas tradicionais e, com isso, surgem novos desafios de segurança que afetam a segurança das informações dentro de uma infraestrutura em cloud. O pessoal designado para projetar a infraestrutura da organização na cloud deve estar familiarizado com os desafios de segurança que a infraestrutura em cloud traz.

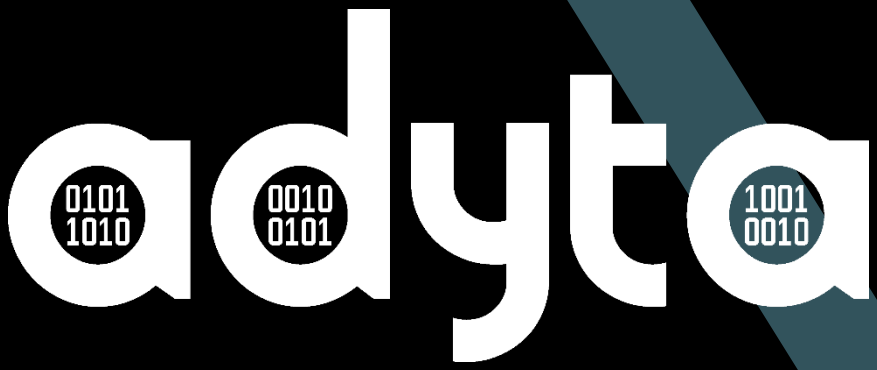
Para cumprir com a formação em cibersegurança, a organização deve:

- Impor a formação do pessoal sobre temas de cibersegurança, com foco na segurança na cloud.
- Impor a formação do pessoal com foco na gestão das informações confidenciais (por exemplo: https://www.nau.edu.pt/pt/curso/introducao-a-seguranca-da-informacao-classificada/)
- - A formação em cibersegurança deve ser realizada pelo menos uma vez por ano

Referências

Referências

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



Obrigado por confiar em nós

Este documento está marcado como PÚBLICO, o que significa que as informações nele contidas podem ser partilhadas com qualquer pessoa sem qualquer prejuízo para a organização.

www.adyta.pt

U.PORTO Spin-off