PÚBLICO

Guias para a Utilização Segura de Ambientes *Cloud*

Cenários Avançados de *Cloud* – *Cloud* Híbrida e *Multi-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 nuvem 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 requisitos para o uso de sistemas de nuvem em conformidade com o esquema de certificação do Gabinete Nacional de Segurança (GNS) de Portugal. Como este é um guia geral, o foco principal é enumerar os requisitos que uma organização deve seguir para garantir a proteção de informações classificadas em cenários de nuvem avançados, como Multi-Cloud e Hybrid-Cloud.

Dependendo das necessidades da organização, às vezes surgiu a necessidade de realizar processos de computação e/ou armazenamento simultaneamente com diferentes provedores de nuvem, o que traz a possibilidade de manter as operações mesmo em caso de falha de um provedor de nuvem. Além do uso de múltiplos provedores de nuvem, a organização também pode precisar utilizar infraestrutura interna adicional para atender às necessidades específicas da empresa.

O uso de múltiplos provedores de nuvem ou a combinação de infraestrutura interna com múltiplos provedores de nuvem traz desafios adicionais em termos de custo, complexidade e segurança. Tradicionalmente, na esteira desses tipos de arquiteturas, a organização assume responsabilidades que pertencem aos provedores de nuvem em uso de nuvem única, por exemplo, garantir o intercâmbio seguro de informações entre os provedores e regiões, garantir a consistência dos dados, garantir disponibilidade alta e garantir escalabilidade adequada de recursos.

O principal objetivo deste guia é fornecer uma visão geral de padrões arquitetónicos de nuvem híbridos e múltiplas, explorando suas fraquezas e forças, e com base nessa informação, construir um conjunto de objetivos de segurança que a organização deve seguir para utilizar nuvem híbrida e múltipla de forma segura com informações classificadas com marca NACIONAL RESERVADO.

Conceitos Chave

Nesta seção é feita uma descrição de cenários Multi-Cloud e Hybrid-Cloud, juntamente com padrões arquiteturais que são comuns a esses cenários. Para cada cenário é construída uma lista de considerações, que detalha as vantagens e os desafios de cada cenário. A informação apresentada nesta seção visa servir de base para o desenho dos requisitos de segurança.

Considerações

Responsabilidade entre provedores *cloud*

Quando são utilizadas arquiteturas multi-cloud, uma maior responsabilidade é transferida para a organização, uma vez que a manutenção da replicação de dados, das chaves de encriptação e dos respetivos mecanismos passa a ser da responsabilidade da própria organização. Cada fornecedor de serviços em nuvem é apenas responsável por proteger os dados que são armazenados e processados dentro dos seus centros de dados, sendo que qualquer comunicação com outro fornecedor de nuvem se torna responsabilidade da organização.

A responsabilidade entre diferentes nuvens, neste sentido, refere-se à divisão de tarefas e de responsabilidades entre vários fornecedores de serviços em nuvem relativamente às ações que estão a ser executadas. Isto pode envolver aspetos de segurança, desempenho, governação e responsabilidades operacionais.

- Modelos de Serviço Divergentes: Cada fornecedor de nuvem oferece diferentes formas de construir aplicações (ou seja, diferentes serviços, APIs e meios de configuração). Gerir e aplicar responsabilidades de forma uniforme em ambientes diversos — como a formulação de políticas de segurança, controlo de acesso e permissões — é complexo e normalmente específico de cada fornecedor.
- Confusão na Responsabilidade Partilhada: Cada fornecedor de nuvem opera segundo o seu próprio modelo de responsabilidade partilhada. Em ambientes multi-cloud, estes modelos podem diferir entre fornecedores, o que pode levar a que a organização fique responsável e vulnerável a possíveis falhas de segurança ou sistemas mal configurados. Gerir as regulamentações de conformidade de forma consistente entre diferentes nuvens pode também originar lacunas de

segurança e violações regulatórias, dado que cada fornecedor tem os seus próprios controlos de segurança e certificações/requisitos de conformidade.

- Gestão de Rede e Latência: Uma arquitetura multi-cloud exigirá, na maioria dos casos, conectividade de rede entre diferentes nuvens, o que introduz latência e outros potenciais problemas de encaminhamento de tráfego. Gerir métricas de qualidade de serviço em ambientes multi-cloud pode ser complexo devido à variação da latência, largura de banda e configurações necessárias.»

Custo e Complexidade

Os custos e a complexidade são questões predominantes para as organizações ao implementarem arquiteturas multi-cloud.

Os custos podem aumentar devido aos diferentes modelos de faturação dos respetivos fornecedores de serviços em nuvem, onde ativos e/ou recursos podem ficar sem monitorização ou ser esquecidos (ou seja, levando a um aumento contínuo dos custos), bem como pela ocorrência de transferências de dados de e para um determinado fornecedor de nuvem, algo que ocorrerá inevitavelmente em virtude dos requisitos, políticas e/ou procedimentos da organização. Esta variabilidade nas transferências e no volume dos dados transferidos pode levar a um aumento dos custos, tendo em conta o tipo de taxa de acesso, tipo de armazenamento e modelo de faturação do fornecedor de nuvem.

A complexidade é outro problema predominante, devido à natureza complexa dos ambientes multi-cloud. Quando se consideram diferentes fornecedores de nuvem, o vendor lock-in (dependência de fornecedor) em funcionalidades e/ou dependências específicas é previsível. Isto complica os procedimentos que as organizações devem adotar para manter a interoperabilidade de serviços e redes, o que pode introduzir sobrecarga e complexidade adicional.

O reforço da segurança numa arquitetura multi-cloud é também uma tarefa complexa, devido à variabilidade na forma como os mecanismos internos são desenvolvidos por cada fornecedor. Por exemplo, diferentes fornecedores de nuvem utilizam diferentes formatos de registos (logs); por isso, a organização poderá ter de os processar e normalizar antecipadamente para um formato comum e padronizado, de modo a garantir capacidades de depuração e resposta a incidentes de forma independente da tecnologia utilizada. Para manter a interoperabilidade da rede em toda a arquitetura, as organizações podem recorrer

a serviços e/ou funcionalidades disponibilizados através das APIs dos fornecedores de nuvem, de forma a oferecer capacidades agnósticas de modo centralizado. Dependendo dos requisitos da organização, esta tarefa pode não ser trivial e pode introduzir complexidade, sobrecarga e custos adicionais, mas permite à organização avaliar os fluxos ponta a ponta entre diferentes fornecedores.

Transparência de Processos

Quando uma arquitetura multi-cloud é implementada, alguns procedimentos que antes eram simples e transparentes para a organização podem tornar-se complexos e exigir maior intervenção da mesma. Procedimentos como a encriptação de dados em repouso e a gestão de chaves, que anteriormente eram automáticos, passarão a requerer intervenção manual.

- Cifra: A organização será responsável pela gestão da orquestração da encriptação dos dados em repouso e pela encriptação dos dados em trânsito durante as transferências entre fornecedores de nuvem. De acordo com o modelo de responsabilidade partilhada, os fornecedores de nuvem são apenas responsáveis pela gestão da segurança dos dados que residem na sua própria infraestrutura.
- Orquestração: Uma vez que cada fornecedor de nuvem opera de forma diferente, a organização será responsável por gerir a disponibilidade dos recursos e pela correta gestão desses mesmos recursos.
- Gestão de Identidades: Uma gestão adequada de identidades é fundamental para uma implementação segura em nuvem. Como cada fornecedor de nuvem funciona de forma distinta, as permissões e atribuições de funções variam, o que aumenta a complexidade na gestão do princípio do menor privilégio e na atribuição de privilégios equivalentes a um utilizador em cada fornecedor. A responsabilidade de gerir a base de dados de identidades e garantir a sua disponibilidade cabe também à organização.

Cloud Híbrida

A Nuvem Híbrida (Hybrid Cloud) incorpora a utilização de infraestruturas de nuvem pública em conjunto com a infraestrutura interna da organização, de forma a disponibilizar funcionalidades específicas aos utilizadores. Este mecanismo permite que uma organização tire partido das propriedades de hyper-scaling da nuvem pública para

processar grandes volumes de pedidos, tratar conjuntos de dados complexos, realizar balanceamento de carga (load balancing) ou implementar proteções contra ataques DDoS. A conectividade entre a nuvem pública e a infraestrutura interna pode ser estabelecida através de TLS/HTTPS ou de VPN, sendo que esta última permite expor redes privadas virtuais na nuvem à infraestrutura interna da organização.

As nuvens públicas podem também ser utilizadas devido à maturidade e facilidade de uso dos serviços que disponibilizam, o que acelera o desenvolvimento de protótipos e simplifica a manutenção. De forma geral, numa arquitetura de Nuvem Híbrida, a infraestrutura interna da organização (nuvem privada) é usada para armazenar informação sensível e processar pedidos de autenticação, tornando a nuvem privada o ativo mais crítico para a continuidade do negócio. A utilização de um fornecedor de serviços em nuvem permite uma alta disponibilidade, tanto no acesso dos utilizadores como em termos de capacidade de processamento, possibilitando à organização escalar conforme a procura. A utilização de nuvens privadas permite um controlo rigoroso sobre tarefas críticas, executadas em infraestrutura sob controlo direto da organização.

Fornecedores de serviços em nuvem, como a AWS, podem também disponibilizar hardware que replica os serviços da nuvem pública, permitindo que uma organização utilize serviços de nuvem dentro da sua própria infraestrutura (por exemplo, AWS Outposts). Estas soluções permitem que as organizações utilizem serviços de nuvem com informação altamente classificada, uma vez que esses dados não saem da infraestrutura da própria organização

Padrões de arquitetura *cloud* híbrida

A arquitetura de Nuvem Híbrida varia consoante os objetivos da organização. No entanto, é possível identificar alguns padrões de arquitetura híbrida que permitem a uma organização conceber de forma mais eficaz a sua própria arquitetura.

Arquitetura orientada a recuperação/backup

Nesta arquitetura, a principal função da nuvem secundária é fornecer um meio para armazenar e obter informações relacionadas com os procedimentos de cópia de segurança (backup), como parte das práticas de backup 3-2-1 offsite. Nesta abordagem, a

organização transfere os dados de backup para a nuvem secundária e, em caso de falha, os dados armazenados nessa nuvem serão utilizados no processo de recuperação.

Arquitetura de Autenticação Federada

Neste padrão arquitetónico, a nuvem privada ou a infraestrutura da organização é utilizada para fornecer serviços de identidade, que serão usados pelos outros fornecedores de nuvem para autenticar os seus utilizadores. Neste cenário, a nuvem privada ou a infraestrutura da organização torna-se o ponto único de falha no processo de autenticação; contudo, obtém-se um aumento no controlo de acesso, uma vez que a autenticação é realizada numa infraestrutura controlada pela própria organização.

Arquitetura de balanceamento de carga

Implementar os componentes de front-end existentes da aplicação em vários fornecedores de nuvem, mantendo os componentes de back-end da aplicação nas instalações locais (on-premises).

Cloud Bursting

Aproveitar *implementações* redundantes de aplicações em vários fornecedores de nuvem, com uma infraestrutura on-premises capaz de agrupar tarefas ou cargas de trabalho pelos diferentes ambientes de nuvem provisionados.

Arquitetura baseada em eventos/entrega de conteúdos

Utilizando um modelo produtor/consumidor, os brokers podem ser distribuídos por vários fornecedores de nuvem, fornecendo uma base para a produção e disseminação de informação, que pode ser organizada entre diferentes fornecedores de nuvem (inter-cloud) ou por nó individual (intra-cloud).

Considerações sobre a *cloud* híbrida

Devido à utilização de nuvens/infraestruturas privadas e públicas, as organizações obtêm controlo adicional sobre a localização dos dados, permitindo decidir quais os dados que permanecem *on-premises* e quais os dados que são armazenados na nuvem. A utilização de Nuvens Híbridas pode também aumentar a disponibilidade de recursos e reduzir a latência de acesso, aproveitando a dispersão geográfica da nuvem pública e as suas elevadas capacidades computacionais e de rede.

No entanto, o aumento da complexidade de gestão pode também gerar riscos de segurança se a arquitetura da nuvem híbrida não for concebida com a segurança em mente. Adicionalmente, a gestão de infraestruturas privadas e públicas aumenta os custos.

Multi-Cloud

Multi-Cloud refere-se à utilização de vários fornecedores de nuvem para fornecer uma funcionalidade, seja ela exposta aos clientes (por exemplo, balanceamento de carga para aumentar a resiliência e disponibilidade), ou mais interna (por exemplo, criar uma cópia da infraestrutura como backup passivo que, em caso de falha da nuvem primária, permite que o backup retome a operação).

O principal objetivo de uma infraestrutura multi-cloud é garantir uma recuperação de desastres robusta, resiliência e alta disponibilidade que não dependam de um único fornecedor de nuvem. O multi-cloud pode ser visto como um mecanismo para assegurar a continuidade do negócio, mesmo em caso de falha parcial ou total de um fornecedor de nuvem, ou bloqueios causados por algum problema operacional (por exemplo, perda de acesso ou bloqueio temporário a recursos). Além disso, uma arquitetura multi-cloud permite a migração para outros fornecedores de nuvem sem períodos adicionais de indisponibilidade.

Como demonstrado, a arquitetura multi-cloud é um mecanismo útil para aumentar a disponibilidade e resiliência da organização, mesmo em situações de falha parcial ou total de um fornecedor de nuvem, ou quando um erro de software ou humano causa um bloqueio temporário das contas da organização junto do fornecedor de nuvem.

Padrões Arquiteturais em Multi-Cloud

As arquiteturas multi-cloud variam de acordo com os objetivos da organização. No entanto, é possível identificar alguns padrões de arquitetura multi-cloud que permitem a uma organização conceber e otimizar melhor a sua própria arquitetura.

Arquitetura baseada em resiliência

Em casos específicos, o principal objetivo de uma organização é manter a continuidade das operações mesmo em caso de falha de um fornecedor de nuvem, recorrendo a outro fornecedor como backup, com tempo de inatividade mínimo.

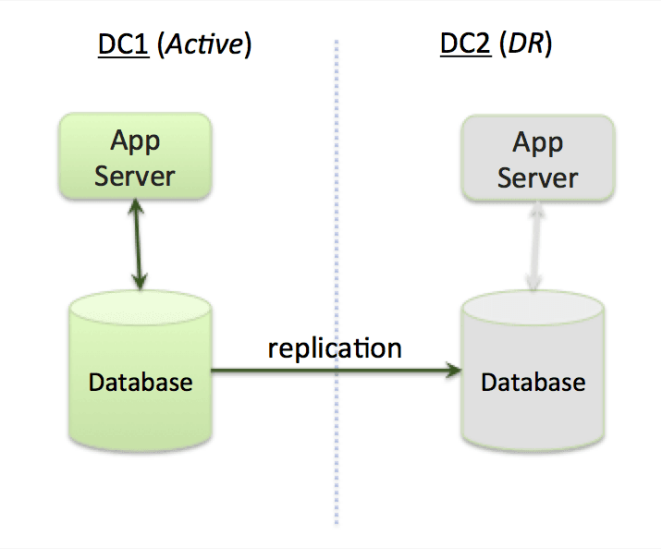
A organização pode também utilizar a nuvem de backup em simultâneo com a nuvem primária, de modo a aumentar o desempenho e a capacidade de resposta aos pedidos dos utilizadores. A partir deste conceito, é possível definir dois tipos de arquiteturas baseadas em resiliência: **ativa-passiva** e **ativa-ativa**.

Ativo-Passivo

Neste cenário arquitetónico, a nuvem primária é utilizada para responder aos pedidos dos utilizadores, e as alterações de informação (por exemplo, escritas em bases de dados) são sincronizadas com a nuvem passiva. Se for detetado um problema na nuvem ativa, a nuvem passiva é ativada, e os pedidos dos utilizadores passam a ser encaminhados para esta.

A seleção entre nuvem ativa e passiva pode ocorrer ao nível do DNS ou do balanceador de carga, e o acionamento da comutação pode ser automático ou manual. Recomenda-se que o acionamento seja automático, de forma a garantir alta disponibilidade e continuidade do negócio.

A arquitetura Ativa-Passiva permite uma redução de custos quando comparada com o cenário Ativo-Ativo, uma vez que os recursos computacionais podem permanecer desligados e ser ativados apenas quando necessário.



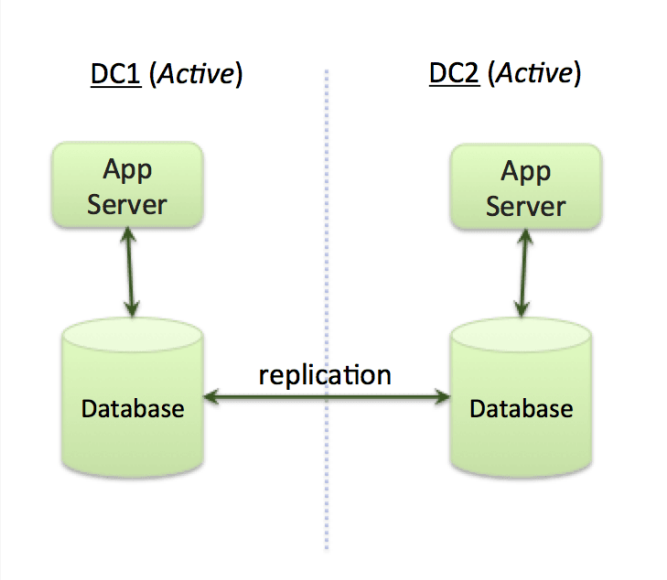
Ativo-Ativo

Neste cenário arquitetónico, as nuvens primária e secundária funcionam em conjunto para responder aos pedidos dos utilizadores. As alterações de informação são sincronizadas entre os fornecedores de nuvem para evitar perdas de dados. Caso seja detetado um problema na nuvem primária, a nuvem secundária assume a resposta aos pedidos dos utilizadores.

A sincronização entre as nuvens é mais complexa e exige que os sistemas de base de dados consigam manter uma sincronização master-master com latências aceitáveis.

Em termos de custos, tanto a nuvem primária como a secundária devem estar totalmente operacionais, o que aumenta os custos e acrescenta complexidade adicional na gestão da sincronização de dados.

A arquitetura Ativa-Ativa é recomendada apenas quando a organização necessita de desempenho combinado das duas nuvens e de tempos de comutação reduzidos em caso de falha da nuvem primária.



Arquitetura Composta

Implementar aplicações ou cargas de trabalho existentes em vários fornecedores de nuvem, podendo a topologia adotada consistir na implementação de réplicas ou de aplicações/cargas de trabalho distintas, conforme os requisitos da organização.

Arquitetura centralizada "broker/orquestrador"

Uma forma de conceber uma arquitetura multi-cloud é em torno de um broker ou orquestrador centralizado, que fornece uma visão unificada dos recursos disponíveis nas várias nuvens. A centralização permite que a organização detete falhas e orquestre remediações automáticas para manter a disponibilidade dos sistemas. A orquestração centralizada é normalmente fornecida por uma entidade terceira, externa aos fornecedores de nuvem.

Com uma orquestração centralizada, a organização pode selecionar os fornecedores de nuvem que serão responsáveis por cada componente da sua infraestrutura, aumentando a flexibilidade. Se dois ou mais fornecedores de nuvem forem utilizados para disponibilizar um mesmo componente, a tolerância a falhas é também aumentada.

Um exemplo de arquitetura centralizada é a utilização de Kubernetes em múltiplas nuvens, com a orquestração realizada on-premises ou por um terceiro externo aos fornecedores de nuvem, responsável pela gestão dos Kubernetes jobs e pods.

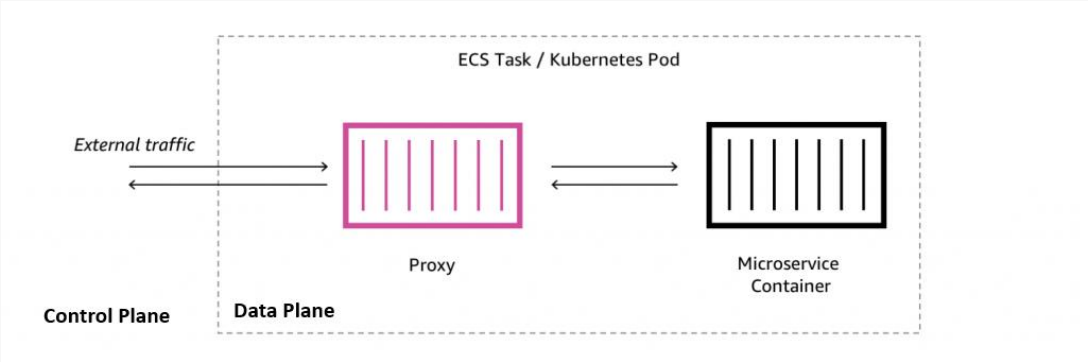
Arquitetura decentralizada

Arquitetura em que os recursos, capacidades e/ou poder computacional são distribuídos por vários fornecedores de nuvem ou nós. Os padrões de design descentralizado devem ser considerados tendo em conta as restrições aplicacionais existentes e de que forma essas restrições podem conduzir a falhas da aplicação num ambiente descentralizado.

Para este tipo de arquiteturas, é crucial que as organizações contextualizem as suas capacidades e requisitos, de modo a compreenderem da melhor forma como devem ser estabelecidas as relações entre cada fornecedor de nuvem e/ou as redes on-premises. É igualmente essencial que a organização reconheça o aumento da responsabilidade e a necessidade de separação de responsabilidades ao conceber uma arquitetura multi-cloud ou híbrida (**OP.APP**).

Arquitetura service mesh

Arquitetura utilizada para gerir micro-serviços implementados de forma independente através de um plano de controlo unificado, garantindo a aplicação consistente de políticas de segurança, a gestão do tráfego e a observabilidade em todos esses serviços.



Exemplos:

- Service Mesh Federado: Utilizando ferramentas de terceiros (por exemplo, Istio ou Linkerd), é possível gerir planos de controlo individualmente por fornecedor de nuvem. A comunicação entre clusters pode então ser estabelecida entre diferentes fornecedores de nuvem através de gateways de malha (mesh gateways). Desta forma, as capacidades computacionais e responsabilidades podem ser descentralizadas, mantendo-se, contudo, um controlo centralizado com autonomia local.
- Service Mesh Plano: Tratar os serviços distribuídos por vários fornecedores de nuvem como se estivessem numa topologia plana, em que um único plano de controlo é acessível a todos os fornecedores de nuvem suportados (por exemplo, **Istio**). Isto permite uma abstração em que cada fornecedor de nuvem executa o seu próprio plano de dados, enquanto o plano de controlo aplica uma gestão centralizada com roteamento unificado de tráfego, garantindo comunicação entre nuvens com menor latência.
- Split/Multi Service Mesh: Implementar um plano de controlo e um plano de dados separados entre vários fornecedores de nuvem ou por fornecedor de nuvem, de forma a garantir que cada fornecedor possa operar de forma autónoma e independente. Podem ser utilizadas APIs ou gateways de malha (mesh gateways) para assegurar a comunicação entre diferentes nuvens.

Padrões de arquitetura decentralizada baseada em capacidade

Padrões arquitetónicos baseados na capacidade desejada e/ou na relação custo-eficácia, como particionar e distribuir dados em *shards*, de forma que cada nó ou fornecedor de nuvem seja responsável por um subconjunto dos dados totais (por exemplo,

particionamento de *shards* por regiões geográficas). Outra possibilidade é a arquitetura Shared Nothing, em que cada nó ou serviço opera completamente de forma independente, sem partilhar quaisquer recursos. No entanto, se for necessária coordenação entre os nós, a complexidade pode aumentar devido à sobrecarga de coordenação. Ambos os cenários podem ser implementados utilizando Cassandra, MongoDB ou Amazon DynamoDB. Para bases de dados relacionais, o CockroachDB também pode ser considerado.

Considerações Multi-Cloud

As implementações multi-cloud aumentam a disponibilidade de recursos e reduzem a dependência de um único fornecedor de nuvem, o que aumenta a flexibilidade da organização. Adicionalmente, podem ser usadas para aumentar a soberania e controlo sobre os dados, uma vez que, dependendo da implementação, nenhum fornecedor de nuvem tem acesso completo à informação.

No entanto, o aumento da complexidade de gestão, aliado ao custo adicional associado à operação de múltiplos fornecedores de nuvem, pode ser uma desvantagem. As implementações multi-cloud também exigem trabalho adicional por parte da organização para garantir uma orquestração adequada e visibilidade completa. O registo de eventos (logging) é feito por nuvem, sendo necessários sistemas capazes de ingerir e processar múltiplas fontes de logs.

Requisitos de Segurança

adyta

Requisitos de Segurança

A presente seção contém a lista de requisitos que a organização deve cumprir, subdividida por cada controlo de segurança. Cada controlo possui uma representação em código (por exemplo, OP.INV.1), que permite referenciar requisitos individuais ao longo do documento.

[OP.INV] Inventário de Ativos

Em arquiteturas complexas, como arquiteturas híbridas e multi-cloud, é essencial dispor de mecanismos adequados para inventários de ativos. Inventários de ativos apropriados permitem que a organização tenha uma visão geral dos ativos provisionados, sejam eles recursos em nuvem ou componentes da infraestrutura interna, e determine a necessidade da existência desses ativos. Adicionalmente, os ativos podem ser etiquetados no inventário como contendo informação classificada, aumentando a visibilidade sobre a exposição de informação sensível na infraestrutura.

Para cumprir o presente requisito, a organização deve:

- Realizar, de forma regular, inventários de ativos em todas as nuvens e na infraestrutura interna em uso.
- Etiquetar os ativos que contêm ou processam informação classificada;
- Eliminar os ativos que não sejam mais necessários.

[OP.IAM] Identidade e Controlo de Acessos

A Identidade e Controlo de Acesso são os componentes mais importantes para proteger o acesso a recursos ou a gestão desses recursos. O acesso não autorizado pode levar à divulgação de informação e a outros problemas de segurança.

Recomenda-se que a gestão de identidades seja centralizada em cenários complexos, como arquiteturas híbridas ou multi-cloud, com o objetivo principal de evitar a configuração de identidades em múltiplos locais. A gestão centralizada de identidades simplifica a administração e permite a eliminação adequada das identidades.

O controlo de acesso deve estar ligado à gestão centralizada de identidades, e as permissões atribuídas a utilizadores ou contas de serviço devem ser mínimas e limitadas ao propósito da conta.

Para cumprir o presente requisito, a organização deve:

- Centralizar a gestão de identidades, mantendo pelo menos uma cópia (carbon copy) armazenada noutros fornecedores de nuvem, sendo que esta cópia deve ser apenas para leitura;
- Atribuir permissões a utilizadores ou contas de serviço com base no princípio do menor privilégio, garantindo que cada permissão tenha uma justificação de negócio válida;
- Garantir que as permissões sejam definidas por fornecedor de nuvem e consistentes entre todos os fornecedores de nuvem;
- Proteger as contas de utilizador com palavras-passe seguras e autenticação multifator (MFA);
- Proteger as contas de serviço, sempre que disponíveis, com chaves de acesso temporárias. Caso não sejam suportadas ou disponíveis chaves temporárias, deve ser emitido um token de API para a conta de serviço, que deve ser eliminado assim que deixar de ser necessário.

[OP.NET] Segurança em Rede

A segurança de rede permite que uma organização proteja o seu perímetro externo. Em cenários híbridos e multi-cloud, o perímetro de rede é expandido a toda a infraestrutura em nuvem e privada em uso, incluindo toda a interconectividade entre elas. Dependendo do caso de uso, todas as infraestruturas de nuvem podem ser integradas numa rede virtual comum utilizando tecnologias como VPNs site-to-site, reduzindo a complexidade do diagrama lógico da rede. Como as comunicações entre nuvens normalmente ocorrem pela Internet, é necessário garantir a confidencialidade e autenticidade das comunicações para evitar a captura de informação sensível ou classificada por terceiros maliciosos.

Para cumprir o presente requisito, a organização deve:

- Minimizar a exposição dos ativos ao mínimo possível através de regras de firewall restritivas (por exemplo, limitar a exposição de portas, IPs de acesso e comunicações de saída permitidas);
- Utilizar VPNs ou APIs seguras para comunicações entre nuvens;
- Aplicar protocolos de comunicação seguros para comunicações de entrada e saída (por exemplo, HTTPS, (D)TLS e SSH);

- Aplicar proteções de segurança nas camadas 3/4 (por exemplo, mecanismos Anti-DDoS);
- Aplicar proteções de segurança na camada 7 (por exemplo, Web Application Firewalls – WAFs).

[OP.STO] Armazenamento

Os procedimentos de armazenamento seguro permitem que as organizações protejam os dados em repouso, prevenindo a divulgação de informação, mesmo em infraestruturas partilhadas, como as nuvens públicas. Em cenários híbridos e multi-cloud, e dependendo do caso de uso, os dados armazenados num fornecedor de nuvem podem necessitar de ser replicados ou partilhados com outro fornecedor de nuvem, o que acarreta desafios adicionais.

Em primeiro lugar, a proteção dos dados armazenados deve ser estendida para quando estes são transportados entre fornecedores de nuvem, como parte de processos de replicação ou partilha, o que impõe os seguintes desafios:

- Os dados precisam estar encriptados em repouso em cada fornecedor de nuvem. Assim, quando os dados precisam ser replicados, devem ser desencriptados antes do envio ou a chave de encriptação deve ser partilhada com o destino.
  A primeira solução aumenta a sobrecarga e pode aumentar a latência associada ao processo de replicação/partilha de dados. A segunda solução pode ser impossível se forem utilizadas chaves geradas por KMS, que é o mecanismo recomendado.

Para cumprir o presente requisito, a organização deve:

- Utilizar encriptação em repouso (at-rest) em todos os recursos que lidem com informação classificada;
- As chaves de encriptação utilizadas para armazenar dados em repouso devem ser armazenadas no KMS do fornecedor de nuvem. A chave usada para encriptar os dados deve ser única para cada fornecedor de nuvem e, se possível, única para cada ficheiro armazenado;
- Quando for necessária replicação ou partilha de dados, o canal de comunicação utilizado deve ser confidencial, íntegro e autêntico. Podem ser utilizados protocolos como HTTPS, TLS, DTLS e SSH;

- Os dados replicados/partilhados devem ter validações de integridade para garantir a transferência correta da informação. Podem ser usados métodos como assinaturas digitais ou métodos de encriptação com validação de integridade (por exemplo, AES-GCM);
- Armazenar a informação classificada de forma segregada da informação não classificada. Deve ser criada uma conta independente em cada fornecedor de nuvem para armazenar apenas informação classificada.

[OP.CRI] Criptografia e Proteção de Dados

A criptografia é um dos principais mecanismos para garantir propriedades de segurança comprováveis numa solução. É utilizada para proteger a confidencialidade da informação partilhada, permitir a validação da integridade, não repúdio e autenticidade da informação. Os protocolos criptográficos permitem a proteção dos dados em trânsito e em repouso. A criptografia deve ser utilizada para garantir a segurança das comunicações em arquiteturas multi-cloud e híbridas.

Para cumprir o presente requisito, a organização deve:

- Utilizar algoritmos de encriptação simétrica para proteger os dados em trânsito e em repouso. O algoritmo deve ser AES e a chave de encriptação deve ter 256 bits;
- Utilizar algoritmos de encriptação assimétrica para assinaturas digitais, estabelecimento de canais de comunicação e encriptação de chaves simétricas. Os algoritmos devem ser RSA com 4096 bits ou curvas elípticas EC-256 ou superiores. Recomenda-se a utilização de algoritmos pós-quânticos para maior segurança futura (referência: USA DoD - Post Quantum Algorithms);
- Utilizar canais de comunicação seguros, como (D)TLS e HTTPS, garantindo o uso de TLS versão 1.2 ou superior.

[OP.CAT] Categorização dos Dados

Conforme identificado no Guia Geral para a utilização segura de serviços *cloud* o GNS é responsável por classificar a informação utilizando a marca Nacional. Quando uma informação é classificada, os requisitos necessários para garantir a sua proteção mudam, incluindo os locais onde os dados podem ser armazenados e as metodologias de armazenamento, acesso e processamento dessa informação.

Para cumprir o presente requisito, a organização deve:

- Utilizar apenas fornecedores de nuvem certificados para armazenar informação classificada com a classificação Nacional Reservado (incluindo backups);
- Não armazenar informação com classificações superiores a Nacional Reservado em nenhum fornecedor de nuvem, salvo autorização prévia e explícita da GNS;
- Segregar o armazenamento, processamento e controlo de acesso relacionado com o acesso, armazenamento e processamento de informação classificada, limitando o acesso a utilizadores autorizados.

[OP.APP] Segurança Aplicacional

Com base na distribuição de responsabilidades, a gestão de ambientes multi-cloud/híbridos recai sobre a organização, uma vez que cada fornecedor de nuvem é responsável apenas pela gestão da sua própria infraestrutura e serviços. As aplicações precisam ser concebidas e implementadas de forma a suportar arquiteturas híbridas/multi-cloud, o que aumenta o risco de que uma vulnerabilidade ou erro de programação possa causar interrupções na implementação multi-cloud/híbrida, reduzindo a resiliência e, em alguns casos, provocando dessincronização e períodos de indisponibilidade.

Recomenda-se que, durante o ciclo de vida de desenvolvimento de software (SDLC), as organizações incluam SAST (Static Application Security Testing) e DAST (Dynamic Application Security Testing) nos ambientes de desenvolvimento e staging, de forma a identificar erros e vulnerabilidades antes da implementação em produção.

Para cumprir o presente requisito, a organização deve:

- Para cada software desenvolvido internamente, incluir testes SAST no SDLC;
- Para todos os softwares que suportem operações multi-cloud/híbridas, realizar testes DAST em cada atualização, incluindo testes de fuzzing de input;
- Realizar análises de segurança internas regulares e um teste de penetração anual, utilizando uma entidade externa como fornecedor dos testes;
- Efetuar monitorização ao nível da aplicação para detetar problemas e permitir uma resposta ágil.

[OP.REC] Recuperação e Resiliência

As capacidades de recuperação e resiliência permitem que as organizações resistam e recuperem de interrupções inesperadas, mantendo um nível de serviço aceitável. Conforme referido nas Diretrizes Gerais, estas capacidades devem ser concebidas com base nos métricos RTO (Recovery Time Objective) e RPO (Recovery Point Objective), previamente definidos (conforme NIST 800-53), considerando todas as decisões organizacionais ou de negócio e a natureza e frequência de utilização dos dados.

Para cumprir o presente requisito, a organização deve:

- Garantir que a periodicidade dos backups está alinhada com os objetivos de RPO definidos, considerando latências e tempos de conclusão impostos pela estratégia de backup predefinida, incluindo possíveis atrasos decorrentes da frequência dos backups;
- Garantir que os procedimentos de backup respeitam as mesmas restrições expressas em OP.STO, assumindo a classificação de dados subjacente e os requisitos de armazenamento (OP.CAT);
- Garantir a versão e capacidades de rollback, bem como as restrições expressas em OP.REC.2.1 nas Diretrizes Gerais, relativamente ao contexto, localidade e níveis de disponibilidade;
- Assegurar que as capacidades de replicação e resiliência estão alinhadas com os requisitos da organização, definindo a estratégia ótima de implementação para garantir tolerância a falhas e continuidade do negócio;
- Definir políticas de retenção e ciclo de vida por níveis com base no caso de uso e nos tipos de armazenamento, podendo estas políticas ser verificadas e revistas através de ferramentas de otimização de custos para avaliar a estratégia ideal.

  Exemplo para *backups*:

  - Considerar armazenamento rápido (hot/fast storage) para backups que exijam RPO/RTO rigorosos;
  - Utilizar armazenamento frio (cold storage) para retenção a longo prazo ou backups não críticos;

- Definir períodos de retenção com base nos tipos de armazenamento definidos:
    - Retenção mínima para backups em hot storage;
    - Retenção intermédia para backups em cold storage;
    - Retenção máxima para backups em archive storage;
- Elaborar políticas e procedimentos de ciclo de vida para mover dados entre períodos de retenção de backup, garantindo eficiência de custos.

[OP.MON] Monitorização

As capacidades de monitorização permitem que as organizações coletem e analisem sistematicamente métricas e dados do sistema, garantindo que os sistemas funcionam conforme esperado, que problemas ou desvios são identificados e facilitando a tomada de decisões, contribuindo para a continuidade do negócio.

As capacidades de monitorização são particularmente importantes em arquiteturas multi/híbridas, uma vez que manter taxas de utilização de recursos consistentes e controladas é crucial para operações contínuas e custo-efetivas.

Para cumprir o presente requisito, a organização deve:

- Garantir capacidade de logging para cada fornecedor de nuvem utilizado, incluindo logs de acesso, autenticação e alterações de configuração, configurados de acordo com os períodos de retenção baseados na classificação da informação subjacente. Logs de serviços que utilizem informação confidencial devem ser armazenados por pelo menos 3 anos;
- Promover e configurar uma segregação adequada de contas e controlo de acesso para armazenamento e acesso aos logs, garantindo que, no mínimo, os logs sejam acessíveis apenas a utilizadores autorizados (por exemplo, criar uma conta isolada por fornecedor de nuvem dedicada ao armazenamento de logs, conforme os requisitos da organização);
- Garantir que a organização seja capaz de monitorizar o consumo de recursos, permitindo rastrear a utilização de recursos por cada fornecedor de nuvem durante operações normais;

- Com as capacidades de monitorização configuradas, garantir a definição de quotas de recursos bem definidas e limites de utilização, de modo a provisionar alarmes e mecanismos de notificação;
- Garantir que não só alarmes de utilização de recursos estejam implementados, mas também mecanismos de notificação para alterações em sistemas ou dados nos fornecedores de nuvem que possam impactar a confidencialidade, integridade e/ou autenticidade da organização.

Sempre que possível, a organização deve considerar, quando aplicável, a consolidação da telemetria, garantindo um "single pane of glass" para monitorização. Se atingível, isto forneceria uma stack centralizada e custo-efetiva, capaz de processar, triagem e alertar a organização sobre eventos, independentemente de onde o evento foi iniciado, ou seja, on-premises, híbrido ou multi-cloud.

Na prática, esta integração pode não ser trivial devido à variabilidade nos formatos de logs e nas ferramentas usadas por cada fornecedor de nuvem. Por isso, pode ser importante considerar o uso de agregadores e ferramentas de gestão de logs (por exemplo, ELK, Splunk), realizando parsing e normalização dos logs quando estes forem enviados através de fronteiras, bem como um hub centralizado de monitorização onde todos os logs da organização sejam entregues para análise. Os formatos de logs devem ser padronizados, utilizando logs compatíveis com todos os fornecedores de nuvem (por exemplo, OCSF).

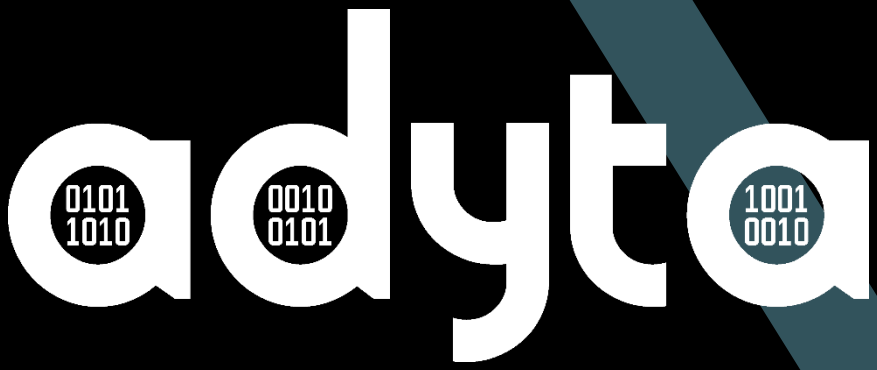
Neste contexto, é fundamental que as organizações assegurem, sempre que possível, um formato de logging padronizado em todos os componentes (on-premises, híbrido e/ou multi-cloud). Isto permite simplificar a análise de dados e a deteção de insights, garantir conformidade com requisitos regulatórios (por exemplo, uma única fonte de verdade) e facilitar resolução de problemas, alertas e capacidades de reporting.

[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 aumentar as capacidades gerais dos respetivos sujeitos, de acordo com o âmbito definido do processo de formação. Os planos de formação geralmente são elaborados com base nas competências e conhecimentos que os indivíduos devem possuir para desempenhar eficazmente o seu papel profissional na organização.

Para cumprir o presente requisito, a organização deve:

- Implementar a formação do pessoal em temas de cibersegurança, com foco em segurança na nuvem, incluindo considerações específicas para cenários multi/híbridos, e assegurar a realização de formação anual em cibersegurança.



Obrigado pela confiança

*Este documento está marcado como **PÚBLICO**, o que significa que a informação contida neste documento pode ser partilhada sem prejuízo para a organização.*

www.adyta.pt

U.PORTO Spin-off