QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA

Centro Nacional de Cibersegurança

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia

QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA

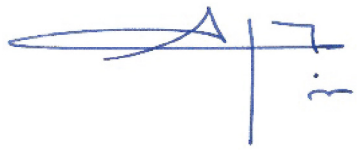
Centro Nacional de Cibersegurança

1 Prefácio

A segurança digital das entidades públicas e privadas do nosso país é uma prioridade. Sem um elevado nível de maturidade em Cibersegurança nas nossas organizações, não estão reunidas as condições para um efetivo e sustentável desenvolvimento económico. Neste contexto, as medidas preventivas e, em particular, a conformidade com as melhores práticas, são aquelas que melhor contribuem para este ambiente desejado.

Neste enquadramento, o Centro Nacional de Cibersegurança reuniu o conjunto das melhores práticas num **Quadro Nacional de Referência para a Cibersegurança**, o qual permite às organizações reduzir o risco associado às ciberameaças, disponibilizando as bases para que qualquer entidade possa, de uma forma voluntária, cumprir os requisitos mínimos de segurança das redes e sistemas de informação, nas suas diversas componentes. Designadamente, na identificação, proteção, deteção, resposta e recuperação a ciberincidentes, incluindo a organização necessária para a sua gestão.

Com uma estrutura simples e clara, este documento pretende servir de guia para decisores e técnicos das organizações. Desta forma, convidamos toda a comunidade a adotar este **Quadro Nacional de Referência para a Cibersegurança**, contribuindo assim para um desenvolvimento económico sustentável.



António Gameiro Marques

Autoridade Nacional de Segurança

Lino Santos

Coordenador do Centro Nacional de Cibersegurança

ÍNDICE

2 Sumário Executivo

A consciencialização das organizações para a temática da segurança das redes e dos sistemas de informação nunca foi tão relevante como é hoje em dia. A cada ano que passa, existe um maior número de dispositivos conectados entre si através da internet, alguns deles mal protegidos ou mal configurados, que acabam por se traduzir em **ameaças aos ativos das organizações**.

A cibersegurança, em todas as suas vertentes, é uma preocupação central nas sociedades atuais. Um ambiente seguro é fundamental para estabelecer e desenvolver qualquer atividade económica ou social. No entanto, a segurança não deve ser a protagonista. Pelo contrário, deve existir para libertar os cidadãos e as empresas de preocupações, de modo a que se possam focar nas suas atividades.

Em alinhamento com a Lei n.º 46/2018, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, este documento tem como missão providenciar às organizações um **guia de cibersegurança** que sistematiza um conjunto de medidas para as problemáticas mais relevantes da atualidade nesta matéria. Pretende disponibilizar as bases para uma organização cumprir os **requisitos mínimos de segurança da informação** recomendados.

Sabendo que as organizações se podem encontrar em diferentes níveis de maturidade e possuir diferentes dimensões (desde micro e pequenas organizações a grandes empresas ou instituições públicas), e que algumas recomendações podem ser desproporcionalmente exigentes para a dimensão da organização ou não ser suficientemente exigentes, sugere-se que o documento seja interiorizado com espírito crítico por cada organização e adequado às suas necessidades.

Está estruturado num conjunto de medidas de segurança que traduzem cinco objetivos específicos: **Identificar**, **Proteger**, **Detetar**, **Responder** e **Recuperar**.

São referenciados exemplos e orientações que permitem sistematizar processos e procedimentos cuja aplicação conduza ao cumprimento desses mesmos objetivos, não na forma de uma lista de controlo de ações a realizar, mas antes na representação dos objetivos chave reconhecidos pelos diversos intervenientes como uma referência de alto nível, assente num conjunto de referenciais internacionais e em diferentes normas técnicas.

Os objetivos são divididos em categorias e subcategorias, sendo que para cada subcategoria este documento referencia um exemplo de implementação tecnológica, de implementação processual e de evidência, consistindo numa descrição genérica de como poderá ser aplicado, contribuindo, desse modo, para uma melhor compreensão do mesmo.

Este documento termina com um conjunto de recomendações adicionais, fundamentais para que as organizações possam cumprir, por um lado, com a legislação em vigor, e por outro possam de forma efetiva estar preparadas, através da definição de uma estratégia que envolva toda a organização, para **gerir o risco** e **mitigar o impacto dos incidentes** que poderão afetar as organizações.

1

Introdução

3.1 Enquadramento

É realidade aceite que uma parcela significativa da nossa economia, assim como do bem-estar social, se encontram consubstanciadas em infraestruturas e serviços disponibilizados no ciberespaço. No presente documento, entendemos o ciberespaço como sendo um ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas e redes e sistemas de informação. Este ambiente complexo e heterogéneo oferece novas possibilidades e oportunidades. No entanto, em igual medida, lança a base para a criação de um novo espaço de ameaça e risco com a ocorrência de incidentes que podem trazer impactos económicos e sociais que não podem ser negligenciados.

Estes incidentes de segurança informática podem não impactar apenas o enquadramento cibernético, estendendo o seu alcance a infraestruturas físicas que suportem serviços críticos ou essenciais ao pleno funcionamento da sociedade.

Na era digital em que vivemos, as infraestruturas funcionam baseadas na premissa de que os elementos tecnológicos são robustos e fiáveis e que tecnologias emergentes e complexas (por exemplo: *IoT, Cloud Computing, Big Data*) têm o potencial para oferecer uma elevada flexibilidade e eficiência na comunicação e coordenação de serviços e processos. Mas este uso crescente de tecnologias de informação também significa que estas se tornam mais **vulneráveis** a atividades ilícitas e maliciosas e a processos de manutenção operacionais mal planeados.

Figura 1 - Intervenientes subjacentes às atividades maliciosas

São variadas as motivações subjacentes às atividades maliciosas que podem ser concretizadas por **terroristas**, **criminosos**, **ativistas** ou **nações estrangeiras**. O impacto de um incidente varia num espectro alargado, com graus de severidade diferentes, desde a indisponibilidade de um sítio institucional, com eventual impacto reputacional, até à redução da capacidade de defesa de um país, a perdas financeiras ou mesmo de vidas humanas.

Numa outra perspetiva, uma gestão adequada dos riscos relacionados com incidentes de cibersegurança pode revelar-se também em oportunidades de melhoria na qualidade dos serviços prestados, na adoção de novas práticas, no desenvolvimento de novos produtos ou serviços e na melhoria da reputação das organizações.

Em 2016, foi aprovada a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a **garantir um elevado nível comum de segurança** das redes e dos sistemas de informação em toda a União (Diretiva SRI). A Diretiva SRI visa assegurar que os operadores de serviços essenciais e os prestadores de serviços digitais tomam as medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações e que notificam as autoridades competentes ou as CSIRT (Equipas de Resposta a Incidentes de Segurança Informática), sem demora injustificada, dos incidentes com um

impacto relevante na continuidade dos serviços essenciais por si prestados.

Com a Diretiva SRI, pretendeu-se criar-se o enquadramento legal para a legislação dos Estados-Membros no domínio da cibersegurança e fornecer bases para desenvolver uma **cultura de cibersegurança** em setores vitais para a economia dos Estados-Membros e para o correto funcionamento da sociedade, setores esses que dependem fortemente das redes e sistemas de informação. Assim, o Anexo II da referida Diretiva prevê os seguintes setores de operadores de serviços essenciais: energia, transportes, bancário, infraestruturas do mercado financeiro, saúde, fornecimento e distribuição de água potável e infraestruturas digitais. O Anexo III foca os seguintes prestadores de serviços digitais: serviços de computação em nuvem, serviços de mercado em linha e serviços de motor de pesquisa em linha.

No entanto, ainda **carecemos de abordagens adequadas** que apoiem e facilitem a cooperação rápida e eficaz entre operadores de serviços essenciais e prestadores de serviços digitais, quer em termos de troca de informações específicas sobre incidentes, quer na partilha de informações sobre riscos e ameaças. Além disso, existe um défice na captura e correlacionamento de eventos e informações associadas a ataques cibernéticos a infraestruturas, para além de que as ferramentas existentes não fornecem orientação técnica adequada aos profissionais de resposta a incidentes sobre como detetar, investigar e reproduzir ataques.

Como tal e, apesar da importância socioeconómica das ferramentas e técnicas para lidar com incidentes, ainda não existe uma maneira fácil, estruturada, padronizada e confiável de gerir e prever incidentes inter-relacionados de cibersegurança, de uma maneira que tenha em conta a heterogeneidade e complexidade do incidente e os tipos de ataques cada vez mais sofisticados. Portanto, há uma **necessidade urgente de criar novos sistemas** para o tratamento eficiente de incidentes e apoiar a compreensão completa e comum de situações de ataques cibernéticos em tempo útil.

As próprias ameaças ao ciberespaço, como potenciais incidentes, não devem comprometer todos os benefícios que as redes e sistemas de informação potenciam na nossa sociedade. A resposta a uma ameaça ou incidente não deverá ser, por isso, encarada apenas numa perspetiva de indisponibilização de um determinado serviço digital afetado, mas deve ser sistemática e focada também na prevenção e na sensibilização de todos os intervenientes, sejam eles cidadãos, organizações públicas e privadas, ou o país em geral.

O Quadro Nacional de Referência para a Cibersegurança, doravante denominado QNRCS, pretende ser uma ferramenta à disposição da sociedade para apoio a essa resposta sistemática. Esta resposta está igualmente alinhada com a Lei n.º 46/2018, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva SRI.

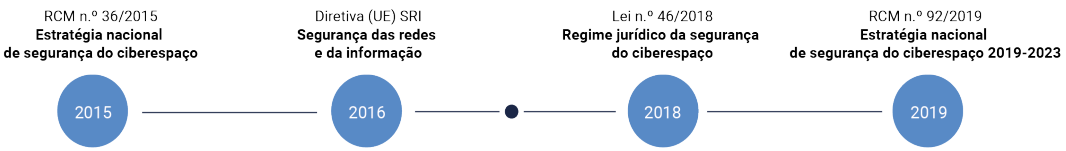


Figura 2- Enquadramento Cronológico

Adicionalmente, o QNRCS dá cumprimento à Estratégia Nacional de Segurança do Ciberespaço, na sua versão atual, aprovada através da Resolução do Conselho de Ministros n.º

92/2019 de 23 de maio[1]. **A Estratégia funda-se no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas.** A Estratégia alicerça-se em três princípios, os quais o QNRCS pretende endereçar da seguinte forma:

a. Subsidiariedade: o QNRCS pretende ser uma ferramenta transversal a todas as organizações intervenientes no ciberespaço, desde os operadores privados até ao Estado, enquanto responsável por garantir a soberania e os princípios constitucionais;
b. Complementaridade: sendo o QNRCS transversal, propõe um conjunto de medidas alargadas e integradoras que têm como objetivo potenciar a consciencialização entre todos os atores intervenientes no ciberespaço e a posição que ocupam no mesmo;
c. Proporcionalidade: no QNRCS, ao longo dos objetivos de segurança, propõe-se a adequação das medidas à organização, quanto à sua aplicabilidade, dimensão, setor de atividade e caraterização dos riscos identificados.

Ter uma visão holística, quer de pessoas, quer de infraestrutura de equipamentos dedicados à temática da segurança e que consiga seguir as medidas propostas no QNRCS, requer um investimento em três pilares. Primeiro, na criação da figura do **CISO**, como responsável máximo da segurança da informação dentro da organização, em segundo, com a constituição de um **SOC**, para dotar a organização das instalações e equipas de suporte necessárias e, em terceiro, da constituição de uma equipa especializada de resposta a incidentes que pode operar nas instalações do SOC, ou seja, a criação da função **CSIRT**. No último capítulo do documento apresentam-se recomendações adicionais, com o objetivo de clarificar estes três pilares e a sua importância nas organizações.

3.2 Objetivos

O contexto da ameaça de cibersegurança deve ser encarado através de uma abordagem sistematizada que tenha por objetivo a **sensibilização das organizações** públicas e privadas.

Neste processo coletivo de crescente sensibilização, é fundamental uma mudança de paradigma materializada por via da definição de **linhas orientadoras de um sistema de processos e procedimentos**, nem sempre de caráter tecnológico, que possa constituir uma linguagem comum, transversal aos diversos setores de atividade e que promova a convergência de práticas conducentes a uma melhor cibersegurança das organizações.

O QNRCS consubstancia-se numa visão homogénea e inclusiva da realidade organizacional (pública e privada) portuguesa, no que diz respeito à necessidade de implementação de medidas de identificação, proteção, deteção, resposta e recuperação contra as ameaças que possam colocar em causa a **segurança das suas redes e sistemas de informação** e, desta forma, da sua informação.

A elaboração do QNRCS tem em consideração, enquanto documento enquadrador legislativo no ordenamento jurídico nacional, o exposto na Lei nº 46/2018, de 13 de agosto, que define o regime jurídico da segurança do ciberespaço.

[1] https://dre.pt/application/conteudo/122498962

O QNRCS não pretende constituir-se como uma norma de cibersegurança, mas sim como uma referência que permita identificar as normas, padrões e boas práticas existentes em vários domínios da segurança da informação. A sua aplicação nas organizações é voluntária e passível de ser adaptada, por forma a melhor endereçar necessidades específicas inerentes ao seu setor, dimensão ou qualquer outro aspeto distintivo que caracterize a organização.

A estrutura central do QNRCS foi definida numa perspetiva de **ciclo de vida da gestão da cibersegurança** de uma organização, tendo em atenção os aspetos humanos, tecnológicos e processuais, com especial enfoque nos processos e procedimentos da gestão do risco.

Uma característica intrínseca do risco é o facto de este não poder ser totalmente eliminado, tornando-se fundamental a concretização de uma estratégia global da organização, para garantir a implementação de um processo eficaz de gestão do risco.

Este é um processo contínuo de **identificação**, **diagnóstico** e **resposta**, sendo que, para que seja possível gerir o risco, as organizações devem compreender a probabilidade de um determinado evento ocorrer, bem como os seus potenciais impactos adversos e vulnerabilidades existentes. Conhecendo esta informação, qualquer organização pode determinar o seu nível aceitável do risco e, desta forma, promover a resiliência da sua atividade enquanto prestador de bens ou serviços. A esta informação corresponde a perceção de tolerância ao risco, condição sine qua non para a priorização das atividades realizadas no âmbito da cibersegurança.

3.3 Estrutura do documento

O documento encontra-se estruturado com uma parte inicial onde se efetua uma introdução ao QNRCS, identificando-se os seus objetivos, o seu contexto, a sua aplicabilidade e as definições das terminologias utilizadas. Explana-se igualmente a temática da gestão do risco, cujo entendimento se considera enriquecedor para enquadramento e melhor perceção do QNRCS.

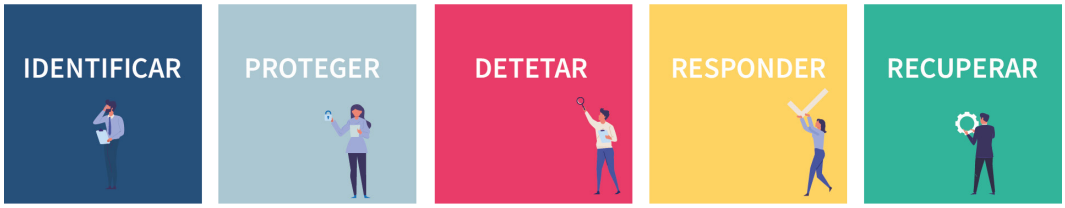


Figura 3- Objetivos de Segurança

No capítulo "Apresentação do Quadro Nacional de Referência para a Cibersegurança" apresentam-se os diversos objetivos do QNRCS: **Identificar**, **Proteger**, **Detetar**, **Responder** e **Recuperar**. Estes objetivos estão organizados por categorias e subcategorias temáticas onde se explanam medidas técnicas e processuais, bem como evidências de implementação que permitam às organizações melhorar a sua capacidade de proteção e de resposta aos desafios do ciberespaço e da segurança da informação.

No final do documento, apresenta-se o papel do CISO (Responsável de Segurança de Informação), que se considera uma posição importante na organização. É sobre o CISO que deve recair a gestão do ciclo de vida das temáticas da segurança da informação e cibersegurança. Reflete-se igualmente sobre a CSIRT (Equipa de Resposta a Incidentes de Segurança Informática) e o SOC (Centro de Operações de Segurança), quais os seus objetivos, a sua constituição e, ainda, sobre a importância da partilha de informação sobre incidentes de cibersegurança com as partes interessadas da organização.

3.4 Definições e Abreviaturas

3.4.1 Definições

Na tabela seguinte, identificam-se os termos utilizados ao longo do documento, cuja definição importa apresentar. Sempre que aplicável, são usados termos definidos em normas ou legislação nacional em vigor. Na coluna "Origem" é indicada a norma ou legislação onde o termo se encontra definido. Sempre que este é definido no âmbito do QNRCS, a coluna "Origem" é preenchida com a respetiva sigla.

TERMO	DEFINIÇÃO	ORIGEM
Aceitação do risco	Decisão de aceitar a persistência de um risco residual após o tratamento do risco.	Decisão do Conselho n.º 2013/488/EU
Ameaça	Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização.	ISO/IEC 27032
Atividade	Processo ou conjunto de processos executados por uma organização (ou em sua representação) que produz ou suporta um ou mais produtos e serviços.	NP EN ISO 22301
Ativo	Qualquer coisa que tenha valor para uma organização.	ISO/IEC 22000
Ativo crítico	Ativo que suporta pelo menos um serviço essencial.	QNRCS
Ciberespaço	Ambiente complexo de valores e interesses materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas e redes e sistemas de informação.	ENSC
Cibersegurança	Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.	ENSC
Ciberdefesa	Atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço.	ENSC
Cibercrime	Factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa.	ENSC
Código de Hamming	O código de Hamming é um código de bloco linear. A sua utilização permite a transferência e armazenamento de dados de forma segura e eficiente, bem como detetar erros nas transferências e recuperação de bits até ao valor de redundância usado.	QNRCS

TERMO	DEFINIÇÃO	ORIGEM
Confidencialidade	A propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas, ou segundo processos não autorizados.	ISO/IEC 27000
Continuidade do negócio	Capacidade da organização para continuar a fornecer produtos ou serviços a níveis aceitáveis pré-definidos, na sequência de um incidente disruptivo.	NP EN ISO 22301
Disponibilidade	Propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada.	ISO/IEC 27000
Documento	Informação e respetivo meio de suporte (exemplo não constante na NP EN ISO 22301: papel, magnético, eletrónico ou unidade de armazenamento de computador, fotografia ou amostra de referência).	NP EN ISO 22301
Entrega Contínua	Abordagem ao processo de engenharia de software, no âmbito da qual se produz código em ciclos curtos, o que permite um alinhamento estreito com metodologias ágeis.	QNRCS
Equipa de resposta a incidentes de segurança informática	A equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma organização, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação.	Lei 46/2018
Especificação técnica	Um documento que define os requisitos técnicos que um produto, processo, serviço ou sistema devem cumprir.	Lei 46/2018
Exercício	Processo para formar, avaliar, praticar e melhorar o desempenho de uma organização.	NP EN ISO 22301
Framework	Modelo de referência.	NP ISO/IEC 27001
Fornecedor	Organização ou pessoa que fornece um produto (sendo produto, o resultado de um processo).	NP EN ISO 9000
Gestão de Topo	Pessoa ou grupo de pessoas que dirige e controla uma organização ao mais alto nível.	NP EN ISO 22301
Gestão do risco	Atividades coordenadas para dirigir e controlar uma organização, no que respeita ao risco.	NP EN ISO 22301
Honeypot	Mecanismo de criação de um sistema que potencia um provável atacante a incorrer numa ação ilegítima, que poderia resultar num incidente. É um recurso criado propositadamente para ser sondado, atacado e comprometido. Um dos seus principais objetivos é o de permitir a monitorização do comportamento dos atacantes.	QNRCS
Incidente	Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação.	Lei 46/2018
Infraestrutura crítica	A componente, sistema ou parte deste, situado em território nacional, que é essencial para a manutenção de funções vitais para a sociedade, saúde, segurança e o bem-estar económico ou social, cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções.	Lei 46/2018

TERMO	DEFINIÇÃO	ORIGEM
Integração Contínua	Prática de engenharia de software que promove a consolidação de código numa cadência curta, tipicamente diária, tendo por objetivo simplificar o processo de integração das várias peças produzidas.	QNRCS
Integridade	A propriedade de salvaguardar o caráter exato e completo da informação e dos ativos.	ISO/IEC 27000
Internet	Sistema global de redes interconectadas e de domínio público.	ISO/IEC 27032
Acordo de nível de serviço	Acordo documentado entre a organização e o cliente, que identifica serviços e o seu desempenho acordado.	ISO/IEC 20000
Norma	Uma especificação técnica, aprovada por um organismo de normalização reconhecido para aplicação repetida ou continuada, cuja observância não é obrigatória.	Lei 46/2018
Melhoria contínua	Atividade recorrente com vista a incrementar a capacidade para satisfazer requisitos.	NP EN ISO 9000
Operador de infraestrutura crítica	Uma entidade pública ou privada que opera uma infraestrutura crítica.	Lei 46/2018
Operador de serviços essenciais	Uma entidade pública ou privada que presta um serviço essencial.	Lei 46/2018
Organização	Pessoa ou conjunto de pessoas que tem as suas próprias funções com responsabilidades, autoridades e relações para atingir os seus objetivos.	NP EN ISO 22301
Parte Interessada	Pessoa ou organização que pode afetar, ser afetada por, ou considerar-se como sendo afetada por uma decisão ou atividade. Pode ser um indivíduo ou um grupo que tem um interesse em qualquer decisão ou atividade de uma organização.	NP EN ISO 22301
Plano da continuidade do negócio	Procedimentos documentados que orientam as organizações para responder, recuperar, retomar e restaurar um nível pré-definido de operacionalização, após disrupção.	NP EN ISO 22301
Política	Intenções e orientação de uma organização, conforme formalmente expressas pela sua gestão de topo.	NP EN ISO 22301
Ponto de troca de tráfego	Uma estrutura de rede que permite a interligação de mais de dois sistemas autónomos independentes, a fim de facilitar a troca de tráfego na Internet.	Lei 46/2018
Prestador de serviços digitais	Uma pessoa coletiva que presta um serviço digital.	Lei 46/2018
Prestador de serviços do sistema de nomes de domínio	Uma entidade que presta serviços do sistema de nomes de domínio (DNS) na Internet.	Lei 46/2018
Processo	Conjunto de atividades interrelacionadas ou interatuantes que transformam entradas em saídas.	NP EN ISO 22301
Procedimento	Modo especificado de realizar uma atividade ou um processo.	NP EN ISO 22301
Rede e sistema de informação	Qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações eletrónicas que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção.	Lei 46/2018

TERMO	DEFINIÇÃO	ORIGEM
Registo de nomes de domínio de topo	Uma entidade que administra e opera o registo de nomes de domínio da Internet de um domínio de topo específico.	Lei 46/2018
Registo	Documento que expressa resultados obtidos ou fornece evidência das atividades realizadas.	NP EN ISO 22301
Representante	Uma pessoa singular ou coletiva, estabelecida na União Europeia, expressamente designada para atuar por conta de um prestador de serviços digitais não estabelecido na União Europeia, que pode ser contactada por uma autoridade competente nacional ou por uma CSIRT, em representação do prestador de serviços digitais, quanto às obrigações que incumbem a este último.	NIS 2016/1148
Risco	Uma circunstância ou um evento razoavelmente identificável, com um efeito adverso potencial na segurança das redes e dos sistemas de informação.	Lei 46/2018
Segurança das redes e dos sistemas de informação	A capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, integridade, disponibilidade, autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através dos mesmos.	Lei 46/2018
Serviço de computação em nuvem	Um serviço digital que permite o acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis.	Lei 46/2018
Serviço de mercado em linha	Um serviço digital que permite aos consumidores ou aos comerciantes celebrarem contratos de venda ou de prestação de serviços por via eletrónica com comerciantes, quer no sítio na Internet do mercado em linha, quer no sítio na Internet de um comerciante que utilize os serviços de computação disponibilizados pelo mercado em linha.	Lei 46/2018
Serviço de motor de pesquisa em linha	Um serviço digital que permite aos utilizadores consultarem todos os sítios na Internet, ou sítios na Internet numa determinada língua, com base numa pesquisa sobre qualquer assunto e que fornece ligações onde podem ser encontradas informações relacionadas com o conteúdo solicitado.	Lei 46/2018
Serviço crítico	Serviço de suporte aos processos chave de uma organização.	QNRCS
Serviço digital	Um serviço da sociedade da informação prestado à distância, por via eletrónica.	Lei 46/2018
Serviço essencial	Um serviço essencial para a manutenção de atividades societais ou económicas cruciais, que dependa de redes e sistemas de informação, e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço.	Lei 46/2018
Sistema de gestão	Conjunto de elementos inter-relacionados ou interatuantes de uma organização para o estabelecimento de políticas, objetivos e de processos para atingir esses objetivos.	NP EN ISO 22301
Sistema de nomes de domínio (DNS)	Um sistema de nomes distribuídos hierarquicamente numa rede, que encaminha pesquisas sobre nomes de domínio.	Lei 46/2018

TERMO	DEFINIÇÃO	ORIGEM
Sistema Legado	Sistema obsoleto que permanece em operação na organização.	QNRCS
Tratamento de incidentes	Todos os procedimentos de apoio à deteção, análise, contenção e resposta a um incidente.	Lei 46/2018
Tolerância ao risco	Disposição da organização ou das partes interessadas para assumirem o risco após o seu o tratamento, por forma a poderem alcançar os seus objetivos.	ISO/IEC 22300
Verificação cíclica de redundância	Método de deteção de erros normalmente usado em redes digitais e dispositivos de armazenamento, para detetar uma mudança acidental em cadeias de dados.	QNRCS
Vulnerabilidade	Fraqueza de um ativo ou de um controlo que pode ser explorada por uma ameaça.	ISO/IEC 27032
Zona desmilitarizada	Rede de perímetro (igualmente conhecida como sub-rede rastreável) que se insere como uma "zona neutra" entre redes.	ISO/IEC 27033

Tabela 1 – Definições

3.4.2 Abreviaturas

ABREVIATURA	DEFINIÇÃO
AVAC	Aquecimento, ventilação e ar condicionado.
CCTV	Closed-circuit television – Circuito fechado de televisão.
CD	Continuous Delivery – Entrega contínua.
CI	Continuous Integration – Integração contínua.
CIS	Center for Internet Security – Centro de segurança para a internet.
CISO	Chief Information Security Officer – Responsável de Segurança de Informação.
COBIT	Control Objectives for Information and Related Technologies – Objetivos de controlo para informações e tecnologias relacionadas.
COO	Chief Operations Officer – Responsável das Operações.
CRC	Cyclic Redundancy Check – Verificação cíclica de redundância.
CSC	Critical Security Controls – Controlos críticos de segurança.
CSIRT	Computer Security Incident Response Team – Equipa de Resposta a Incidentes de Segurança Informática.
CVE	Lista de registos que contêm um número de identificação, uma descrição e, pelo menos, uma referência pública para vulnerabilidades de segurança.
DLP	Data Loss Prevention – Prevenção de perda de informação.
DMZ	Demilitarized Zone – Zona desmilitarizada.
DNS	Domain Name System – Sistema de resolução de nomes de domínio.
ENSC	Estratégia Nacional de Segurança do Ciberespaço 2019-2023.
IDS	Intrusion Detection System – Sistema de deteção de intrusões.
IoT	Internet of Things – Internet das coisas.
IP	Internet Protocol – Protocolo de comunicações.
IPS	Intrusion Prevention System – Sistema de prevenção de intrusões.
ISACA	Information Systems Audit and Control Association – Associação de auditoria e controlo de sistemas de informação.

ABREVIATURA	DEFINIÇÃO
ISO	International Organization for Standardization – Organização internacional de normalização.
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission – Organização internacional de normalização/Comissão eletrotécnica internacional.
MITRE	Base de dados de vulnerabilidades mantida por organização não governamental Norte-americana, internacionalmente reconhecida como a líder nesta matéria.
NIST	National Institute of Standards and Technology – Instituto Nacional de Padrões e Tecnologia (Norte-americano).
QNRCS	Quadro Nacional de Referência para a Cibersegurança.
RACI	***Responsible*** – Responsável, ***Accountable*** – Aprovador, ***Consulted*** – Consultado e ***Informed*** – Informado. Matriz de atribuição de Responsabilidades.
SOC	***Security Operations Center*** – Centro de Operações de Segurança.
SRI	Segurança das Redes e da Informação.
SWOT	***Strengths*** – Forças, ***Weaknesses*** – Fraquezas, ***Opportunities*** – Oportunidades, ***Threats*** – Ameaças.
VPN	*Virtual Private Network* – Rede privada virtual.
SGSI	Sistema de Gestão de Segurança da Informação.
TI	Tecnologias de Informação.
UPS	*Uninterruptible Power Source* – Unidade de alimentação ininterrupta.
WAF	*Web Application Firewall* – Firewall de aplicações web.
WWW	*World Wide Web* – Rede mundial de computadores.

Tabela 2 - Abreviaturas

3.5 Gestão do Risco

3.5.1 Introdução

O QNRCS propõe uma implementação processual orientada à gestão do risco, que permite às organizações a tomada de decisão de forma priorizada e informada, no contexto da cibersegurança. Estas decisões devem, sempre, estar igualmente orientadas à garantia da confidencialidade, disponibilidade e integridade na prestação do bem ou serviço para uma determinada organização. Neste âmbito, entende-se risco como uma circunstância ou um evento identificável, com um efeito adverso potencial na segurança das redes e dos sistemas de informação.

Neste contexto, são propostas várias abordagens ao processo de avaliação periódica dos riscos e de aferição da forma como estes se relacionam no âmbito da prestação de um bem ou serviço. O resultado destas avaliações deve permitir à organização caracterizar a situação atual, definir objetivos e elencar um conjunto de ações que fomentem uma evolução positiva da sua situação no contexto da cibersegurança. Assim, o QNRCS permite, a quem o aplica, que escolha e direcione ao longo do tempo as melhorias pretendidas na gestão dos riscos.

A gestão do risco, quando efetuada de forma sistematizada e numa lógica de melhoria, é uma prática que permite às organizações identificar, quantificar e estabelecer as prioridades face a critérios de aceitação do risco e objetivos relevantes para a organização.

A gestão do risco de uma organização pode ser entendida como a gestão da incerteza e determinação das ações necessárias, para que esta possa ser minimizada para níveis considerados aceitáveis por parte da organização. É um exercício sistematizado, no âmbito do qual a organização identifica possíveis ameaças que possam construir sobre as vulnerabilidades dos ativos, bem como quais os níveis do risco associado, avaliando-se a probabilidade de ocorrência e possíveis impactos.

A ISO/IEC 31000[1] disponibiliza um conjunto de princípios e de orientações genéricas sobre gestão do risco para as organizações. Por outro lado, a ISO/IEC 27005[2] especifica orientações e processos para gestão do risco de segurança dos sistemas de informação de uma organização, suportando-se, em particular, nos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI), implementado de acordo com a norma ISO/IEC 27001[3].

A ISO/IEC 27005 não fornece uma metodologia específica para a gestão dos riscos de segurança da informação. Cabe às organizações definirem qual a sua abordagem para a gestão dos riscos. Em geral, a metodologia de gestão do risco ISO/IEC 27005, por ser direcionada a sistemas de informação, pode ser aplicável a todos os tipos de organização.

A segurança da informação tem como preocupação primária a proteção dos ativos da organização contra ameaças internas e externas, sendo estas categorizadas de acordo com o potencial dano que possam causar aos ativos a proteger.

---

1 NP ISO/IEC 31000 – Gestão do Risco – Linhas de orientação

2 ISO/IEC 27005 – Information Technology – Security techniques – Information security risk management

3 NP ISO/IEC 27001 – Tenologia de Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos

No domínio da segurança, é dada maior atenção às ameaças relacionadas com atividades maliciosas ou de origem humana. A figura em baixo, retirada da norma ISO/IEC 27032[4], ilustra esses conceitos e relações de alto nível.

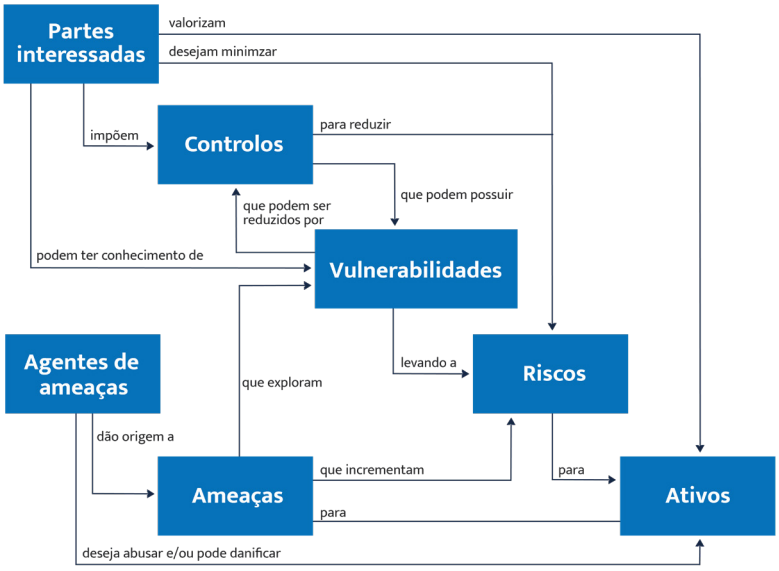


Figura 4 - Fonte: ISO/IEC 27032, Conceitos básicos e relações de alto nível

Tal como será explicado mais à frente neste capítulo de gestão do risco, o plano de tratamento dos riscos é executado tendo por base a avaliação realizada pela organização sobre riscos identificados, no âmbito do processo de análise. Existem quatro opções disponíveis para tratamento do risco: Evitar, Aceitar, Mitigar e Transferir.

Para todos os riscos cuja opção de tratamento tenha sido a mitigação, a organização deverá elaborar um plano de tratamento que identifique os constrangimentos e eventuais dependências, prioridades atuais da organização, prazos de execução, recursos necessários e o caminho crítico da implementação de medidas de mitigação.

As medidas processuais e de caráter técnico a implementar poderão ser identificadas tendo por base o QNRCS e o enquadramento do risco, devendo ainda ter por objetivo a redução do nível do risco, ao ponto em que este possa ser considerado aceitável pela organização.

3.5.2 Enquadramento

Tal como se pode observar na figura seguinte, a Gestão do Risco em Segurança da Informação baseada na norma ISO/IEC 27005, é composta pelas seguintes fases: Estabelecer Contexto (1), o Levantamento do Risco (2) - que inclui a identificação (2.1), análise (2.2) e avaliação do risco (2.3) -, a fase de tratamento do risco (3), de aceitação do risco (4), dando-se depois sequência às fases de comunicação e consulta (5) e de monitorização e revisão do risco (6).

[4] ISO/IEC 27032 – Information Technology – Security techniques – Guidelines for cybersecurity

Figura 5 - Fonte: ISO/IEC 27005, Fases da gestão do risco

No presente capítulo, iremos densificar cada uma das fases indicadas, seguindo as diretrizes da norma ISO/IEC27005, culminando com um exemplo prático da aplicabilidade da gestão de um risco.

3.5.3 Estabelecer Contexto

Organização na gestão do risco

A organização deverá identificar quais os recursos humanos e materiais necessários para poder garantir a correta execução de todo o processo de gestão do risco. A organização deverá:

- Definir uma metodologia de gestão do risco que seja adequada para a realidade da organização;
- Efetuar a identificação das partes interessadas internas e externas;
- Identificar o modelo de governo a aplicar na gestão do risco e definir um processo de escalonamento apropriado;
- Definir os papéis e responsabilidades, internos e externos, na gestão do risco e atribuir os mesmos aos recursos humanos elegíveis. Alguns exemplos desses papéis, são:

    - Gestor do risco – Elemento responsável pelo processo de gestão do risco;
    - Membro da equipa de gestão do risco – Elemento participante no processo de gestão do risco. Poderá ser um responsável de ativos, de departamento ou representante de uma parte interessada relevante;
- Identificar uma ferramenta para suportar a gestão e o tratamento do risco;
- Definir e identificar quais os registos a criar e a manter (por exemplo: atas de reuniões, plano de acompanhamento da análise do risco, relatórios de progresso).

Todas estas decisões devem ser analisadas e aprovadas pela gestão de topo da organização.

Abordagem à gestão do risco

Na sequência do ponto anterior, a organização deverá, igualmente, identificar os recursos necessários para:

- Poder definir e implementar as políticas, processos e procedimentos no âmbito da gestão e tratamento do risco;
- Poder efetuar o levantamento e o plano de tratamento dos riscos;
- Poder efetuar a monitorização dos controlos implementados;
- Poder efetuar o acompanhamento da eficácia da implementação do plano de tratamento do risco.

Critérios de avaliação do risco

Os critérios de avaliação do risco devem ser identificados para se avaliar a relevância do risco na organização, considerando-se:

- O valor estratégico dos processos referentes à atividade da organização;
- A criticidade dos ativos de informação envolvidos;
- A importância operacional e comercial em termos de confidencialidade, integridade e disponibilidade da informação;
- A expectativa e as perceções das partes interessadas.

Podem ser identificados critérios de avaliação adicionais, que poderão suportar a priorização do tratamento dos riscos.

Critérios de impacto

A organização deverá definir quais os níveis de impacto que deverão suportar a sua gestão do risco. O critério de impacto deve ser determinado em termos de grau de danos ou custos que um evento de segurança da informação tem para a organização.

Na identificação dos níveis de impacto a assignar aos riscos, a organização deverá ter em atenção os seguintes indicadores:

- Importância e classificação dos ativos de informação;
- Falhas na segurança de informação, avaliando-se em termos de confidencialidade, integridade e disponibilidade da informação;
- Custos para a organização;
- Disrupção de planos e prazos;
- Danos de reputação.

Critérios de aceitação do risco

A organização deve definir quais são os seus critérios de aceitação do risco. Deverá identificar a partir de que nível do risco terá de ser necessária a aprovação da gestão de topo, para que o mesmo possa ser aceite.

A organização deve definir as suas próprias escalas de níveis de aceitação dos riscos. Na definição dos critérios de aceitação do risco, a organização deve ter em consideração os seguintes pontos:

- Os critérios de aceitação podem incluir diversos limites, existindo um nível do risco aceitável, sendo que a aceitação dos riscos acima desse nível deve ser formalmente aprovada pela gestão de topo;

- Os critérios de aceitação podem incluir requisitos para o futuro tratamento adicional. Por exemplo, o risco pode ser aceite se existir aprovação e compromisso de se tomar medidas que possibilitem a sua redução para níveis aceitáveis dentro de um período de tempo, acordado e estipulado em sede de gestão do risco;

- Os critérios de aceitação podem diferir de acordo com o seu tempo de vida. Por exemplo, o risco pode estar associado a uma atividade temporária ou de curto prazo, da organização.

Os critérios de aceitação devem ser estabelecidos considerando-se os seguintes fatores:

- Fatores inerentes à atividade;
- Fatores operacionais;
- Fatores tecnológicos;
- Fatores financeiros;
- Fatores sociais e humanitários.

Definição de âmbito e fronteiras

A organização deverá definir o âmbito e as fronteiras do seu sistema de gestão do risco de segurança e organização da informação. A definição do âmbito é relevante, tendo em conta que é necessário garantir que todos os ativos relevantes para a organização sejam incluídos na fase de levantamento.

A definição dos pontos fronteira é igualmente importante, para que a organização consiga endereçar os riscos que podem ser identificados através dessas mesmas fronteiras.

Ao definir o âmbito ou as fronteiras da gestão do risco, a organização deve ter em linha de conta:

- Os seus objetivos estratégicos de negócio;
- Os processos referentes à sua atividade;
- As suas funções e estrutura interna;
- A sua política de segurança da informação;
- As expetativas das suas partes interessadas;
- O seu ambiente sociocultural;
- Os seus ativos de informação.

Exemplos da definição de âmbito para um processo de gestão do risco podem ser:

- Edifício/Localização;
- Plataforma de infraestrutura;
- Plataforma aplicacional;
- Processos referentes à atividade da organização.

O que não estiver incluído no âmbito deverá ser formalmente justificado pela organização.

3.5.4 Identificação do risco

A fase de identificação é a primeira fase da etapa de levantamento dos riscos. Nesta fase, dever-se-á identificar, reconhecer e descrever os riscos que possam criar constrangimentos ou impedir a organização de atingir os seus objetivos.

O propósito da identificação é determinar as ocorrências que poderão causar uma potencial perda à organização. Os passos descritos nas próximas etapas são essenciais para se efetuar a coleta de dados para alimentar a análise do risco.

Identificação dos ativos

A organização deve identificar quais os ativos que suportam o âmbito definido na gestão do risco de segurança da informação. Os ativos são tudo o que tem valor e que requer proteção na ótica da organização.

Os ativos poderão ser (mas não só) das seguintes categorias:

- Tecnológicos (hardware, software);
- Dispositivos de rede;
- Pessoas;
- Localizações, (etc.).

A organização deve ter um inventário dos seus ativos com, pelo menos:

- O número de inventário do ativo;
- Uma descrição das funções dos mesmos;
- A identificação do responsável;
- A sua localização;
- Categoria ou tipo.

Esta informação deverá ser acrescida de:

- Classificação do ativo de acordo com a sua criticidade para a organização;
- Identificação dos processos referentes à atividade da organização que os ativos suportam;
- Identificação de dependências com outros ativos.

Identificar ameaças

Uma ameaça tem o potencial de poder criar impactos e consequências negativas nos ativos da organização. Adicionalmente, esta pode ser de origem natural ou humana e pode ser acidental ou deliberada.

A informação relativa à identificação de ameaças pode ser obtida das seguintes formas:

- Revisão de incidentes ocorridos;
- Responsáveis pelo ativo;
- Utilizadores;

- Especialistas de segurança da informação;
- Especialistas de segurança física;
- Departamentos legais;
- Catálogo de ameaças.

A experiência adquirida pela organização na gestão e aprendizagem com incidentes e nas avaliações de ameaças anteriores deve ser tida em conta na avaliação do risco atual.

Pode ser relevante para a organização consultar outros catálogos (eventualmente, específicos da sua área de atuação) para completar a lista de ameaças genéricas.

Identificar controlos

A organização deverá ter sistematizado os planos de gestão do risco anteriormente efetuados, com a identificação dos respetivos controlos implementados. Acresce a esta informação, a identificação do estado de implementação e de utilização dos controlos.

Para a identificação dos controlos existentes ou planeados, as seguintes atividades poderão ser úteis para a organização:

- Revisão de documentos que contenham informações sobre a implementação dos controlos (por exemplo: planos anteriores de implementação de processos de gestão do risco). Se os processos de gestão da segurança da informação estiverem corretamente documentados, todos os controlos planeados e/ou existentes e o seu respetivo estado de implementação deverão estar disponíveis para análise;

- Verificação, junto das pessoas responsáveis pela segurança da informação (por exemplo: CISO, COO), sobre quais são os controlos que se encontram efetivamente implementados;

- Realização de uma avaliação presencial, no local, para aferir a implementação dos controlos físicos, comparando os que estão devidamente implementados com a lista dos controlos que deveriam estar e, verificando entre os implementados, se estes se encontram correta e eficazmente operacionalizados.

No final desta atividade, a organização deverá ter uma lista de todos os controlos existentes e planeados com o seu respetivo estado de implementação.

Identificação de vulnerabilidades

Com base na lista de ameaças e dos ativos (não esquecendo os controlos implementados), a organização deverá identificar uma lista de potenciais vulnerabilidades que poderão ser associadas aos seus ativos. As vulnerabilidades podem ser identificadas nas seguintes áreas:

- Organização;
- Processos e procedimentos;
- Rotinas de gestão;
- Colaboradores;
- Ambientes físicos;
- Configuração dos sistemas de informação;
- Hardware, software e equipamento de rede;
- Dependência com partes externas interessadas.

A existência de uma vulnerabilidade não causa danos por si só. Para que cause danos, é necessário que exista uma ameaça que possa explorar essa mesma vulnerabilidade.

Uma vulnerabilidade pode não exigir a implementação de um controlo, mas deve ser conhecida e monitorizada pela organização. Releva-se que, um controlo ou conjunto de controlos que estejam incorretamente implementados, podem traduzir-se em potenciais vulnerabilidades para a organização. A eficácia de um controlo depende do ambiente em que o mesmo está a operar.

A organização pode identificar uma lista complementar de vulnerabilidades que não estejam relacionadas com ameaças e/ou ativos concretos. Esta lista pode fazer parte da sua base de dados de conhecimento de gestão do risco.

Identificação de impacto

A organização deve identificar as consequências dos riscos e aferir qual o impacto que a possível exploração de uma vulnerabilidade, por parte de uma ameaça, poderá ter em termos de confidencialidade, integridade e/ou disponibilidade dos ativos que se encontrem no âmbito do processo de gestão do risco.

Um impacto deve ser avaliado em várias dimensões, nomeadamente (e não somente), na geração de condições operacionais adversas, na perda de negócio por parte da organização ou em danos de reputação e imagem.

Esta atividade identifica os danos ou impactos para a organização que podem ser causados por um cenário de incidente. Um cenário de incidente pode ser originado pela exploração de uma vulnerabilidade por parte de uma determinada ameaça ou por um conjunto de ameaças a um sistema de informação.

O impacto dos cenários de incidentes deve ser determinado considerando-se os critérios ponderadores que são definidos no estabelecimento do contexto. Uma determinada ameaça pode ter impacto em um ou mais ativos, ou em partes de ativos.

Os ativos devem ter classificações atribuídas em função do seu valor para a organização, mediante as consequências no seu negócio, no caso de estes serem danificados e/ou comprometidos. O impacto pode ser temporário ou permanente (como no caso da destruição de um ativo).

O impacto do risco deverá ser identificado com base nas vulnerabilidades e ameaças associadas. Deve ser igualmente tido em atenção, na identificação do impacto, quais as consequências para os ativos e, inerentemente, para os processos referentes à atividade da organização que estes suportam.

Na aferição de impacto, a organização poderá identificar potenciais consequências operacionais em termos de, mas não se limitando a:

- Tempo de investigação e de reparação;
- Tempo (de trabalho) perdido;
- Oportunidades perdidas;
- Segurança e saúde;
- Custos financeiros com reparação;
- Danos de reputação.

3.5.5 Análise do risco

A análise do risco envolve a consideração das incertezas, fontes do risco, consequências, eventos, cenários, controlos e a sua eficácia.

Um evento pode ter múltiplas causas e consequências, e pode afetar um ou mais objetivos da organização. A abordagem ao processo de análise do risco pode ser realizada com níveis distintos de granularidade, dependendo da criticidade dos ativos, da extensão das vulnerabilidades existentes, das ameaças a ter em consideração e dos incidentes anteriormente ocorridos que envolvam a organização e que estejam inseridos no âmbito e fronteiras do processo de gestão do risco.

Nos critérios de aferição do impacto do risco, devem ser igualmente observadas as seguintes dimensões:

- Reputação – A ocorrência de determinado risco pode colocar em causa a reputação da organização (por exemplo: perda de confiança por parte de partes interessadas);
- Legal ou Regulatório – A ocorrência de determinado risco poderá colocar em causa responsabilidades legais e/ou regulatórias da organização (por exemplo: responsabilidades regulatórias sectoriais);
- Serviço a clientes – A ocorrência de determinado risco poderá colocar em causa o serviço prestado aos clientes da organização (por exemplo: incumprimento de um nível de serviço);
- Financeiro – A ocorrência de determinado evento pode levar a que a organização possa incorrer em custos financeiros não previstos (por exemplo: coimas, recursos adicionais).

A probabilidade de ocorrência de um risco é a possibilidade de o mesmo ocorrer num determinado período de tempo. É possível identificar a probabilidade de um risco com base na sensibilidade da equipa, na experiência de quem o identifica e/ou outros indicadores internos e externos.

Metodologia de análise

A metodologia de análise do risco pode ser consubstanciada por uma abordagem analítica de caráter qualitativo, quantitativo ou por uma combinação de ambas. Na prática, a análise qualitativa é mais utilizada, numa primeira abordagem, para a obtenção de indicadores gerais do nível do risco e para identificar os riscos mais relevantes.

O método de análise deverá ser consistente com os critérios de avaliação do risco, definidos na fase de definição de contexto do risco.

Análise qualitativa do risco

A análise qualitativa dos riscos utiliza uma escala de atributos de qualificação para identificar a severidade dos potenciais impactos (por exemplo: Baixo, Médio e Alto) e a probabilidade de tais ocorrências. Uma vantagem da análise qualitativa é a facilidade de compreensão por parte dos intervenientes, sendo que se identifica como desvantagem a subjetividade da escala em questão.

Os riscos qualitativos podem ser utilizados:

- Como uma atividade de triagem inicial para identificar os riscos que exigem uma análise mais detalhada;
- Quando este tipo de análise é apropriado para a tomada de decisão;
- Quando os dados ou recursos numéricos são inadequados para uma análise quantitativa do risco.

As análises qualitativas deverão utilizar dados e informações factuais.

Análise quantitativa do risco

A análise quantitativa utiliza uma escala de valores numéricos (em oposição às escalas descritivas usadas na análise do risco qualitativa) para aferição dos impactos e probabilidades, devendo suportar-se em diversas fontes.

A qualidade da análise depende da exatidão e integridade dos valores numéricos e da validade dos modelos utilizados. A análise quantitativa dos riscos utiliza, na maioria dos casos, dados de históricos de incidentes, apresentando, assim, a vantagem de poder ser diretamente relacionada com os objetivos e preocupações de segurança da informação da organização.

A análise quantitativa poderá ser desvantajosa, caso não existam dados factuais e/ou auditáveis. Esta situação pode criar uma ilusão de precisão e de eficácia do processo de avaliação do risco.

Levantamento dos impactos

Para execução desta fase, a organização deverá dispor de uma lista dos cenários de incidentes relevantes, da identificação das ameaças e vulnerabilidades anteriormente analisadas, dos ativos afetados e das respetivas consequências para esses ativos e para os processos referentes à atividade da organização, inseridos no âmbito do processo de gestão do risco.

Deve ser avaliado o impacto nos serviços prestados pela organização, que possam resultar na ocorrência de incidentes de segurança. O levantamento do impacto deverá ser igualmente avaliado no contexto da perda de confidencialidade, integridade e/ou disponibilidade dos ativos em análise.

O impacto do risco deve ter como base as vulnerabilidades, as ameaças identificadas e as respetivas consequências do risco nos ativos e processos referentes à atividade da organização.

O impacto pode ser avaliado em diversas perspetivas, nomeadamente, técnica, financeira, humana, de imagem ou, por uma outra perspetiva não referida, mas que seja relevante para a organização.

A avaliação dos ativos começa com a sua classificação, de acordo com a sua importância para o cumprimento dos objetivos de negócio da organização. Pode ser determinada usando duas medidas:

- O valor de reposição do ativo: o custo de recuperação, a limpeza ou a substituição da informação (se possível);
- As consequências operacionais da perda ou do comprometimento do ativo, tais como as consequências negativas para a prestação do serviço, consequências jurídicas ou regulatórias decorrentes da indisponibilidade e/ou destruição dos ativos de informação.

Análise de probabilidade

Com base nas ameaças, vulnerabilidades e listas de incidentes (incluindo lições aprendidas) existentes, a organização deverá avaliar qual a probabilidade de ocorrência do risco.

Uma vez identificados os cenários de incidentes, incluindo identificação de ameaças, ativos afetados, vulnerabilidades exploradas e o impacto para os ativos e para os processos referentes à atividade da organização, deve ser tido em linha de conta a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades poderão ser exploradas, considerando:

- Experiência e estatísticas aplicáveis para a probabilidade de ameaça;
- Para fontes de ameaças humanas: a motivação e as capacidades que mudam com o tempo e os recursos disponíveis para um possível atacante, bem como a perceção de atratividade e da vulnerabilidade dos ativos para um possível atacante;
- Para fontes de ameaças acidentais: fatores geográficos, como por exemplo proximidade com indústrias químicas ou petrolíferas, a possibilidade de condições climáticas;
- Vulnerabilidades, individualmente ou em conjunto.

Determinação do nível do risco

Na análise do risco, é assignado a cada cenário identificado um valor ao impacto e probabilidade. Esses valores poderão ser qualitativos ou quantitativos, dependendo da metodologia utilizada pela organização.

Nesta fase, todos os riscos identificados deverão ter o seu nível determinado.

3.5.6 Avaliação do risco

A natureza das decisões relativas à avaliação e aos critérios de avaliação dos riscos utilizados para tomar essas decisões são estabelecidos no momento de definição do contexto. Estas decisões, bem como o contexto, devem ser revisitadas com maior detalhe nesta fase, tendo em conta que existe mais informação sobre os riscos específicos identificados.

No decorrer do processo de avaliação, as organizações devem comparar os riscos estimados com os critérios de avaliação do risco, definidos durante o processo de definição do contexto.

Os critérios de avaliação do risco devem ser utilizados para suportar as tomadas de decisões. Devem ser consistentes com o contexto externo e interno da gestão dos riscos de segurança da informação e serem considerados, por exemplo, nos objetivos das organizações e na visão das partes interessadas.

As decisões tomadas na avaliação do risco baseiam-se principalmente no nível aceitável do risco. No entanto, os impactos e a probabilidade, bem como o grau de confiança na identificação e análise do risco, também devem ser considerados.

A agregação de vários riscos, baixos ou médios, pode resultar em riscos gerais mais altos. Na fase de avaliação, deve ser elaborada uma lista dos riscos que podem ser agrupados. Os riscos devem ser priorizados de acordo com os critérios de avaliação e em relação aos cenários de incidentes que originaram os riscos identificados.

3.5.7 Tratamento do risco

Ao âmbito do tratamento do risco, a organização deve definir qual a opção de tratamento que achar adequada, deve proceder à identificação dos controlos que podem ser implementados para mitigar, evitar ou transferir o risco, bem como definir um plano de tratamento do mesmo. Na escolha das opções de tratamento do risco, deve ser colocado em consideração:

- Como o risco é percebido pelas partes interessadas afetadas;
- A forma mais adequada para comunicar com as partes interessadas.

Assim que o plano de tratamento do risco seja definido, os riscos residuais necessitam de ser determinados. Este processo envolve uma atualização ou uma nova iteração com a fase de avaliação, tendo como base os efeitos esperados pelo tratamento do risco proposto.

Caso o risco residual ainda não cumpra com os critérios de aceitação do risco da organi-

zação, poderá ser necessária uma iteração adicional do tratamento do risco antes de se proceder à aceitação do mesmo.

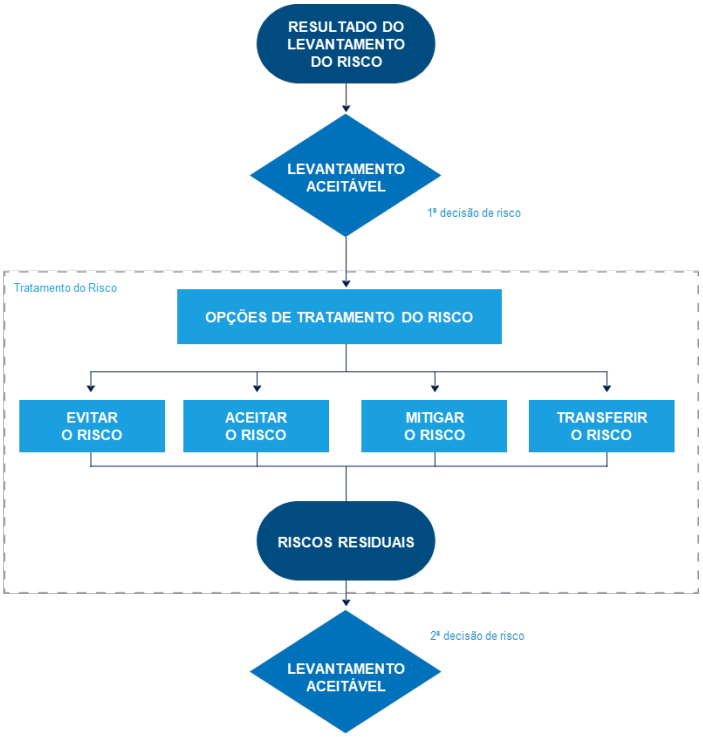


Figura 6 - Fonte: ISO/IEC 27005, Tratamento do Risco

Tal como indicado na Figura 6, as opções de tratamento de risco a serem consideradas, são:

- Evitar o risco: Colocar a probabilidade ou impacto tendencialmente próximo de zero, tornando mais difícil a sua ocorrência e/ou eliminar totalmente o seu impacto;
- Aceitar o risco: Decisão de aceitação do risco. A assunção de responsabilidade por essa decisão deve ser formalmente registada pela organização;
- Mitigar o risco: Reduzir a probabilidade e/ou impacto de um evento adverso para limites aceitáveis, através da implementação de controlos ou contramedidas;
- Transferir o risco: Transferir, total ou parcialmente, para terceiras partes, o impacto em relação a uma ameaça (por exemplo: efetuar a contratualização de um seguro).

3.5.8 Comunicação e consulta do risco

A informação e as decisões referentes aos riscos devem ser partilhadas com todas as partes interessadas relevantes. A comunicação do risco deve ser realizada, de modo a:

- Providenciar a garantia do resultado da gestão dos riscos da organização;
- Recolher informações do risco;
- Partilhar os resultados da avaliação dos riscos e apresentar o plano de tratamento dos riscos;
- Evitar ou reduzir a ocorrência e o impacto das quebras de segurança da informação devido à falta de entendimento mútuo entre quem toma as decisões e as partes interessadas;
- Suportar as tomadas de decisão;
- Enriquecer os conhecimentos sobre as temáticas da segurança da informação na organização;
- Coordenar com outras partes interessadas e planear respostas para reduzir o impacto dos incidentes;
- Disponibilizar, a quem toma as decisões e às partes interessadas da organização, uma demonstração de responsabilidade sobre os riscos;
- Melhorar a consciencialização sobre a importância do processo de gestão dos riscos.

A organização deve desenvolver planos de comunicação de suporte aos processos de gestão do risco, comuns e de emergência. Desta forma, a atividade de comunicação deve ser realizada de forma contínua.

3.5.9 Monitorização e revisão do risco

Os riscos e os seus fatores (por exemplo: valor dos ativos, impactos, vulnerabilidades e probabilidades de ocorrência) devem ser monitorizados e revistos com regularidade, de modo a que se identifique atempadamente qualquer alteração que possa ter existido no contexto da organização e que se possa traduzir numa alteração à perceção do risco.

A organização deve garantir que os seguintes pontos são monitorizados de forma contínua:

- Novos ativos que foram incluídos no âmbito do processo de gestão do risco;
- Alterações na criticidade dos ativos para a organização (por exemplo: devido a requisitos de negócios modificados);
- Novas ameaças que podem estar ativas, tanto dentro como fora organização, e que ainda não foram avaliadas;
- Possibilidade de novas vulnerabilidades serem exploradas por ameaças;
- Possível aumento do impacto, consequências das ameaças, vulnerabilidades ou dos riscos agrupados que resultem num nível inaceitável do risco;
- Incidentes de segurança da informação que possam ocorrer.

O resultado das atividades de monitorização pode ser inserido noutras atividades de revisão dos riscos. A organização deve efetuar a revisão de forma regular ou sempre que ocorram alterações significativas.

3.5.10 Exemplo

João, responsável do Gabinete de Gestão de Projeto da Organização, identificou no seu processo de análise do risco que existe uma elevada possibilidade de roubo das palavras-passe dos utilizadores da plataforma de gestão de ficheiros, alojada num serviço de computação em nuvem, que é utilizada pela organização para disponibilização de toda a documentação gerada no âmbito da execução dos seus projetos.

O risco identificado por João, teve por base:

- A sua experiência na utilização da plataforma é indicativa de que o seu fornecedor não tem uma política de palavras-passe alinhada com as suas práticas internas;
- O conhecimento de que outro cliente da plataforma foi alvo de um ataque malicioso.

Durante o processo, identificou que a ameaça poderia ter efetivamente origem num ataque malicioso externo, levado a cabo tirando partido da vulnerabilidade anteriormente identificada (política de palavras-passe deficiente) e, observou igualmente, que este vetor de ataque poderia colocar em causa a confidencialidade e a integridade da informação que se encontrava alojada neste ativo (plataforma de gestão de ficheiros).

João efetuou a avaliação de impacto com base na matriz sistematizada na metodologia do risco da organização (1 – Pequeno, 2 – Moderado, 3 – Elevado, 4 – Catastrófico), tendo atribuído um impacto “4 – Catastrófico” ao risco em causa.

De seguida, efetuou o exercício de avaliação da probabilidade de o risco ocorrer. Consultou a metodologia e face às possibilidades apresentadas - 1 – Improvável, 2 – Provável, 3 – Muito Provável, 4 – Quase certa - decidiu que a probabilidade seria “4 – Quase certa”.

Com base no cálculo do impacto e probabilidade, o nível do risco (resultado do produto entre o impacto e a probabilidade) é 16. Desta forma, João concluiu que o risco identificado é Muito Alto. Esta conclusão é sustentada nos critérios de identificação do nível do risco da tabela de níveis, publicada no âmbito da metodologia de gestão do risco da organização:

a. [1; 2] – Nível baixo;
b. [3 a 6] – Nível Médio;
c. [8 a 12] – Alto;
d. [16] – Muito Alto.

Face ao nível identificado, a organização não o pode aceitar, uma vez que todos os riscos de nível “Muito Alto” devem ser obrigatoriamente tratados, exceto se tiverem sido formalmente aceites pela Gestão de Topo. Nesse caso, a organização, na sua sessão de gestão do risco, pode tomar a decisão estratégica de o mitigar e de executar as seguintes atividades:

1 Garantir que o fornecedor da plataforma de gestão de ficheiros altera a sua política de gestão de palavras-passe em conformidade com as suas práticas internas, no espaço de tempo a definir;

2 Avaliar outras plataformas que prestem o mesmo serviço, com as condições consideradas como adequadas pela organização.

Foi igualmente identificada uma responsável (Inês – Diretora dos Sistemas de Informação) pela execução das atividades, tendo sido igualmente acordada uma data estimada de resolução. A data foi escolhida de acordo com as prioridades atribuídas aos riscos identificados, tendo em conta o nível do risco e a criticidade dos ativos envolvidos.

Toda esta informação foi atualizada na ferramenta de gestão do risco da organização.

Tabela de Resumo

CAMPOS	VALORES
#ID	1
Descrição do Risco	Possibilidade de acesso indevido a informação de projetos da organização
Ativo	Plataforma de gestão de ficheiros
Responsável do Risco	João – Responsável Gabinete de Gestão de Projeto
Ameaça	Ataque malicioso de força bruta às palavras-passe
Vulnerabilidade	Política de palavras-passe deficiente
Confidencialidade	Sim
Integridade	Sim
Disponibilidade	Não
Impacto	4 – Catastrófico
Probabilidade	4 – Quase Certa
Nível do Risco	16 – Muito Alta
Estratégia	Mitigar/Tratar
Ações	- Garantir que o fornecedor da plataforma de gestão de ficheiros altere a sua política de palavras-passe em conformidade com as suas práticas internas, no espaço de tempo a definir; - Avaliar plataformas que prestem o mesmo serviço, com as condições consideradas como adequadas pela organização
Responsável pelo tratamento de ações	Inês – Responsável dos Sistemas de Informação
Data do tratamento	DD-MM-AAAA

Tabela 3 - Resumo do Risco

3.6 Âmbito e aplicabilidade

O QNRCS tem aplicabilidade em todas as organizações públicas e privadas nacionais, nomeadamente:

1 Administração Pública;

2 Operadores de infraestruturas críticas;

3 Operadores de serviços essenciais;

4 Prestadores de serviços digitais;

5 Quaisquer outras organizações que utilizem redes e sistemas de informação.

De outra forma, o QNRCS pode ser aplicado pelos prestadores de serviços digitais que tenham o seu estabelecimento principal em território nacional ou, não o tendo, que designem um representante estabelecido em território nacional, desde que aí prestem serviços digitais.

Uma organização deve utilizar o QNRCS como instrumento de suporte ao processo de gestão do risco na cibersegurança. Não tendo sido elaborado com o objetivo de substituir processos existentes, este pode ser utilizado em complemento a esses mesmos processos, permitindo a identificação de lacunas na estratégia de cibersegurança e promovendo a definição de um caminho de melhoria futura.

São várias as abordagens para a aplicação do QNRCS. Entre elas, destacamos as seguintes:

Revisão de práticas de cibersegurança

A estrutura central do QNRCS sistematiza um universo essencial de medidas de segurança que pode ser utilizado para comparar com as medidas de cibersegurança colocadas em prática pela organização. Desta forma, a organização pode criar o seu perfil atual e medir a extensão do cumprimento dos propósitos descritos nas categorias e subcategorias devidamente alinhadas com os objetivos de segurança: Identificar, Proteger, Detetar, Responder e Recuperar.

Uma organização pode, entre outras, concluir que se encontra num nível de maturidade que lhe permite cumprir os resultados desejados e dar enfoque no processo de monitorização e gestão do risco. Alternativamente, a organização pode identificar oportunidades ou necessidades de melhoria dos seus processos. Por outro lado, a organização poderá utilizar esta informação para identificar áreas de sub-investimento e, assim, priorizar e reorientar os seus recursos.

Sistematização de processos ou melhoria dos existentes

Os passos seguintes ilustram, de forma não exaustiva, uma metodologia que pode ser utilizada pela organização para, tendo por base o QNRCS, criar um programa de cibersegurança ou introduzir melhorias ao existente. Cada um destes passos deve ser repetido conforme for necessário, por forma a criar uma dinâmica de melhoria contínua dos seus processos e procedimentos de segurança da informação e cibersegurança.

Passo 1 – Prioridade e âmbito: A organização identifica os seus objetivos e prioridades de alto nível. Com esta informação, a organização define as suas opções estratégicas no que se refere à implementação de medidas de cibersegurança e define qual o universo de sistemas e ativos que suportam a atividade crítica da organização. O QNRCS pode ser adaptado às diversas realidades da organização no que se refere à sua atividade e, inclusivamente, às diferentes necessidades no contexto dos seus processos internos, que podem ter diferentes níveis de tolerância ao risco.

Passo 2 – Linhas orientadoras: Uma vez definido o âmbito do programa de cibersegurança, a organização identifica e define as redes e sistemas de informação e respetivos ativos relacionados com a atividade, requisitos regulatórios e a estratégia de gestão do risco. Adicionalmente, a organização identifica ameaças e vulnerabilidades aplicáveis aos ativos previamente definidos.

Passo 3 – Criação do Perfil Atual: A organização cria aquele que é o seu "Perfil Atual", indicando para cada categoria e subcategoria quais os objetivos de segurança que cumpre atualmente. Caso cumpra parcialmente alguns dos objetivos, deve documentar esta situação, por forma a consubstanciar o seu nível de maturidade e informação de base para futura aferição.

Passo 4 – Aferição do risco: A Análise do risco pode ser guiada de acordo com o processo de gestão do risco em vigor na organização ou tendo por base ações anteriores. A organização analisa o seu ambiente operacional para aferir o grau de probabilidade de ocorrência de um evento ou incidente de cibersegurança e o impacto que este possa ter na organização. Este processo deve ter em linha de conta fontes de informação, internas e externas, relativas a vulnerabilidades e ameaças emergentes, por forma a obter um melhor entendimento quanto à probabilidade e impacto expetáveis.

Passo 5 – Criação do Perfil Alvo: A organização cria o seu "Perfil Alvo" com base nas categorias e subcategorias descritas no QNRCS, refletindo aqueles que são os resultados pretendidos. A organização poderá definir as suas próprias categorias e subcategorias, por forma a melhor endereçar as características e riscos particulares inerentes à sua atividade. Por outro lado, a organização também poderá considerar contributos e requisitos de intervenientes externos, tais como outras entidades do setor e fornecedores.

Passo 6 – Identificar, analisar e priorizar lacunas: A organização compara o "Perfil Atual" com o "Perfil Alvo" e identifica lacunas que devem ser endereçadas. Para este efeito, elabora um plano de ação que reflita a relevância, custos, benefícios e riscos associados das lacunas identificadas e projeta as ações a levar a cabo para atingir os resultados definidos no "Perfil Alvo".

Passo 7 – Implementação do plano de ação: A organização determina quais as ações a levar a cabo, por forma a endereçar as lacunas identificadas no passo anterior, e ajusta as práticas de cibersegurança que tenha atualmente em vigor, de modo a atingir o seu "Perfil Alvo".

As organizações devem repetir este processo sempre que necessário e, inclusivamente, com uma cadência projetada e sistematizada. A título de exemplo, uma organização pode definir uma maior cadência de repetição do **Passo 2 – Linhas orientadoras**, por forma a melhorar a qualidade dos seus processos de análise do risco. Por outro lado, as organizações podem monitorizar o progresso e evolução do seu nível de maturidade, procedendo a atualizações periódicas do seu "Perfil Atual" e, subsequentemente, comparando-o com o seu "Perfil Alvo".

Comunicação de requisitos de cibersegurança

O QNRCS procura disponibilizar uma linguagem comum para a comunicação de requisitos entre partes interessadas, que são responsáveis pela prestação de bens ou serviços essenciais. Esta comunicação é especialmente importante entre organizações em todo o alcance do espectro de uma cadeia logística. Estas cadeias podem atingir níveis de complexidade elevados, que se refletem numa interdependência de recursos e processos.

Este universo de partes interessadas está compreendido no ecossistema de cibersegurança, relevante para a prestação dos bens ou serviços da organização. Considerando as categorias e subcategorias estabelecidas no QNRCS, bem como os perfis definidos, estão identificados os mecanismos contextuais, processuais e semânticos conducentes a uma comunicação acessível e facilmente aferida pelo ecossistema.

3.7 Estrutura do QNRCS

No âmbito da construção da estrutura central do QNRCS, são definidas todas as categorias, subcategorias e controlos/referências que se entendem relevantes, atendendo (mas não apenas) aos seguintes princípios:

1 Considerar todos os aspetos definidores de um ecossistema de cibersegurança nas organizações nacionais, independentemente da sua dimensão, natureza (pública ou privada), criticidade ou orientação tecnológica;

2 Abranger transversalmente todos os setores de atividade;

3 Atender às características específicas e definidoras do tecido social e económico do país;

4 Permitir e promover que determinadas organizações (por exemplo: reguladores) possam definir o respetivo contexto de aplicação do QNRCS para o seu sector de atividade/regulação.

A estrutura central do QNRCS é constituída por:

1 Objetivos de segurança;

2 Medidas de segurança.

Figura 7 - A estrutura do documento

As medidas de segurança traduzem-se em categorias que se dividem em subcategorias.

A cada objetivo de segurança, pode corresponder uma ou mais categorias. A cada categoria pode corresponder uma ou mais subcategorias.

A cada subcategoria está associado um ou mais controlos ou referências. O objetivo passa por interligar cada uma das subcategorias a referenciais de boas práticas de segurança da informação e de cibersegurança, por intermédio de um conjunto de práticas de referência e de maior aceitação/popularidade em Portugal.

Para cada subcategoria, referencia-se um exemplo de implementação tecnológica e outro de implementação processual, consistindo numa descrição genérica de como pode ser aplicado, contribuindo, desse modo, para uma melhor compreensão da aplicabilidade do mesmo. São ainda referenciados exemplos genéricos de possíveis evidências que podem ser utilizadas na demonstração da aplicação de determinada medida de segurança.

A estrutura base do QNRCS apresenta-se, assim, da seguinte forma:

OBJETIVO	MEDIDAS DE SEGURANÇA					
IDENTIFICAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
PROTEGER	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
DETETAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
RESPONDER	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
RECUPERAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas

Tabela 4 - Estrutura base do QNRCS

3.7.1 Contexto Referencial

De seguida, contextualiza-se sobre os quatros referenciais que suportam as práticas e controlos sugeridos por este QNRCS. Estes referenciais abordam o tema da segurança da informação e da cibersegurança de forma complementar. Todos estes referenciais são internacionalmente reconhecidos como base para a implementação e avaliação de controlos de tratamento do risco e de (boas) práticas de governo, segurança da informação e/ou cibersegurança.

CIS CSC 7.0

O Catálogo de controlos críticos de cibersegurança (CSC) é publicado pelo *Center for Internet Security* (CIS[1]). Este catálogo disponibiliza uma lista de ações, priorizada, que é regularmente revista pela comunidade académica, de forma a ser utilizável pelas organizações.

[1] https://www.cisecurity.org

COBIT 5

Da responsabilidade do ISACA[1], o COBIT é uma *framework* de boas práticas para governo de TI. Ajuda as organizações a criar valor a partir das TI e contribui para o equilíbrio entre os benefícios, a otimização dos níveis do risco e a utilização dos recursos disponíveis pelas organizações.

ISO/IEC 27001:2013

A norma ISO/IEC 27001[2] especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados, de acordo com as necessidades e realidade da organização.

NIST SP-800-53 Rev4

Publicado pela NIST9[3], é um catálogo de controlos de segurança e de privacidade para redes e sistemas de informação de organismos do governo. Disponibiliza, também, um processo de seleção de controlos para proteção da operação e dos ativos das organizações, de incidentes, desastres naturais, falhas estruturais ou erro humano.

3.8 Contextualização

O QNRCS pretende ser aplicável, essencialmente, a organizações que assentem a sua atividade em tecnologia, quer seja numa perspetiva de cibersegurança para Tecnologias de Informação, de controlos de sistemas industriais, sistemas de interface homem-máquina, dispositivos *IoT* ou, de uma forma mais generalista, todos os dispositivos conectados de alguma forma a redes e sistemas de informação.

A estrutura apresentada é uma proposta de um conjunto de práticas de segurança da informação para a cibersegurança. Reforça-se o aspeto de que, no âmbito da aplicação voluntária, qualquer organização é livre para definir o que deseja implementar, quais as medidas de segurança a implementar ou outros atributos adicionais que entenda como relevantes, de acordo com o seu tipo de atividade, dimensão e perfil do risco associado.

A título de exemplo, apresentam-se algumas situações em que se pode justificar a adaptação/aplicação do QNRCS numa organização:

1 Um regulador definir o contexto de aplicação no seu setor de atividade, selecionando subcategorias e definindo as medidas de segurança que considere apropriados para cada subcategoria, de acordo com um perfil de risco genérico associado, na sua área de atuação;

2 Uma organização efetuar a sua própria contextualização do QNRCS, escolhendo as subcategorias e definindo as medidas de segurança que se enquadrem com o perfil de risco associado aos seus ativos;

[1] https://www.isaca.org/

[2] https://www.iso.org/isolec-27001-information-security.html

[3] https://www.nist.gov/

3 Ferramenta de suporte para identificar um conjunto de práticas que podem ser implementadas pelas partes interessadas da organização;

4 Uma organização pode identificar no QNRCS possíveis práticas que podem ser transformadas em requisitos contratuais, que visem a melhoria das relações de troca de bens e serviços entre as organizações, enquadradas na temática da segurança da informação e cibersegurança.

Apresentação do Quadro Nacional de Referência para a Cibersegurança

4.1 Objetivos de segurança

O QNRCS disponibiliza e descreve um conjunto de medidas de segurança que traduzem objetivos específicos. São referenciados exemplos e orientações que permitem sistematizar processos, procedimentos e ferramentas, cuja aplicação permita atingir esses mesmos objetivos. O QNRCS não é uma lista de controlo de ações a realizar, mas antes uma representação dos objetivos chave reconhecidos pelos diversos intervenientes como sendo um importante suporte ao processo de gestão do risco de cibersegurança.

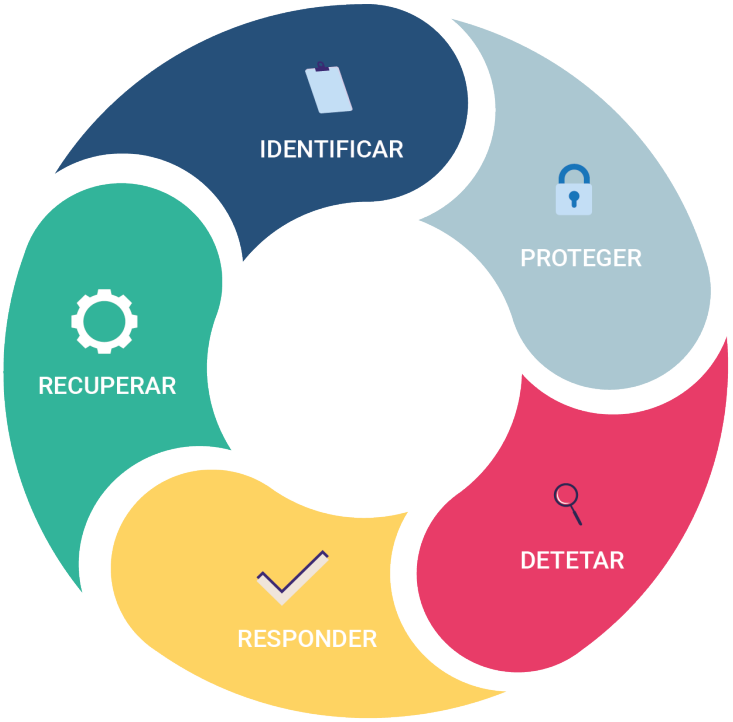


Figura 8- Objetivos de Segurança

Também a utilização do QNRCS deve ser feita numa perspetiva de melhoria contínua. Não deve ser efetuada uma utilização estática das práticas identificadas no QNRCS mas, sim, evoluir de acordo com a maturidade da organização e o seu contexto.

No quadro seguinte concretizam-se os objetivos de segurança propostos:

OBJETIVO	DESCRIÇÃO
Identificar	Compreensão do contexto da organização, dos ativos que suportam os processos críticos da atividade da organização e dos riscos associados relevantes. Esta compreensão permite que a organização consiga definir e priorizar os seus recursos e investimentos, de acordo com os seus objetivos gerais e com a sua estratégia de gestão do risco.
Proteger	Implementação de medidas destinadas a proteger os processos organizativos e os ativos da organização, independentemente da sua natureza tecnológica. Assim, nesta categoria, são definidas medidas orientadas à proteção da organização nas suas três dimensões: Pessoas, Processos e Tecnologia.
Detetar	Definição e implementação de medidas destinadas a identificar, de forma atempada, os incidentes. Ou seja, a deteção de eventos com um efeito adverso real na segurança das redes e dos sistemas de informação.

OBJETIVO	DESCRIÇÃO
Responder	Definição e implementação de medidas de ação apropriadas, em caso de deteção de um incidente. As medidas propostas no âmbito deste objetivo pretendem mitigar o impacto do incidente, ou seja, reduzir os seus potenciais efeitos adversos.
Recuperar	Definição e implementação de atividades, que visam a gestão de planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança. As medidas pertencentes a este objetivo pretendem assegurar a resiliência da organização nas suas dimensões: Pessoas, Processos e Tecnologia. E que, no caso de existência de um incidente, a organização consiga utilizar as medidas para suporte à recuperação em tempo útil da sua atividade.

Tabela 5 - Objetivos de Segurança

4.2 Medidas de segurança

Neste âmbito, estão compreendidos três elementos basilares: Medidas de Segurança, Categorias e Subcategorias.

As medidas de segurança constituem atividades de elevado nível de abstração, que suportam as organizações no processo de sistematização da sua estratégia de gestão do risco de cibersegurança. Estas medidas simplificam o processo de organização da informação, a tomada de decisão no âmbito da gestão do risco e o endereçamento de ameaças e fomentam a melhoria contínua recorrendo a lições aprendidas no âmbito de atividades realizadas.

Adicionalmente, as medidas identificadas estão alinhadas com as metodologias de gestão de incidentes de maior adoção e permitem demonstrar o impacto do investimento na cibersegurança. Por exemplo, o investimento no planeamento e na execução de exercícios que suportem atividades de resposta atempada e de recuperação, que resultem na redução do impacto causado à prestação de bens ou serviços.

Uma medida de segurança subdivide-se em categorias que agrupam propósitos e objetivos de caráter programático e atividades particulares. As categorias, por sua vez, dividem-se ainda em subcategorias que traduzem um conjunto de efeitos específicos de uma atividade técnica ou de gestão. Estes resultados, descritos de forma não exaustiva, promovem o atingimento dos propósitos e objetivos das categorias em que se enquadram.

Nos subcapítulos seguintes, identificam-se as categorias e subcategorias correspondentes às medidas de segurança a aplicar.

4.2.1. Identificar

Pretende-se estabelecer um entendimento, transversal à organização, para a abordagem à gestão do risco de cibersegurança no contexto da envolvência das suas redes e sistemas de informação, pessoas, ativos, dados e respetivas capacidades. As práticas que se enquadram no objetivo **Identificar** são basilares para a efetiva utilização do QNRCS. Conhecer, num contexto organizacional, os recursos que suportam as suas funções importantes e os respetivos riscos associados, permite à organização priorizar os seus esforços de forma consistente.

Descreve-se, no quadro seguinte, as categorias existentes com a identificação das respetivas subcategorias associadas.

CATEGORIA	DESCRIÇÃO	SUBCATEGORIAS
ID.GA **Gestão de ativos**	A organização deve identificar os dados, colaboradores, equipamentos, sistemas e instalações que permitem cumprir os seus objetivos no decorrer da sua atividade. Devem ser identificados e geridos de forma consistente com aquela que é a sua relevância no cumprimento dos objetivos da organização e com a estratégia de gestão do risco.	ID.GA-1 ID.GA-2 ID.GA-3 ID.GA-4 ID.GA-5
ID.AO **Ambiente da Organização**	A organização compreende e prioriza a sua missão, os seus objetivos, as partes interessadas e as suas atividades. Esta informação é utilizada para identificar os papéis e responsabilidades no contexto da cibersegurança e a tomada de decisões no âmbito da gestão dos riscos.	ID.AO-1 ID.AO-2 ID.AO-3 ID.AO-4 ID.AO-5
ID.GV Governação	A organização entende as políticas, processos e procedimentos para gerir e monitorizar as responsabilidades regulamentares, legais, de risco, ambientais e operacionais. Estas políticas, processos e procedimentos contribuem para a sensibilização e consolidação do conhecimento por parte dos órgãos de gestão, tendo em vista a identificação dos riscos no contexto da cibersegurança.	ID.GV-1 ID.GV-2
ID.AR **Avaliação do risco**	A organização tem noção dos riscos de cibersegurança no âmbito da sua atividade (incluindo missão, funções, imagem ou reputação), ativos organizacionais e pessoas.	ID.AR-1 ID.AR-2 ID.AR-3 ID.AR-4 ID.AR-5
ID.GR **Estratégia de gestão do risco**	Devem ser estabelecidas as prioridades, restrições, níveis de tolerância ao risco e assunções que são utilizadas para suportar a tomada de decisão, no âmbito da gestão do risco operacional.	ID.GR-1 ID.GR-2 ID.GR-3
ID.GL **Gestão do risco da cadeia logística**	Devem ser estabelecidas as prioridades, restrições, níveis de tolerância ao risco e assunções que são utilizadas para suportar a tomada de decisão, no âmbito da gestão do risco operacional da cadeia logística. A organização deve estabelecer e implementar os processos para identificar, avaliar e gerir os riscos inerentes à cadeia logística.	ID.GL-1 ID.GL-2 ID.GL-3 ID.GL-4 ID.GL-5

Tabela 6 – Categoria Identificar das Medidas de Segurança

4.2.2 Proteger

Pretende-se, como resultado do objetivo **Proteger**, proporcionar o desenvolvimento e a implementação das salvaguardas necessárias à garantia de prestação de serviços ou bens, suportando e reforçando a capacidade de a organização limitar ou conter o impacto de eventual ocorrência de um incidente de cibersegurança.

Esta capacidade suporta-se, entre outras, na gestão da identidade eletrónica e respetivas autorizações, na realização de ações de formação e de sensibilização e na definição e implementação de procedimentos, processos e tecnologias de proteção da informação.

Descreve-se, no quadro seguinte, as categorias existentes com a identificação das respetivas subcategorias associadas.

CATEGORIA	DESCRIÇÃO	SUBCATEGORIAS
PR.GA **Gestão de identidades, autenticação e controlo de acessos**	Os acessos aos ativos físicos, lógicos e às instalações associadas devem ser limitados às pessoas, processos e equipamentos autorizados. Estes devem ser geridos de acordo com a avaliação do risco de acesso não autorizado.	PR.GA-1 PR.GA-2 PR.GA-3 PR.GA-4 PR.GA-5 PR.GA-6 PR.GA-7
PR.FC **Formação e sensibilização**	Devem ser ministradas sessões de sensibilização em cibersegurança a colaboradores e fornecedores. Estes, devem ser formados para cumprirem as suas responsabilidades e os seus deveres relacionados com a cibersegurança, em concordância com as políticas, processos, procedimentos e acordos relevantes.	PR.FC-1 PR.FC-2 PR.FC-3 PR.FC-4
PR.SD **Segurança de dados**	As informações e os dados devem ser geridos de acordo com a estratégia de gestão do risco organizacional, por forma a proteger a confidencialidade, integridade e disponibilidade da informação.	PR.SD-1 PR.SD-2 PR.SD-3 PR.SD-4 PR.SD-5 PR.SD-6 PR.SD-7 PR.SD-8
PR.PI **Procedimentos e processos de proteção da informação**	As políticas de segurança, processos e procedimentos devem ser mantidas e utilizadas por forma a permitir gerir a proteção das redes e sistemas de informação.	PR.PI-1 PR.PI-2 PR.PI-3 PR.PI-4 PR.PI-5 PR.PI-6 PR.PI-7 PR.PI-8 PR.PI-9 PR.PI-10 PR.PI-11 PR.PI-12
PR.MA **Manutenção**	A manutenção e reparação das redes e sistemas de informação devem ser realizadas em concordância com as políticas, processos e procedimentos instituídos.	PR.MA-1 PR.MA-2

CATEGORIA	DESCRIÇÃO	SUBCATEGORIAS
PR.TP **Tecnologia de proteção**	As soluções técnicas de segurança devem ser geridas por forma a garantir a confidencialidade, integridade e disponibilidade das redes e sistemas de informação, em concordância com as políticas relacionadas, processos, procedimentos e acordos relevantes.	PR.TP-1 PR.TP-2 PR.TP-3 PR.TP-4 PR.TP-5

Tabela 7 – Categoria Proteger das Medidas de Segurança

4.2.3 Detetar

No contexto do objetivo **Detetar**, pretende-se desenvolver práticas adequadas e atempadas à deteção da ocorrência de eventos de cibersegurança, por via da monitorização contínua das redes e sistemas de informação e da implementação de processos de deteção.

Descrevem-se, no quadro seguinte, as categorias existentes com a identificação das respetivas subcategorias associadas.

CATEGORIA	DESCRIÇÃO	SUBCATEGORIAS
DE.AE **Anomalias e eventos**	Devem ser detetadas as atividades anómalas em tempo útil, bem como deve ser assegurada a compreensão do impacto potencial dos eventos.	DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5
DE.MC **Monitorização Contínua de Segurança**	As redes e sistemas de informação devem ser monitorizadas para identificação de eventos de cibersegurança e verificação da eficácia das medidas de proteção aplicadas.	DE.MC-1 DE.MC-2 DE.MC-3 DE.MC-4 DE.MC-5 DE.MC-6 DE.MC-7 DE.MC-8
DE.PD **Processos de Deteção**	Os processos de deteção e respetivos procedimentos devem ser mantidos e testados para garantir o reconhecimento de eventos anómalos.	DE.PD-1 DE.PD-2 DE.PD-3 DE.PD-4 DE.PD-5

Tabela 8 – Categoria Detetar das Medidas de Segurança

4.2.4 Responder

Pretende-se, como resultado para o objetivo **Responder**, desenvolver e implementar práticas que levem a cabo ações de resposta a um incidente de cibersegurança que tenha sido detetado.

Estas práticas devem capacitar a organização para a contenção dos impactos de um potencial incidente, através do planeamento da resposta a incidentes, da comunicação com as partes interessadas relevantes, da análise e mitigação de incidentes e da melhoria por intermédio das lições aprendidas.

Descrevem-se, no quadro seguinte, as categorias existentes com a identificação das respetivas subcategorias associadas.

CATEGORIA	DESCRIÇÃO	SUBCATEGORIAS
RS.PR **Planeamento de resposta**	Os processos de resposta e respetivos procedimentos devem ser executados e mantidos para garantir resposta aos incidentes detetados.	RS.PR-1
RS.CO **Comunicações**	As atividades de resposta a incidentes devem ser coordenadas com as partes interessadas.	RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5
RS.AN **Análise**	A análise de incidentes deve ser conduzida de forma a garantir uma resposta efetiva e apoiar as atividades de recuperação.	RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4 RS.AN-5
RS.MI **Mitigação**	Devem ser realizadas atividades para conter, mitigar ou resolver um incidente ocorrido.	RS.MI-1 RS.MI-2 RS.MI-3
RS.ME **Melhorias**	As atividades de resposta organizacionais devem ser melhoradas incorporando lições aprendidas, tendo por base ocorrências anteriores.	RS.ME-1 RS.ME-2

Tabela 9 – Categoria Responder das Medidas de Segurança

4.2.5 Recuperar

No âmbito do objetivo **Recuperar**, pretende-se desenvolver e implementar práticas e manter planos de resiliência para restaurar qualquer capacidade e/ou serviço que tenha sido comprometido na sequência de um evento de cibersegurança.

Estas práticas promovem a recuperação adequada das operações da organização, por for-

ma a reduzir os impactos do incidente ocorrido. Entre outras, promove-se a execução de planos de continuidade de negócio, de recuperação, da execução de exercícios de simulação de situações de crise e de atualizações dos planos com vista à melhoria dos mesmos.

Descrevem-se, no quadro seguinte, as categorias com a identificação das respetivas subcategorias associadas.

CATEGORIA	DESCRIÇÃO	SUBCATEGORIAS
RC.PR **Plano de recuperação**	Os processos e procedimentos de recuperação devem ser executados e mantidos para garantir a recuperação das redes e sistemas de informação afetados pelos incidentes.	RC.PR-1
RC.ME **Melhorias**	Os planos e processos de recuperação devem ser melhorados através da incorporação de lições aprendidas, resultantes de incidentes passados e correntes.	RC.ME-1 RC.ME-2
RC.CO **Comunicações**	As atividades de recuperação devem ser coordenadas com as partes interessadas envolvidas ou afetadas pelo incidente.	RC.CO-1 RC.CO-2

Tabela 10 – Categoria Recuperar das Medidas de Segurança

MEDIDAS DE SEGURANÇA

IDENTIFICAR

4.3.1 ID.GA Gestão de Ativos

R.N. CIS CSC 1; COBIT 5 BAI09.01, BAI09.02; ISO/IEC 27001:2013 A.8.1.1, A.8.1.2; NIST SP 800-53 Rev. 4 CM-8, PM-5.

ID.GA-1 - Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser inventariados

Descrição

A organização deve inventariar os seus dispositivos físicos, redes e sistemas de informação existentes, por forma a garantir que existe um mapeamento estruturado dos mesmos. Todos os dispositivos e sistemas inventariados devem ser classificados de acordo com a sua relevância para a organização.

Implementação Técnica

1 Ferramentas/aplicações de gestão de ativos.

Implementação Processual

A organização deve efetuar o inventário dos seus equipamentos, de acordo com as seguintes regras:

1 Os dispositivos físicos e sistemas devem ser inventariados com a seguinte informação:
   a. Número de inventário;
   b. Nome do equipamento;
   c. Número de série;
   d. Localização;

2 Os dispositivos de rede devem ter a seguinte informação complementar:
   a. Endereço IP;
   b. Endereço de hardware;

3 Os responsáveis dos dispositivos e sistemas devem ser identificados com, pelo menos, os seguintes elementos:
   a. Nome;
   b. Contacto;
   c. Departamento;

4 Os dispositivos físicos e sistemas devem ser classificados de acordo com a sua criticidade para a organização.

Evidências

1 Inventário atualizado dos ativos com:
   a. Informação de inventário;
   b. Identificação dos responsáveis pelos ativos;
   c. Classificação dos ativos em função da sua criticidade.

R.N. CIS CSC 2;
COBIT 5 BAI09.01, BAI09.02, BAI09.05;
ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1;
NIST SP 800-53 Rev. 4 CM-8, PM-5.

ID.GA-2 - As aplicações e plataformas de software que suportam os processos dos serviços críticos devem ser inventariadas

Descrição

As aplicações e plataformas de software da organização, que suportam os processos dos serviços críticos, devem ser inventariadas e classificadas de acordo com a sua relevância para a organização.

Implementação Técnica

1 Ferramentas/aplicações de gestão de ativos.

Implementação Processual

A organização deve elaborar o inventário de todas as suas aplicações, identificando:

1 Informação necessária ao inventário de uma aplicação;

2 Os responsáveis pelas aplicações com, pelo menos, os seguintes elementos: Nome, contacto e departamento;

3 A classificação em função da criticidade da aplicação para a organização;

4 Quando aplicável, o tipo de contrato de suporte em vigor com o fornecedor da aplicação ou plataforma de software.

Evidências

1 A organização deve possuir um inventário atualizado de todas as suas aplicações e plataformas de software, com a identificação da sua criticidade e dos seus responsáveis.
   - **a.** Informação de inventário;
   - **b.** Identificação dos responsáveis;
   - **c.** Classificação das aplicações ou plataformas de software ou em função da sua criticidade.

R.N. CIS CSC 2;
COBIT 5 DSS05.2;
ISO/IEC 27001:2013 A.13.2.1, A.13.2.2;
NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8.

ID.GA-3 - As redes e fluxos de dados devem ser mapeados

Descrição

A organização deve possuir um inventário com todas as suas redes de comunicações e o mapeamento dos seus fluxos de comunicação internos e externos. Esta informação é essencial para que a organização tenha conhecimento dos ativos que suportam a sua infraestrutura de comunicações e dos respetivos fluxos de comunicação existentes.

Implementação Técnica

1 Ferramentas/aplicações de gestão de ativos.

Implementação Processual

A organização deve executar as seguintes atividades:

1 Inventariar os seus ativos de rede de comunicações;

2 Desenhar a sua topologia de rede de comunicações;

3 Elaborar procedimentos de transferência de informação entre si e terceiras partes;

4 Efetuar o mapeamento dos fluxos de comunicação entre os seus sistemas internos e sistemas de partes interessadas externas.

Evidências

1 A organização deve apresentar:
   a. Registos do inventário dos ativos de rede de comunicações;
   b. Lista dos fluxos de comunicação entre os seus sistemas internos e sistemas de partes interessadas externas;
   c. Mapeamentos de informação;
   d. Documentos que identifiquem os procedimentos de transferência segura de informação.

R.N. CIS CSC 12;
COBIT 5 APO02.02, APO10.04, DSS01.02;
ISO/IEC 27001:2013 A.11.2.6;
NIST SP 800-53 Rev. 4 AC-20, SA-9.

ID.GA-4 - As redes e sistemas de informação externos devem ser identificados e catalogados

Descrição

As redes e sistemas de informação da organização, que se encontram no exterior das suas instalações físicas, devem ser identificados e catalogados para que a organização tenha conhecimento da localização dos seus ativos.

Implementação Técnica

1 Ferramentas/aplicações de gestão de ativos.

Implementação Processual

A organização deve possuir um mapeamento das suas redes e sistemas de informação que se encontram no exterior, identificando pelo menos:

1 Número de inventário;

2 Tipo de equipamento;

3 Descrição;

4 Localização;

5 Responsável (nome, contacto e departamento).

Evidências

1 A organização deve possuir um inventário atualizado dos seus ativos de rede e sistemas de informação externos.

R.N. IS CSC 13, 14;
COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02;
ISO/IEC 27001:2013 A.8.2.1;
NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6.

ID.GA-5 - Os ativos necessários para a prestação de bens e serviços devem ser classificados

Descrição

A organização deve classificar os seus ativos (humanos, tecnológicos de *hardware* e *software*, dispositivos, dados, tempo e aplicações), de acordo com a criticidade e valor que estes ativos representem para si. No processo de inventariação, a organização deve:

1 Identificar um método de classificação de ativos que seja aprovado internamente;

2 Garantir que os responsáveis pelos ativos os classificam de acordo com a importância dos mesmos para a organização.

Implementação Técnica

1 Ferramentas/aplicações de gestão de ativos.

Implementação Processual

A organização deve garantir que:

1 A classificação dos ativos é efetuada de acordo com a sua importância para a atividade da organização;

2 Os seus ativos críticos são identificados.

Evidências

1 Registos da classificação dos ativos.

4.3.2 ID.AO Ambiente da Organização

ID.AO-1 - O papel da organização na cadeia logística deve ser identificado e comunicado

R.N. COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05; ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2; NIST SP 800-53 Rev. 4 CP-2, SA-12.

Descrição

A organização deve ter a capacidade de identificar e tipificar os seus fornecedores na cadeia logística e de acordo com as prestações contratualizadas com os mesmos.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve definir uma política de gestão de fornecedores que estabeleça critérios orientadores quanto aos procedimentos, comportamentos e modos de agir, que devem ser adotados nos processos de contratação e de gestão de fornecedores.

Após o processo de contratualização, deve ser registado:

1. A identificação do fornecedor;
2. A abrangência e o âmbito da relação com o fornecedor;
3. Os serviços:
   a. Essenciais e permanentes (por exemplo: segurança física das instalações, limpeza, conservação patrimonial, entre outros);
   b. Eventuais, para exercer atividade de curta duração (por exemplo: manutenção de impressoras, pequenos arranjos, manutenção de hardware, entre outros);
4. Os processos, departamentos e funcionários da organização que tenham usufruto dos serviços eventuais ou permanentes prestados pelo fornecedor;
5. Um ponto de contacto na organização, que poderá ser de um gestor do contrato com o fornecedor, que tenha a responsabilidade de responder pelo desempenho técnico e comportamentos do mesmo;
6. As restrições administrativas que possam existir (conflitos de interesse, contratação de ex-colaboradores sem autorização expressa da direção, idoneidade, entre outras).

Evidências

1. Documentos de suporte à política de gestão de fornecedores;
2. Registos de tipificação e identificação de fornecedores.

R.N. COBIT 5 APO02.06, APO03.01;
ISO/IEC 27001:2013 Cláusula 4.1;
NIST SP 800-53 Rev. 4 PM-8.

ID.AO-2 - O posicionamento da organização no seu setor de atividade deve ser identificado e comunicado

Descrição

A organização deve ser capaz de:

1 Identificar o seu enquadramento no respetivo setor de atividade;

2 Identificar as partes interessadas, internas e externas, que são relevantes para a sua atividade.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve identificar, na sua política de segurança da informação, a sua missão, objetivos e partes interessadas.

A organização deve efetuar uma análise SWOT nos contextos externo e interno, que identifique os seus pontos fortes, pontos fracos, oportunidades e ameaças.

Evidências

Documento da política de segurança da informação na organização, que deve incluir:

1 Identificação da visão, missão e objetivos de segurança da informação;

2 Identificação das partes interessadas, no âmbito da segurança da informação;

3 Análise SWOT.

R.N. COBIT 5 APO02.01, APO02.06, APO03.01;
NIST SP 800-53 Rev. 4 PM-11, SA-14.

ID.AO-3 - A missão, visão, valores, estratégias e objetivos da organização devem ser definidas e comunicadas

Descrição

A missão, visão, valores, estratégias e objetivos são os princípios fundamentais de orientação de uma organização. Indicam a forma como esta se posiciona no seu setor de atividade e como procura ser reconhecida pelos colaboradores, clientes, fornecedores e outras organizações terceiras.

Implementação Técnica

Não aplicável.

Implementação Processual

1 Documentar a missão, visão, valores e objetivos da organização;

2 Identificar as partes interessadas na política de segurança da informação.

Evidências

1 Documentos de suporte à política de segurança da informação, com a identificação da visão, missão, objetivos e partes interessadas, internas e externas, à organização.

ID.AO-4 - Os ativos críticos devem ser identificados e registados

R.N. COBIT 5 APO10.01, BAI04.02, BAI09.02;
ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3;
NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14.

Descrição

A organização deve garantir a identificação e o registo de ativos críticos, uma vez que estes contribuem para a prestação dos serviços essenciais. No registo de ativos, devem estar incluídos:

1 Redes e sistemas de suporte a serviços críticos para a atividade da organização, que necessitem de ser protegidos contra falhas de energia ou outras disrupções, causadas por anomalias nos serviços de suporte;

2 Cablagem elétrica e/ou de redes de comunicações, que suportem os seus serviços e que necessitem de proteção adequada contra danos e interferências;

3 Monitorização da capacidade das suas redes e sistemas de suporte a serviços críticos para a atividade da organização, de modo a poder efetuar projeções de necessidades futuras e análises de resiliência contra falhas e ataques.

Implementação Técnica

1 Ferramentas/aplicações de gestão de ativos;

2 Programas de gestão e planeamento de capacidade.

Implementação Processual

A organização deve efetuar a identificação e o registo dos ativos que suportam os seus serviços críticos, seguindo as diretrizes indicadas em ID.GA-1, bem como acautelar a sua capacidade e respetiva redundância em caso de falha. Exemplo de redundâncias:

1 UPS de suporte;

2 Ligações de comunicações redundantes;

3 Sistema AVAC;

4 Pontos de rede com mapeamento de:
   a. Correspondência com as portas nos equipamentos de rede;
   b. Localização.

A organização deve implementar um processo de monitorização e de gestão de capacidade dos seus ativos críticos.

Evidências

1 Documentos e registos de ativos de suporte primários e respetiva capacidade;

2 Documentos de identificação de ativos de suporte redundantes ou secundários e respetiva capacidade.

R.N. COBIT 5 BAI03.02, DSS04.02; ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1; NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14.

ID.AO-5 - Os requisitos de resiliência necessários para suportar a prestação de serviços críticos devem ser definidos

Descrição

A organização deve identificar e definir quais são os requisitos de resiliência adequados para suportar a prestação dos seus serviços críticos.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Identificar cenários de crise;

2 Identificar uma estratégia de recuperação[1] face a desastres naturais e/ou ataques maliciosos;

3 Definir um plano de recuperação dos serviços críticos que, em caso de desastre e/ou ataque malicioso, permita à organização:

   a. Identificar as atividades, tempos e necessidades de recuperação da sua operação;

[1] Ver ISO/IEC 22301 - Society security -- Business continuity management systems -- Requirements

b. Identificar os planos de testes de recuperação adequados.

Evidências

1 Documentos de suporte à estratégia de proteção contra desastres naturais e ataques maliciosos;

2 Documentos de suporte à estratégia da continuidade do negócio para a atividade da organização no contexto da segurança da informação;

3 Documentos de justificação de capacidade e planeamento.

4.3.3 ID.GV Governação

R.N. CIS CSC 19; COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02; ISO/IEC 27001:2013 A.5.1.1; NIST SP 800-53 Rev. 4 -1 todos os controlos de segurança.

ID.GV-1 - A política de segurança da informação deve ser definida e comunicada

Descrição

A organização deve:

1 Definir a sua política de segurança da informação;

2 Garantir o compromisso da gestão de topo na aprovação da política de segurança da informação;

3 Comunicar às partes interessadas a existência da política de segurança da informação.

Implementação Técnica

Efetuar a publicação da política de segurança da informação em repositório de fácil acesso a todos os colaboradores da organização. Exemplos de locais para alojamento e publicação:

1 Intranet;

2 Sistema de gestão documental.

Implementação Processual

A organização deve garantir que a sua política de segurança da informação:

1 Identifica qual a base que conduziu à sua definição;

2 É formalmente aprovada pela sua gestão de topo;

3 É formalizada junto das partes interessadas;

4 É publicada em local de acesso simples.

Evidências

1 Documento com a política de segurança da informação;

2 Aprovação da política de segurança da informação pela gestão de topo;

3 Publicação da política em formato digital, de fácil acesso pelas partes interessadas;

4 Entrevista ou registo da tomada de conhecimento das políticas de segurança.

R.N. CIS CSC 19;
COBIT 5 BAI02.01, MEA03.01, MEA03.04;
ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5;
NIST SP 800-53 Rev. 4 -1 todos os controlos de segurança.

ID.GV-2 - Os requisitos legais e regulamentares para a cibersegurança devem ser cumpridos

Descrição

A organização deve garantir que cumpre as leis e regulamentos de cibersegurança, de acordo com a legislação nacional e europeia em vigor. Para esse efeito, deve definir-se quais são os requisitos legais, regulamentares e contratuais nacionais e europeus que necessitam de ser observados e seguidos.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Identificar, na sua política de segurança da informação, as conformidades legais (nacionais e europeias) aplicáveis e as garantias de proteção de propriedade intelectual;

2 Criar uma política de privacidade, de acordo com a legislação nacional e europeia em vigor.

Evidências

1 Documento com a lista de requisitos legais, regulamentares e contratuais;

2 Relatórios de auditorias que comprovem a conformidade com a legislação e regulamentação;

3 Existência de política de privacidade, de acordo com a legislação nacional e europeia em vigor.

4.3.4 ID.AR Avaliação do Risco

ID.AR-1 - As vulnerabilidades dos ativos devem ser identificadas e documentadas

R.N. CIS CSC 4; COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02; ISO/IEC 27001:2013 A.12.6.1, A.18.2.3; NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5.

Descrição

Uma das bases da avaliação do risco da organização deve ser o processo de gestão de vulnerabilidades. Nomeadamente, todas as vulnerabilidades conhecidas que não foram mitigadas e/ou solucionadas.

Estas vulnerabilidades devem ser avaliadas em sede de análise do risco da organização e deve ser formalmente definida qual a estratégia a aplicar, respeitando a metodologia de gestão e risco da organização.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve garantir que no seu processo de análise do risco:

1 Efetua a tipificação de vulnerabilidades dos seus ativos que possam ser exploradas por possíveis ameaças;

2 Identifica as vulnerabilidades já conhecidas, que são resultantes do seu processo de gestão de vulnerabilidades e que não estão mitigadas/solucionadas.

Evidências

1 Documentos de suporte à gestão do risco;

2 Registos de execução da gestão do risco.

ID.AR-2 - A organização deve partilhar informações sobre ameaças de cibersegurança com grupos de interesse da especialidade

R.N. CIS CSC 4; COBIT 5 BAI08.01; ISO/IEC 27001:2013 A.6.1.4; NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16.

Descrição

A organização deve estabelecer contacto com grupos de interesse sobre a temática da segurança da informação, para que possa trocar experiências sobre boas práticas e ter acesso a informações relevantes sobre segurança da informação.

As informações sobre ameaças de cibersegurança podem ser recolhidas junto de fóruns ou em fontes de partilha de informações da especialidade.

Implementação Técnica

Caso as fontes de partilha de informação sejam de formato eletrónico e passíveis de ser consumidas por interfaces aplicacionais, devem ser sistematizados processos automáticos de recolha, tratamento e armazenamento das mesmas, para posterior correlação pelos sistemas de gestão de eventos.

Implementação Processual

A organização deve:

1 Estabelecer contactos com grupos de interesse e especialistas técnicos;

2 Ter acesso a:
   a. Bases de dados e a listas de distribuição sobre vulnerabilidades e correções;
   b. Fontes públicas e/ou privadas de conhecimento sobre ameaças.

Evidências

1 Registo estruturado de contactos estabelecidos com grupos de interesse, listas de distribuição e especialistas técnicos;

2 Registo de integrações com fontes de conhecimento externas.

R.N. CIS CSC 4; COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04; ISO/IEC 27001:2013 Cláusula 6.1.2; NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16.

ID.AR-3 - As ameaças internas e externas devem ser identificadas e documentadas na metodologia de gestão do risco

Descrição

No âmbito do processo de gestão do risco, a organização deve identificar e documentar as possíveis ameaças que possam explorar vulnerabilidades eventualmente existentes nos seus ativos.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve, em sede de análise do risco, identificar as ameaças que possam colocar em causa a integridade, confidencialidade ou disponibilidade dos seus ativos.

Evidências

1 Documentos que suportem a metodologia de gestão do risco;

2 Registos de suporte à gestão do risco.

R.N. CIS CSC 4; COBIT 5 APO12.02; ISO/IEC 27001:2013 A.12.6.1; NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16.

ID.AR-4 - A gestão do risco deve ser efetuada com base na análise de ameaças, vulnerabilidades, probabilidades e impactos

Descrição

A organização deve identificar, na sua metodologia de gestão do risco, quais os critérios associados à aferição de probabilidade e impacto dos riscos, por forma a calcular o nível do risco associado. As vulnerabilidades e ameaças devem ser tidas em linha de conta no processo de identificação dos riscos.

Implementação Técnica

Não aplicável.

Implementação Processual

Devem ser identificados, na metodologia de gestão do risco, os níveis de impacto e de probabilidade a serem considerados. Estas identificações são essenciais para a aferição da severidade associada aos riscos a analisar.

A identificação do valor do ativo poderá ser importante para a definição das prioridades de tratamento dos riscos.

A introdução de uma função para o cálculo do nível do risco, torna menos subjetiva e mais consistente a avaliação do mesmo.

Fatores críticos para a função:

1 Impacto;

2 Probabilidade;

3 Relevância do ativo para a organização (se aplicável).

A organização poderá atribuir um intervalo de níveis[1] a cada um destes fatores, de acordo com a probabilidade de o risco ocorrer, do impacto esperado do mesmo ou da relevância do ativo para a organização.

O nível do risco é o resultado do produto de dois ou mais fatores acima identificados. Poderá ser: *Impacto X Probabilidade ou Impacto X Probabilidade X Valor do ativo*.

[1] Ver capítulo de gestão dos riscos

Evidências

1 Documentos que suportem a metodologia de gestão do risco, garantindo a identificação de:
   a. Níveis de impacto;
   b. Níveis de probabilidade;
   c. Importância do ativo para a organização (se aplicável);
   d. Função para cálculo do nível do risco.

2 Registos de suporte à gestão do risco.

R.N. CIS CSC 4; COBIT 5 APO12.05, APO13.02; ISO/IEC 27001:2013 Cláusula 6.1.3; NIST SP 800-53 Rev. 4 PM-4, PM-9.

ID.AR-5 - A organização deve garantir que as respostas aos riscos são identificadas e priorizadas

Descrição

A organização deve definir a resposta adequada ao nível do risco encontrado. A prioridade de tratamento dos riscos deve ser definida de acordo com o nível do risco observado e a criticidade do ativo para a organização.

Implementação Técnica

Não aplicável.

Implementação Processual

A metodologia de análise e tratamento do risco da organização deve contemplar:

1 A definição da estratégia de resposta aos riscos;

2 A definição da estratégia de priorização, de acordo com:
   a. O nível do risco identificado;
   b. A importância do ativo para a organização.

Evidências

1 Documento de suporte à metodologia de gestão do risco, com a definição da resposta e priorização dos riscos;

2 Registos de suporte à gestão do risco.

4.3.5 ID.GR Estratégia de Gestão do Risco

R.N. CIS CSC 4; COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02; ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3; NIST SP 800-53 Rev. 4 PM-9.

ID.GR-1 - A organização deve definir um processo de gestão do risco

Descrição

A organização deve garantir que o seu processo de gestão do risco se encontra devidamente definido e gerido, assim como, acordado entre as partes interessadas relevantes.

A organização deve, no âmbito da gestão do risco:

1 Definir uma estratégia compreensiva de gestão dos riscos associados com a utilização e operação das redes e sistemas de informação;

2 Procurar que a estratégia definida seja seguida de forma consistente por toda a organização;

3 Nomear responsáveis pelo processo de gestão do risco;

4 Nomear responsáveis pelo tratamento do risco.

Implementação Técnica

A organização deve suportar-se em sistemas de informação orientados para a gestão do risco.

Implementação Processual

1 A organização deve definir uma estratégia de governação para riscos, que garanta a gestão de todo o ciclo de vida dos mesmos;

2 Devem ser contemplados os riscos organizacionais e operacionais sobre os ativos relacionados com as redes e sistemas de informação;

3 A metodologia de gestão do risco a escolher poderá ser baseada na norma ISO/IEC 27005, que orienta as organizações no processo de definição e identificação de regras e práticas de gestão dos riscos de segurança da informação;

4 Deve ser consistente por toda a organização e identificada de forma não ambígua:
   a. A estratégia de tolerância ao risco, aceite e assumida pela organização;
   b. As metodologias de definição, avaliação e tratamento dos riscos;
   c. A metodologia de monitorização da evolução dos riscos ao longo do tempo.

Evidências

1 Documento com a definição da estratégia de identificação, avaliação e tratamento dos riscos.

R.N. COBIT 5 APO12.06;

ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3;

NIST SP 800-53 Rev. 4 PM-9.

ID.GR-2 - A organização deve determinar e identificar a sua tolerância ao risco

Descrição

A organização deve definir, na sua metodologia de gestão do risco, a sua estratégia de tratamento do risco, tendo em consideração os níveis dos riscos existentes e a sua tolerância ao risco.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve identificar, na sua metodologia de gestão do risco:

1 A sua estratégia de tratamento do risco;

2 Qual o processo de aprovação da estratégia de tratamento dos riscos por parte da gestão de topo.

Evidências

1 Documento que suporta a metodologia de gestão do risco.

R.N. COBIT 5 APO12.02;

ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3;

NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11.

ID.GR-3 - A organização deve definir a sua estratégia de tratamento do risco

Descrição

A organização deve definir a resposta de tratamento do risco a aplicar aos seus ativos críticos, tendo em conta a sua tolerância ao risco, de acordo com o seu papel no seu setor de atividade.

Implementação Técnica

Não aplicável.

Implementação Processual

Na metodologia de gestão do risco, deve ser identificada a estratégia de respostas aos riscos associados aos ativos críticos observados. As respostas para tratamento do risco da organização devem ser:

1 Evitar o risco – Colocar a probabilidade ou impacto tendencialmente próximos de zero, tornando mais difícil a sua ocorrência e/ou eliminar totalmente o seu impacto;

2 Aceitar o risco – Decisão de aceitação do risco. A assunção de responsabilidade por essa decisão deve ser formalmente registada pela organização;

3 Mitigar o risco – Reduzir a probabilidade e/ou impacto de um evento adverso para limites aceitáveis, através da implementação de controlos ou contramedidas;

4 Transferir o risco – Transferir, total ou parcialmente, para terceiras partes, o impacto em relação a uma ameaça (por exemplo: efetuar a contratualização de um seguro).

Evidências

1 Documento que suporta a metodologia de gestão do risco.

4.3.6 ID.GL Gestão do Risco da Cadeia Logística

R.N. CIS CSC 4; COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02; ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2; NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9.

ID.GL-1 - A organização deve definir, avaliar e gerir processos de gestão do risco da cadeia logística

Descrição

A organização deve garantir que efetua uma análise às partes interessadas pertencentes à sua cadeia logística, utilizando a mesma metodologia de análise e de gestão interna do risco.

Implementação Técnica

Não aplicável.

Implementação Processual

Na política de gestão de fornecedores, a organização deve identificar:

1 Os responsáveis internos pela execução da análise do risco;

2 A periodicidade da análise dos riscos.

Evidências

1 Documento de suporte à política de gestão de fornecedores.

R.N.COBIT 5
APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03;
ISO/IEC 27001:2013 A.15.2.1, A.15.2.2;
NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9.

ID.GL-2 - A organização deve avaliar o risco da cadeia logística de cibersegurança

Descrição

Os fornecedores de redes e sistemas de informação, componentes e serviços de cibersegurança devem ser identificados, priorizados e avaliados, recorrendo a um processo de avaliação do risco da cadeia logística de cibersegurança.

A organização deve categorizar os seus fornecedores, tendo em conta:

1 A exposição da sua informação aos fornecedores;

2 O impacto na cadeia logística;

3 O tipo de bens e serviços fornecidos.

Implementação Técnica

Não aplicável.

Implementação Processual

A categorização geral dos fornecedores deve ser efetuada na política de gestão de fornecedores.

Os fornecedores devem ser categorizados por níveis, de acordo com a exposição da informação da organização perante os mesmos.

A organização deve efetuar a categorização dos seus fornecedores, identificando a seguinte informação:

1 Nome do fornecedor;

2 Tipo de fornecedor (categoria);

3 Criticidade para a prestação dos serviços críticos;

4 Nível de exposição:
   a. Confidencialidade;
   b. Integridade;
   c. Disponibilidade.

Evidências

1 Política de gestão de fornecedores, com a identificação das regras de categorização dos fornecedores;

2 Registo dos fornecedores com a respetiva categorização.

R.N. COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05;
ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3;
NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9.

ID.GL-3 - Os contratos com fornecedores devem respeitar o plano de gestão do risco para a cadeia logística

Descrição

A organização deve garantir que os seus fornecedores cumprem as suas regras de tratamento e segurança da informação.

Os contratos com fornecedores devem ser utilizados para implementar medidas adequadas, de modo a garantir o cumprimento dos objetivos da política de segurança da informação da organização e do plano de gestão do risco para a cadeia logística.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve garantir que a sua política de gestão de fornecedores contempla a obrigatoriedade de:

1 Inclusão de cláusulas de confidencialidade nos contratos estabelecidos com fornecedores;

2 Implementação de acordos de não divulgação com os fornecedores e os seus colaboradores.

As cláusulas de confidencialidade e acordos de não divulgação devem garantir a confidencialidade no tratamento de informação:

1 Da organização;

2 Dos seus clientes;

3 Restantes fornecedores.

Evidências

1 Política de gestão de fornecedores, com a identificação das regras contratuais e de colaboração da organização com os seus fornecedores.

R.N. COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05;

ID.GL-4 - Os fornecedores devem ser periodicamente avaliados

Descrição

A organização deve ter implementados mecanismos contratuais com os seus fornecedores, que lhe permitam medir a qualidade do serviço prestado ou do produto fornecido pelos mesmos.

ISO/IEC 27001:2013 A.15.2.1, A.15.2.2;
NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12.

Os fornecedores devem ser periodicamente avaliados por meio de auditorias, resultados de testes ou outras formas de avaliação, para que a organização verifique se estão a cumprir com as suas obrigações contratuais, as quais devem incluir medidas de cibersegurança.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve identificar na sua política de gestão de fornecedores:

1 O plano de auditoria;

2 Os métodos de auditoria e de teste;

3 Processo de monitorização e melhoria contínua dos serviços prestados ou do produto fornecido pelos seus fornecedores.

Os pontos anteriores deverão ser avaliados de acordo com a categorização que a organização atribui aos seus fornecedores. Esta categorização deverá ser definida mediante avaliação da exposição da informação da organização aos mesmos.

Evidências

1 Documentos de suporte da política de gestão de fornecedores;

2 Lista dos fornecedores.

R.N. CIS CSC 19;20; COBIT 5 DSS04.04;
ISO/IEC 27001:2013 A.17.1.3;
NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9.

ID.GL-5 - O plano de resposta e recuperação de desastre deve ser exercitado com o acompanhamento de fornecedores

Descrição

A organização deve identificar quais dos seus fornecedores devem participar nos seus planos de resposta e recuperação e garantir que os mesmos são envolvidos nos testes e nos exercícios planeados.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve garantir que:

1 Identifica na lista de fornecedores se o mesmo faz parte de um plano de resposta e/ou de recuperação e, em caso afirmativo, qual o plano associado;

2 Por intermédio de planeamento prévio, os fornecedores elegíveis acompanham os testes e exercícios associados aos planos de resposta e recuperação.

Evidências

1 Documento de registo e identificação de fornecedores;

2 Relatório dos exercícios e dos testes de recuperação de desastre.

MEDIDAS DE SEGURANÇA

PROTEGER

4.4.1 PR.GA Gestão de Identidades, Autenticação e Controlo de Acessos

PR.GA-1 - O ciclo de vida de gestão de identidades deve ser definido

R.N. CIS CSC 1, 5, 15, 16;
COBIT 5 DSS05.04, DSS06.03;
ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3;
NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11.

Descrição

A organização deve garantir que as identidades e credenciais de acesso às suas redes e sistemas de informação são emitidas, geridas, verificadas, revogadas e auditadas em conformidade com os processos instituídos.

Implementação Técnica

1 Sistema de informação para a gestão de identidades e acessos;

2 Diretório central de utilizadores e grupos;

3 Serviços de autenticação federada.

Implementação Processual

A organização deve criar, disseminar, rever e atualizar:

1 Processo de gestão de acessos a ativos da organização;

2 Perfis funcionais e acessos associados;

3 Procedimentos de implementação do processo de gestão de acessos.

No sistema de gestão de identidades e processo de gestão de acessos, a organização deve:

1 Identificar os tipos de contas existentes por tipo de utilização, tais como: nominais, privilegiadas, serviço, aplicacionais, temporárias, emergência, entre outras;

2 Definir as regras e condições para pertença a grupos e perfis;

3 Definir os utilizadores autorizados para um dado sistema de informação;

4 Definir as aprovações necessárias para a atribuição de cada acesso;

5 Criar, ativar, inativar, modificar e remover contas;

6 Notificar os responsáveis, no caso de determinado acesso:
   a. Se tornar obsoleto;
   b. O utilizador ser reenquadrado funcionalmente e/ou organizacionalmente;
   c. Quando o utilizador cessa o seu relacionamento profissional com a organização;
   d. Quando se verifique qualquer situação que possa provocar alterações ao perfil do utilizador.

Evidências

1 Documentação de suporte ao processo de gestão do ciclo de vida dos utilizadores;
2 Catálogo de acessos aos ativos da organização;

3 Registo de gestão de utilizadores no sistema de gestão de identidades.

R.N. COBIT 5 DSS01.04, DSS05.05; ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8; NIST SSP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8.

PR.GA-2 - Devem existir controlos de acesso físico às redes e sistemas de informação

Descrição

A organização deve proteger e gerir o acesso físico às suas infraestruturas de rede e de sistemas de informação.

A organização deve aplicar este controlo aos seus colaboradores e visitantes, a zonas da organização que sejam de acesso restrito e/ou a áreas sensíveis que alojem informação confidencial, redes e/ou sistemas de informação.

Implementação Técnica

A organização deve:

1 Efetuar o controlo de acessos baseado em cartões magnéticos (ou utilizando outro método de autenticação equivalente) e criando barreiras de acesso com torniquetes e/ou portas de segurança que restrinjam o acesso às zonas que se pretende proteger;

2 Garantir a integração do sistema de controlo de acessos com o sistema de gestão de identidades, com a instanciação do acesso parametrizado a zonas físicas e com a autorização validada centralmente;

3 Manter o registo de entradas e saídas com informação de pessoas externas com, pelo menos, os seguintes elementos: Nome, empresa, data/hora de início da visita, data/hora de fim da visita, acompanhante interno e o propósito da visita.

Implementação Processual

A organização deve:

1 Criar e manter uma lista das pessoas com acessos autorizados a zonas reservadas, onde as redes e os sistemas de informação estão alojados;

2 Emitir credenciais de autorização específicas por acesso (por exemplo: cartões magnéticos e credenciais de acesso único);

3 Rever e aprovar as listas de acessos e credenciais de autorização específicas, com a periocidade a ser definida pela organização;

4 Controlar o acesso às zonas de segurança definidas:
   a. Verificando a identidade de indivíduos antes de lhes permitir a entrada;
   b. Controlando entradas e saídas, usando os mecanismos de restrição física adequados;
   c. Mantendo um registo de auditoria de passagem por pontos chave;
   d. Garantindo acompanhamento de visitantes por pessoas autorizadas;

5 Providenciar os controlos de segurança considerados necessários para garantir acessos a zonas públicas.

Evidências

1 Registo de entradas e saídas de zonas de acesso reservado;

2 Existência de meios físicos que garantam a restrição de acessos a pessoas devidamente autenticadas.

R.N. CIS CSC 12;
COBIT 5 APO13.01, DSS01.04, DSS05.03;
ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1;
NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15.

PR.GA-3 - A organização deve gerir os seus acessos remotos

Descrição

A organização deve documentar, gerir e controlar os acessos remotos às suas redes e sistemas de informação.

São considerados acessos remotos, todos os acessos feitos às redes e sistemas de informação por colaboradores que comuniquem através de redes de comunicações externas à organização. As VPN, quando criadas, devem ser consideradas redes de comunicações internas, observando-se os controlos de segurança apropriados.

Cumulativamente, apenas são considerados acessos remotos a redes e sistemas de informação, aqueles que sejam realizados a sistemas cujo propósito original não seja disponibilizar informação para consulta pública.

Implementação Técnica

1 Gestão de Identidades e Acessos;

2 Diretório de Utilizadores e Grupos;

3 Serviços de Autenticação Federada;

4 Solução tecnológica para acesso remoto.

Implementação Processual

A organização deve:

1 Documentar a política de acessos remotos a redes e sistemas de informação;

2 Documentar a política de teletrabalho;

3 Estabelecer regras e restrições de utilização de cada tipo de acesso remoto;

4 Monitorizar acessos remotos não autorizados;

5 Autorizar formalmente os acessos a redes e sistemas de informação, via acesso remoto, antes do acesso ser atribuído;

6 Definir e garantir os requisitos para acessos de ligações remotas a redes e sistemas de informação.

Evidências

1 Documentos de suporte às políticas de gestão do teletrabalho e acessos remotos;

2 Existência de solução tecnológica que permita o acesso remoto cifrado/seguro a redes e sistemas de informação.

R.N. CIS CSC 3, 5, 12, 14, 15, 16, 18; COBIT 5 DSS05.04; ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5; NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24.

PR.GA-4 - A organização deve aplicar na gestão de acessos, os princípios do menor privilégio e da segregação de funções

Descrição

As permissões de acesso e as autorizações devem ser geridas de acordo com os princípios de acesso adequados à função, de acordo com os princípios de necessidade de conhecer e de segregação de funções.

Entende-se, por menor privilégio, que a concessão de acessos às redes e sistemas de informação da organização aos colaboradores devem ser as estritamente necessárias para o correto desempenho das suas funções. Por segregação de funções, entende-se a prática da divisão do conhecimento e de privilégios entre múltiplos indivíduos, de forma a que um processo em particular não possa ser executado ou controlado apenas por um deles.

O principal fundamento, para a aplicação desta prática de segregação de funções, é a prevenção de incidentes de segurança com impacto significativo nas atividades operacionais da organização. Existindo múltiplas pessoas envolvidas, minimiza-se a oportunidade de transgressões e fomenta-se a probabilidade de estas serem detetadas e reportadas.

O princípio de segregação de funções pode ser aplicado nos seguintes tipos de processos:

1 Sequenciais: Quando as atividades podem ser executadas em tarefas sequenciais e por pessoas diferentes (por exemplo: na atribuição de acessos, uma pessoa solicita, outra aprova e uma terceira atribui os acessos);

2 Quórum: Quando as atividades requerem um quórum mínimo de aprovações para poderem ser executadas (por exemplo: a recuperação de uma chave de cifra, onde é requerida a presença de dois ou mais administradores de sistemas);

3 Geoespacial: Quando as atividades podem ser divididas em tarefas que são realizadas em locais diferentes (por exemplo: gestão de sistemas de informação, cujas tarefas são efetuadas por colaboradores sediados em diferentes zonas geográficas).

Implementação Técnica

1 Gestão do ciclo de vida de Identidades e Acessos.

Implementação Processual

A organização deve:

1 Criar um mapeamento de funções por perfis;

2 Criar um mapeamento de perfis por acessos;

3 Ter um processo formal para a gestão do ciclo de vida de acessos;

4 Praticar os princípios de menor privilégio;

5 Aplicar o princípio de segregação de funções e identificar os acessos que correspondem a atividades críticas.

Evidências

1 Documentos de suporte ao processo de gestão de acessos;

2 Registos da identificação de acessos a sistemas e aplicações por perfil funcional;

3 Matriz de segregação de funções por acessos e respetivas atribuições.

R.N. CIS CSC 9, 14, 15, 18;
COBIT 5 DSS01.05, DSS05.02;
ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3;
NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7.

PR.GA-5 - A organização deve proteger a integridade das redes de comunicações

Descrição

A integridade das redes de comunicações deve ser protegida por intermédio da sua segregação e segmentação.

A rede de comunicações deve ser desenhada de forma a não ser possível aceder-se a qualquer sistema, a partir de qualquer ponto da mesma.

Devem ser criadas zonas de segurança com propósitos identificados e com barreiras bem definidas e forçadas por equipamentos de rede de comunicações com capacidade para o efeito (routers, gateways, firewalls, entre outros).

As segregações da rede de comunicação devem ser documentadas em políticas que definam o seu modelo de governo, nomeadamente, que autorizações são necessárias para a aprovação de novos fluxos e que fluxos entre zonas são pré-aprovados. Os fluxos de informação entre sistemas devem obrigar a autorizações específicas e estar de acordo com as políticas definidas para o efeito.

Exemplos do que as restrições de fluxos devem incluir:

1 Impedimentos de transmissão de informação sensível em claro para a Internet;

2 Bloqueio de tráfego externo que indica ser interno (forjado);

3 Restrição de acessos diretos à Internet que não sejam feitos através de um proxy corporativo;

4 Limitação de transferências de informação, com base em estruturas de dados e conteúdos.

O controlo dos fluxos de comunicação deve ser efetuado com base nas características da informação e no caminho que a mesma efetua ao longo do seu transporte. A aplicação de restrições deve ser efetuada nos equipamentos de fronteira, como *routers*, *firewalls* ou *proxies*.

Implementação Técnica

1 Firewall;

2 Criação de redes de comunicações reservadas com perfis específicos (por exemplo: Gestão, DMZ, *Internet*, *Intranet*, entre outras).

Implementação Processual

A organização deve:

1 Criar uma norma de segregação de redes de comunicações;

2 Definir zonas exclusivas, sub-redes associadas e funcionalidades atribuídas;

3 Definir regras de fluxos de comunicação pré-aprovadas para cada zona e entre zonas;

4 Definir e implementar os procedimentos de alteração de regras de fluxos;

5 Definir e implementar os procedimentos de revisão de regras de fluxos antigos ou não utilizados, por um período temporal a definir pela organização;

6 Garantir a segregação de funções nas diferentes atividades da gestão dos fluxos de comunicação;

7 Criar uma política de transferência de informação que garanta a cifra da comunicação;

8 Criar regras de utilização de acesso às redes de comunicações.

Evidências

1 Documento com a política de segregação de redes de comunicações e de zonas de segurança;

2 Documento de suporte à política de transferência de informação;

3 Documento de suporte à política de utilização e acesso às redes de comunicações;

4 Documentos operacionais de suporte das redes de comunicações;

5 Registos de pedidos e aprovações de alteração de fluxos das redes de comunicações.

R.N. CIS CSC, 16; COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03; ISO/IEC 27001:2013, A.7.1.1, A.9.2.1; NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3.

PR.GA-6 - A organização deve verificar a identidade dos colaboradores e vinculá-las às respetivas credenciais

Descrição

A identidade dos colaboradores deve ser vinculada, revista e as suas credenciais confirmadas interativamente, quando necessário.

A verificação de antecedentes deve ser efetuada respeitando a legislação laboral aplicável.

Implementação Técnica

1 Gestão de Identidades e Acessos.

Implementação Processual

A organização deve:

1 Efetuar a verificação de credenciais e referências dos novos colaboradores nos termos permitidos por lei e de forma adequada às funções que o mesmo irá exercer;

2 Implementar um processo formal de registo de novos colaboradores (onde é associado um utilizador único e nominal);

3 Implementar um processo formal de cancelamento de registo de ex-colaboradores;

4 Implementar um processo formal de gestão de acessos.

Evidências

1 Registos das verificações de antecedentes efetuadas;

2 Documentos de suporte ao processo de gestão de acessos;

3 Documentos de suporte ao processo de entrada e saída de colaboradores;

4 Registos de funcionamento do processo de entrada e saída de colaboradores e do processo de gestão de acessos.

PR.GA-7 - Devem ser definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação

R.N. CIS CSC 1, 12, 15, 16; COBIT 5 DSS05.04, DSS05.10, DSS06.10; ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4; NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11.

Descrição

Os mecanismos de autenticação devem ser definidos e mantidos de acordo com as características dos sistemas e dos perfis de acessos, por forma a permitir a manutenção da integridade e a confidencialidade da informação.

Implementação Técnica

1 Gestão de Identidades e Acessos;

2 Diretório de utilizadores e grupos;

3 Serviços de autenticação federada;

4 Sistemas com múltiplos fatores de autenticação.

Implementação Processual

A organização deve:

1 Criar e manter uma política de gestão de palavras-passe;

2 Criar, manter e disseminar a política de gestão de acessos;

3 Implementar múltiplos fatores de autenticação em redes e sistemas de informação que considere suficientemente críticos.

Evidências

1 Documentos de suporte à política de gestão de palavras-passe;

2 Documentos de suporte à política de gestão de acessos;

3 Relatórios de auditoria da solução de múltiplos fatores de autenticação.

4.4.2 PR.FC Formação e Sensibilização

R.N. CIS CSC 17, 18;
COBIT 5 APO07.03, BAI05.07;
ISO/IEC 27001:2013 A.7.2.2, A.12.2.1;
NIST SP 800-53 Rev. 4 AT-2, PM-13.

PR.FC-1 - Os colaboradores devem ter formação em segurança da informação

Descrição

A organização deve estabelecer um plano de ações de formação em segurança da informação, bem como definir os processos e procedimentos necessários para garantir a sua correta implementação.

A organização deve medir o sucesso das suas ações de formação.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve criar, disseminar e atualizar:

1 Um plano de ações de formação;

2 Ações de formação em segurança da informação às partes interessadas relevantes;

3 Processos e procedimentos formais que simplifiquem a implementação do ponto anterior;

4 Medir o sucesso das ações de formação realizadas através de entrevistas aos formandos das mesmas.

Evidências

1 Plano de ações de formação em segurança da informação;

2 Registo das ações de formação efetuadas e das respetivas presenças;

3 Registo dos conteúdos programáticos das ações de formação efetuadas;

4 Entrevista com os destinatários das ações de formação.

R.N. CIS CSC 5, 17, 18;
COBIT 5APO07.02, DSS05.04, DSS06.03;
ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;
NIST SP 800-53 Rev. 4 AT-3, PM-13.

PR.FC-2 - Os utilizadores com acesso privilegiado devem compreender quais são os seus papéis e responsabilidades

Descrição

Os colaboradores, com acessos privilegiados às redes e sistemas de informação da organização, devem ser devidamente consciencializados sobre as suas funções e compreender os seus papéis e responsabilidades. A organização deve definir os conteúdos programáticos necessários para que as ações de formação sobre acessos privilegiados sejam eficazes.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve providenciar ações de formação sobre a utilização de acessos privilegiados aos colaboradores:

1 Antes de estes darem início ao exercício de funções que requeiram este tipo de acessos;

2 Sempre que exista alteração aos acessos concedidos;

3 Em periodicidade a ser definida pela organização.

Evidências

1 Plano de ações de formação respeitante à temática de acessos privilegiados;

2 Registo dos conteúdos programáticos das ações de formação;

3 Registo das ações de formação efetuadas e das respetivas presenças.

R.N. CIS CSC 17;
COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05;
ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2;
NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16.

PR.FC-3 - As partes interessadas externas devem compreender quais são os seus papéis e responsabilidades

Descrição

Todas as partes interessadas, externas e relevantes para a organização, devem ter conhecimento dos seus papéis e responsabilidades no âmbito do sistema de segurança da organização. Este entendimento é essencial para aumentar o nível de segurança da informação da organização.

A organização deve efetuar ações de sensibilização para garantir que o entendimento das partes interessadas sobre este tema é o adequado e necessário.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Estabelecer os requisitos mínimos de segurança, funções e responsabilidades que os clientes e fornecedores devem seguir;

2 Requerer que os clientes e fornecedores cumpram os requisitos definidos;

3 Formar, consciencializar e auditar.

Evidências

1 Documento com requisitos mínimos de segurança a requerer aos clientes e fornecedores;

2 Relatórios de auditorias aos clientes e fornecedores sobre o cumprimento dos requisitos definidos;

3 Registos das ações de sensibilização.

R.N. CIS CSC 17, 19;
COBIT 5 EDM01.01, APO01.02, APO07.03;
ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;
NIST SP 800-53 Rev. 4 AT-3, PM-13.

PR.FC-4 - A gestão de topo deve compreender as suas funções e responsabilidades

Descrição

A gestão de topo deve demonstrar estar comprometida com a temática da segurança da informação e cibersegurança. A gestão de topo deve compreender qual é o seu papel e responsabilidade nesta temática.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve garantir que a gestão de topo:

1 Tem os seus papéis e responsabilidades definidos;

2 Participa em ações de formação sobre segurança da informação e cibersegurança.

Evidências

1 Definição de papéis e responsabilidades;

2 Matriz RACI com a envolvência da gestão de topo nas atividades de cibersegurança;

3 Registo das ações de formação.

4.4.3 PR.SD Segurança de Dados

R.N. CIS CSC 13, 14;
COBIT 5APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06;
ISO/IEC 27001:2013 A.8.2.3;
NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28.

PR.SD-1 - A organização deve proteger os dados armazenados

Descrição

As redes e sistemas de informação devem proteger a confidencialidade e integridade da informação armazenada na organização.

Implementação Técnica

1 Serviços de cifra de ficheiros, bases de dados e cópias de segurança;

2 Validação criptográfica dos dados armazenados.

Implementação Processual

A organização deve garantir que:

1 Os dados são armazenados de acordo com a classificação que lhes for atribuída para o nível de confidencialidade pretendido;

2 São estabelecidas regras de armazenamento de documentos nos diversos tipos de dispositivos da organização;

3 A política de cifra de informação contempla a proteção dos dados armazenados de acordo com a sua localização e classificação.

Evidências

1 Documentos de suporte à classificação de informação;

2 Documentos de suporte à política de cifra de informação;

3 Documentos de suporte à cifra de dados offline (por exemplo: cópias de segurança).

R.N. CIS CSC 13, 14;
COBIT 5 APO01.06, DSS05.02, DSS06.06;
ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3;
NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12.

PR.SD-2 - A organização deve proteger os dados em circulação

Descrição

A organização deve proteger a integridade e a confidencialidade da informação transmitida. Este controlo deve ser aplicado, quer a redes de comunicações internas, como externas.

Para sistemas distribuídos, este controlo deve aplicar-se em toda a linha, por forma a garantir a integridade entre os componentes e serviços que geram a informação e os componentes e serviços que a recebem.

Quando for impraticável ou impossível garantir os controlos de segurança necessários e as garantias de controlo efetivo através dos veículos contratuais apropriados, a organização deve implementar os controlos compensatórios necessários ou explicitamente aceitar o risco adicional e/ou transferir o risco para o fornecedor contratual.

Implementação Técnica

1 Serviços de cifra de comunicações.

Implementação Processual

A organização deve garantir que:

1 Efetua o transporte da informação de forma segura e de acordo com as suas regras de classificação de informação definidas;

2 A política de cifra de informação contempla controlos de proteção da confidencialidade e integridade da informação em circulação.

Evidências

1 Documentos de suporte à classificação de informação;

2 Documentos de suporte à política de transferência de informação;

3 Documentos de suporte à política de cifra de informação.

R.N. CIS CSC 1;
COBIT 5 BAI09.03;
ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7;
NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16.

PR.SD-3 - A organização deve gerir formalmente os ativos durante os procedimentos de remoção, transferência e aprovisionamento dos mesmos

Descrição

A organização deve garantir a existência de procedimentos de autorização, monitorização, registo e de controlo dos dados de redes e sistemas de informação e dos componentes que entram e saem das suas instalações.

Quando a informação deixar de ser necessária para a organização, devem ser aplicados mecanismos de higienização, que devem estar associados à classificação de segurança associada à informação.

Implementação Técnica

1 *Software* para destruição de dados;

2 *Software* de cifra para componentes amovíveis.

Implementação Processual

A organização deve:

1 Elaborar procedimentos de gestão do ciclo de vida de ativos;

2 Elaborar procedimentos de remoção e transferência de dados em suporte físico amovível.

Evidências

1 Documentos de suporte ao processo de gestão de ciclo de vida de ativos;

2 Documentos de suporte à classificação de informação;

3 Registo de execução dos pedidos de atribuição e/ou remoção de ativos a utilizadores.

R.N. CIS CSC 1, 2, 13;
COBIT 5 APO13.01, BAI04.04;
ISO/IEC 27001:2013 A.12.1.3, A.17.2.1;
NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5.

PR.SD-4 - A organização deve providenciar a capacidade adequada para garantir a disponibilidade das redes e dos sistemas de informação

Descrição

A capacidade das redes e dos sistemas de informação deve ser monitorizada. Devem ser efetuadas previsões sobre as necessidades de capacidade futura, para garantir que a performance dos sistemas está alinhada com os requisitos de prestação dos serviços críticos.

Implementação Técnica

1 Monitorização de métricas e histórico de capacidade dos recursos informáticos;

2 Implementação de redundância nas redes e sistemas de informação que suportam os serviços críticos da organização.

Implementação Processual

A organização deve:

1 Criar procedimentos para gerir os três tipos primários de capacidade:
   a. Capacidade de armazenamento (base de dados, sistemas de ficheiros, entre outros);
   b. Capacidade de memória e de processamento (poder computacional);
   c. Largura de banda e latência das redes de comunicações;

2 Ser proativa utilizando a previsão de capacidade futura para desencadear melhorias;

3 Recorrer a alertas de monitorização, antes que a capacidade instalada atinja pontos críticos que possam provocar a degradação dos serviços disponibilizados.

Evidências

1 Documentos de suporte ao processo de gestão de capacidade;

2 Relatórios de gestão de capacidade;

3 Registos das ações de avaliação da gestão de capacidade;

4 Avaliação da redundância aplicada às redes e sistemas de informação que suportam os serviços críticos.

R.N. CIS CSC 13, COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02; ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3; NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4.

PR.SD-5 - A organização deve implementar proteções que evitem exfiltração de informação

Descrição

A organização deve implementar controlos de segurança nas fronteiras das suas instalações ou das suas redes e sistemas de informação, para detetar e impedir a exfiltração não autorizada de informação.

Deve ser definido o âmbito de atuação e frequência da aplicação, com o objetivo de se adequar a mitigação do risco associado. Risco este, que deve ser calculado tendo por base a classificação de confidencialidade da informação.

Implementação Técnica

1 Implementação de sistemas de prevenção de perda de informação (DLP);

2 Sistema de classificação de informação de mensagens de correio eletrónico e documentos.

Implementação Processual

A organização deve:

1 Implementar medidas de salvaguarda para prevenir a exfiltração não autorizada de informação dos seus sistemas, como por exemplo:
   a. Obrigatoriedade de usar formatos e protocolos predefinidos;
   b. Monitorização para esteganografia;
   c. Restringir uso de interfaces externas de rede ao estritamente necessário;
   d. Monitorização dos cabeçalhos de pacotes de rede;
   e. Efetuar análises aos padrões de tráfego de rede para detetar desvios, quer de tipo, quer de volume;

2 Criar procedimentos que tornem eficaz e consistente a adoção das suas regras de classificação da informação.

Evidências

1 Documentos de suporte à política de utilização aceitável de ativos;

2 Política de classificação de informação:
   a. Tratamento e transporte de informação confidencial;

3 Registos de classificação e informação.

R.N. CIS CSC 2, 3;
COBIT 5 APO01.06, BAI06.01, DSS06.02;
ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4;
NIST SP 800-53 Rev. 4 SC-16, SI-7.

PR.SD-6 - A organização deve utilizar mecanismos de verificação para confirmar a integridade de software, firmware e dados

Descrição

A organização deve utilizar mecanismos de verificação que garantam a integridade de *software*, *firmware* e dados. Estes controlos têm como objetivo detetar manipulações não autorizadas ou erros inesperados devido a má utilização.

Implementação Técnica

1 Testes estáticos de segurança a redes e sistemas de informação;

2 Testes dinâmicos de segurança a redes e sistemas de informação;

3 Testes interativos de segurança a redes e sistemas de informação;

4 Implementação de algoritmos de verificação de integridade (verificação de paridade, códigos de Hamming, CRC e resumos criptográficos);

5 Implementação de sistema central de ferramentas de verificação de integridade.

Implementação Processual

A organização deve:

1 Definir processos/procedimentos de controlo de qualidade que exijam verificação de integridade de software e/ou firmware;

2 Definir procedimentos de verificação de integridade da informação;

3 Aplicar testes estáticos, dinâmicos e interativos ao código fonte existente.

Evidências

1 Documentos de suporte a processos/procedimentos de verificação de integridade;

2 Relatórios de execução de verificações de integridade.

R.N. CIS CSC 18, 20;
COBIT 5 BAI03.08, BAI07.04;
ISO/IEC 27001:2013 A.12.1.4;
NIST SP 800-53 Rev. 4 CM-2.

PR.SD-7 - Os ambientes de desenvolvimento e de teste devem ser separados de ambientes de produção

Descrição

A organização deve efetuar a separação dos ambientes das suas redes e dos seus sistemas de informação, de forma física ou lógica, de acordo com as suas funções.

Os ambientes de desenvolvimento e testes devem estar segregados dos ambientes de produção, quer em termos de acessos, como em termos de dados.

Implementação Técnica

1 Zonas de segurança de redes de comunicações;

2 Segregação física ou lógica de ambientes;

3 Anonimização de dados de produção para ambientes de teste.

Implementação Processual

A organização deve:

1 Criar, disseminar e atualizar uma política de desenvolvimento seguro de software;

2 Proteger os ambientes de produção, as suas redes e sistemas de informação, de eventos não planeados ou inesperados que possam estar relacionados com atividades de teste ou desenvolvimento;

3 Efetuar a gestão de configurações de ambientes, de forma independente e da maneira adequada a cada tipo de ambiente (estabilidade em produção e flexibilidade em desenvolvimento);

4 Anonimizar dados de produção antes de os copiar para ambientes de teste ou desenvolvimento;

5 Garantir que as colocações de novas versões de software em produção passam por processos de gestão de versões e de alterações.

Evidências

1 Documentos de suporte ao desenvolvimento seguro de software;

2 Documentos de suporte aos processos de gestão de alterações e versões;

3 Registos de execução dos processos de gestão de alterações e versões;

4 Registo de segregação de ambientes.

R.N. COBIT 5 BAI03.05;
ISO/IEC 27001:2013 A.11.2.4;
NIST SP 800-53 Rev. 4 SA-10, SI-7.

PR.SD-8 - A organização deve implementar mecanismos de validação e verificação de integridade do hardware

Descrição

A organização deve garantir a integridade do hardware, promovendo validações e verificações periódicas pelo fabricante ou por um fornecedor certificado.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve garantir:

1 A manutenção do seu hardware pelo fabricante ou por um fornecedor certificado.

Evidências

1 Plano de manutenção do hardware;

2 Registo dos contratos de manutenção.

4.4.4 PR.PI Procedimentos e Processos de Proteção da Informação

R.N. CIS CSC 3, 9, 11;
COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05;
ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4;
NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10.

PR.PI-1 - Deve ser criada e mantida uma configuração base de redes e sistemas de informação que incorpore os princípios de segurança

Descrição

A organização deve estabelecer uma configuração base para redes e sistemas de informação, para os seus componentes e para as suas comunicações e conectividades.

Por configuração base, entende-se:

1 Programas informáticos instalados em estações de trabalho;

2 Equipamentos pessoais, tais como computadores portáteis, impressoras e outros dispositivos móveis;

3 Servidores e elementos de rede;

4 Versões e atualizações aplicadas a sistemas operativos e aplicações, configurações e parâmetros por omissão, topologia de rede e composição lógica das arquiteturas das redes e sistemas de informação.

Implementação Técnica

1 Sistema de integração/entrega contínua (CI/CD);

2 Sistema de gestão de atualizações de segurança.

Implementação Processual

A organização deve:

1 Desenvolver, documentar e manter sob controlo de versões a configuração atual das suas redes e sistemas de informação;

2 Criar, documentar e manter uma política de segurança das redes e sistemas de informação que:
   a. Aplique os princípios de funcionalidades mínimas necessárias;
   b. Autorize, proíba e restrinja a utilização de algumas funções, portos, protocolos e serviços.

Evidências

1 Documentos de suporte à política de desenvolvimento seguro de software;

2 Registos de execução de controlo de versões.

R.N. CIS CSC 18;
COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03;
ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5;
NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17.

PR.PI-2 - Deve ser implementado um ciclo de vida de desenvolvimento seguro de software

Descrição

A organização deve aplicar princípios de engenharia de segurança da informação na especificação, desenho, desenvolvimento, implementação e modificação das suas redes e sistemas de informação. Estes princípios devem ser aplicados, quer a novos sistemas, como a sistemas que estejam a passar por alterações significativas.

Para sistemas legados, estes princípios devem ser aplicados, na medida do possível, tendo em conta o estado atual do hardware, software e firmware desses sistemas.

Implementação Técnica

1 Ferramentas de integração contínua (CI);

2 Gestão de código fonte em ferramenta de controlo de versões;

3 Gestão de documentação sobre redes e sistemas de informação em ferramenta de gestão documental.

Implementação Processual

A organização deve:

1 Definir os requisitos de segurança da informação nos seus projetos;

2 Gerir o ciclo de vida de desenvolvimento de redes e sistemas de informação, incorporando considerações de segurança:
   a. Proteções multicamada;
   b. Princípios de segurança por omissão;
   c. Definição das fronteiras físicas e lógicas e áreas de ataque;
   d. Identificação de casos de uso, ameaças, perfis de atacantes, vetores de ataque e padrões para encontrar os controlos compensatórios necessários;

3 Definir e documentar funções e responsabilidades no ciclo de vida de desenvolvimento;

4 Identificar colaboradores que tenham, no âmbito das suas funções e responsabilidade, a preocupação com a segurança da informação no ciclo de vida de desenvolvimento;

5 Integrar informação da gestão do risco de segurança da informação no ciclo de vida de desenvolvimento.

Evidências

1 Documentos com requisitos de segurança da informação de projeto;

2 Política de desenvolvimento seguro de software;

3 Registo de execução de testes de segurança de software.

R.N. CIS CSC 3, 11; COBIT 5 BAI01.06, BAI06.01; ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4; NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10.

PR.PI-3 - Deve ser implementado um processo de gestão de alterações

Descrição

A organização deve implementar um processo formal de gestão de alterações.

Implementação Técnica

1 Sistema de gestão de alterações;

2 Sistema de integração contínua (CI);

3 Sistema de entrega contínua (CD);

4 Sistema de controlo de versões para configurações e código fonte.

Implementação Processual

A organização deve garantir que:

1 A configuração base das redes e sistemas de informação é formalmente revista, tendo em conta os conceitos de funcionalidade mínima necessária e políticas de robustecimento de segurança definidas;

2 Cria, documenta e mantém procedimentos de gestão de alterações:
   a. Que determina os tipos de alterações às redes e sistemas de informação que devem ser alvo de controlo de versões;
   b. Identifica os ativos em que as alterações podem ter impacto direto ou indireto;
   c. Define o processo de aprovação ou rejeição de alterações;
   d. Documenta as tarefas de execução, testes às alterações e tarefas de recuperação, caso necessário;
   e. Documenta as decisões tomadas e as alterações aplicadas;

3 Analisa as alterações às redes e sistemas de informação para determinar potenciais impactos de segurança antes da sua implementação.

Evidências

1 Documento com o processo de gestão de alterações;

2 Registos de execução do processo de gestão de alterações.

R.N. CIS CSC 10;
COBIT 5 APO13.01, DSS01.01, DSS04.07;
ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3;
NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9.

PR.PI-4 - Devem ser realizadas, mantidas e testadas cópias de segurança dos dados da organização

Descrição

A organização deve ter a garantia que as suas cópias de segurança podem ser utilizadas, caso seja necessário efetuar-se o restauro das mesmas.

Deve garantir que as suas cópias de segurança são testadas e validadas regularmente, através da execução de planos de testes de restauro. Estes testes poderão ser efetuados no âmbito dos planos da continuidade do negócio da organização ou através de exercícios periódicos e planeados, para validação da integridade das cópias de segurança efetuadas.

Implementação Técnica

1 Ferramenta de cópias de segurança.

Implementação Processual

A organização deve:

1 Proteger a confidencialidade, integridade e disponibilidade das cópias de segurança;
2 Equacionar a possibilidade de guardar as suas cópias de segurança em local seguro, fora das suas instalações;
3 Executar cópias de segurança regulares da informação dos utilizadores, sistemas e documentação das redes e sistemas de informação;
4 Testar periodicamente o restauro das cópias de segurança e iniciar medidas corretivas em caso de falha.

Evidências

1 Documentos de suporte a política de cópias de segurança;

2 Registos de cópias de segurança e de restauro das cópias de segurança;

3 Registos de exercícios e testes de reposição.

R.N. COBIT 5 DSS01.04, DSS05.05;
ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3;
NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18.

PR.PI-5 - As políticas e regulamentações associadas à operacionalização dos ambientes físicos dos ativos da organização devem ser seguidas

Descrição

A organização deve seguir as políticas e regulamentação existentes, relativas à proteção de redes e sistemas de informação contra desastres naturais, falhas de energia, incêndios e inundações.

Implementação Técnica

1 Proteção contra picos de corrente elétrica;

2 Dispositivos físicos para simplificar e tornar seguro o controlo de energia;

3 Gerador de eletricidade de emergência;

4 Sensores de fumo, humidade, inundação e temperatura.

Implementação Processual

A organização deve:

1 Instalar sensores de fumo, temperatura, humidade e inundação nos locais adequados;

2 Proteger a capacidade destes sistemas de ativações não autorizadas;

3 Providenciar a capacidade de se desligar as redes e sistemas de informação em caso de emergência;

4 Executar, dentro dos prazos previstos, a devida manutenção dos sistemas acima mencionados;

5 Proteger a cablagem física contra acessos externos não autorizados.

Evidências

1 Registos de controlo de acesso;

2 Contratos de manutenção e relatórios de intervenção;

3 Registos dos testes no plano da continuidade do negócio.

R.N. COBIT 5 BAI09.03, DSS05.06;
ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7;
NIST SP 800-53 Rev. 4 MP-6.

PR.PI-6 - Os dados devem ser destruídos de acordo com a política definida

Descrição

As informações digitais e físicas devem ser sujeitas aos métodos apropriados de destruição, de acordo com a sua classificação de informação.

Implementação Técnica

1 Higienização de ficheiros e sistemas de ficheiros, com destruidor de ficheiros;

2 Destruidor de papel.

Implementação Processual

1 No final do ciclo de vida da informação, a organização deve implementar controlos que garantam a sua destruição (em formato digital ou físico), de acordo com a sua classificação e respeitando as regras que poderão ser aplicáveis face a leis nacionais e setoriais existentes;

2 Quando efetuado por terceiros, a organização deve aplicar controlos adicionais, no sentido de garantir que a informação foi devidamente destruída;

3 A organização deve aplicar mecanismos de destruição (em formato digital ou físico), de acordo com a sua classificação de informação e com as leis nacionais e setoriais aplicáveis:
   a. Antes da eliminação da mesma;
   b. Quando levada para fora do controlo da organização.

Evidências

1 Documentos de suporte à classificação da informação;

2 Processo de gestão do ciclo de vida de ativos;

3 Registos de eliminação de ativos.

R.N. COBIT 5 APO11.06, APO12.06, DSS04.05;
ISO/IEC 27001:2013 A.16.1.6, Cláusula 9, Cláusula 10;
NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6.

PR.PI-7 - Os processos de proteção devem ser continuamente melhorados

Descrição

A organização deve avaliar e atualizar regularmente os seus processos de proteção, de forma a que as possíveis fragilidades existentes sejam identificadas e alvo de plano de correção.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Monitorizar, analisar, auditar e avaliar a performance dos seus controlos, processos e sistemas de gestão implementados;

2 Efetuar auditorias internas;

3 Definir e implementar planos de ação para melhorias.

Evidências

1 Relatórios das auditorias internas;

2 Planos de ação para melhorias;

3 Registos de tratamento do plano de ação para melhorias.

R.N. COBIT 5 BAI08.04, DSS03.04;
ISO/IEC 27001:2013 A.16.1.6;
NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4.

PR.PI-8 - A efetividade das tecnologias de proteção deve ser tida em conta na melhoria dos processos de proteção

Descrição

A organização deve ter um compromisso contínuo com a melhoria, efetuando sessões de lições aprendidas e analisando os incidentes ocorridos. Estas lições têm como objetivo a redução dos riscos de ocorrência de incidentes futuros.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Praticar de forma regular o processo de lições aprendidas com base nos incidentes ocorridos;

2 Promover a partilha do conhecimento aprendido na investigação e resolução de incidentes;

3 Rever e atualizar o processo de tratamento de incidentes.

Evidências

1 Registos, com a identificação das ações de melhoria contínua, originados por incidentes ocorridos;

2 Processo de resposta a incidentes: Avaliação da eficácia dos métodos de proteção;

3 Aprendizagem com incidentes: Melhoria nos processos de proteção;

4 Atualizações das versões do plano de resposta a incidentes.

R.N. CIS CSC 19;
COBIT 5 APO12.06, DSS04.03;
ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3;
NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17.

PR.PI-9 - Os planos de resposta a incidentes, da continuidade de negócio, de recuperação de incidentes e de recuperação de desastres devem ser atualizados

Descrição

Os planos de resposta a incidentes, da continuidade de negócio, de recuperação a incidentes e de recuperação de desastres devem ser atualizados com frequência.

A organização deve garantir que as partes interessadas relevantes, internas e externas, tenham o conhecimento apropriado de todas as atualizações efetuadas.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Criar um plano de resposta e de recuperação de incidentes que:
   a. Contenha um plano de implementação para a capacidade de resposta a incidentes;
   b. Descreva a estrutura e organização da resposta inicial;
   c. Defina o que são incidentes;
   d. Defina os recursos necessários para suportar a resposta a incidentes;
   e. Defina os procedimentos de resposta a perdas de informação;

2 Criar um plano da continuidade do negócio que:
   a. Defina o propósito, âmbito, papéis, responsabilidades, comprometimento da gestão de topo e coordenação com partes interessadas externas;
   b. Identifique as funções essenciais ao bom funcionamento da organização e requisitos de contingência das mesmas;
   c. Defina prioridades de recuperação, objetivos e métricas;
   d. Enderece a recuperação total das funções essenciais;

3 Disseminar os planos de resposta e recuperação pelas partes relevantes;

4 Rever regularmente os planos da continuidade do negócio.

Evidências

1 Plano da continuidade do negócio;

2 Planos de resposta e recuperação de incidentes;

3 Registos de resposta e de recuperação de incidentes.

R.N. CIS CSC 19, 20;
COBIT 5 DSS04.04;
ISO/IEC 27001:2013 A.17.1.3;
NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14.

PR.PI-10 - Os planos de resposta e recuperação devem ser testados e exercitados

Descrição

A organização deve garantir que os planos de resposta e de recuperação de incidentes e da continuidade do negócio da organização são testados, para que se possa determinar a eficácia dos mesmos e identificar possíveis pontos de falha.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve conduzir os seguintes tipos de teste:

1 Exercícios dos planos da continuidade do negócio;

2 Simulacros de casos reais;

3 Verificação de listas de conformidade.

Evidências

1 Registos da execução dos exercícios e testes da continuidade do negócio e de resposta/recuperação de incidentes.

R.N. CIS CSC 5, 16;
COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05;
ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4;
NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21.

PR.PI-11 - A cibersegurança deve ser contemplada nos processos de gestão de recursos humanos

Descrição

Os processos organizacionais que gerem os recursos humanos, como a triagem de candidatos, contratação, categorização das posições e de cessação de vínculo laboral, devem ser avaliados e revistos com base nos requisitos de segurança estabelecidos.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve atualizar os processos de gestão de recursos humanos, aquando da entrada, alteração e saída de colaboradores, devendo:

1 Efetuar a categorização da posição em termos de funções, âmbito, responsabilidades e risco;

2 Executar a triagem na contratação, com base no risco percecionado para a posição;

3 Executar a triagem com base no risco percecionado para a posição, de forma regular;

4 Em caso de transferência:
   a. Efetuar a revisão de acessos físicos e lógicos às redes e sistemas de informação e instalações;
   b. Efetuar a confirmação das necessidades operacionais para continuidade dos acessos;
   c. Efetuar a atualização de acessos com base nas novas funções;

5 Em caso de cessação contratual:
   a. Efetuar o cancelamento de acessos às redes e sistemas de informação do ex-colaborador;
   b. Recolher todos os ativos relevantes na posse do ex-colaborador;

6 Em caso de não cumprimento das políticas de segurança da informação instituídas, deve acionar o processo de ação disciplinar.

Evidências

1 Documentos que suportam o processo de gestão de colaboradores;

2 Dossier de colaborador.

R.N. CIS CSC 4, 18, 20;
COBIT 5 BAI03.10, DSS05.01, DSS05.02;
ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3;
NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2.

PR.PI-12 - Deve ser definido e implementado um processo de gestão de vulnerabilidades

Descrição

A organização deve definir e implementar um plano para gestão das vulnerabilidades nas redes e sistemas de informação.

Implementação Técnica

1 Ferramenta de rastreamento de vulnerabilidades.

Implementação Processual

A organização deve definir e implementar um processo de gestão de vulnerabilidades que:

1 Efetue um planeamento do rastreamento de vulnerabilidades às suas redes e sistemas de informação, garantindo que identifica:
   a. A sequência da execução do rastreamento;
   b. As janelas temporais para a execução do rastreamento;
   c. Um relatório das vulnerabilidades encontradas;

2 Possibilite a submissão de report de possíveis vulnerabilidades, pelas partes interessadas relevantes;

3 Analise os relatórios de vulnerabilidades e identificação das respostas a efetuar;

4 Determine decisões de tratamento de vulnerabilidades, alinhadas com a tolerância ao risco da organização, tal como definido na sua metodologia de gestão do risco;

5 Partilha de informação sobre as vulnerabilidades com as equipas técnicas, definidas pela organização, para ajudar a eliminar vulnerabilidades similares noutras redes e sistemas de informação;

6 Partilha de informação com as partes interessadas externas relevantes, de acordo com o tipo de vulnerabilidade encontrada.

Evidências

1 Documento de suporte ao processo de gestão de vulnerabilidades;

2 Registos da execução das diversas fases do processo de gestão de vulnerabilidades;

3 Relatórios de testes de penetração e/ou rastreamento de vulnerabilidades.

4.4.5 PR.MA Manutenção

R.N. COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05;
ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6;
NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6.

PR.MA-1 - As atividades de manutenção e reparação dos ativos da organização devem ser realizadas e registadas em programas e planos aprovados e controlados

Descrição

A organização deve executar as tarefas de manutenção dos seus ativos críticos, de forma regular e atempada.

A manutenção deve ser registada, efetuada e supervisionada por colaboradores com as autorizações e competências adequadas.

Implementação Técnica

1 Ferramenta de gestão de pedidos.

Implementação Processual

A organização deve:

1 Desenvolver, disseminar, rever e atualizar um processo de manutenção de sistemas, definindo o âmbito, propósito, perfis e responsabilidades das partes interessadas envolvidas;

2 Desenvolver, disseminar, rever e atualizar os procedimentos de manutenção, de acordo com o processo referido no ponto anterior;

3 Marcar, planear, executar, documentar e rever os registos de manutenção nas redes e sistemas de informação;

4 Estabelecer um processo de autorizações ao pessoal de manutenção e manter uma lista das pessoas autorizadas;

5 Garantir que, as pessoas que executam as manutenções às redes e sistemas de informação, têm as devidas autorizações;

6 Referenciar colaboradores internos para supervisionar presencialmente as tarefas de manutenção que sejam efetuadas por elementos externos à organização;

7 Executar, de forma regular e dentro das janelas temporais previstas, a manutenção dos ativos críticos da organização.

Evidências

1 Implementação de controlo e registos de acessos em áreas seguras;

2 Processo de manutenção dos equipamentos físicos;

3 Planos e registos de manutenção;

4 Registo das intervenções efetuadas aos ativos da organização.

R.N. CIS CSC 3, 5; COBIT 5 DSS05.04; ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1; NIST SP 800-53 Rev. 4 MA-4.

PR.MA-2 - As operações de manutenção remota das redes devem ser revistas, aprovadas, executadas e registadas

Descrição

A manutenção remota das redes e sistemas de informação da organização deve ser sujeita a processos de aprovação, devendo ser registada e executada de forma a impedir a existência de acessos não autorizados.

Implementação Técnica

1 Registo dos pedidos de intervenção em sistema de gestão de pedidos.

Implementação Processual

A organização deve:

1 Aprovar e monitorizar as manutenções remotas e atividades de diagnóstico;

2 Utilizar mecanismos de autenticação forte para estabelecimento de sessões remotas;

3 Manter um registo das manutenções remotas e das atividades de diagnóstico;

4 Terminar todas as ligações quando a manutenção for dada como concluída.

Evidências

1 Documentos de suporte à política de fornecedores;

2 Registo de garantias e de manutenção de equipamentos;

3 Registos dos pedidos executados e rejeitados de manutenção remota;

4 Registo de acordos de confidencialidade com fornecedores.

4.4.6 PR.TP Tecnologia de Proteção

R.N. CIS CSC 1, 3, 5, 6, 14, 15, 16;
COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01;
ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1;
NIST SP 800-53 Rev. 4 família AU.

PR.TP-1 - Os registos de auditoria e de histórico devem ser documentados, implementados e revistos de acordo com as políticas

Descrição

Os registos de auditoria e de histórico da organização devem ser determinados, documentados, implementados e revistos de acordo com as políticas correspondentes.

Implementação Técnica

1 Gestão de eventos de segurança da informação;

2 Gestão e recolha centralizada de registos para histórico e de auditoria.

Implementação Processual

A organização deve:

1 Criar, disseminar, rever e atualizar uma política de gestão de registos e eventos;

2 Criar, disseminar, rever e atualizar procedimentos para recolha de registos e eventos;

3 Determinar os tipos de registos de auditoria que as redes e sistemas de informação devem ser capazes de suportar;

4 Providenciar as razões pelas quais se justifica que registos de histórico e de auditoria são necessários para a análise de incidentes;

5 Determinar que tipos de eventos devem ser alvo de registos de auditoria dentro das redes e sistemas de informação;

6 Determinar qual a taxonomia dos registos de auditoria (por exemplo: quando, onde, o quê, quem e porquê);

7 Definir a capacidade local e central para efetuar o armazenamento dos registos de auditoria, bem como a definição dos períodos de retenção máximos;

8 Garantir que os registos de auditoria estão todos sincronizados, utilizando a mesma fonte e fuso horário;

9 Garantir que as redes e sistemas de informação protegem os registos de auditoria contra acessos não autorizados, modificação e remoção;

10 Garantir que as redes e sistemas de informação são desenhados para evitar o repúdio dos registos de auditoria.

Evidências

1 Política de gestão de eventos, registos de auditoria e histórico;

2 Sistema de recolha centralizada de registos.

PR.TP-2 - Os suportes de dados amovíveis devem ser protegidos e a sua utilização deve ser restrita, de acordo com a política definida

R.N. CIS CSC 8, 13;
COBIT 5 APO13.01, DSS05.02, DSS05.06;
ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9;
NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8.

Descrição

A organização deve implementar procedimentos que garantam o cumprimento das regras de utilização de suportes de dados amovíveis, de acordo com a classificação de informação definida.

Implementação Técnica

1 Restringir o acesso físico a todos os suportes de dados amovíveis (por exemplo: cofres nas estações de trabalho) ou lógicas, removendo a capacidade de inserir, ler ou escrever discos amovíveis via software para esse efeito;

2 Gestão de cifra para suporte de dados amovíveis.

Implementação Processual

A organização deve:

1 Restringir o acesso a suporte de dados amovíveis, de acordo com a classificação de informação;

2 Definir uma política de cifra de informação que contemple a cifra de suporte de dados amovíveis;

3 Implementar controlos físicos ou lógicos para cumprir com as regras de gestão da informação identificadas na classificação de informação;

4 Disponibilizar os programas de destruição e higienização de ficheiros, de acordo com a política de classificação de informação;

5 Proteger e controlar os discos amovíveis em circulação fora das suas instalações ou em áreas controladas;

6 Restringir a atividade de transporte às pessoas com as autorizações necessárias.

Evidências

1 Documentos de suporte à classificação da informação;

2 Documentos de suporte à utilização aceitável de ativos;

3 Documentos de suporte à política de cifra de informação.

R.N. CIS CSC 3, 11, 14;
COBIT 5 DSS05.02, DSS05.05, DSS06.06;
ISO/IEC 27001:2013 A.9.1.2;
NIST SP 800-53 Rev. 4 AC-3, CM-7.

PR.TP-3 - O princípio da minimização de funcionalidades deve ser incorporado na configuração de sistemas, de modo a fornecer apenas os recursos essenciais

Descrição

A organização deve aplicar o princípio da funcionalidade mínima na configuração das redes e sistemas de informação. A funcionalidade mínima deve garantir que apenas sejam autorizados acessos aos utilizadores que necessitem dessas mesmas funcionalidades, por forma a executarem as tarefas a si atribuídas de acordo com os seus perfis funcionais.

Implementação Técnica

1 Gestão de identidades e acessos.

Implementação Processual

A organização deve:

1 Aplicar os princípios da funcionalidade mínima para tarefas relacionados com a gestão das redes e sistemas de informação:
   a. Restrição de funcionalidades, portos, protocolos e serviços;
   b. Restrição de processos para desempenhar as funções necessárias;
   c. Restrição de níveis de privilégios mínimos para cumprir a missão da organização ou funções necessárias;
   d. Restrição de acessos a funções de segurança;
   e. Restrição de acessos de rede a comandos privilegiados;
   f. Restrição de domínios de processamento;
   g. Restrição de contas privilegiadas;
   h. Restrição de privilégios para a execução de código.

Evidências

1 Documentos de suporte ao processo de gestão de acessos;

2 Definição de papéis, responsabilidades e segregação de funções;

3 Perfis funcionais mapeados com acessos aos sistemas e aplicações.

PR.TP-4 - As redes de comunicações e de controlo devem ser protegidas

R.N. CIS CSC 8, 12, 15;
COBIT 5 DSS05.02, APO13.01;
ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3;
NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43.

Descrição

Os fluxos regulam a transferência de informação e os caminhos que podem ser abertos dentro de cada sistema ou entre sistemas. Estes, devem ser controlados operacionalmente e devem ser sempre requeridas as autorizações prévias para que possam ser alterados.

Implementação Técnica

1 Sistema de Deteção e Prevenção de Intrusões (IDS/IPS);

2 *Firewall*;

3 *Proxy*;

4 *Firewall* de aplicações *web* (WAF).

As componentes tecnológicas em cima identificadas não são exaustivas e, como tal, a organização poderá efetuar a implementação de controlos de segurança adicionais.

Implementação Processual

A organização deve garantir que:

1 As alterações efetuadas nas suas redes de comunicações são executadas dentro do processo de gestão de alterações.

Evidências

1 Existência de dispositivos de rede de comunicações com funções de segurança;

2 Registos de segregação de redes de comunicações;

3 Registos de suporte aos pedidos de alterações da rede de comunicações.

PR.TP-5 - Devem ser implementados mecanismos para cumprir os requisitos de resiliência em situações adversas

R.N. COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05; ISO/IEC 27001:2013 A.17.1.2, A.17.2.1; NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6.

Descrição

A organização deve implementar os mecanismos necessários, para que possa cumprir os requisitos de resiliência básicos em situações incomuns e garantir a alocação de recursos e equipamentos adicionais. Caso seja necessário responder a situações adversas, coloca-se em prática a estratégia da continuidade do negócio.

Implementação Técnica

1 Sistemas de alta disponibilidade;

2 Soluções de balanceamento de carga;

3 Redundância dos sistemas.

Implementação Processual

A organização deve:

1 Determinar o tempo máximo aceitável de falha para os ativos e serviços críticos, aprovisionando componentes de substituição para a reposição do serviço em caso de avaria dos componentes em operação;

2 Garantir que as redes e sistemas de informação passam a funcionar em modo de segurança de operação, quando as condições definidas para o efeito pela organização forem detetadas;

3 Proteger a disponibilidade das redes e sistemas de informação, alocando os recursos de computação considerados necessários e priorizando os sistemas de acordo com a sua criticidade;

4 Estabelecer um local alternativo, que garanta os contratos necessários para permitir, de forma segura, a transferência das suas redes e sistemas de informação para as funções e atividades críticas para a organização;

5 Garantir que existem os recursos computacionais, redes de comunicações e equipamentos necessários, com os requisitos de segurança apropriados e equivalentes ao seu local primário de trabalho.

Evidências

1 Documentos de suporte ao plano da continuidade do negócio;

2 Registo das redundâncias implementadas.

MEDIDAS DE SEGURANÇA

DETETAR

4.5.1 DE.AE Anomalias e Eventos

R.N. CIS CSC 1, 4, 6, 12, 13, 15, 16; COBIT 5 DSS03.01; ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2; NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4.

DE.AE-1 - A organização deve definir e gerir um modelo de referência de operações de rede e fluxos de dados esperados para utilizadores e sistemas

Descrição

A organização deve garantir que as operações efetuadas na sua infraestrutura de rede de comunicações são executadas de forma sistematizada, por pessoal qualificado, e que seja garantida a integridade, confidencialidade e disponibilidade da informação.

Para cada sistema de informação, a organização deve medir, criar e manter um modelo do padrão de referência para os fluxos de comunicações esperados, quer estes sejam originados por utilizadores, quer por sistemas internos ou externos.

Implementação Técnica

1 Sistema de Deteção e Prevenção de Intrusões (IDS/IPS);

2 *Firewall*;

3 *Proxy*;

4 *Firewall* de aplicações *web* (WAF).

Implementação Processual

Na operação da infraestrutura de rede de comunicações, onde se incluem todos os equipamentos de rede de comunicações e de segurança, a organização deve:

1 Garantir que existe um padrão de referência para os fluxos de dados de utilizadores e sistemas;

2 Garantir que o padrão de referência é atualizado com base nas alterações relevantes feitas nas redes e sistemas de informação;

3 Garantir que as alterações efetuadas são executadas de acordo com o processo de gestão de alterações.

Evidências

1 Modelo para registo de fluxos de dados;

2 Registos dos modelos de fluxos de dados das redes e sistemas de informação;

3 Registos de suporte das alterações efetuadas.

R.N. CIS CSC 3, 6, 13, 15;
COBIT 5 DSS05.07;
ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4;
NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4.

DE.AE-2 - Os eventos detetados devem ser analisados por forma a se identificarem os alvos e os métodos de ataque

Descrição

A organização deve implementar um processo de gestão e de correlação de eventos de segurança que:

1 Suporte o seu processo de análise e tratamento de eventos;

2 Suporte o processo de identificação de possíveis incidentes.

Implementação Técnica

1 Gestão e correlação de eventos de segurança.

Implementação Processual

A organização deve:

1 Implementar um processo de monitorização das suas redes e sistemas de informação, que permita analisar os eventos ocorridos nos mesmos;

2 Criar um conjunto de mecanismos processuais, que permitam efetuar a gestão dos eventos e determinar se os mesmos deverão ser avaliados com maior detalhe;

3 Garantir que é recolhida a informação suficiente sobre os eventos detetados, para que seja possível identificar as origens, alvos e métodos de ataque;

4 Garantir que sejam abertos incidentes nos casos em que se confirme o incidente.

Evidências

1 Documentos de suporte ao processo de gestão e correlação de eventos;

2 Documentos de suporte ao processo de gestão de incidentes;

3 Relatórios de resposta a incidentes.

R.N. CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16;
COBIT 5 BAI08.02;
ISO/IEC 27001:2013 A.12.4.1, A.16.1.7;

DE.AE-3 - Os eventos devem ser coletados e correlacionados a partir de várias fontes e sensores

Descrição

A organização deve implementar os mecanismos tecnológicos e processuais necessários,

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4.

que permitam a coleta e correlação dos eventos gerados nas suas redes e sistemas de informação e nos dispositivos de segurança.

Estes eventos devem ser correlacionados entre si e, se possível, enriquecidos com fontes de conhecimento externas sobre ameaças.

Implementação Técnica

1 Gestão e correlação de eventos de segurança;

2 Utilização de fontes de conhecimento sobre ameaças de segurança informática;

3 Disseminar honeypots, pela sua rede de comunicações e segurança, para servirem como sensores de alertas.

Implementação Processual

A organização deve:

1 Garantir a recolha e armazenamento de eventos de segurança dos sistemas de informação, equipamentos de rede de comunicações e dispositivos de segurança;

2 Correlacionar os eventos coletados com informação de incidentes passados;

3 Correlacionar os eventos coletados entre si, para detetar padrões anómalos;

4 Correlacionar os eventos com fontes de conhecimentos sobre ameaças;

5 Avaliar a relevância de notificar e comunicar incidentes de segurança, em curso ou finalizados, a autoridades, a terceiros, a clientes e ao público, consoante aplicável ou necessário.

Evidências

1 Documentos de suporte ao processo de gestão de eventos;

2 Registos de coleta e correlação de eventos;

3 Existência de *honeypots* geridos pela organização na sua rede de comunicações.

R.N. CIS CSC 4, 6; COBIT 5 APO12.06, DSS03.01; ISO/IEC 27001:2013 A.16.1.4;

DE.AE-4 - O impacto dos eventos deve ser classificado

Descrição

A organização deve efetuar uma categorização e tipificação dos eventos, por forma a aferir qual o impacto dos mesmos sobre as suas redes e sistemas de informação.

A categorização dos eventos irá suportar a organização no processo de decisão sobre que

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4.

ações desencadear para cada tipo de evento. Os eventos poderão dar origem a incidentes.

Implementação Técnica

1 Gestão de eventos de segurança da informação.

Implementação Processual

O processo de gestão de eventos deve ser complementado com:

1 Categorização e tipificação de eventos;

2 Aferição dos respetivos impactos;

3 Possibilidade de se acionar o processo de gestão de incidentes.

Evidências

1 Documento de suporte ao processo de gestão de eventos;

2 Registo dos eventos tipificados;

3 Registo de tipificações existentes;

4 Ligação entre gestão de eventos e gestão de incidentes.

R.N. CIS CSC 6, 19;
COBIT 5 APO12.06, DSS03.01;
ISO/IEC 27001:2013 A.16.1.4;
NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8.

DE.AE-5 - Devem ser definidos os limites de alerta para incidentes

Descrição

Tendo como base a tipificação e categorização dos eventos do seu sistema de gestão de eventos, a organização deve definir quais são os critérios que devem justificar a necessidade de abertura de incidentes.

Implementação Técnica

1 Gestão de eventos de segurança da informação.

Implementação Processual

A organização deve:

1 Definir a taxonomia das prioridades de incidentes;

2 Definir quais os limites a considerar quando um evento, conjunto de eventos ou correlação de múltiplos eventos, configura um incidente;

3 Definir quais os limites para que um incidente de cibersegurança suba ou desça de prioridade.

Evidências

1 Documentos de suporte ao processo de gestão de eventos;

2 Documentos de suporte ao processo de gestão de incidentes;

3 Registos de categorização e priorização de incidentes.

4.5.2 DE.MC Monitorização Contínua de Segurança

R.N. CIS CSC 1, 7, 8, 12, 13, 15, 16; COBIT 5 DSS01.03, DSS03.05, DSS05.07; NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4.

DE.MC-1 - As redes e sistemas de informação devem ser monitorizados para detetar potenciais incidentes

Descrição

A organização deve efetuar a monitorização da sua rede e dos seus sistemas de informação. A monitorização deve estar integrada com o processo de gestão de eventos.

Implementação Técnica

1 Gestão e correlação de eventos de segurança da informação;

2 Implementação de sistemas de monitorização de segurança para redes e sistemas de informação;

3 Sistemas de deteção e prevenção de intrusões;

4 *Firewall* de aplicações web.

Implementação Processual

A organização deve:

1 Desenvolver uma estratégia de monitorização contínua da segurança e privacidade;

2 Monitorizar os sistemas de informação, de forma a poder detetar ataques e recolher indicadores potenciais de incidentes, de acordo com a estratégia definida;

3 Monitorizar as ligações de rede de comunicações locais e remotas, para detetar acessos não autorizados;

4 Ajustar o nível de monitorização de atividade quando existe uma mudança no risco sobre ativos ou indivíduos;

5 Monitorizar pontos estratégicos para controlar tipos específicos de transações de interesse (por exemplo: detetar, nas firewalls, ligações HTTP de dentro para fora, sem passar por proxies corporativos aprovados).

Evidências

1 Documentos de suporte à gestão e correlação de eventos;

2 Documentos de suporte à gestão de incidentes;

3 Sistema de gestão e correlação de eventos de segurança;

4 Existência de dispositivos de segurança mantidos e atualizados pela organização.

R.N. COBIT 5 DSS01.04, DSS01.05;

ISO/IEC 27001:2013 A.11.1.1, A.11.1.2;

NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20.

DE.MC-2 - O ambiente físico deve ser monitorizado para se detetar potenciais incidentes de segurança

Descrição

A organização deve garantir que os seus perímetros de segurança física são monitorizados. A monitorização dos controlos de proteção física deve ser inserida no processo de gestão de eventos, associados a categorização e tipificação especifica.

Implementação Técnica

1 Soluções de CCTV/Controlo de Acessos;

2 Gestão de eventos de segurança da informação.

Implementação Processual

A organização deve garantir que:

1 Os pontos de controlo de segurança física produzem registos de auditoria;

2 Os registos de auditoria são coletados e correlacionados pelo sistema de gestão de eventos de segurança da informação;

3 Sejam criadas alarmísticas específicas para a deteção de intrusão de acessos não autorizados.

Evidências

1 Documentos de suporte ao processo de gestão e correlação de eventos;

2 Registos de eventos de segurança com a tipificação representativa de evento de segurança física.

DE.MC-3 - A atividade dos colaboradores deve ser monitorizada para se detetar potenciais incidentes

R.N. CIS CSC 5, 7, 14, 16;
COBIT 5 DSS05.07;
ISO/IEC 27001:2013 A.12.4.1, A.12.4.3;
NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11.

Descrição

A monitorização das atividades dos colaboradores deve estar integrada no âmbito do processo de gestão de eventos.

Esta atividade tem como objetivo recolher informação que possibilite uma atuação célere da organização, no caso de existência de algum incidente que possa ter origem na atividade de um colaborador.

A organização deve garantir que a informação recolhida e o seu respetivo tratamento respeitam o enquadramento jurídico aplicável e a política de privacidade da organização.

Implementação Técnica

1 Sistema de gestão de eventos de segurança da informação;

2 Correlação de atividade dos colaboradores com padrões de utilização normais.

Implementação Processual

A monitorização das atividades dos colaboradores deve:

1 Ser garantida nas suas atividades regulares, quando interagindo com os sistemas e redes de comunicações da organização;

2 Ser garantida em caso de necessidade de utilização de acessos privilegiados nos sistemas e redes de comunicações da organização;

3 Ser correlacionada com o modelo padrão de atividades para colaboradores;

4 Poder gerar alertas que sejam elevados a incidentes nos casos apropriados;

5 Ser efetuada garantindo os princípios essenciais de proteção e tratamento de dados pessoais.

Evidências

1 Documentos de suporte do processo de gestão e correlação de eventos;

2 Relatórios de alertas de incidentes com tipificação representativa de evento e comportamento anómalo na atividade de colaboradores.

R.N. CIS CSC 4, 7, 8, 12;
COBIT 5 DSS05.01;
ISO/IEC 27001:2013 A.12.2.1;
NIST SP SP 800-53 Rev. 4 SI-3, SI-8.

DE.MC-4 - A organização deve identificar e implementar mecanismos para deteção de código malicioso

Descrição

A organização deve implementar mecanismos que permitam a deteção e a prevenção de existência de código malicioso nas suas redes e sistemas de informação.

Implementação Técnica

A organização deve:

1 Implementar ferramentas de deteção e de proteção contra a existência de código malicioso nos equipamentos dos utilizadores e nas suas redes e sistemas de informação que:
   a. Efetuem uma verificação periódica e em tempo real das redes e sistemas de informação;
   b. Analisem ficheiros com origem externa ao sistema (tal como ficheiros retirados da internet ou copiados de suportes amovíveis);
   c. Bloqueiem e/ou coloquem em quarentena como resposta imediata à deteção de código malicioso;

2 Implementar ferramentas e atividades de revisão e análise de código e análise e revisão de dependências com bibliotecas externas;

3 Gerir e correlacionar eventos de segurança da informação.

Implementação Processual

A organização deve:

1 Garantir que os mecanismos de deteção e prevenção de código malicioso produzem registos de auditoria;

2 Garantir que os registos de auditoria são coletados e correlacionados pelo sistema de gestão de eventos de segurança da informação;

3 Criar alarmísticas específicas para a deteção e prevenção de código malicioso;

4 Endereçar falsos positivos e o potencial impacto na disponibilidade dos sistemas;

5 Analisar a técnica do código fonte desenvolvido.

Evidências

1 Documentos de suporte ao desenvolvimento seguro de *software*;

2 Documentos de suporte do processo de gestão e correlação de eventos;

3 Existência de ferramentas de deteção e prevenção de código malicioso;

4 Relatórios de alertas de incidentes sobre código malicioso.

R.N. CIS CSC 7, 8; COBIT 5 DSS05.01; ISO/IEC 27001:2013 A.12.5.1, A.12.6.2; NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44.

DE.MC-5 - A utilização de aplicações não autorizadas em dispositivos móveis deve ser detetada

Descrição

A organização deve ter a capacidade de detetar instalações indevidas de aplicações nas suas redes e sistemas de informação. A deteção deste tipo de atividades deve estar integrada com o processo de gestão de eventos da organização.

Implementação Técnica

Gestão de equipamentos de trabalho com ferramentas de controlo de atividade aplicacional.

Implementação Processual

A organização deve:

1 Definir, documentar e disseminar uma lista de aplicações e de tecnologias permitidas e não permitidas;

2 Informar os seus colaboradores que não deverão instalar aplicações indevidas, solicitando a leitura e assinatura de termo de responsabilidade;

3 Implementar ferramentas de monitorização que permitam alertar no caso de existência de instalações indevidas nos seus equipamentos;

4 Integrar as atividades de instalação indevida com o processo de gestão de eventos;

5 Autorizar formalmente possíveis exceções à lista definida, quando a mesma for requerida para:
   a. Um colaborador cumprir com as suas funções;
   b. Um sistema de informação funcionar de acordo com os requisitos definidos pelo fabricante.

Evidências

1 Lista de *software* autorizado e não autorizado;

2 Documento e registos de termos de responsabilidade de boa utilização de recursos informáticos;

3 Documentos de suporte ao processo de gestão de eventos.

R.N. COBIT 5 APO07.06, APO10.05;
ISO/IEC 27001:2013 A.14.2.7, A.15.2.1;
NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4.

DE.MC-6 - As atividades dos prestadores de serviços externos devem ser monitorizadas para deteção de incidentes

Descrição

As atividades dos prestadores de serviços externos devem ser monitorizadas pela organização, para detetar se as redes e os sistemas de informação da organização são acedidos sem autorização.

Implementação Técnica

1 Gestão e correlação de eventos de segurança da informação;

2 Sistema de deteção e prevenção de intrusões.

Implementação Processual

A organização deve:

1 Identificar na política de gestão de fornecedores:
   a. As atividades de monitorização do serviço prestado à organização;
   b. Quais os requisitos de segurança, perfis e responsabilidades para fornecedores;

2 Requerer que as organizações prestadoras de serviços sigam as políticas de segurança estabelecidas;

3 Garantir que os colaboradores externos respeitam a confidencialidade da informação à qual acedem no exercício das suas funções;

4 Requerer que os prestadores de serviços a informem acerca de todos os colaboradores externos que abandonem os seus quadros e que tenham executado tarefas na organização;

5 Monitorizar os eventos gerados por estes, criar e investigar todos os incidentes que daí possam derivar.

Evidências

1 Documentos de suporte à política de gestão de fornecedores;

2 Relatórios de incidentes derivados das atividades de prestadores de serviços externos.

R.N. CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16;
COBIT 5 DSS05.02, DSS05.05;
ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1;
NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4.

DE.MC-7 - Deve ser efetuada a monitorização de acessos não autorizados de colaboradores, conexões, dispositivos e software

Descrição

A organização deve garantir a monitorização de acessos às redes e sistemas de informação por colaboradores, dispositivos, equipamentos e processos que não tenham as devidas autorizações.

Implementação Técnica

1 Gestão e correlação de eventos de segurança da informação;

2 Sistema de deteção e prevenção de intrusões.

Implementação Processual

A organização deve:

1 Monitorizar os acessos às redes e sistemas de informação e correlacioná-los com a lista definida de acessos autorizados;

2 Colecionar dados em localizações ad-hoc para tentar detetar acessos anómalos;

3 Reportar eventos de deteção de acessos não autorizados;

4 Criar, investigar e resolver incidentes que derivem desses eventos.

Evidências

1 Registos de eventos de acesso a sistemas e aplicações;

2 Registos de correlação de eventos de acessos não autorizados;

3 Relatórios de incidentes relativos a acessos não autorizados.

R.N. CIS CSC 4, 20;
COBIT 5 BAI03.10, DSS05.01;
ISO/IEC 27001:2013 A.12.6.1;
NIST SP 800-53 Rev. 4 RA-5.

DE.MC-8 - Devem ser efetuados rastreamentos de vulnerabilidades

Descrição

A organização deve executar o processo de gestão de vulnerabilidades definido, efetuando rastreamentos de vulnerabilidades regulares, de forma automática e manual.

Implementação Técnica

1 Ferramentas de análise e rastreamento de vulnerabilidades.

Implementação Processual

A organização deve:

1 Efetuar um plano de execução das análises de vulnerabilidades;

2 Identificar as falhas encontradas e reportá-las[1], enumerando:
   a. Plataformas, versões, falhas e configurações deficientes;
   b. Impactos da vulnerabilidade;
   c. Descrição da vulnerabilidade;
   d. Procedimentos de correções;
   e. Testes de validação de falsos positivos;

3 Atuar sobre os relatórios de vulnerabilidades, implementando as correções ou as mitigações identificadas.

Evidências

1 Documentos de suporte ao processo de gestão de vulnerabilidades;

2 Relatórios de análise de vulnerabilidades;

3 Registo de ações de correção ou mitigação (quando aplicável).

4.5.3 DE.PD Processos de Deteção

R.N. CIS CSC 19;
COBIT 5 APO01.02, DSS05.01, DSS06.03;
ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;
NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14.

DE.PD-1 - Devem ser definidos os papéis e responsabilidades na deteção de eventos anómalos

Descrição

A organização deve efetuar sessões de esclarecimento, que visem o claro entendimento das partes interessadas nos processos, bem como os limites de responsabilidades e de atividades respetivos.

[1] Caso exista processo legal, este deve ser aplicado

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve definir, no âmbito dos processos de gestão de eventos e de incidentes:

1 Quais as partes interessadas;

2 Quais os papéis e responsabilidades das partes interessadas;

3 Em que fases do processo cada parte intervém;

4 Qual o processo de escalonamento;

5 Qual a taxonomia de classificação de eventos;

6 Que sessões de sensibilização devem ser realizadas.

Evidências

1 Documentos de suporte ao processo de gestão e correlação de eventos;

2 Documentos de suporte ao processo de gestão de incidentes;

3 Registos das sessões de sensibilização.

R.N. COBIT 5 DSS06.01, MEA03.03, MEA03.04;

ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3;

NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14.

DE.PD-2 - As atividades de deteção devem cumprir com todos os requisitos aplicáveis

Descrição

A organização deve implementar atividades de auditoria interna, que lhe permitam aferir o funcionamento dos seus serviços de deteção e identificar possibilidades de melhoria.

Implementação Técnica

1 Gestão e correlação de eventos de segurança da informação.

Implementação Processual

A organização deve:

1 Elaborar um plano de auditoria anual;

2 Definir qual a sua metodologia de avaliação, por forma a poder medir a eficácia das atividades de deteção;

3 Verificar se os ambientes, papéis, responsabilidades e equipas estão adequadamente definidos;

4 Verificar se a conformidade e o funcionamento das atividades de deteção estão adequados ao pretendido;

5 Elaborar um plano de atividades, caso sejam identificadas oportunidades de melhoria.

Evidências

1 Plano de auditoria;

2 Relatórios de auditoria;

3 Registos de ações de melhoria.

R.N. COBIT 5 APO13.02, DSS05.02;

ISO/IEC 27001:2013 A.14.2.8;

NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14.

DE.PD-3 - Os processos de deteção devem ser testados

Descrição

A organização deve efetuar testes e a verificação do funcionamento dos seus sistemas de deteção, sempre que:

1 É efetuada uma alteração significativa a um sistema;

2 É efetuado um novo desenvolvimento aplicacional significativo;

3 Seja incluído um novo sistema na sua infraestrutura;

4 Tenha conhecimento da existência de uma nova vulnerabilidade.

Implementação Técnica

Gestão e correlação de eventos de segurança da informação.

Implementação Processual

A organização deve:

1 Identificar os objetivos a atingir com os testes;

2 Elaborar planos de testes;

3 Identificar as atividades a executar;

4 Formalizar a execução dos testes e elaborar relatório das atividades;

5 Validar se os resultados obtidos são os esperados ou se é necessário efetuar melhorias;

6 Elaborar um plano de implementação de melhorias (caso aplicável).

Evidências

1 Registos de planos de testes;

2 Registos de planos de melhoria.

R.N. CIS CSC 19; COBIT 5 APO08.04, APO12.06, DSS02.05; ISO/IEC 27001:2013 A.16.1.2, A.16.1.3; NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4.

DE.PD-4 - Informações sobre deteções de eventos devem ser comunicadas

Descrição

A organização deve definir uma estratégia de comunicação, que mantenha informadas as partes interessadas relevantes sobre a ocorrência de eventos e/ou incidentes. A estratégia deve ser suportada num plano de comunicação que poderá ser consolidado com os outros planos de comunicação que a organização disponha.

Implementação Técnica

1 Plataforma de resposta a incidentes.

Implementação Processual

O processo de gestão de incidentes da organização deve ter um plano de comunicação definido. No plano deve identificar:

1 O que comunicar: Que conteúdo (por exemplo: a descrição de um incidente e os seus impactos);

2 Que mensagem: Forma e formato, que tipo de meio será usado, desde pequenos textos a imagens, metáforas, vídeos, entre outros;

3 Quem deve comunicar: Deve ser nomeado um responsável que tenha a autoridade e autonomia para comunicar, particularmente com organizações externas;

4 A quem comunicar: Destinatários da comunicação;

5 Como comunicar: Que canais devem ser usados para obter maior eficácia na difusão da mensagem (por exemplo: mensagens de correio eletrónico e protetores de ecrã);

6 Quando comunicar: A comunicação deve ser regularmente exercitada em condições comuns (por exemplo: divulgação da política de segurança da informação), mas poderá ter frequências e modos de atuação muito diferentes em contexto de incidente.

Evidências

1 Documentos de suporte ao processo de gestão de incidentes;

2 Registo de comunicações de eventos que geram incidentes.

DE.PD-5 - Os processos de deteção devem ser objeto de melhoria contínua

R.N. COBIT 5 APO11.06, APO12.06, DSS04.05;
ISO/IEC 27001:2013 A.16.1.6;
NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14.

Descrição

A organização deve garantir que aprende com os incidentes que ocorrem nas suas redes e sistemas de informação, identificando medidas operacionais e/ou processuais que possam melhorar a capacidade de deteção de novos incidentes.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve executar:

1 Procedimento de revisão e aprendizagem de processos de deteção de eventos;

2 Atividades de melhoria identificadas nos planos de testes aos processos de deteção.

Evidências

1 Plano de melhoria dos processos de deteção;

2 Registo de tratamento de ações de melhoria.

MEDIDAS DE SEGURANÇA

RESPONDER

4.6.1 RS.PR Planeamento da Resposta

R.N. CIS CSC 19; COBIT 5 APO12.06, BAI01.10; ISO/IEC 27001:2013 A.16.1.5; NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8.

RS.PR-1 - O plano de resposta deve ser executado durante ou após a ocorrência de um incidente

Descrição

A organização deve sistematizar o seu processo de resposta a incidentes, por forma a garantir uma correta alocação de recursos (humanos, tecnológicos e processuais) na resolução do mesmo.

A resolução dos incidentes deve seguir um processo sistematizado, no âmbito do qual tem de ser identificado um responsável pelo seu tratamento.

No processo de análise de evidências de um incidente, é relevante garantir-se a integridade das evidências analisadas e recolhidas.

Implementação Técnica

1 Plataforma de resposta a incidentes.

Implementação Processual

A organização deve:

1 Implementar um processo de resposta a incidentes, que inclua as fases de contenção e erradicação;

2 Identificar o responsável pelo tratamento dos incidentes, que vai coordenar as atividades de resposta e contingência;

3 Definir o processo de escalonamento de incidentes;

4 Garantir que o rigor, âmbito, aplicabilidade e resultados das atividades de resposta a incidentes são consistentes e transversais a toda a organização e a todos os incidentes.

Evidências

1 Documentos de suporte ao plano de resposta a incidentes;

2 Registo de resposta e tratamento de incidentes.

4.6.2 RS.CO Comunicações

R.N. CIS CSC 19; COBIT 5 EDM03.02, APO01.02, APO12.03; ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1; NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8.

RS.CO-1 - Na resposta a um incidente, os colaboradores devem conhecer os seus papéis e a ordem de execução de atividades

Descrição

Na resposta a um incidente, a organização deve garantir que os colaboradores envolvidos têm conhecimento de quem são as partes interessadas relevantes envolvidas, do seu papel no processo de resposta a incidentes e dos passos de execução para resolução do mesmo.

Implementação Técnica

1 Plataforma de resposta a incidentes.

Implementação Processual

A organização deve, no seu processo de resposta a incidentes, identificar:

1 Os passos de execução da resposta a incidentes;

2 As partes interessadas;

3 Os papéis e responsabilidades dos intervenientes.

A organização deve efetuar ações de sensibilização, por forma a que o entendimento seja o mesmo para todos os colaboradores.

Evidências

1 Documento de suporte ao processo de resposta a incidentes;

2 Registo das ações de sensibilização.

R.N. CIS CSC 19; COBIT 5 DSS01.03; ISO/IEC 27001:2013 A.6.1.3, A.16.1.2; NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8.

RS.CO-2 - Os incidentes devem ser reportados de acordo com critérios estabelecidos

Descrição

A organização deve estabelecer e divulgar, às partes interessadas relevantes, os canais adequados para se reportarem incidentes e deve, também, estabelecer a tipificação de incidentes de segurança da informação.

Implementação Técnica

1 Plataforma de resposta a incidentes.

Implementação Processual

A organização deve garantir que, no seu plano de resposta a incidentes, estabelece e divulga:

1 Os canais de reporte de incidentes;

2 A categorização dos incidentes;

3 O processo de notificação e comunicação de incidentes de segurança, em curso ou finalizados, a autoridades, a terceiros, a clientes e ao público, consoante aplicável ou necessário.

Evidências

1 Documentos de suporte ao processo de resposta a incidentes;

2 Registos de abertura de incidentes, por equipas externas.

RS.CO-3 - As informações devem ser partilhadas de acordo com o plano de resposta

R.N. CIS CSC 19; COBIT 5 DSS03.04; ISO/IEC 27001:2013 A.16.1.2, Cláusula 7.4, Cláusula 16.1.2; NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4.

Descrição

A organização deve divulgar às partes interessadas relevantes, utilizando os canais adequados, as informações referentes aos incidentes. Esta ação tem como objetivo ajudar as partes interessadas a detetar, conter e solucionar problemas semelhantes nos seus sistemas de informação.

A estratégia de comunicação deve ser identificada num plano de comunicação produzido para o efeito. O plano poderá ser consolidado com outros planos de comunicação existentes na organização.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Identificar o plano de comunicação a adotar. O plano poderá ser consolidado com outros planos de comunicação existentes;

2 Identificar as partes interessadas relevantes, pelas quais deve ser disseminada a informação sobre incidentes;

3 Ter canais seguros definidos para a comunicação de informação confidencial;

4 Partilhar, em tempo útil, informação sobre os incidentes com as partes interessadas relevantes.

Evidências

1 Registos da identificação das principais partes interessadas;

2 Documentos de suporte ao plano de resposta a incidentes;

3 Registo de comunicações feitas às partes interessadas.

R.N. CIS CSC 19; COBIT 5 DSS03.04; ISO/IEC 27001:2013 Cláusula 7.4; NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RS.CO-4 - A coordenação com as partes interessadas deve ocorrer conforme os planos de resposta

Descrição

A organização deve implementar um plano de comunicação, de coordenação e de escalonamento de incidentes, alinhado com a categorização e criticidade dos mesmos. O plano poderá ser consolidado com outros planos de comunicação que a organização disponha.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve, no âmbito do seu plano de resposta a incidentes, identificar a seguinte informação:

1 As partes interessadas relevantes;

2 Plano de comunicação, identificando:
   a. O que comunicar: Que conteúdo (por exemplo: a descrição de um incidente e os seus impactos);
   b. Que mensagem: Forma e formato, que tipo de meio será usado, desde pequenos textos a imagens, metáforas, vídeos, entre outros;
   c. Quem deve comunicar: Deve ser nomeado um responsável que tenha a autoridade e autonomia para comunicar, particularmente com organizações externas;
   d. A quem comunicar: Destinatários da comunicação;

e. Como comunicar: Que canais devem ser usados para obter maior eficácia na difusão da mensagem (por exemplo: mensagens de correio eletrónico e protetores de ecrã);
f. Quando comunicar: A comunicação deve ser regularmente exercitada em condições comuns (por exemplo: divulgação da política de segurança da informação), mas poderá ter frequências e modos de atuação muito diferentes em contexto de incidente;
g. Ponto único de contacto de cada parte interessada;

3 Definição das responsabilidades, limites de atuação e tempos de resposta das diferentes partes;

4 Os contactos de autoridades competentes, se tal for necessário.

Evidências

1 Documentos de suporte ao plano de resposta a incidentes;

2 Relatórios de resposta a incidentes passados, que demonstrem a coordenação com as partes interessadas.

R.N. CIS CSC 19; COBIT 5 BAI08.04; ISO/IEC 27001:2013 A.6.1.4; NIST SP 800-53 Rev. 4 SI-5, PM-15.

RS.CO-5 - Deve ocorrer partilha voluntária de informação com partes interessadas externas

Descrição

No processo de resposta a um incidente, a organização deve identificar qual a informação que tem de ser partilhada com as partes interessadas externas, para se alcançar uma consciência mais abrangente sobre cibersegurança.

Nestas situações, a organização deve partilhar informações sobre indicadores de compromisso a grupos de interesse, para que estes possam, também, beneficiar da partilha e melhorar tempos de resposta a identificar, detetar, conter e erradicar essas ameaças na sua circunscrição e no seu círculo de influência.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Manter uma lista atualizada das partes interessadas relevantes;

2 Ter canais seguros estabelecidos com os pontos de contacto das partes interessadas externas relevantes, para partilha de informação de forma segura.

Evidências

1 Registos com contactos de reguladores e grupos de interesse técnico e legislativo;

2 Plano de comunicação.

4.6.3 RS.AN Análise

R.N. CIS CSC 4, 6, 8, 19;
COBIT 5 DSS02.04, DSS02.07;
ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5;
NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4.

RS.AN-1 - As notificações dos sistemas de deteção devem ser investigadas

Descrição

A organização deve garantir que os eventos originados nos sistemas de deteção são analisados, categorizados e tratados de forma sistematizada. A organização deve identificar que eventos devem evoluir para incidentes.

Implementação Técnica

1 Plataforma de gestão e correlação de eventos.

Implementação Processual

A organização deve:

1 Monitorizar os eventos gerados nos sistemas de deteção;

2 Efetuar a ativação do processo de gestão de incidentes, quando necessário;

3 Responder a incidentes, de acordo com a sua tipificação no plano de resposta a incidentes.

Evidências

1 Documentos de suporte ao processo de gestão e correlação de eventos;

2 Documentos de suporte ao plano de resposta a incidentes;

3 Registos de notificações de deteção que foram elevadas a incidentes.

R.N. COBIT 5 DSS02.02;
ISO/IEC 27001:2013 A.16.1.4, A.16.1.6;
NIST SP 800-53 Rev. 4 CP-2, IR-4.

RS.AN-2 - O impacto do incidente deve ser avaliado

Descrição

No processo de categorização dos incidentes, a organização deve avaliar o impacto que os incidentes causam aos seus ativos e, consequentemente, à sua operação, usando essa avaliação para definir qual a severidade a atribuir ao incidente.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Definir níveis de impacto de incidentes, tendo em conta o impacto que os mesmos podem causar no contexto definido;

2 Definir tempos de resposta, tempos de resolução, níveis de alerta e prioridade, com base no impacto de cada incidente.

Evidências

1 Documentos de suporte ao processo de gestão e correlação de eventos;

2 Documentos de suporte ao plano de resposta a incidentes: Taxonomia de impacto de incidentes.

R.N. COBIT 5 APO12.06, DSS03.02, DSS05.07;
ISO/IEC 27001:2013 A.16.1.7;
NIST SP 800-53 Rev. 4 AU-7, IR-4.

RS.AN-3 - Devem ser realizadas análises forenses

Descrição

A organização deve criar as condições necessárias para que lhe seja possível efetuar análises forenses, no âmbito do processo de resposta a incidentes.

Implementação Técnica

1 Gestão e correlação de eventos;

2 *Software* de captura de dados em bruto, de discos, memórias e/ou pacotes de rede.

Implementação Processual

Para o efeito, a organização deve garantir:

1 Procedimentos que permitam a identificação, coleta e aquisição de registos e informação;

2 Procedimentos que permitam a recolha e captura de dados em bruto de discos, memória e redes de comunicações;

3 Procedimentos que garantam a integridade e cadeia de custódia das evidências recolhidas.

Evidências

1 Documentos de suporte ao processo de gestão e correlação de eventos;

2 Documentos de suporte ao plano de resposta a incidentes.

R.N. CIS CSC 19; COBIT 5 DSS02.02; ISO/IEC 27001:2013 A.16.1.4; NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8.

RS.AN-4 - Os incidentes devem ser categorizados de acordo com o plano de resposta

Descrição

A organização deve garantir que a categorização dos incidentes é efetuada de acordo com as regras definidas no seu plano de resposta a incidentes.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Definir a taxonomia de categorização de incidentes, tendo em conta o tipo de incidente. Por exemplo, seguindo a classificação da Taxonomia Nacional para a classificação de incidentes[1] na sua atual redação:
   a. Malware;
   b. Disponibilidade;
   c. Recolha de Informação;
   d. Tentativa de Intrusão;
   e. Intrusão;
   f. Segurança da Informação;
   g. Fraude;
   h. Conteúdo Abusivo;
   i. Outro.

[1] Informação disponível no sítio de internet do Centro Nacional de Cibersegurança

2 Garantir que a categorização dos incidentes é efetuada na resposta a incidentes, de acordo com a taxonomia definida;

3 Definir as atividades a executar, tendo por base a tipologia de cada incidente.

Evidências

1 Documentos de suporte ao plano de resposta a incidentes: Taxonomia de categorização de incidente;

2 Registo da categorização dos incidentes.

R.N. CIS CSC 4, 19;
COBIT 5 EDM03.02, DSS05.07;
NIST SP 800-53 Rev. 4 SI-5, PM-15.

RS.AN-5 - A organização deve definir processos para receber, analisar e responder a vulnerabilidades provenientes de fontes internas e externas

Descrição

A organização deve ter definido um processo formal para receber a submissão de vulnerabilidades, provenientes de fontes internas ou externas (por exemplo: testes internos, relatórios de segurança ou investigadores de segurança).

Cada submissão deve ser analisada, verificada e, no caso de ser real, deve seguir o processo de resposta a vulnerabilidades definido pela organização.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Dispor de um processo para submissão de vulnerabilidades, disponível de forma interna e externa;

2 Dispor de um processo para receber alertas de segurança, recomendações, diretrizes de fornecedores, fabricantes, grupos de interesse, entre outros;

3 De forma sistemática, avaliar, tratar e responder a cada submissão.

Evidências

1 Documento de suporte ao processo de gestão de vulnerabilidades;

2 Evidência de inscrição em grupos de interesse técnico;

3 Registo de receção e tratamento de vulnerabilidades reportadas.

4.6.4 RS.MI Mitigação

R.N. CIS CSC 19; COBIT 5 APO12.06; ISO/IEC 27001:2013 A.12.2.1, A.16.1.5; NIST SP 800-53 Rev. 4 IR-4.

RS.MI-1 - Os incidentes devem ser contidos

Descrição

A organização deve definir processos e procedimentos sistematizados, para resolução e tratamento de incidentes que lhe permitam conter, efetivamente, os incidentes ocorridos.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Ter capacidade para investigar e tomar a decisão sobre a direção a tomar:
   a. Análise de malware;
   b. Análise forense (recolha, investigação e custódia);
   c. Análise e correlação de registos;

2 Ter capacidade de sumarização das evidências e de elaboração de recomendações:
   a. Recomendar o que fazer no curto prazo para conter o incidente;
   b. Recomendar o que fazer no longo prazo;
   c. Recomendar o que deve ser segregado do restante ambiente;
   d. Identificar o que está salvaguardado em cópias de segurança e pode ser restaurado;
   e. Recomendar que credenciais devem ser alteradas ou fortalecidas;
   f. Recomendar que mecanismos de autenticação devem ser alterados ou fortalecidos com multi-fator;
   g. Recomendar que ligações de rede e sessões devem ser quebradas;
   h. Recomendar que sistemas devem receber de imediato as atualizações de segurança.

Evidências

1 Documentos de suporte ao plano de resposta a incidentes;

2 Registo de resposta e tratamento de incidentes.

R.N. CIS CSC 4, 19;
COBIT 5 APO12.06;
ISO/IEC 27001:2013 A.12.2.1, A.16.1.5;
NIST SP 800-53 Rev. 4 IR-4.

RS.MI-2 - Os incidentes devem ser mitigados

Descrição

A organização deve ter processos e procedimentos sistematizados, para resolução e tratamento de incidentes que lhe permitam indicar que os incidentes são, efetivamente, mitigados.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve:

1 Conter o incidente (bloquear contas, serviços e websites, segregar redes ou contas de utilizadores, suspender o acesso à internet, alterar palavras-passe, fechar portos de comunicação e desligar sistemas da rede de comunicações);

2 Reduzir o impacto (provisionar novos servidores, degradação graciosa de serviço e procurar serviços alternativos temporários);

3 Erradicar:
   a. Remover o *malware* usado no ataque;
   b. Aplicar atualizações de segurança;
   c. Restaurar as cópias de segurança que forem necessárias;
   d. Forçar alterações de palavras-passe e/ou requerer segundos fatores de autenticação;

4 Documentar:
   a. Que sistemas foram alvo de comprometimento;
   b. Efetuar uma análise de causa raiz;
   c. Que informação foi perdida ou exfiltrada.

Evidências

1 Documentos de suporte ao plano de resposta a incidentes;

2 Registo de resposta e tratamento de incidentes.

R.N. CIS CSC 4;
COBIT 5 APO12.06;
ISO/IEC 27001:2013 A.12.6.1;
NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5.

RS.MI-3 - As novas vulnerabilidades identificadas devem ser mitigadas ou documentadas como riscos aceites

Descrição

As novas vulnerabilidades identificadas devem ser formalmente avaliadas pela organização, no âmbito das suas atividades de gestão de vulnerabilidades. Deve ser identificado pela organização qual o tratamento a efetuar às vulnerabilidades encontradas.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve avaliar novas vulnerabilidades:

1 E remediar a mesmas;

2 Ou executar os formalismos necessários para a aprovação do risco associado, justificando as razões da decisão tomada.

Evidências

1 Documentos que sustentam o processo de gestão de vulnerabilidades;

2 Registo de execução do processo de gestão de vulnerabilidades;

3 Registo de vulnerabilidades, cujo risco foi aceite pela gestão.

4.6.5 RS.ME Melhorias

R.N. COBIT 5 BAI01.13;
ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;
NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RS.ME-1 - Os planos de resposta a incidentes devem incorporar as lições aprendidas

Descrição

A organização deve efetuar uma observação dos incidentes ocorridos, após a finalização dos mesmos, para poder identificar possíveis lições aprendidas.

A organização deve promover sessões de trabalho com a equipa de resposta a incidentes, onde deve ser discutido o que foi aprendido no incidente. Nestas sessões de trabalho, deve ser analisado e documentado tudo o que é conhecido sobre o incidente, identificando-se o que funcionou bem e o que precisa de ser melhorado no plano de resposta, para tornar a organização e os seus sistemas mais resilientes no tratamento de incidentes futuros.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve implementar um plano de melhoria com base nas lições aprendidas, como por exemplo:

1 Que alterações podem ser efetuadas para melhorar a segurança;

2 O que pode ser feito de forma diferente;

3 O que deve ser feito de forma diferente;

4 Quem necessita de ser formado de forma diferente;

5 Que fragilidades foram exploradas;

6 Como se garante que não volta a acontecer.

Evidências

1 Documentos de suporte ao plano de resposta a incidentes;

2 Registo de tratamento de ações de melhoria, resultante de incidentes ocorridos.

RS.ME-2 - As estratégias de resposta a incidentes devem ser atualizadas

R.N. COBIT 5 BAI01.13; DSS04.08;

ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

Descrição

As ameaças e vulnerabilidades estão em constante evolução. Para que o plano de resposta a incidentes não fique desatualizado e irrelevante, a organização deve atualizá-lo continuamente à luz das práticas implementadas.

A própria organização é dinâmica. Podem existir mudanças ao nível dos ativos, a nível dos colaboradores ou dos responsáveis por cada ativo e, como tal, os planos de resposta devem ser atualizados de acordo com estas transformações internas.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve atualizar:

1 A lista de redes e sistemas de informação de suporte aos serviços críticos;

2 A resposta tática a ameaças específicas;

3 As listas de contactos com organizações externas;

4 As listas de contactos internos.

Evidências

1 Documentos de suporte ao plano de resposta a incidentes;

2 Registo de atualizações ao plano de resposta a incidentes.

MEDIDAS DE SEGURANÇA

RECUPERAR

4.7.1 RC.PR Plano de Recuperação

R.N. CIS CSC 10; COBIT 5 APO12.06, DSS02.05, DSS03.04; ISO/IEC 27001:2013 A.16.1.5; NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8.

RC.PR-1 - A organização deve seguir um plano de recuperação durante ou após um incidente

Descrição

A organização deve sistematizar o seu processo de recuperação de incidentes, por forma a garantir uma correta alocação de recursos (humanos/tecnológicos e processuais) à resolução dos mesmos.

No processo de recuperação de um incidente de segurança da informação, é relevante garantir a integridade e disponibilidade dos sistemas.

Implementação Técnica

1 Plataforma de cópias de segurança e restauro.

Implementação Processual

A organização deve:

1 Implementar um processo de recuperação de incidentes;

2 Garantir que o rigor, âmbito, aplicabilidade e resultados das atividades de recuperação a incidentes são consistentes e transversais a toda a organização e a todos os incidentes;

3 Avaliar previamente as medidas de recuperação de incidentes, tendo em conta outros planos (por exemplo: plano da continuidade do negócio).

Evidências

1 Documentos de suporte ao plano de resposta a incidentes;

2 Registo de recuperação de incidentes.

4.7.2 RC.ME Melhorias

R.N. COBIT 5 APO12.06, BAI05.07, DSS04.08; ISO/IEC 27001:2013 A.16.1.6, Cláusula 10; NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RC.ME-1 - Os planos de recuperação devem incorporar as lições aprendidas

Descrição

A organização deve garantir que são executadas ações resultantes de lições aprendidas após a execução do plano de recuperação.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve implementar um plano de melhoria com base nas lições aprendidas.

A organização deve contemplar:

1 Avaliação da eficácia dos planos de recuperação existentes;

2 Identificação das fragilidades nos planos existentes;

3 Identificação das oportunidades de melhoria que possam ser implementadas;

4 Atualização do plano com as melhorias encontradas.

Evidências

1 Documentos de suporte ao processo de recuperação de incidentes;

2 Plano de ações resultante da avaliação de lições aprendidas.

RC.ME-2 - As estratégias de recuperação devem ser continuamente revistas e atualizadas

R.N. COBIT 5 APO12.06, BAI07.08;
ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;
NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

Descrição

As organizações são dinâmicas e existem mudanças quer a nível dos ativos, quer a nível dos recursos humanos e dos responsáveis por cada ativo. Os planos de recuperação devem seguir esta evolução natural, com atualizações dos pontos de contacto, ativos e prioridades.

A organização deve, assim, assegurar que as suas estratégias de recuperação são revistas e atualizadas de acordo com as suas necessidades.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve atualizar:

1 A lista de prioridades das redes e sistemas de informação que suportam os serviços críticos;

2 As técnicas de recuperação dos sistemas de informação;

3 As listas de contactos dos responsáveis técnicos;

4 As listas de contactos dos responsáveis funcionais.

Evidências

1 Documentos de suporte ao plano de recuperação de incidentes;

2 Registo de atualizações ao plano de recuperação de incidentes.

4.7.3 RC.CO Comunicações

R.N. COBIT 5 EDM03.02;

ISO/IEC 27001:2013 A.6.1.4, Cláusula 7.4.

RC.CO-1 - A organização deve implementar um plano de comunicação

Descrição

Especialmente em contexto de cibersegurança, a organização deve comunicar o que é relevante. O fluxo de comunicação deve ser controlado pela organização para minimizar potenciais impactos na sua credibilidade e reputação.

A organização deve definir uma estratégia de comunicação baseada num plano de comunicação produzido para o efeito. O plano poderá ser consolidado com outros planos de comunicação existentes na organização.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve definir um plano de comunicação com as partes interessadas que identifique:

1 O que comunicar: Que conteúdo (por exemplo: a forma adequada como foi tratado um incidente de cibersegurança);

2 Que mensagem: Forma e formato, que tipo de meio será usado, desde pequenos textos a imagens, metáforas, vídeos, entre outros;

3 Quem deve comunicar: Deve ser nomeado um responsável que tem a autoridade e autonomia para comunicar, particularmente com organizações externas;

4 A quem comunicar: Destinatários da comunicação;

5 Como comunicar: Que canais devem ser usados para obter a melhor eficácia na difusão da mensagem (por exemplo: mensagens de correio eletrónico e protetores de ecrã);

6 Quando comunicar: A comunicação deve ser regularmente exercitada em condições comuns (por exemplo: divulgação da política de segurança da informação), mas poderá ter frequências e modos de atuação muito diferentes em contexto de incidente.

Evidências

1 Plano de comunicação associado à recuperação de incidentes.

R.N. COBIT 5 APO12.06;
ISO/IEC 27001:2013 Cláusula 7.4;
NIST SP 800-53 Rev. 4 CP-2, IR-4.

RC.CO-2 - As atividades de recuperação devem ser comunicadas às partes interessadas, internas e externas, bem como às equipas executivas e de gestão

Descrição

A organização deve garantir que as partes interessadas, internas e externas, são informadas no caso de existência de incidentes que assim o justifiquem.

A organização deve definir uma estratégia de comunicação baseada num plano de comunicação produzido para o efeito. Este poderá ser consolidado com outros planos de comunicação existentes na organização.

Implementação Técnica

Não aplicável.

Implementação Processual

A organização deve identificar:

1 Procedimento de escalonamento de incidentes;

2 Que tipificação de incidentes poderá motivar contactar-se as partes interessadas externas;

3 Qual o plano de comunicação a instituir;

4 Quais as partes interessadas a contactar.

Evidências

1 Plano de comunicação documentado e disseminado pelos responsáveis pela sua execução.

Recomendações Adicionais

5.1 Introdução

Atualmente, quase todas as organizações têm equipamentos de segurança nas suas redes de comunicações, como *firewall*, sistemas de deteção de intrusão, filtros de pedidos de resolução de nomes, proteção contra mensagens de correio eletrónico contendo *spam* ou *phishing*, ferramentas de deteção de ameaças persistentes, entre outras. Estes equipamentos são uma primeira linha de defesa, constituindo medidas básicas para a segurança dos colaboradores e das redes e sistemas de informação da organização, contra ciberataques e tráfego não regulado da internet.

Serão estas tecnologias, por si só, suficientes para se garantir a segurança da informação da organização?

Não é possível dar-se uma resposta concreta a esta questão, tendo em conta que a mesma depende de diversas variáveis de avaliação, que são alteradas de acordo com a tecnologia, recursos, contexto e ambiente envolvente da organização. Na prática, estes equipamentos providenciam uma proteção imediata contra as ameaças conhecidas (se devidamente parametrizados), mas poderão ser ineficientes com o que ainda é desconhecido.

Segundo o MITRE[1], a lista de CVEs, ou seja, o número de vulnerabilidades publicadas por ano, tem aumentado de forma significativa nos últimos anos, como se pode constatar no gráfico abaixo.

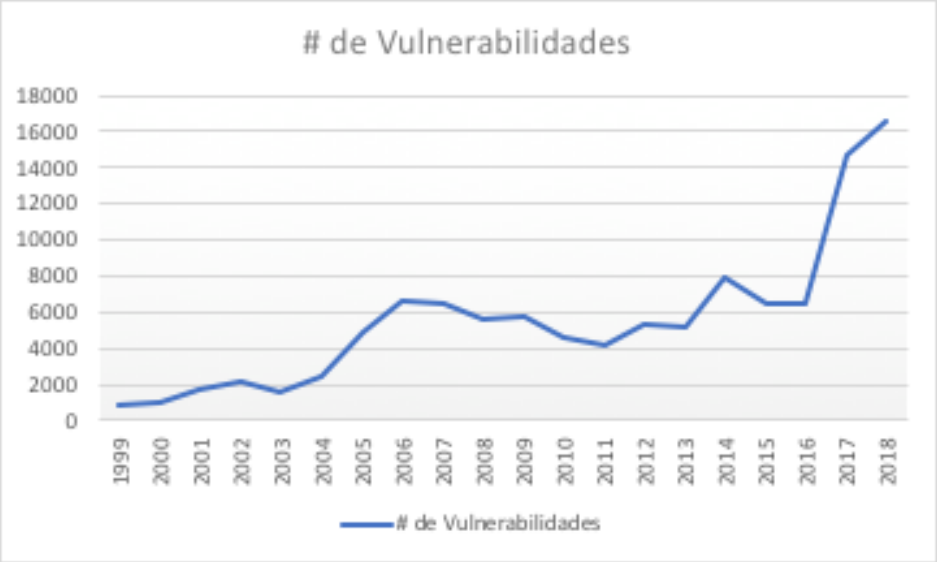


Figura 9 - Número de vulnerabilidades publicadas por ano

Cada uma destas possíveis vulnerabilidades existentes nas redes e sistemas de informação da organização pode ser explorada por uma nova ameaça.

Os perímetros de defesa são habitualmente estáticos e não são atualizados de forma contínua. Daqui deriva outro grande desafio para as organizações, tendo em conta que as ameaças existentes originadas no ciberespaço são bastante dinâmicas.

Como resposta a estes desafios, torna-se necessário ter uma equipa especializada e multidisciplinar que possa servir a organização, atualizando de forma continuada a proteção das

[1] https://cve.mitre.org/

suas redes e sistemas de informação contra novas ameaças de cibersegurança ou mesmo evoluções de ameaças antigas.

5.2 A função do CISO

O CISO, *Chief Information Security Officer*, é uma função exercida na organização, para a qual se estabelece uma relação contratual, com o objetivo de garantir a segurança da informação dessa mesma organização.

Deve reportar à gestão de topo e, dado que o impacto da sua responsabilidade é potencialmente transversal, o CISO deve ter conhecimento pleno dos processos chave da organização onde se insere.

De uma forma geral, o CISO deve ser capaz de traduzir os objetivos da organização em requisitos de segurança da informação e, também por este motivo, deve ser um bom comunicador.

Entre outras responsabilidades atribuídas ao CISO, este deve:

- Assegurar a implementação e manter a estratégia de segurança da informação;
- Implementar boas práticas de segurança da informação holísticas e estruturadas;
- Pesquisar, definir e comunicar requisitos de segurança da informação;
- Desenvolver e implementar políticas, processos e procedimentos de segurança da informação;
- Ter conhecimento sobre a legislação e regulamentação específica do setor de atividade da organização;
- Ter conhecimento sobre a legislação e regulamentação referente à segurança de informação, nomeadamente, a ISO/IEC 27001 e o Regulamento Geral de Proteção de Dados Pessoais[2];
- Coordenar esforços referentes à proteção de dados pessoais;
- Definir e implementar estratégias de avaliação e de resposta aos riscos;
- Acompanhar e avaliar a execução do processo de gestão de alterações;
- Acompanhar e participar no processo de gestão de incidentes;
- Acompanhar auditorias de segurança e implementação de medidas de melhorias;
- Suportar a organização na estratégia e desempenho e monitorização das tecnologias de informação;

[2] https://www.cnpd.pt/bin/rgpd/rgpd.html, https://gdpr.eu/

- Dinamizar sessões de sensibilização em segurança da informação e cibersegurança.

O CISO tem um papel fulcral na análise do QNRCS e na identificação das medidas que possam ser adequadas para implementação da sua organização. Deve acompanhar todo o processo de implementação, definição de prioridades e atividades de melhoria contínua, que garantam que a organização está preparada e adequadamente resiliente em termos de segurança da informação e cibersegurança.

5.3 Constituição de SOC

Segundo a definição da Gartner[1], um SOC é: *"Um centro de operações de segurança, é tanto a equipa, que frequentemente opera em turnos de 24h/7 dias da semana, como as instalações dedicadas e organizadas para prevenir, detetar, avaliar e responder a ameaças e incidentes de cibersegurança, e para avaliar e cumprir com a conformidade das leis locais em vigor"*.

As principais tarefas de um SOC são:

1 Identificação, catalogação, categorização e monitorização das redes e sistemas de informação, para que a equipa possa estar consciente de que vulnerabilidades se podem tornar ameaças à organização;

2 Proatividade na deteção de atividade maliciosa nas redes e sistemas de informação. Quanto mais rápida for a deteção e resposta, menores poderão ser os efeitos da ameaça;

3 Efetuar gestão de vulnerabilidades, por forma a garantir que as redes e sistemas de informação estão devidamente atualizados com os pacotes de segurança disponíveis para estarem protegidos contra ameaças;

4 Atualização das defesas contra novas ameaças. O perímetro de segurança da organização deve ser revisto com frequência e ajustado com as proteções consideradas como necessárias;

5 Gestão de eventos e de registos de sistemas, segurança e auditoria, para permitir às equipas de resposta a incidentes efetuar análises forenses quando a organização é exposta a incidentes ou a falhas de segurança.

Existem diversos modelos de SOC que vão desde o virtual, com recursos alocados a tempo parcial e sem exclusividade, até ao modelo multifunções onde as equipas realizam não só as tarefas de segurança, mas também tarefas de operação e monitorização das redes e sistemas de informação. De seguida, identificamos os tipos mais comuns de SOC e quais as suas características mais relevantes:

[1] https://www.gartner.com/en/newsroom/press-releases/2017-10-12-security-operations-centers-and-their-role-in-cybersecurity

SOC Virtual

1 Sem instalações dedicadas;

2 Equipa com alocação parcial e sem exclusividade;

3 Operação 9x5 com resposta no próximo dia útil;

4 Reativo, apenas despoletado quando aparece um alerta crítico ou incidente.

SOC Dedicado

1 Instalações dedicadas;

2 Equipa interna com alocação total e em exclusividade;

3 Operação 24x7;

4 Reativo e pró-ativo.

SOC Distribuído

1 Instalações dedicadas;

2 Equipas internas com alocação total ou parcial;

3 Operação 24x7 ou 9x5, dependendo do local físico;

4 Reativo e pró-ativo;

5 Possibilidade de partilha de responsabilidades com parceiros especializados em cibersegurança.

SOC de Comando

1 Instalações dedicadas;

2 Equipas internas com alocação total;

3 Operação 9x5;

4 Reativo e pró-ativo;

5 Providencia inteligência sobre ameaças e visão situacional global;

6 Não está habitualmente envolvido nas atividades de operação diárias.

SOC Multifunções

1 Instalações dedicadas;

2 Equipas internas com alocação total;

3 Operação 24x7;

4 Reativo e pró-ativo;

5 Providencia, também, serviços de operação e manutenção de redes ou sistemas de informação. É uma forma de otimização de custos para não ter de suportar duas equipas distintas em suporte 24x7.

SOC de Fusão

1 Instalações dedicadas;

2 Equipas internas com alocação total;

3 Operação 24x7;

4 Reativo e pró-ativo;

5 Integra as equipas de resposta a incidentes (CSIRT) ou de operação dos equipamentos de segurança e rede.

SOC Externalizado

1 Sem instalações dedicadas;

2 Equipas externas com alocação total;

3 Operação 24x7;

4 Reativo e pró-ativo;

5 Supervisão das atividades por alguém interno à organização.

Para o planeamento e implementação do SOC, o CISO ou o responsável geral pela segurança da informação e cibersegurança da organização deve:

1 Efetuar um estudo realista da análise custo/benefício dos diferentes modelos de SOC antes de iniciar a construção de um SOC totalmente interno;

2 Focar o alinhamento dos entregáveis do SOC com a missão, visão, valores, estratégias e objetivos da organização;

3 Definir os objetivos e métricas que devem ser cumpridos;

4 Identificar quais as funções críticas de segurança que devem ser internalizadas;

5 Considerar a possibilidade de recorrer a serviços de um parceiro especialista, para minimizar os custos de operação 24x7 do SOC e/ou para suprir necessidades adicionais de capacidade de recursos internos.

5.4 Constituição de CSIRT

A abreviatura CSIRT significa *Computer Security Incident Response Team* (Equipa de Resposta a Incidentes de Segurança Informática).

Trata-se de um termo predominantemente utilizado na Europa e que corresponde ao termo protegido CERT, registado nos EUA pelo CERT Coordination Center (CERT/CC) (Centro de Coordenação CERT) da Carnegie Mellon University.

Uma equipa de CSIRT é uma equipa de peritos de segurança informática que tem como principal atividade responder aos incidentes. Presta os serviços necessários para os gerir e ajudar os seus utilizadores a recuperarem das violações da segurança que ocorram.

Ter ao serviço uma equipa de segurança informática dedicada ajuda as organizações a reduzir o impacto e a prevenir os incidentes graves.

Outros benefícios possíveis são os seguintes:

1 Ter uma coordenação centralizada para as questões de segurança informática na organização, com um ponto único de contacto;

2 Gestão e resposta centralizadas e especializadas em matéria de incidentes informáticos;

3 Contar com peritos disponíveis para apoiarem e ajudarem os utilizadores a recuperarem rapidamente dos incidentes;

4 Tratar das questões jurídicas e preservar as provas em caso de ação judicial;

5 Acompanhar a evolução no domínio da segurança;

6 A cooperação, em matéria de segurança informática, no seio da comunidade de especialistas.

Para iniciar adequadamente o processo de criação de um CSIRT é importante ter uma visão clara dos eventuais serviços que este pode prestar aos seus clientes, geralmente denominados por "comunidade utilizadora". Importa compreender, portanto, quais são as necessidades dos utilizadores para lhes prestar os serviços adequados, no momento certo e com a qualidade apropriada[1].

Como referência internacional, o RFC2350[2] da IETF (*Internet Engineering Task Force*) documenta a estrutura de um CSIRT, que deve ser preenchida e publicada por forma a facilitar a comunicação sobre políticas, procedimentos e serviços à comunidade abrangida, ou mesmo a outras organizações e/ou equipas de resposta a incidentes.

A nível europeu, e com uma definição mais recente, podemo-nos inspirar na ENISA[3] e classificar os serviços típicos de uma equipa de CSIRT em três categorias:

[1] https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-portugese/at_download/fullReport

[2] https://tools.ietf.org/html/rfc2350#appendix-E

[3] https://www.enisa.europa.eu/topics/csirt-cert-services

Serviços reativos

1 Alertas e avisos;

2 Resposta a incidentes:
   a. Análise de incidentes;
   b. Resposta a incidentes no local;
   c. Suporte a resposta a incidentes;
   d. Coordenação de resposta a incidentes;

3 Gestão de vulnerabilidades:

   a. Análise de vulnerabilidades;
   b. Resposta a vulnerabilidades;
   c. Coordenação da resposta a vulnerabilidades;

4 Gestão de artefactos:
   a. Análise de artefactos;
   b. Resposta a artefactos;
   c. Coordenação da resposta a artefactos.

Serviços Proativos

1 Campanhas de sensibilização;

2 Acompanhamento de tecnologia;

3 Auditorias e avaliações de segurança;

4 Configuração e manutenção de ferramentas de segurança, aplicações e infraestrutura;

5 Desenvolvimento de ferramentas de segurança;

6 Serviços de deteção de intrusão;

7 Disseminação de informação de segurança.

Serviços de gestão da qualidade de segurança

1 Análise do risco;

2 Planeamento da continuidade do negócio e de recuperação pós desastre;

3 Consultoria de segurança;

4 Sensibilização em segurança;

5 Treino e formação;

6 Avaliação e certificação de produtos.

A criação de um CSIRT permite às organizações prepararem a sua capacidade de resposta a incidentes de segurança da informação e cibersegurança. Permite, igualmente, à organização incrementar a sua capacidade de resposta a incidentes de segurança de informação, de forma conjunta com outras partes interessadas, tendo em conta que a estrutura do CSIRT releva a importância da partilha de informação de incidentes de segurança de informação durante o ciclo de vida dos processos de gestão inerentes.

Portugal dispõe de uma Rede Nacional de CSIRT[1], composta por organizações do setor público e privado, que tem como objetivo:

- Estabelecer laços de confiança entre elementos responsáveis pela segurança informática, de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança;
- Criar indicadores e informação estatística nacional sobre incidentes de segurança, com vista à melhor identificação de contramedidas pró-ativas e reativas;
- Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão;
- Promover uma cultura de segurança em Portugal.

A constituição de um CSIRT deverá ser efetuada à medida da realidade da organização, tendo em conta a sua dimensão, setor de atividade e a sua utilização de tecnologias de informação e exposição ao ciberespaço.

Em termos de maturidade das equipas CSIRT, existe já o modelo SIM3 (*Security Incident Management Maturity Model*) que se baseia em quatro vetores: organizacional, humano, ferramentas e processos. Este modelo de maturidade inclui a avaliação de 44 diferentes parâmetros de uma equipa nos referidos quatro vetores, e permitirá a qualquer equipa, depois de constituída e de operar durante algum tempo, realizar uma autoavaliação. Esta circunstância potenciará a melhoria contínua da equipa.

[1] https://www.redecsirt.pt/

Anexo 1 - Quadro Resumo

O quadro seguinte serve de apoio para análise das informações de referência que suportam as subcategorias do QNRCS.

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
IDENTIFICAR (ID)	Gestão de ativos (ID.GA)	ID.GA-1 – Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser inventariados	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.GA-2 – As aplicações e plataformas de software que suportam os processos dos serviços críticos devem ser inventariadas	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.GA-3 – As redes e fluxos de dados devem ser mapeados	CIS CSC 12 COBIT 5 DSS05.02 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.GA-4 – As redes e sistemas de informação externos devem ser identificados e catalogados	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.GA-5 – Os ativos necessários para a prestação de bens e serviços devem ser classificados	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
	Ambiente da Organização (ID.AO)	ID.AO-1 – O papel da organização na cadeia logística deve ser identificado e comunicado	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.AO-2 – O posicionamento da organização no seu setor de atividade deve ser identificado e comunicado	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
		ID.AO-3 – A missão, visão, valores, estratégias e objetivos da organização devem ser definidas e comunicadas	COBIT 5 APO02.01, APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.AO-4 – Os ativos críticos devem ser identificados e registados	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.AO-5 – Os requisitos de resiliência necessários para suportar a prestação de serviços críticos devem ser definidos	COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	Governação (ID.GV)	ID.GV-1 – A política de segurança da informação deve ser definida e comunicada	CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls from all security control families
		ID.GV-2 – Os requisitos legais e regulamentares para a cibersegurança devem ser cumpridos	CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 4 -1 controls from all security control families
	Avaliação de risco (ID.AR)	ID.AR-1 – As vulnerabilidades dos ativos devem ser identificadas e documentadas	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.AR-2 – A organização deve partilhar informações sobre ameaças de cibersegurança com grupos de interesse da especialidade	CIS CSC 4 COBIT 5 BAI08.01 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
		ID.AR-3 – As ameaças internas e externas devem ser identificadas e documentadas na metodologia de gestão do risco	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.AR-4 – A gestão do risco deve ser efetuada com base na análise de ameaças, vulnerabilidades, probabilidades e impactos	CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.AR-5 – A organização deve garantir que as respostas aos riscos são identificadas e priorizadas	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9
	Estratégia de Gestão de Risco (ID.GR)	ID.GR-1 – A organização deve definir um processo de gestão do risco	CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9
		ID.GR-2 – A organização deve determinar e identificar a sua tolerância ao risco	COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9
		ID.GR-3 – A organização deve definir a sua estratégia de tratamento do risco	COBIT 5 APO12.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	ID.GL – Gestão do Risco da Cadeia Logística	ID.GL-1 – A organização deve definir, avaliar e gerir processos de gestão do risco da cadeia logística	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
		ID.GL-2 – A organização deve avaliar o risco da cadeia logística de cibersegurança	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.GL-3 – Os contratos com fornecedores devem respeitar o plano de gestão do risco para a cadeia logística	COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9
		ID.GL-4 – Os fornecedores devem ser periodicamente avaliados	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.GL-5 – O plano de resposta e recuperação de desastre deve ser exercitado com o acompanhamento de fornecedores	CIS CSC 19, 20 COBIT 5 DSS04.04 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
PROTEGER (PR)	PR.GA – Gestão de Identidades, Autenticação e Controlo de Acessos	PR.GA-1 – O ciclo de vida de gestão de identidades deve ser definido	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.GA-2 – Devem existir controlos de acesso físico às redes e sistemas de informação	COBIT 5 DSS01.04, DSS05.05 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.GA-3 – A organização deve gerir os seus acessos remotos	CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.GA-4 – A organização deve aplicar na gestão de acessos, os princípios do menor privilégio e da segregação de funções	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.GA-5 – A organização deve proteger a integridade das redes de comunicações	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
		PR.GA-6 – A organização deve verificar a identidade dos colaboradores e vinculá-las às respetivas credenciais	CIS CSC, 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.GA-7 – Devem ser definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação	CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	PR.FC – Formação e Sensibilização	PR.FC-1 – Os colaboradores devem ter formação em segurança da informação	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13
		PR.FC-2 – Os utilizadores com acesso privilegiado devem compreender quais são os seus papéis e responsabilidades	CIS CSC 5, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.FC-3 – As partes interessadas externas devem compreender quais são os seus papéis e responsabilidades	CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
		PR.FC-4 – A gestão de topo deve compreender as suas funções e responsabilidades	CIS CSC 17, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	PR.SD – Segurança de Dados	PR.SD-1 – A organização deve proteger os dados armazenados	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
		PR.SD-2 – A organização deve proteger os dados em circulação	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
		PR.SD-3 – A organização deve gerir formalmente os ativos durante os procedimentos de remoção, transferência e aprovisionamento dos mesmos	CIS CSC 1 COBIT 5 BAI09.03 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.SD-4 – A organização deve providenciar a capacidade adequada para garantir a disponibilidade das redes e dos sistemas de informação	CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.SD-5 –A organização deve implementar proteções que evitem exfiltração de informação	CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.SD-6 – A organização deve utilizar mecanismos de verificação para confirmar a integridade de software, firmware e dados	CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7
		PR.SD-7 – Os ambientes de desenvolvimento e de teste devem ser separados de ambientes de produção	CIS CSC 18, 20 COBIT 5 BAI03.08, BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2
		PR.SD-8 – A organização deve implementar mecanismos de validação e verificação de integridade do hardware	COBIT 5 BAI03.05 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	PR.PI – Procedimentos e Processos de Proteção da Informação	PR.PI-1 – Deve ser criada e mantida uma configuração base de redes e sistemas de informação que incorpore os princípios de segurança	CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.PI-2 – Deve ser implementado um ciclo de vida de desenvolvimento seguro de *software*	CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.PI-3 – Deve ser implementado um processo de gestão de alterações	CIS CSC 3, 11 COBIT 5 BAI01.06, BAI06.01 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
		PR.PI-4 – Devem ser realizadas, mantidas e testadas cópias de segurança dos dados da organização	CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
		PR.PI-5 – As políticas e regulamentações associadas à operacionalização dos ambientes físicos dos ativos da organização devem ser seguidas	COBIT 5 DSS01.04, DSS05.05 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.PI-6 – Os dados devem ser destruídos de acordo com a política definida	COBIT 5 BAI09.03, DSS05.06 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6
		PR.PI-7 – Os processos de proteção devem ser continuamente melhorados	COBIT 5 APO11.06, APO12.06, DSS04.05 ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.PI-8 – A efetividade das tecnologias de proteção deve ser tida em conta na melhoria dos processos de proteção	COBIT 5 BAI08.04, DSS03.04 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.PI-9 – Os planos de resposta a incidentes, continuidade de negócio, a recuperação de incidentes e recuperação de desastres devem ser atualizados	CIS CSC 19 COBIT 5 APO12.06, DSS04.03 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.PI-10 – Os planos de resposta e recuperação devem ser testados e exercitados	CIS CSC 19, 20 COBIT 5 DSS04.04 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
		PR.PI-11 – A cibersegurança deve ser contemplada nos processos de gestão de recursos humanos	CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.PI-12 – Deve ser definido e implementado um processo de gestão de vulnerabilidades	CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	PR.MA – Manutenção	PR.MA-1 – As atividades de manutenção e reparação dos ativos da organização devem ser realizadas e registadas em programas e planos aprovados e controlados	COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6
		PR.MA-2 – As operações de manutenção remota das redes devem ser revistas, aprovadas, executadas e registadas	CIS CSC 3, 5 COBIT 5 DSS05.04 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4
	PR.TP – Tecnologia de Proteção	PR.TP-1 – Os registos de auditoria e de histórico devem ser documentados, implementados e revistos de acordo com as políticas	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family
		PR.TP-2 – Os suportes de dados amovíveis devem ser protegidos e a sua utilização deve ser restrita, de acordo com a política definida	CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, DSS05.06 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.TP-3 – O princípio da minimização de funcionalidades deve ser incorporado na configuração de sistemas de modo a fornecer apenas os recursos essenciais	CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7
		PR.TP-4 – As redes de comunicações e de controlo devem ser protegidas	CIS CSC 8, 12, 15 COBIT 5 DSS05.02, APO13.01 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.TP-5 – Devem ser implementados mecanismos para cumprir os requisitos de resiliência em situações adversas	COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
DETETAR (DE)	DE.AE – Anomalias e Eventos	DE.AE-1 – A organização deve definir e gerir um modelo de referência de operações de rede e fluxos de dados esperados para utilizadores e sistemas	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2 – Os eventos detetados devem ser analisados por forma a se identificarem os alvos e os métodos de ataque	CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3 – Os eventos devem ser coletados e correlacionados a partir de várias fontes e sensores	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4 – O impacto dos eventos deve ser classificado	CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
		DE.AE-5 – Devem ser definidos os limites de alerta para incidentes	CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	DE.MC – Monitorização Contínua de Segurança	DE.MC-1 – As redes e sistemas de informação devem ser monitorizados para detetar potenciais incidentes	CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.MC-2 – O ambiente físico deve ser monitorizado para se detetar potenciais incidentes de segurança	COBIT 5 DSS01.04, DSS01.05 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.MC-3 – A atividade dos colaboradores deve ser monitorizada para se detetar potenciais incidentes	CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.MC-4 – A organização deve identificar e implementar mecanismos para deteção de código malicioso	CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8
		DE.MC-5 – A utilização de aplicações não autorizadas em dispositivos móveis deve ser detetada	CIS CSC 7, 8 COBIT 5 DSS05.01 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44
		DE.MC-6 – As atividades dos prestadores de serviços externos devem ser monitorizadas para deteção de incidentes	COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.MC-7 – Deve ser efetuada a monitorização de acessos não autorizados de colaboradores, conexões, dispositivos e software	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.MC-8 – Devem ser efetuados rastreamentos de vulnerabilidades	CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	DE.PD – Processos de Deteção	DE.PD-1 – Devem ser definidos os papéis e responsabilidades na deteção de eventos anómalos	CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.PD-2 – As atividades de deteção devem cumprir com todos os requisitos aplicáveis	COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.PD-3 – Os processos de deteção devem ser testados	COBIT 5 APO13.02, DSS05.02 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.PD-4 – Informações sobre deteções de eventos devem ser comunicadas	CIS CSC 19 COBIT 5 APO08.04, APO12.06, DSS02.05 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
		DE.PD-5 – Os processos de deteção devem ser objeto de melhoria contínua	COBIT 5 APO11.06, APO12.06, DSS04.05 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPONDER (RS)	RS.PR – Planeamento da Resposta	RS.PR-1 – O plano de resposta deve ser executado durante ou após a ocorrência de um incidente	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	RS.CO – Comunicações	RS.CO-1 – Na resposta a um incidente, os colaboradores devem conhecer os seus papéis e a ordem de execução de atividades	CIS CSC 19 COBIT 5 EDM03.02, APO01.02, APO12.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2 – Os incidentes devem ser reportados de acordo com critérios estabelecidos	CIS CSC 19 COBIT 5 DSS01.03 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3 – As informações devem ser partilhadas de acordo com o plano de resposta	CIS CSC 19 COBIT 5 DSS03.04 ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4 – A coordenação com as partes interessadas deve ocorrer conforme os planos de resposta	CIS CSC 19 COBIT 5 DSS03.04 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5 – Deve ocorrer partilha voluntária de informação com partes interessadas externas	CIS CSC 19 COBIT 5 BAI08.04 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
	RS.AN – Análise	RS.AN-1 – As notificações dos sistemas de deteção devem ser investigadas	CIS CSC 4, 6, 8, 19 COBIT 5 DSS02.04, DSS02.07 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2 – O impacto do incidente deve ser avaliado	COBIT 5 DSS02.02 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3 – Devem ser realizadas análises forenses	COBIT 5 APO12.06, DSS03.02, DSS05.07 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4 – Os incidentes devem ser categorizados de acordo com o plano de resposta	CIS CSC 19 COBIT 5 DSS02.02 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
		RS.AN-5 – A organização deve definir processos para receber, analisar e responder a vulnerabilidades provenientes de fontes internas e externas	CIS CSC 4, 19 COBIT 5 EDM03.02, DSS05.07 NIST SP 800-53 Rev. 4 SI-5, PM-15
	RS.MI – Mitigação	RS.MI-1 – Os incidentes devem ser contidos	CIS CSC 19 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2 – Os incidentes devem ser mitigados	CIS CSC 4, 19 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3 – As novas vulnerabilidades identificadas devem ser mitigadas ou documentadas como riscos aceites	CIS CSC 4 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	RS.ME – Melhorias	RS.ME-1 – Os planos de resposta a incidentes devem incorporar as lições aprendidas	COBIT 5 BAI01.13 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.ME-2 – As estratégias de resposta a incidentes devem ser atualizadas	COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA
RECUPERAR (RC)	RC.PR – Plano de Recuperação	RC.PR-1 – A organização deve seguir um plano de recuperação durante ou após um incidente	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	RC.ME – Melhorias	RC.ME-1 – Os planos de recuperação devem incorporar as lições aprendidas	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.ME-2 – As estratégias de recuperação devem ser continuamente revistas e atualizadas	COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RC.CO – Comunicações	RC.CO-1 – A organização deve implementar um plano de comunicação	COBIT 5 EDM03.02 ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
		RC.CO-2 – As atividades de recuperação devem ser comunicadas às partes interessadas, internas e externas, bem como às equipas executivas e de gestão	COBIT 5 MEA03.02 ISO/IEC 27001:2013 Clause 7.4

Tabela 11 – Quadro resumo

www.cncs.gov.pt
cncs@cncs.gov.pt

Rua da Junqueira 69,
1300-342 Lisboa
+351 210 497 400

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL