# QUADRO DE AVALIAÇÃO DE CAPACIDADES DE CIBERSEGURANÇA

**Centro Nacional de Cibersegurança**

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia


# QUADRO DE AVALIAÇÃO DE CAPACIDADES DE CIBERSEGURANÇA

## Centro Nacional de Cibersegurança

Versão 1.0

Janeiro de 2020

## ÍNDICE

# 1 Níveis de capacidade

## 1.1 Introdução

Este documento é um produto complementar ao Quadro Nacional de Referência para a Cibersegurança (QNRCS), dando seguimento à estratégia do Centro Nacional de Cibersegurança (CNCS) para o suporte das organizações à sua capacitação, através da disponibilização de referenciais e ferramentas. Como complemento ao QNRCS apresenta, para cada uma das medidas de cibersegurança, a definição de três níveis de capacidade para que seja possível às organizações o cumprimentos dos cinco objetivos do quadro, tendo em conta o seu contexto e dimensão.

A lista abaixo categoriza as medidas de segurança em três níveis de capacidade quanto à sua implementação. Cada nível contém as práticas propostas para atingir satisfatoriamente o objetivo proposto e as evidências que devem ser fornecidas para verificar a implementação efetiva da medida de segurança. Na tabela abaixo, descrevem-se os três níveis apresentados.

| NÍVEIS DE CAPACIDADE | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Inicial** | Medidas de segurança básicas que poderiam ser implementadas para alcançar o objetivo de segurança, nomeadamente em iniciativas *ad-hoc*, por iniciativas isoladas e pouco formais. | Evidência de implementação das medidas de nível Inicial. |
| **2 – Intermédio** | Medidas de segurança que atendem à maioria dos casos e necessidades para atingir os objetivos de segurança da informação. As medidas são atingidas formalmente. | Evidência de implementação das medidas de nível Intermédio. |
| **3 – Avançado** | Medidas de segurança avançadas que envolvem a monitorização contínua dos controlos, avaliação e revisão recorrentes, levando em consideração alterações, incidentes, testes e exercícios, para melhoria proativa das mesmas. | Evidência de implementação das medidas de nível Avançado. |

Propõe-se a aplicação cumulativa das medidas definidas. Ou seja, para que uma organização esteja posicionada no nível de capacidade "3 – Avançado", terá de implementar as medidas de nível "1 – Inicial" e "2 – Intermédio".

Os níveis de capacidade podem ser aplicados de forma independente a cada objetivo. Como resultado, uma organização pode posicionar-se em níveis de capacidade distintos para um mesmo objetivo de segurança. Os níveis de capacidade aplicáveis a uma determinada organização dependem das suas características específicas, tais como dimensão e serviços fornecidos. Por exemplo, para uma organização com apenas 5 colaboradores, pode não ser necessária a definição de uma política de segurança totalmente alinhada com os padrões de mercado e práticas recomendadas ou possuir um procedimento formal documentado para a contratação de pessoal.

As medidas de segurança têm os seus níveis de sofisticação distribuídos conforme a classificação apresentada e estão organizadas conforme a estrutura proposta de objetivos de segurança, descritos no QNRCS.

## 1.2 Definições e Abreviaturas

### 1.2.1 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 |
| **Confidencialidade** | A propriedade da 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 constantes 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 |

| TERMO | DEFINIÇÃO | ORIGEM |
|---|---|---|
| **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 um 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 |
| **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 |
| **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 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 |
| **Processo** | Conjunto de atividades interrelacionadas ou interatuantes que transformam entradas em saídas. | NP EN ISO 22301 |

| TERMO | DEFINIÇÃO | ORIGEM |
|---|---|---|
| **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 |
| **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 |
| **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 |
| **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 |
| **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 |
| **Vulnerabilidade** | Fraqueza de um ativo ou de um controlo que pode ser explorada por uma ameaça. | ISO/IEC 27032 |

*Tabela 1 – Definições*

### 1.2.2 Abreviaturas

| ABREVIATURA | DEFINIÇÃO |
|---|---|
| **CSIRT** | *Computer Security Incident Response Team* – Equipa de Resposta a Incidentes de Segurança Informática. |
| **ENSC** | Estratégia Nacional de Segurança do Ciberespaço 2019-2023. |
| **IDS** | *Intrusion Detection System* – Sistema de deteção de intrusões. |
| **IP** | *Internet Protocol* – Protocolo de comunicações. |
| **IPS** | *Intrusion Prevention System* – Sistema de prevenção de intrusões. |
| **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. |
| **QNRCS** | Quadro Nacional de Referência para a Cibersegurança. |
| **RASIC** | *Responsible* – Responsável, *Accountable* – Aprovador, *Supports* – Suporte, *Consulted* – Consultado e *Informed* – Informado. Matriz de atribuição de Responsabilidades. |
| **SOC** | *Security Operations Center* – Centro de Operações de Segurança. |
| **SWOT** | *Strengths* – Forças, *Weaknesses* – Fraquezas, *Opportunities* – Oportunidades e *Threats* – Ameaças. |
| **VPN** | *Virtual Private Network* – Rede privada virtual. |
| **TI** | Tecnologias de Informação. |
| **UPS** | *Uninterruptible Power Source* – Unidade de alimentação ininterrupta. |
| **WAF** | *Web Application Firewall* – Firewall de aplicações web. |

*Tabela 2 – Abreviaturas*

# IDENTIFICAR

## 1.3.1 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os ativos da organização são registados de forma isolada e pouco sistémica;<br>• Existem algumas iniciativas isoladas de identificação dos responsáveis pelos ativos;<br>• Alguns setores da organização já conseguem manter o seu inventário, ainda que isoladamente. | • Ficheiros isolados de registo dos ativos com alguma informação sobre os ativos;<br>• Alguma identificação de responsáveis por ativos. |
| **2 – Intermédio** | • Os ativos são registados sistematicamente com informação completa e pertinente a cada ativo;<br>• Os ativos são identificados individualmente na organização;<br>• A cada ativo corresponde a associação de um único responsável;<br>• Existe uma política formalmente divulgada de inventário dos ativos. | • Ferramentas/aplicações de gestão integrada de ativos;<br>• Políticas de inventário de ativos;<br>• Registos de endereços IP, número de inventário, dados do equipamento, etc.;<br>• Associação de nome e contacto do colaborador responsável pelo ativo;<br>• Classificação dos ativos quanto à sua criticidade. |
| **3 – Avançado** | • O inventário é monitorizado e acompanhado recorrentemente;<br>• A gestão de ativos é integrada com a gestão de alterações;<br>• Ocorrem revisões periódicas no inventário dos ativos para atestar a sua efetividade;<br>• São propostas e avaliadas melhorias no processo de gestão dos inventários. | • Indicadores e registos de acompanhamento dos inventários;<br>• Sistemas de monitorização dos inventários;<br>• Sistema de identificação automatizada de novos ativos ou alterações dos ativos existentes;<br>• Avaliações e auditorias dos sistemas e processos de inventário de ativos. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os sistemas da organização são registados de forma isolada e pouco sistémica;<br>• Existem algumas iniciativas isoladas de identificação dos responsáveis pelos sistemas;<br>• Alguns setores da organização já conseguem manter um inventário de sistemas utilizados, ainda que isoladamente;<br>• Os inventários são registados em controlos pouco sistémicos. | • Ficheiros isolados de registo dos sistemas com alguma informação;<br>• Alguma identificação de responsáveis pelos sistemas utilizados na organização. |
| **2 – Intermédio** | • As aplicações e plataformas são registadas sistematicamente com informação completa e pertinente;<br>• As aplicações e plataformas são identificadas individualmente na organização;<br>• A cada aplicação e plataforma tem-se a associação de um único responsável;<br>• Existe uma política formalmente divulgada de inventário dos ativos. | • Ferramentas/aplicações de gestão integrada de sistemas;<br>• Políticas de inventário de ativos;<br>• Associação de nome e contacto de colaborador responsável pelo sistema;<br>• Classificação dos sistemas quanto à sua criticidade. |
| **3 – Avançado** | • O inventário é monitorizado e acompanhado regularmente;<br>• A gestão de sistemas é integrada com a gestão de alterações;<br>• Ocorrem revisões periódicas no inventário de sistemas para atestar a sua efetividade;<br>• São propostas e avaliadas melhorias no processo de gestão dos inventários. | • Indicadores e registos de acompanhamento dos inventários;<br>• Sistemas de monitorização dos inventários;<br>• Sistema de descoberta automatizada de novos sistemas ou alterações dos ativos existentes;<br>• Avaliações e auditorias dos sistemas e processos de inventário de sistemas. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os ativos de redes de comunicações são identificados;<br>• Existe uma perceção sobre a topologia de rede. | • Registo dos ativos de redes;<br>• Esquema da rede com identificação das zonas. |
| **2 – Intermédio** | • Os ativos de redes de comunicações são identificados e inventariados;<br>• A topologia de rede é registada com identificação de zonas, endereços IP e identificação de ativos críticos;<br>• Identificação do fluxo de comunicação entre os sistemas internos e externos;<br>• Existe uma política e grupo de procedimentos que definem regras de inventários. | • Mapa de endereços IP;<br>• Mapa da topologia da rede;<br>• Mapa de fluxo de comunicações;<br>• Procedimentos que tratem do mapeamento de rede;<br>• Documento que identifique o fluxo seguro de dados. |
| **3 – Avançado** | • O inventário de rede de comunicação é mantido com ferramentas automáticas de descoberta;<br>• São mantidas métricas de acompanhamento dos ativos;<br>• O inventário é revisto periodicamente para garantir a sua atualização e melhoria contínua nos processos. | • Uso de ferramenta/aplicações automatizadas de descoberta de ativos de rede;<br>• Indicadores relacionados com o inventário de rede de comunicação;<br>• Relatórios de avaliação e acompanhamento dos fluxos de dados. |

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

**R.N.** 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os ativos de rede localizados externamente são identificados de maneira *ad hoc*. | • Identificação dos ativos de rede em ambientes externos. |
| **2 – Intermédio** | • Os ativos de rede localizados externamente possuem dados completos de identificação;<br>• Existe um registo georeferencial de onde os equipamentos se encontram;<br>• Existem equipas dedicadas no acompanhamento e manutenção destes ativos;<br>• Existem políticas e procedimentos para a segurança destes ativos e da informação que suportam. | • Registo do ativo contendo endereço IP, inventário, tipologia do ativo, responsável, geolocalização, etc.;<br>• Política de segurança para ativos em ambientes externos. |
| **3 – Avançado** | • Os ativos são monitorizados e geridos remotamente;<br>• É efetuada uma monitorização dos indicadores de performance;<br>• Os ativos são vistoriados periodicamente para fins preventivos. | • Inventário automatizado dos ativos de rede em ambientes externos;<br>• Relatórios de acompanhamento dos indicadores de performance;<br>• Evidências de vistorias (relatórios, pareceres técnicos, registos de manutenções, etc.). |

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

**R.N.** 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os ativos são classificados de forma *ad hoc*;<br>• Só alguns dos responsáveis pelos ativos estão identificados. | • Registos possivelmente incompletos com classificação de ativos. |
| **2 – Intermédio** | • A organização definiu métodos de classificação dos seus ativos por criticidade e valor percebido;<br>• Existe uma política de classificação dos ativos consoante a sua importância percebida para o negócio;<br>• Os responsáveis pelos ativos são orientados a classificá-los adequadamente. | • Política de classificação de ativos;<br>• Formalização dos procedimentos de classificação;<br>• Base de corelacionamento entre ativos e responsáveis;<br>• Base de identificação dos ativos. |
| **3 – Avançado** | • A classificação dos ativos é revista em períodos regulares;<br>• O nível da classificação dos ativos influencia na seleção dos controlos de segurança aplicados;<br>• São feitas avaliações periódicas aos critérios e controlos de classificação dos ativos. | • Registo atualizado da classificação dos ativos;<br>• Mapa de tipos de controlos de segurança por níveis de classificação dos ativos;<br>• Relatório de avaliação dos critérios de classificação. |

## 1.3.2 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os fornecedores de cada subgrupo da organização encontram-se identificados, ainda que de forma isolada. | • Registo formal de fornecedores por subgrupo da organização. |
| **2 – Intermédio** | • O governo, no relacionamento entre a organização e os seus fornecedores, encontra-se estabelecido e tem o suporte documental necessário;<br>• Existem controlos de restrições (ex-.: colaboradores, anti branqueamento, etc.);<br>• São mantidos registos integrados e de tipificação dos fornecedores em cada âmbito da organização;<br>• Os fornecedores são tipificados consoante a sua criticidade para a organização. | • Políticas e procedimentos para a relação com fornecedores;<br>• Sistema de cadastro integrado dos fornecedores. |
| **3 – Avançado** | • Os contratos são revistos em intervalos regulares;<br>• Os fornecedores de serviços críticos para a organização, têm os seus controlos de segurança validados, para atenderem aos requisitos da organização;<br>• A tipificação dos fornecedores é revista e avaliada em intervalos regulares. | • Relatório da análise e avaliação de riscos na cadeia de fornecedores;<br>• Resultados de auditorias à cadeia crítica de fornecedores da organização. |

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

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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A organização tem a sua missão e objetivo definidos e consegue identificar partes interessadas, internas e externas, para o efeito. | • Contrato ou estatuto de formação da organização;<br>• Relação de fornecedores, parceiros e demais interessados. |
| **2 – Intermédio** | • A política de segurança da informação faz referência à missão, objetivos da organização e às suas partes interessadas;<br>• A política de segurança da informação está divulgada e é de conhecimento de todas as partes interessadas;<br>• A gestão da organização realizou uma análise de forças, oportunidades, ameaças e fraquezas (SWOT) da sua atividade. | • Referência à missão e objetivos da organização na política de segurança;<br>• Registos comprovativos da divulgação da política de segurança pelas partes interessadas;<br>• Relatório da análise SWOT da organização. |
| **3 – Avançado** | • As políticas e os relacionamentos com as partes interessadas são revistos em intervalos regulares;<br>• Ocorrem regularmente ações de sensibilização sobre as políticas de segurança;<br>• A relação dos interessados é revista regularmente pela gestão da organização. | • Controlo de ações de sensibilização das partes interessadas quanto às políticas de segurança, missão e objetivo da organização;<br>• Registos de revisão das relações com partes interessadas;<br>• Registo de revisão dos estudos 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A organização tem a sua missão, visão, valores e objetivos estratégicos definidos e consegue identificar partes interessadas, internas e externas, para o efeito. | • Contrato ou estatuto de formação da organização;<br>• Relação de fornecedores, parceiros e demais interessados.<br>• Plano de negócio ou equivalente que indique as estratégias da organização. |
| **2 – Intermédio** | • A política de segurança da informação faz referência à missão, visão, objetivos e valores da organização e às suas partes interessadas;<br>• A política de segurança da informação está divulgada e é de conhecimento de todas as partes interessadas. | • Referência à missão e objetivos da organização na política de segurança da informação;<br>• Registos comprovativos da divulgação da política de segurança de informação pelas partes interessadas. |
| **3 – Avançado** | • As políticas e a relação com as partes interessadas são revistas em intervalos regulares;<br>• Ocorrem regularmente ações de sensibilização sobre as políticas de segurança;<br>• O plano de negócio (ou equivalente) é revisto conforme a estratégia da organização;<br>• A relação com os interessados é revista regularmente pela gestão da organização. | • Controlo de ações de sensibilização das partes interessadas quanto às políticas de segurança, missão e objetivo da organização;<br>• Registos de revisão das relações com as partes interessadas. |

## 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os ativos críticos são identificados de forma *ad hoc*. | • Registo possivelmente incompleto dos ativos críticos. |
| **2 – Intermédio** | • Os ativos que suportam os processos críticos são identificados em sistema de gestão de ativos consolidado;<br>• É utilizada uma ferramenta/aplicação para a gestão integrada dos ativos da organização;<br>• A capacidade produtiva dos ativos de infraestrutura, redes e sistemas é registada e monitorizada de modo a garantir a operação. | • Registo em ferramenta de gestão dos ativos críticos de infraestrutura, redes e sistemas da organização;<br>• Política de classificação de ativos conforme a sua criticidade;<br>• Monitorização e gestão das capacidades produtivas dos ativos críticos. |
| **3 – Avançado** | • Os registos dos ativos são atualizados dinamicamente conforme as alterações realizadas nos ambientes existentes (p. ex. desenvolvimento, qualidade e produção);<br>• São realizadas manutenções preventivas planeadas, nos ativos críticos de infraestrutura e redes;<br>• São realizadas revisões das capacidades de cada ativo para garantir que atendem às necessidades da organização. | • Sistema de descoberta automática de ativos;<br>• Registo de manutenções preventivas aos equipamentos de infraestrutura;<br>• Planeamento da redundância e estratégias de recuperação e restauro de desastres. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existem notas *ad hoc* sobre os requisitos mínimos para prestação de serviços críticos. | • Documentação com os requisitos mínimos de infraestrutura para suportar os serviços críticos;<br>• Fornecedores críticos identificados. |
| **2 – Intermédio** | • Existe um plano de continuidade registado e testado com estratégias de recuperação;<br>• A organização mantém contratos com fornecedores para a manutenção dos serviços críticos;<br>• A organização possui procedimentos de recuperação da infraestrutura bem definidos. | • Documentação do Plano de Continuidade de Negócio (PCN) e registo de testes efetivos realizados;<br>• Registo nos contratos com fornecedores críticos de cláusulas de continuidade;<br>• Registo de procedimentos relativos à recuperação das infraestruturas. |
| **3 – Avançado** | • O plano de continuidade é revisto regularmente;<br>• Agentes externos em cadeia crítica da organização são auditados quanto às suas capacidades no atendimento à resiliência da organização;<br>• A organização mantém um *hot site* de contingência. | • Resultados de simulacros em ambientes de produção;<br>• Registos de ações de sensibilização de colaboradores;<br>• Relatórios de auditorias de fornecedores e parceiros para o efeito;<br>• Capacidade de operação imediata no *hot site*. |

## 1.3.3 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existe uma política de segurança estabelecida e divulgada internamente. | • Documento com a política da informação;<br>• Comunicação interna para disseminação da política de informação. |
| **2 – Intermédio** | • Os colaboradores são informados e participam em ações de sensibilização sobre a existência da política e os seus termos. | • Publicação oficial da política de segurança da informação pela gestão de topo;<br>• Registo de comprovação de leitura da política pelos colaboradores;<br>• Armazenamento da política em local de fácil acesso aos colaboradores. |
| **3 – Avançado** | • A política de segurança é relacionada com outras políticas ligadas à segurança da informação dentro da organização (p. ex. antifraude, anti-branqueamento de capitais, etc.);<br>• A política é mantida num sistema de Gestão Eletrónica de Documentação (GED) e divulgada pela intranet da organização;<br>• A política é revista com regularidade mínima anual. | • Acompanhamento de documentos de segurança;<br>• Conjunto de políticas de segurança para temas específicos;<br>• Sistema eletrónico de registo e armazenamento das políticas. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os colaboradores têm conhecimento informal das leis e regulamentações aplicáveis. | • Não aplicável. |
| **2 – Intermédio** | • Identificação de leis e regulamentações aplicáveis à organização nas políticas de segurança;<br>• Publicação da política relativa à privacidade dos dados. | • Secção na política de segurança que faz referência a leis e regulamentações pertinentes;<br>• Divulgação e consciencialização sobre a política de privacidade. |
| **3 – Avançado** | • Revisão regular de publicações de novos diplomas legais aplicáveis à organização;<br>• Estabelecimento de equipa específica para cumprimento das leis e regulamentações aplicáveis;<br>• Auditorias e comités internos de tratamento dos controlos de privacidade. | • Registo da execução de procedimento e/ou sistema de monitorização/ *clipping* das publicações de leis pertinentes;<br>• Criação de equipa de conformidade interna ou contrato com fornecedor externo para o efeito;<br>• Relatórios de auditorias internas e/ou de parceiros, quanto ao cumprimento das leis pertinentes;<br>• Atas de reuniões do comité de conformidade com temas relativos à segurança da informação e controlos de privacidade. |

## 1.3.4 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As vulnerabilidades são identificadas, mas não existe processo formal de tratamento;<br>• Não existe uma equipa dedicada à gestão de vulnerabilidades. | • Não aplicável. |
| **2 – Intermédio** | • As vulnerabilidades são identificadas e tipificadas nos ativos de informação;<br>• Existe um processo de gestão de vulnerabilidades que monitoriza os ativos, de acordo com as suas vulnerabilidades atuais e novas;<br>• Existe uma equipa dedicada ao acompanhamento de publicações de novas vulnerabilidades. | • Relatórios de pesquisa de vulnerabilidades;<br>• Classificação das vulnerabilidades por "facilidade de exploração" ou qualquer outro critério definido pela organização. |
| **3 – Avançado** | • Existe um processo formal de revisão e análise recorrente das vulnerabilidades identificadas;<br>• As vulnerabilidades são identificadas automaticamente por sistemas de pesquisa de vulnerabilidades dedicados;<br>• As vulnerabilidades, em cada ativo de uma cadeia de acesso, são correlacionadas para reduzir o risco de "escalada". | • Relatórios de avaliação e revisão dos processos de análises de vulnerabilidades;<br>• Sistema automatizado de deteção de vulnerabilidades;<br>• Sistema de novos ativos na infraestrutura. |

**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.

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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • São estabelecidos contactos informais com grupos de interesse. | • Não aplicável. |
| **2 – Intermédio** | • Existem canais de comunicação estabelecidos com grupos de interesse, sobre ameaças e temas de segurança da informação;<br>• São identificados responsáveis pela comunicação das vulnerabilidades com os grupos de interesse. | • Procedimentos de comunicação de vulnerabilidades;<br>• Indicação de responsáveis pela comunicação de vulnerabilidades com os grupos de interesse;<br>• Acesso a grupos e fontes públicas ou privadas de dados e listas de distribuição sobre vulnerabilidades e correções;<br>• Relação de fontes fiáveis de informações sobre vulnerabilidades pertinentes à organização. |
| **3 – Avançado** | • Os canais de comunicação são otimizados de forma a garantir controlos e métricas de acompanhamento;<br>• Todas as comunicações que forem possíveis são sistematizadas em processos automáticos;<br>• As comunicações são revistas periodicamente para avaliar a sua assertividade e efetividade. | • Registos das comunicações feitas e dos resultados obtidos (ex.: vulnerabilidades tratadas, riscos mitigados, etc.);<br>• Sistema de coleta e tratamento de comunicações de vulnerabilidades integrado com os processos de gestão das vulnerabilidades;<br>• Registo de avaliação das comunicações e dos meios utilizados para o efeito. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existe uma lista genérica de ameaças, sem mapeamento ou documentação na metodologia de gestão do risco. | • Documento com lista de ameaças. |
| **2 – Intermédio** | • Existe um mapa de ameaças conhecidas, associado a cada tipo de ativo;<br>• Existe uma indicação de tratamento de cada ameaça mapeada. | • Mapa de ameaças por vulnerabilidade, por ativo;<br>• Estratégias de tratamento dos riscos estabelecidas. |
| **3 – Avançado** | • O processo de gestão de riscos encontra-se estabelecido com critérios definidos e os seus resultados e estratégias de tratamento são revistos em intervalos regulares;<br>• O processo de gestão de riscos é avaliado e testado quanto à sua efetividade;<br>• Existe suporte de um sistema de gestão de riscos que permite uma melhor eficiência e garante a integridade do processo. | • Registos da análise e avaliação de riscos nos ambientes e ativos da organização;<br>• Registo da participação da gestão de topo nas tomadas de decisão sobre o tratamento dos riscos;<br>• Relatórios de avaliação do processo de gestão de riscos;<br>• Apoio sistémico ao processo e aos *workflows* de tratamento dos riscos. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existe uma metodologia de gestão do risco estabelecida. | • Documento com a metodologia de gestão do risco. |
| **2 – Intermédio** | • Os critérios de probabilidade e impacto dos riscos foram formalmente definidos;<br>• As vulnerabilidades e ameaças são categorizadas conforme os critérios de probabilidade e impacto estabelecidos;<br>• Existe uma perceção de relevância dos ativos para a organização, estabelecida numa escala própria;<br>• As avaliações de risco são associadas a funções para o cálculo, de forma a identificar o nível de risco de cada ativo. | • Procedimentos que descrevem as metodologias de análise de riscos;<br>• Catálogo das ameaças e vulnerabilidades identificadas na estrutura da organização;<br>• Categorização dos ativos quanto à sua relevância para a organização. |
| **3 – Avançado** | • Os ativos têm a sua relevância associada ao grau de importância para o negócio ou têm um valor monetário associado;<br>• As avaliações de riscos são suportadas por sistemas específicos para o efeito. | • Relatórios de avaliação quantitativa de riscos;<br>• Sistema de suporte à avaliação de riscos. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os riscos são tratados, mas de forma não sistematizada. | • Não aplicável. |
| **2 – Intermédio** | • A metodologia de riscos estabelece formalmente estratégias para o tratamento dos riscos identificados, de acordo com o apetite ao risco da organização;<br>• Os riscos são priorizados conforme os critérios de tratamento estabelecidos, de acordo com o nível de exposição percebida e a importância do ativo para a organização. | • Formalização em documentação interna de riscos sobre a metodologia de tratamento de riscos;<br>• Critérios formais e aceites pela gestão de topo para definição dos critérios de tratamento dos riscos, conforme a importância dos ativos para a organização. |
| **3 – Avançado** | • Os riscos são categorizados numa escala de importância para a priorização dos tratamentos;<br>• O tratamento dos riscos tem em conta o custo financeiro e operacional entre o dano previsto e o custo financeiro e operacional de implementação dos controlos definidos. | • Revisão periódica das classificações dos riscos e critérios de classificação;<br>• Avaliação operacional e financeira da relação custo-benefício, pela implementação de controlos em ativos, por tipo de risco. |

## 1.3.5 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 Cláusula 6.1.3; 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As estratégias para a gestão de riscos não estão definidas ou não são consistentes em toda a organização. | • Não aplicável. |
| **2 – Intermédio** | • Existem estratégias definidas para a gestão de riscos e as estratégias para a gestão de riscos são consistentes em toda a organização;<br>• A gestão de risco tem claramente definidos responsáveis pela gestão do processo e pelo tratamento dos riscos identificados ( gestão do risco);<br>• A gestão de riscos considera o vínculo dos riscos aos ativos e processos produtivos da organização. | • Política de gestão de riscos;<br>• Exercício de análise e avaliação de riscos transversais à organização;<br>• Nomeação formal através de e-mail ou de descritivo de função do responsável pela coordenação da gestão de riscos;<br>• Identificação de responsáveis pelo tratamento dos riscos nos resultados das análises;<br>• Mapa dos riscos por ativos e processos. |
| **3 – Avançado** | • Existe uma cultura de risco na organização, percebida em diversos níveis;<br>• A gestão de riscos é suportada por um sistema dedicado;<br>• Existe um registo histórico de revisão dos riscos. | • As estratégias de tolerância, apetite e tratamento dos riscos, a estrutura de governo da gestão de riscos e as dinâmicas de identificação, análise, avaliação e medição dos riscos devem ser consistentes em toda a organização e identificadas de forma não ambígua entre os colaboradores;<br>• Software ou plataforma de suporte à gestão de riscos em pleno uso;<br>• Registo de avaliações dos riscos identificados e reavaliações de controlos implementados. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A tolerância ao risco é decidida arbitrariamente e/ou de forma *ad hoc*. | • Não aplicável. |
| **2 – Intermédio** | • As estratégias de tratamento de riscos são relacionadas ao nível de risco aceite pela organização;<br>• Os processos de aprovação dos riscos são definidos e aprovados pela gestão de topo. | • Registo formal na documentação da gestão de riscos:<br>- da tolerância ao risco aceite;<br>- da estratégia de tratamento de riscos conforme o nível do risco percebido;<br>- dos riscos aceites pela gestão de topo. |
| **3 – Avançado** | • Nas revisões das estratégias de riscos, os indicadores de tolerância ao risco são atualizados. | • Evidências de que as estratégias de riscos são revistas, juntamente com seus indicadores de tolerância. |

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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • O tratamento dos riscos é feito de forma *ad hoc* e não sistematizada. | • Não aplicável. |
| **2 – Intermédio** | • É identificada a estratégia de resposta aos riscos associados aos ativos críticos observados. | • Existem registos de riscos indicados, pelo menos para uma das quatro estratégias clássicas (negar, mitigar, transferir ou aceitar). |
| **3 – Avançado** | • Orientações e boas práticas de tratamento de riscos no setor de atuação são consideradas para a seleção da estratégia de tratamento. | • Consideram-se resultados de *benchmarks* de mercado, regulações e orientações do governo ou do mercado para a seleção da estratégia de tratamento do risco. |

## 1.3.6 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**

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A cadeia de logística está identificada. | • Documento com a identificação dos diferentes fornecedores e parceiros da cadeia logística. |
| **2 – Intermédio** | • A organização aplica a gestão de riscos na sua cadeia logística. | • A política de gestão de fornecedores indica a necessidade de tratamento da gestão de riscos nas atividades da organização, dos seus responsáveis e uma periodicidade de análise. |
| **3 – Avançado** | • Os fornecedores e parceiros são categorizados de acordo com o nível de risco atribuído após avaliação;<br>• A organização avalia regularmente os controlos de segurança dos seus fornecedores críticos. | • Existe um mapa de riscos que indica o risco dos fornecedores;<br>• Existem registos de avaliações de riscos dos fornecedores e dos seus impactos. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os fornecedores da organização, que fazem parte da cadeia de logística de cibersegurança são identificados. | • Documento com listagem de fornecedores envolvidos na cadeia de logística de cibersegurança. |
| **2 – Intermédio** | • A política de fornecedores indica controlos específicos para a cadeia logística crítica da organização;<br>• Os fornecedores da organização são classificados quanto à sua criticidade. | • Os fornecedores são categorizados conforme indicado nos critérios da política de gestão de fornecedores;<br>• Os fornecedores críticos e de cibersegurança são categorizados quanto à criticidade que têm para o negócio. |
| **3 – Avançado** | • Existe capacidade de, proativamente, definir controlos de segurança para novos fornecedores;<br>• A organização encarrega-se que o impacto na cadeia logística seja evitado. | • A organização possui critérios de classificação proativa de risco dos seus fornecedores;<br>• Formulário de registo de fornecedores integrado com a avaliação de riscos. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existe um processo formal de contratação de fornecedores. | • Existem contratos formais com os fornecedores relevantes para a cadeia de logística. |
| **2 – Intermédio** | • A organização garante que o tema da segurança da informação é incluído nos contratos da cadeia logística;<br>• A política de fornecedores inclui controlos de segurança na cadeia logística. | • Existem cláusulas sobre confidencialidade e privacidade nos contratos e termos de contratação da organização;<br>• Os parceiros e fornecedores registam a sua tomada de conhecimento e aceitação das políticas de segurança nas relações com a organização. |
| **3 – Avançado** | • A organização avalia os controlos de segurança dos seus fornecedores, em intervalos regulares. | • Indicadores de acompanhamento dos controlos de segurança que dão visibilidade sobre a forma como a cadeia logística atende à gestão de riscos;<br>• Os registos de conhecimento e aceitação das políticas são validados periodicamente. |

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

**R.N.** 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A avaliação dos fornecedores é feita de forma não sistematizada. | • Não aplicável. |
| **2 – Intermédio** | • As políticas internas da organização devem prever a possibilidade de os seus fornecedores serem avaliados no âmbito da segurança da informação;<br>• Devem existir planos de auditoria orientados pela perceção do risco, que incluam os fornecedores no âmbito. | • Referência nas políticas e contratos com fornecedores, sobre a possibilidade de auditorias por parte da organização;<br>• Plano anual de auditoria de segurança da informação com a cadeia de fornecedores no âmbito, listados pelo nível de exposição ao risco. |
| **3 – Avançado** | • Mecanismos de acompanhamento e monitorização dos controlos de riscos na cadeia logística;<br>• Evidências de tratamento dos pontos identificados nas auditorias aos fornecedores. | • Procedimentos e ferramentas de monitorização dos indicadores de segurança na cadeia logística;<br>• Revisões das auditorias realizadas e acompanhamento dos pontos identificados. |

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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Identificar os fornecedores que suportam os processos críticos da organização. | • Registos de fornecedores críticos à organização. |
| **2 – Intermédio** | • Os planos de resposta e recuperação de desastres definidos consideram a cadeia de fornecedores. | • Identificação de dependências a fornecedores externos na cadeia crítica da organização;<br>• Os planos de resposta a incidentes e recuperação de desastres fazem referência aos fornecedores. |
| **3 – Avançado** | • Validação dos planos de resposta e recuperação de desastres da organização, com a participação ativa de fornecedores críticos envolvidos no âmbito. | • Tratamento dos resultados de testes de recuperação e resposta a incidentes com o envolvimento dos fornecedores;<br>• Registos de testes realizados nos procedimentos de resposta e recuperação de desastres, com o envolvimento da cadeia de fornecedores críticos. |

# PROTEGER

## 1.4.1 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A associação de acessos de identidades é feita com base nos acessos atribuídos no passado. | • Registo da associação de acessos atribuídos a identidades. |
| **2 – Intermédio** | • Existem políticas de gestão de identidades e acessos;<br>• As etapas dos ciclos de acessos são bem definidas e transversais às tecnologias e acessos em geral;<br>• Base única de identidades e regras de acessos. | • Políticas destinadas à gestão das identidades e dos acessos nos sistemas e acessos em geral;<br>• Os procedimentos relativos à gestão de acessos são definidos minimamente para as etapas de emissão, gestão, verificação e revogação dos acessos;<br>• Existe um diretório centralizado, pelo qual as identidades e os acessos são geridos. |
| **3 – Avançado** | • Os acessos são estabelecidos e limitados de acordo com perfis funcionais;<br>• Os acessos são revistos em intervalos regulares. | • Os acessos são geridos conforme o perfil funcional para cada tipo de acesso;<br>• Existem controlos que evitam acessos excessivos sem a justificação pelo descritivo funcional;<br>• Todos os acessos são revistos e reavaliados em intervalos regulares. |

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

**R.N.** COBIT 5 DSS01.04, DSS05.05; COBIT 5 DSS04.04; 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existem controlos que restringem os acessos físicos às zonas que se pretende proteger;<br>• Os acessos são registados de forma a ser possível a identificação individual. | • Estão instalados controlos de acessos a áreas físicas, como portas, torniquetes ou qualquer outra barreira semelhante;<br>• Existem registos de entrada e saída dos ambientes físicos. |
| **2 – Intermédio** | • Os acessos físicos são integrados com um sistema transversal de gestão de identidades e acessos. | • Os acessos físicos são associados a um sistema integrado de identidades e acessos, pelo que as permissões são geridas de forma centralizada. |
| **3 – Avançado** | • Os acessos de pessoas externas são monitorizados;<br>• Os acessos físicos são avaliados regularmente. | • Os acessos de pessoas externas são monitorizados e acompanhados por colaboradores;<br>• Pessoas externas são acompanhadas por um colaborador com autorização de acesso a zonas seguras;<br>• Os registos de acessos físicos são revistos regularmente, de acordo com os perfis de acesso;<br>• Existem registos das avaliações regulares dos procedimentos para acessos físicos. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A organização suporta acessos remotos, mas não controla nem monitoriza os acessos. | • Existem soluções de acesso remoto, como por exemplo VPNs, Citrix e *Jumpservers*. |
| **2 – Intermédio** | • Existem políticas internas que tratam de acessos remotos e teletrabalho;<br>• Os acessos remotos são controlados de maneira centralizada e integrada aos sistemas internos;<br>• Os acessos remotos são controlados por soluções tecnológicas que apliquem a segurança específica para o efeito. | • Registo de aceitação da política de acesso remoto através de VPN;<br>• Registo de aceitação da política de teletrabalho pelos colaboradores beneficiados;<br>• Sistema de VPN implementado com uso da criptografia adequada na autenticação e no tráfego. |
| **3 – Avançado** | • Bloqueios proativos contra acessos remotos não autorizados;<br>• Autenticação federada aos demais sistemas da organização;<br>• Autenticação com multi-fatores para acessos remotos;<br>• Monitorização dos acessos remotos;<br>• Revisão regular dos acessos e tráfego. | • Tecnologias de acesso com bloqueio proativo pelas regras de *logon* interativo, tempo de sessão e/ou origem das ligações;<br>• Integração da autenticação externa aos perfis de acessos definidos internamente;<br>• Utilização de duplo fator de autenticação para acessos remotos;<br>• Registo de monitorização específica dos acessos remotos;<br>• Registo de revisões e revalidações dos acessos remotos. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • São atribuídos acessos de forma nominal e não são partilhados entre múltiplos colaboradores ou entidades;<br>• Os acessos são concedidos copiando os acessos anteriores de colaboradores com perfis similares. | • Não aplicável. |
| **2 – Intermédio** | • Os acessos são concedidos conforme o perfil funcional;<br>• Perfis de acessos elevados devem ser atribuídos com critérios de restrição;<br>• A política de gestão de acessos prevê o princípio do menor privilégio;<br>• Acessos com elevado privilégio (p. ex. administração de sistemas) são atribuídos tendo em conta a restrição por sequenciais, quórum ou geoespacial (ver QNRCS). | • Registos de pedidos de acesso por perfil funcional;<br>• Registos de pedidos e aprovações apropriadas para acessos privilegiados. |
| **3 – Avançado** | • A definição de funções e níveis de acessos são revistos regularmente;<br>• Os acessos concedidos com privilégios elevados são revistos regularmente;<br>• Os acessos são monitorizados ao pormenor;<br>• Existem controlos complementares para os acessos elevados, tais como férias obrigatórias e *job rotation*;<br>• Utilizadores com acessos elevados são submetidos a controlos compensatórios. | • Registos da execução da revisão de acessos;<br>• Listagem de acessos removidos, alterados e criados na última revisão;<br>• Registos correspondentes aos acessos disponíveis;<br>• Alertas de segurança sobre acessos privilegiados;<br>• Incidentes de segurança abertos, referentes ao uso indevido de acessos privilegiados. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As redes internas encontram-se segregadas conforme a sua finalidade. | • Existem *routers*, *firewalls* e demais tecnologias de redes de comunicações, que possibilitem a segmentação da rede;<br>• Impossibilidade de aceder a qualquer sistema a partir de qualquer zona. |
| **2 – Intermédio** | • A rede tem a sua topologia documentada e regras de acessos definidas;<br>• As regras de acesso são documentadas;<br>• Qualquer alteração nas regras de conexão é registada. | • Documentação que indique as regras permitidas de conexão entre cada segmento da rede;<br>• Os equipamentos de segurança de redes produzem registos de eventos de operação e de auditoria;<br>• Registos de pedidos de alteração de regras de firewalls ou outros equipamentos para segurança de redes de comunicações. |
| **3 – Avançado** | • São efetuadas revisões das regras de conexão;<br>• Monitorização dos equipamentos das redes de comunicações;<br>• As alterações são efetuadas após resultados de validações específicas;<br>• Testes dos controlos gerais de segurança. | • Os registos de eventos dos equipamentos de redes são monitorizados e acompanhados;<br>• Relatórios de testes de intrusão no âmbito da infraestrutura da rede de comunicação. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os colaboradores têm as suas credenciais e identidades registadas e vinculadas. | • Registo da atribuição de credenciais nominais aos colaboradores. |
| **2 – Intermédio** | • Os procedimentos de validação das identidades são registados em políticas;<br>• A organização conta com o apoio sistémico na gestão dos acessos e, quando necessário, na validação interativa das credenciais;<br>• Existe um processo de gestão de identidades e acessos estabelecido, com base na identificação dos colaboradores. | • Documentos com a política e procedimentos que suportam o processo de gestão de identidades e acessos. |
| **3 – Avançado** | • A gestão de acessos é revista e avaliada com recorrência e os resultados são utilizados para a melhoria do processo;<br>• Os antecedentes são igualmente revistos com uma determinada periodicidade. | • Existem registos de revisão dos procedimentos de concessão de acessos, suportados pela verificação de antecedentes;<br>• Existe uma equipa dedicada a validar e atribuir identidades. |

**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.

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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os mecanismos de autenticação foram definidos de acordo com os sistemas. | • Conjunto de soluções de autenticação com palavras-passe, estabelecido consoante o sistema. |
| **2 – Intermédio** | • Existe um sistema de gestão de identidades e acessos estabelecido e que abrange utilizadores, dispositivos e outros ativos de sistemas;<br>• A autenticação é implementada através de grupos funcionais;<br>• Existe uma política de acessos estabelecida. | • Os acessos são concedidos conforme o registo em sistema de autenticação transversal aos sistemas;<br>• Os acessos são autenticados consoante a identificação e autorização independente de utilizadores e dispositivos. |
| **3 – Avançado** | • As autenticações são realizadas de forma integrada e transversal entre sistemas;<br>• As autenticações são reforçadas para evitar fraudes e/ou falhas em pontos únicos de validação. | • São implementados serviços de autenticação federada entre sistemas diversos;<br>• São observados múltiplos fatores de autenticação em sistemas críticos. |

## 1.4.2 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os colaboradores apresentam alguma consciência sobre os temas de segurança da informação e como a organização os trata;<br>• São realizadas intervenções de consciencialização para o tema de segurança da informação. | • Observação do comportamento dos colaboradores perante a temática da segurança da informação;<br>• Registos de sessões de formação e consciencialização dos colaboradores sobre o tema. |
| **2 – Intermédio** | • As ações de formação e consciencialização são registadas em planos, procedimentos e metas da organização;<br>• As formações são planeadas consoante a audiência. | • Formalização de um plano com calendarização de ações de formação estabelecida;<br>• Registo das ações de formação às partes interessadas. |
| **3 – Avançado** | • Os resultados das ações de formação e consciencialização são medidos;<br>• Ações periódicas de formação. | • Registos de avaliação do conhecimento e da absorção das formações e consciencializações;<br>• Utilização de meios de comunicação distintos para a otimização e ampliação das comunicações de segurança da informação. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os utilizadores com acessos privilegiados são informalmente notificados das responsabilidades acrescidas, relativas aos acessos providenciados. | • Não aplicável. |
| **2 – Intermédio** | • Os utilizadores de acessos privilegiados têm formação específica sobre segurança da informação;<br>• Existem procedimentos de registo da aceitação de condições especiais de acessos para os utilizadores de acessos privilegiados. | • Plano de formação específico para os utilizadores com acessos privilegiados;<br>• Conteúdo programático da formação específica para utilizadores com acessos privilegiados;<br>• Registo das presenças de utilizadores com acessos privilegiados em ações de formação;<br>• Registo do termo de responsabilização sobre a utilização de sistemas com acessos privilegiados. |
| **3 – Avançado** | • São medidos os resultados das ações de formação e consciencialização aos utilizadores com acessos privilegiados;<br>• Garantia da atualidade da aceitação das condições especiais de acessos com privilégios elevados;<br>• Ações periódicas de formação. | • Registos de avaliação do conhecimento e da absorção das formações e consciencializações;<br>• Registo da renovação regular dos termos de responsabilidade sobre os sistemas;<br>• Evidências da recorrência de ações de formação ou consciencialização específicas, com os utilizadores de acessos privilegiados;<br>• Procedimento de ações de consciencialização aquando do encerramento do contrato do colaborador com acessos privilegiados. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Estabelecimento de requisitos mínimos de segurança da informação para a sua cadeia de clientes e fornecedores. | • Registo dos requisitos mínimos de segurança, no âmbitos de relacionamento com fornecedores, parceiros e clientes. |
| **2 – Intermédio** | • Formação e sensibilização sobre os requisitos de segurança que os clientes, parceiros e fornecedores devem seguir. | • Registo de formação para os agentes externos;<br>• Material de divulgação dos requisitos de segurança a serem seguidos (p. ex. folhetos, termos em contratos, etc.). |
| **3 – Avançado** | • Os clientes, parceiros e fornecedores têm como dever cumprir os requisitos de segurança definidos;<br>• As partes interessadas externas são envolvidas no processo de melhoria contínua. | • Registos de termos de compromisso com os requisitos de segurança da organização;<br>• Registos de auditorias aos clientes e fornecedores sobre o cumprimento dos requisitos de segurança estipulados. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A gestão de topo tem as suas funções e responsabilidades definidas de forma informal. | • Não aplicável. |
| **2 – Intermédio** | • Os papéis e responsabilidades da gestão de topo no âmbito da segurança da informação estão estabelecidos. | • Matriz "RACI" da segurança da informação, onde se inclua a gestão de topo;<br>• Registo de papéis e responsabilidades dos membros da gestão de topo no tema da segurança da informação. |
| **3 – Avançado** | • Estão estabelecidos o envolvimento e a consciencialização da gestão de topo em temas de segurança da informação. | • Registo da participação da gestão de topo em ações de consciencialização;<br>• Registo de políticas e documentos de segurança da informação aceites e "endossados" pela gestão de topo. |

## 1.4.3 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Estão estabelecidas regras de proteção da confidencialidade, integridade e disponibilidade dos ficheiros, documentos e dados. | • Políticas de cifras;<br>• Evidências de regras para a salvaguarda de ficheiros, consoante o nível de segurança necessário. |
| **2 – Intermédio** | • Está estabelecida a classificação da informação consoante a sua sensibilidade e relevância. | • Política, procedimentos e documentos complementares relativos à classificação da informação;<br>• Evidência de controlos de proteção da informação ajustados à classificação da mesma. |
| **3 – Avançado** | • Os dados são armazenados consoante os seus níveis de classificação;<br>• Os dados *offline* (p. ex. em cópias de segurança) são geridos consoante a classificação adequada. | • Gestão de controlos e sistemas criptográficos;<br>• Evidência de armazenamentos adequados consoante o local, tipo de informação armazenada e controlos implementados. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existência de perceção de riscos sobre os dados em circulação;<br>• Adoção de controlos genéricos de proteção de dados em circulação. | • Evidências de que existe uma perceção de risco sobre alguns tipos de dados mais críticos ao negócio;<br>• Utilização da criptografia em casos comuns (p. ex. sítios de internet, formulários de páginas de internet, bancos de dados, etc.). |
| **2 – Intermédio** | • As políticas e os procedimentos que tratem da proteção de dados em circulação são registados formalmente;<br>• Adoção de solução criptográfica específica para cada tecnologia/ ambiente. | • Políticas e procedimentos que enderecem a proteção de dados em circulação (p. ex. criptografia, classificação da informação, transferência da informação, etc.);<br>• Utilização estruturada de serviços de criptografia para dados em circulação. |
| **3 – Avançado** | • É adotada a utilização de tecnologias de cifra dedicadas, consoante a classificação da informação;<br>• São adotados os controlos compensatórios para situações adversas. | • Procedimentos para definição da tecnologia de cifra consoante a classificação da informação;<br>• Registo de análise e avaliação de riscos para os casos adversos (p. ex. controlos compensatórios, registo da aceitação do risco, etc.). |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existe o registo informal ou *ad hoc* dos dados que entram e saem por meio de armazenamento físico;<br>• Os dados em suporte amovível são protegidos de forma não sistematizada. | • Utilização de *software* de cifra para componentes amovíveis de forma não padronizada (por exemplo, departamentos diferentes usam ferramentas diferentes). |
| **2 – Intermédio** | • Existe o registo formal dos controlos de dados que entram e saem por meio de armazenamento físico. | • Políticas, normas e procedimentos que enderecem o ciclo de vida da informação, armazenada em ativos físicos amovíveis;<br>• Registos de responsáveis atribuídos em dispositivos amovíveis que possam conter dados;<br>• Adoção de *software* de cifra para componentes amovíveis. |
| **3 – Avançado** | • Existe a garantia de que a destruição dos dispositivos amovíveis não exporá dados sigilosos;<br>• É realizada uma revisão periódica dos procedimentos de descarte de dispositivos de armazenamento amovíveis e destruição definitiva de dados. | • Procedimentos de destruição de dispositivos amovíveis;<br>• Adoção de *software* para destruição definitiva de dados;<br>• Registo de testes de eficácia dos procedimentos de destruição de dispositivos de armazenamento e de destruição definitiva de dados. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A gestão da capacidade é efetuada sem ter em conta métricas bem definidas;<br>• Não existe um processo formal para garantir a disponibilidade das redes e dos sistemas de informação. | • Não aplicável. |
| **2 – Intermédio** | • As capacidades dos sistemas de informação são monitorizadas. | • Procedimentos e documentos de suporte à gestão de capacidades;<br>• Sistemas de monitorização das capacidades primárias (armazenamento, memória e processamento e conectividade). |
| **3 – Avançado** | • A partir de indicadores pré-estabelecidos, existe a capacidade de agir pela previsibilidade;<br>• A disponibilidade dos recursos de redes e sistemas é garantida;<br>• Existe uma gestão pró-ativa da capacidade instalada, com base em modelos de previsão fundamentados na utilização passada e crescimento futuro. | • Alarmística estabelecida para indicadores fora do esperado;<br>• Estabelecer redundâncias dos recursos de redes e sistemas;<br>• Registos das ações de avaliação da gestão de capacidade. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Estão formalizados os procedimentos de salvaguarda da informação contra meios de exfiltração. | • Implementação de procedimentos de salvaguarda e prevenção contra exfiltração (p. ex. definição de protocolos e formas de comunicação, restrição de uso de interfaces de extração de informação, etc.). |
| **2 – Intermédio** | • Os controlos de proteção da informação que mitigue o risco de exfiltração de dados estão implementados;<br>• Adoção de controlos com base em avaliação de risco. | • Classificação de informação em sistemas de mensagens e troca de emails;<br>• Bloqueios preventivos a sistemas não autorizados de partilha de ficheiros. |
| **3 – Avançado** | • Implementação de processos e mecanismos de prevenção contra a perda de informação;<br>• Revisão regular dos controlos contra a exfiltração de informação. | • Implementação de soluções de *Data Loss Protection* (DLP);<br>• Registo de auditorias e avaliação dos controlos implementados. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Verificação manual ou não sistematizada da integridade dos sistemas de informação, *firmware* e dados. | • Não aplicável. |
| **2 – Intermédio** | • As ações que avaliem e atestem a integridade dos sistemas estão estabelecidas;<br>• É avaliada a integridade de bibliotecas desenvolvidas por terceiros, que sejam utilizadas no desenvolvimento ou operação dos sistemas de informação. | • Documentos de suporte a processos/ procedimentos de verificação da integridade;<br>• Resultados dos testes estáticos, dinâmicos e interativos de segurança dos sistemas e infraestrutura. |
| **3 – Avançado** | • É avaliada de forma transversal e regular a integridade dos sistemas e dados e dependências de bibliotecas desenvolvidas por terceiros. | • Utilização de algoritmos de verificação de integridade;<br>• Sistema de ferramentas centralizadas de verificação de integridade;<br>• Relatórios de integridade dos diferentes sistemas. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A segregação de ambientes é efetuada de forma *ad hoc* e não sistematizada. | • Registo de alguns sistemas com ambientes de desenvolvimento segregados dos ambientes de produção. |
| **2 – Intermédio** | • Estão estabelecidas zonas distintas para desenvolvimento e produção;<br>• Estão estabelecidos normativos internos sobre desenvolvimento seguro. | • Documentos de suporte ao desenvolvimento seguro de *software*;<br>• Registo da segregação de todos os diferentes ambientes. |
| **3 – Avançado** | • Os ambientes de produção são protegidos de eventos não planeados;<br>• Estão implementadas soluções tecnológicas para a proteção dos dados de teste;<br>• É garantido o controlo do acompanhamento da evolução do software em ambiente de produção. | • Registos de execução dos processos de gestão de alterações e versões;<br>• Soluções para anonimizar dados de produção para fins de testes;<br>• Controlo de versionamento de *software*. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A integridade do hardware é verificada de forma manual e não sistematizada. | • Não aplicável. |
| **2 – Intermédio** | • A integridade do hardware é gerida. | • Registo de contrato de manutenção dos equipamentos pelo fabricante ou fornecedor certificado. |
| **3 – Avançado** | • A manutenção preventiva e preditiva é realizada. | • Registo de plano de manutenção periódica;<br>• Sistemas de monitorização e alarmística para a integridade do hardware. |

## 1.4.4 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**

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A definição de uma configuração base de redes e sistemas de informação é feita de forma informal e não sistematizada. | • Não aplicável. |
| **2 – Intermédio** | • Existem regras que definem a configuração base de redes e sistemas;<br>• As configurações base para cada tipo de sistema e/ou para cada finalidade estão estabelecidas. | • Criar políticas que definam as configurações base;<br>• Estabelecer procedimentos de configurações dos equipamentos conforme requisitos base;<br>• Registo da especificação de configurações base para as tecnologias utilizadas. |
| **3 – Avançado** | • As configurações base dos sistemas são monitorizadas;<br>• A atualização de segurança dos sistemas é garantida;<br>• As regras de configurações base estão integradas em processos contínuos de entrega. | • Registo de monitorização contra alterações das configurações base dos sistemas;<br>• Sistema de gestão de atualizações de segurança;<br>• Sistema de integração/entrega contínua (CI/CD). |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Está definido um conjunto rudimentar de requisitos de segurança mínimos para os projetos de desenvolvimento. | • Conjunto rudimentar de medidas de segurança a aplicar para projetos de desenvolvimento. |
| **2 – Intermédio** | • Existe a definição exaustiva dos requisitos de segurança a seguir nos projetos de desenvolvimento;<br>• Existem regras internas para o desenvolvimento seguro. | • Registos de análise de riscos de projetos e indicação de requisitos de segurança;<br>• Conjunto de políticas, procedimentos e requisitos de segurança para o desenvolvimento seguro. |
| **3 – Avançado** | • Os controlos dinâmicos de segurança nos ciclos de desenvolvimento estão implementados;<br>• O código fonte é monitorizado e gerido de maneira segura. | • Processos de testes e validações de segurança estabelecidos no ciclo de desenvolvimento;<br>• Uso de ferramentas de integração contínua (CI);<br>• Evidências da gestão de códigos-fonte e controlo de versão. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existe um processo informal para a gestão de alterações. | • Evidências *ad hoc* de alterações passadas. |
| **2 – Intermédio** | • Estão estabelecidas regras internas para a gestão de alterações;<br>• Os processos de avaliação e aprovação prévia de alterações estão definidos. | • Cria, documenta e mantém procedimentos de gestão de alterações;<br>• Estabelecer sistema de controlo de versões;<br>• Evidências de análise e avaliação prévia às alterações. |
| **3 – Avançado** | • Os mecanismos técnicos para acompanhar as alterações estão estabelecidos;<br>• É realizada a revisão periódica dos procedimentos e registos de alterações. | • Adoção de sistema de integração e entrega contínua (CI/CD);<br>• Evidência de avaliação dos registos e procedimentos de alterações, conforme procedimentos e aprovações. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • São realizadas cópias de segurança de sistemas e ficheiros. | • Evidência da cópia de segurança de sistemas e ficheiros importantes. |
| **2 – Intermédio** | • Estão estabelecidas regras internas formais para a realização das cópias de segurança;<br>• A integridade das cópias de segurança é verificada de forma independente em relação ao ambiente protegido. | • Documentos de suporte às cópias de segurança (políticas, procedimentos, registos, padrões, etc.);<br>• Armazenar as cópias de segurança em local fisicamente separado do ambiente protegido;<br>• Realizar testes de restauro das cópias de segurança em ambiente isolado. |
| **3 – Avançado** | • A confidencialidade, integridade e disponibilidade da informação armazenada das cópias de segurança são garantidas;<br>• Os procedimentos realizados para as cópias de segurança são verificados. | • Utilização de sistemas criptográficos de dados, cuja confidencialidade seja necessária;<br>• Estabelecer ciclos de diferentes tipos de restauro e uso das cópias de segurança;<br>• Emprego de soluções automatizadas para a validação da integridade das cópias de segurança;<br>• Evidências de avaliação regular dos sistemas, ficheiros e procedimentos de cópias de segurança. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A proteção de infraestruturas é feita de forma não sistematizada (por exemplo, apenas alguns sistemas são protegidos por UPS). | • Não aplicável. |
| **2 – Intermédio** | • As infraestruturas estão protegidas contra alterações elétricas que causem danos;<br>• As alterações no ambiente e que possam afetar os sistemas são monitorizadas e detetadas. | • Aplicação de sistemas de proteção contra variações na corrente elétrica, que possam danificar os sistemas;<br>• Utilização de sensores de fumo, humidade e temperatura. |
| **3 – Avançado** | • A prevenção contra alterações elétricas que possam causar danos é feita de forma proativa;<br>• Existem mecanismos que garantem a constância no fornecimento de energia;<br>• A eficácia dos controlos para manter a organização funcional é auditada. | • Existência de sistemas de gestão automática do fornecimento de eletricidade;<br>• Utilização de fontes alternativas de eletricidade (ex.: geradores);<br>• Registo de testes do plano de continuidade, considerando controlos físicos. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os dados são destruídos de forma *ad hoc*. | • Não aplicável. |
| **2 – Intermédio** | • A informação sensível é destruída apropriadamente;<br>• Estão documentados procedimentos de destruição de informação sigilosa. | • Destruidor de papel;<br>• Procedimentos e políticas que tratem da higienização de ficheiros;<br>• Sistemas de higienização de ficheiros. |
| **3 – Avançado** | • É realizada a avaliação da eficácia da destruição da informação em meio físico e digital. | • Registo de revisão dos mecanismos utilizados para a higienização de ficheiros, tanto físicos quanto digitais;<br>• Evidência do comprometimento de parceiros e prestadores de serviços com a higienização de ficheiros compartilhados ou de responsabilidade da organização;<br>• Registo das eliminações realizadas. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os processos de proteção são efetuados de forma não sistematizada. | • Não aplicável. |
| **2 – Intermédio** | • Estão estabelecidos procedimentos e controlos de monitorização e melhoria contínua. | • Procedimentos de controlo e monitorização. |
| **3 – Avançado** | • Os procedimentos e controlos são revistos regularmente;<br>• São realizadas auditorias internas recorrentes, aos controlos de segurança. | • Registos de atualizações dos procedimentos e controlos;<br>• Planeamento de auditoria interna;<br>• Registo de auditorias internas, realizadas no âmbito da segurança da informação;<br>• Planos de ação para tratamento de resultados de auditoria. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os processos de proteção são melhorados de forma não sistematizada. | • Não aplicável. |
| **2 – Intermédio** | • A eficácia das tecnologias de proteção é medida e avaliada;<br>• Existe um processo estabelecido de evolução, através de lições aprendidas. | • Registos de melhorias aos processos de proteção;<br>• KPIs das tecnologias de proteção. |
| **3 – Avançado** | • Os processos de tratamento de incidentes são revistos regularmente;<br>• As lições aprendidas são comunicadas às partes relevantes. | • Registo de lições aprendidas com eventos de segurança;<br>• Registo de revisões e/ou auditorias nos processos de tratamento de 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os planos de resposta são atualizados de forma *ad hoc*. | • Não aplicável. |
| **2 – Intermédio** | • Existem processos, formalmente definidos, para as atividades relativas a resposta a incidentes e garantia da resiliência da organização;<br>• Os planos de resposta são medidos e avaliados quando executados. | • Registo formal de processos e políticas para a resposta a incidentes;<br>• Registo formal de processos e políticas para a continuidade de negócio;<br>• Estabelecer sessões de consciencialização ou outras formas de divulgação dos planos de continuidade. |
| **3 – Avançado** | • As estratégias e ações para a resposta a incidentes e para a garantia da continuidade da organização são avaliadas regularmente. | • Registo de revisão dos planos de continuidade de negócio;<br>• Registo de ações para o tratamento 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os planos de resposta são exercitados de forma não sistematizada. | • Registo de exercícios pontuais e isolados. |
| **2 – Intermédio** | • Os planos de continuidade são registados e testados quanto ao âmbito definido. | • Registo de exercícios sistematizado (ex.: restauro de ambientes, "*table top*", etc.). |
| **3 – Avançado** | • O plano de continuidade é testado pela sua eficiência em âmbito realista. | • Registo de simulacros de casos reais em departamentos da organização ou transversais;<br>• Registo de revisão das estratégias de continuidade e garantia da sua atualização. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • O registo dos colaboradores é realizado. | • Dossier dos colaboradores com dados cadastrais identificativos. |
| **2 – Intermédio** | • Estão estabelecidas regras para a seleção, recrutamento e contratação;<br>• Estão estabelecidas regras para a cessação da contratação. | • Procedimentos e políticas de contratação, mobilidade e cessação de funções de colaboradores. |
| **3 – Avançado** | • Existem perfis funcionais com competências em cibersegurança e segurança da informação, para as contratações;<br>• As ações para o tratamento do não cumprimento das normas internas de segurança da informação estão definidas. | • Estabelecimento de perfis funcionais com competências em cibersegurança e segurança da informação;<br>• Ações disciplinares para casos de infração contra a segurança da informação. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A pesquisa de vulnerabilidades é executada em intervalos regulares. | • Plano de avaliação das vulnerabilidades;<br>• Relatório de ferramentas automáticas de pesquisa de vulnerabilidades. |
| **2 – Intermédio** | • As vulnerabilidades são identificadas com equipas de tratamento adequadas;<br>• A análise de vulnerabilidades é regular e sistemática;<br>• As vulnerabilidades são exploradas, para atestar o seu nível de risco real. | • Registo de submissão de vulnerabilidades para serem tratadas por partes interessadas;<br>• Registo de análise de vulnerabilidades, realizado regularmente, e do seu devido tratamento;<br>• Adoção de ferramenta de pesquisa de vulnerabilidades;<br>• Relatório recente (<= 1 ano) de testes de intrusão nos sistemas e infraestrutura. |
| **3 – Avançado** | • É avaliado regularmente o processo de análise de vulnerabilidades;<br>• As partes interessadas, externas, são envolvidas no tratamento das vulnerabilidades;<br>• Estão estabelecidos planos de ação formais para o tratamento das vulnerabilidades. | • Registo da revisão regular do processo de análise de vulnerabilidades e tratamento de dados;<br>• Tratamento das vulnerabilidades com apoio de fornecedores, parceiros e entidades competentes;<br>• Tratar os resultados dos testes de intrusão com planos de ação. |

## 1.4.5 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**

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As atividades de manutenção são realizadas sem seguir um processo formal;<br>• O registo das atividades não é controlado. | • Registos ocasionais de manutenções efetuadas. |
| **2 – Intermédio** | • Os processos de manutenção são realizados formalmente e envolvem as pessoas adequadas;<br>• Os colaboradores têm a formação adequada para realizarem a manutenção dos ativos. | • Políticas e procedimentos de manutenções;<br>• Evidências da consciencialização e formação de colaboradores para realizar as manutenções necessárias;<br>• Registo de autorizações de perfis de acessos para fins de manutenção. |
| **3 – Avançado** | • As manutenções realizadas por pessoas externas são acompanhadas adequadamente;<br>• O fluxo de trabalho de requisições de manutenção e reparação é automatizado;<br>• Estão estabelecidos períodos de manutenção preventiva aos ativos da organização. | • Registo de manutenções preventivas planeadas;<br>• Ferramenta de gestão de pedidos para acompanhar as manutenções;<br>• Implementação de controlo e registo de acesso em áreas seguras. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As manutenções remotas são realizadas sem um processo formal de aprovação. | • Registos ocasionais de manutenções remotas. |
| **2 – Intermédio** | • As manutenções remotas são realizadas conforme aprovação;<br>• Estão estabelecidos meios seguros para a manutenção remota ser realizada. | • Registo dos fluxos de avaliação e aprovação das manutenções remotas, conforme procedimentos definidos;<br>• Infraestrutura de conexão e autenticação forte com agentes externos para as manutenções. |
| **3 – Avançado** | • Os controlos de acompanhamento do fluxo de solicitações e aprovações para as manutenções remotas estão automatizados;<br>• Estão estabelecidas métricas de acompanhamento e garantia das manutenções;<br>• Existe a garantia de que a conexão é encerrada sempre que não for necessária à sua manutenção. | • Uso de sistema de gestão de *workflow* para pedidos e fluxos de aprovação das manutenções;<br>• Contratos, SLAs e demais registos que atestem a garantia das manutenções;<br>• Registos tecnológicos que indiquem a terminação das conexões sempre que não for necessário estarem ativas. |

## 1.4.6 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**

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os registos de auditoria não seguem um processo de gestão formal. | • Existência ocasional de registos de auditoria. |
| **2 – Intermédio** | • Estão estabelecidos critérios formais para a auditoria de sistemas;<br>• Os registos de eventos para auditorias são geridos de maneira sistémica;<br>• Os formatos e taxonomias de registos estão definidos. | • Políticas e normas relativas à coleta e análise de registos de eventos;<br>• Execução de procedimentos documentados sobre a coleta e tratamento dos registos de eventos para a análise;<br>• Utilização de sistema de coleta, tratamento e análise dos registos de eventos. |
| **3 – Avançado** | • A integridade dos registos de eventos para fins de auditorias deve ser garantida;<br>• Os registos de auditorias transversais aos sistemas da organização são geridos centralmente. | • Existência de controlos técnicos de integridade dos registos, tais como validação por função *hash*, sincronização dos relógios e garantia do *timestamping*.<br>• Armazenamento, tratamento e correlação de registos de eventos em sistema centralizado de análise para fins de auditorias. |

**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.

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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Existe uma implementação básica e *ad hoc* de medidas de proteção aos suportes de dados amovíveis. | • *Bitlocker* ativo em discos amovíveis;<br>• Políticas de domínio aplicadas para restrição de acesso a discos amovíveis. |
| **2 – Intermédio** | • Estão estabelecidas regras de uso e boas práticas sobre dispositivos amovíveis;<br>• É feita a promoção de ações de sensibilização dos utilizadores sobre os riscos associados aos dispositivos amovíveis;<br>• Estão estabelecidos mecanismos técnicos para a proteção de dados em dispositivos amovíveis. | • Registar políticas, padrões, normas e boas práticas sobre a utilização de dispositivos amovíveis;<br>• Ações de sensibilização sobre a utilização aceitável de dispositivos amovíveis;<br>• Utilização de soluções criptográficas para dispositivos amovíveis. |
| **3 – Avançado** | • A utilização de dispositivos amovíveis é bloqueada;<br>• É garantida a higienização dos dispositivos amovíveis no momento da sua destruição. | • Emprego de bloqueios físicos ou lógicos para o uso de dispositivos amovíveis de armazenamento;<br>• Restrição a pessoal autorizado;<br>• Procedimentos de descarte seguro de dispositivos amovíveis;<br>• Utilização de sistemas de destruição segura de dados em dispositivos amovíveis. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os sistemas são configurados com os recursos necessários de forma não sistematizada. | • Registos ocasionais e isolados de sistemas configurados apenas com as funcionalidades mínimas necessárias. |
| **2 – Intermédio** | • Os acessos concedidos são os mínimos necessários;<br>• São estabelecidas funcionalidades mínimas para cada necessidade de operação. | • Integração com gestão de identidades e acessos;<br>• Registo formal de políticas e padrões de configurações de recursos mínimos por defeito. |
| **3 – Avançado** | • Os requisitos mínimos são revistos e atualizados periodicamente;<br>• Os acessos são condizentes com as necessidades mínimas para as funções. | • Registo de revisões periódicas aos padrões e procedimentos de configurações de sistemas;<br>• Registo da revisão dos acessos concedidos;<br>• Revisão das definições de perfis funcionais por necessidades de acessos. |

## 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As zonas de rede são segregadas de forma não sistematizada;<br>• A tecnologia de encriptação é aplicada de forma *ad hoc*. | • Registo de sistemas protegidos com SSL/TLS;<br>• Impossibilidade de chegar a qualquer ponto da rede a partir dos postos de trabalho dos colaboradores. |
| **2 – Intermédio** | • As zonas de rede são segmentadas conforme a finalidade;<br>• São utilizadas soluções tecnológicas de filtro de fluxo de dados. | • Diagrama de redes a indicar a segmentação por zonas;<br>• Utilização de IDS/IPS, *firewalls*, *proxies*, *WAFs* e outras soluções tecnológicas para filtro e bloqueio de dados em transmissão. |
| **3 – Avançado** | • São revistas periodicamente as configurações dos sistemas de filtro das conexões;<br>• As alterações na rede obedecem a processos de validação sistematizados. | • Registo de revisões regulares das definições e dos sistemas de segurança definidos (IDS/IPS, *firewalls*, *proxies*, *WAFs*, etc.);<br>• Registo de processos da gestão da alteração. |

## 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A incorporação de resiliência nos sistemas e redes de comunicações é aplicada de forma não sistematizada. | • Redundância ocasional e isolada de sistemas ou equipamentos de rede de comunicações. |
| **2 – Intermédio** | • Os sistemas críticos são resilientes;<br>• Os sistemas são protegidos contra a sobrecarga de acessos. | • Redundância dos sistemas críticos;<br>• Adoção de soluções de balanceamento de carga. |
| **3 – Avançado** | • A resiliência das infraestruturas às situações adversas é gerida;<br>• Existe a garantia de que eventos inesperados não causam negação de serviço das operações. | • Garantir a alta disponibilidade dos sistemas críticos;<br>• Documentos de suporte ao plano de continuidade de negócios. |

# DETETAR

## 1.5.1 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**

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Não aplicável. | • Não aplicável. |
| **2 – Intermédio** | • As alterações nas infraestruturas e fluxos de comunicação são detetadas;<br>• Os colaboradores são capazes de tratar e detetar alterações nos modelos de referência estabelecidos;<br>• Estão estabelecidos modelos de referência para equipamentos e fluxos de dados. | • Utilização de tecnologias de filtro e deteção de requisições anómalas (ex.: *firewall*, *proxy*, IDS/IPS);<br>• Registo de formação/consciencialização dos colaboradores no tema de deteção de anomalias e eventos de segurança;<br>• Registo de padrões e procedimentos padrão para modelos de referências internas. |
| **3 – Avançado** | • É feita, periodicamente, a revisão dos modelos de referência. | • Registos de alterações conforme descrito nos procedimentos internos da gestão de alteração. |

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

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • É realizada uma análise *ad hoc* dos eventos, sem procedimento de tratamento formalizado e implementado. | • Não aplicável. |
| **2 – Intermédio** | • As tentativas de ataques e incidentes de segurança são detetadas;<br>• Está estabelecido o tratamento apropriado de incidentes de segurança;<br>• É realizada a comunicação apropriada de incidentes com as partes interessadas. | • Registo de incidentes de segurança, originados pela deteção e monitorização de eventos;<br>• Registo de incidentes de segurança, de forma suficiente à sua análise e tratamento;<br>• Registo de incidentes a informar as partes interessadas relevantes. |
| **3 – Avançado** | • É realizada a identificação de incidentes de segurança, através da análise dos eventos coletados transversalmente nas infraestruturas;<br>• Está estabelecida a resposta apropriada a incidentes detetados. | • Implementação de um sistema de correlação de eventos;<br>• Registos de incidentes reportados com o devido tratamento. |

## DE.AE-3 - Os eventos devem ser coletados e correlacionados a partir de várias fontes e sensores

**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; NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os eventos são coletados centralmente;<br>• Existe correlação *ad hoc* com fontes não sistematizadas. | • Registo de eventos coletados num sistema central. |
| **2 – Intermédio** | • Os eventos de segurança são geridos e analisados;<br>• São considerados eventos de diversas fontes internas e externas. | • Políticas e procedimento de gestão e correlação de eventos de segurança;<br>• Registo de fontes de conhecimento utilizadas para as análises dos eventos;<br>• Utilização de sistema de correlação de eventos. |
| **3 – Avançado** | • Existe melhoria contínua dos controlos, a partir do tratamento de eventos anteriores;<br>• Estão estabelecidos mecanismos de controlo de um evento de segurança nas suas infraestruturas. | • Utilização de registos e tratamentos anteriores como lições aprendidas;<br>• Existência da *honeypots* geridos nas estruturas da organização. |

## DE.AE-4 - O impacto dos eventos deve ser classificado

**R.N.** CIS CSC 4, 6; COBIT 5 APO12.06, DSS03.01; ISO/IEC 27001:2013 A.16.1.4;

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os eventos de segurança são classificados conforme o seu impacto percebido. | • Registo dos eventos categorizados. |
| **2 – Intermédio** | • Está estabelecido um processo de gestão de eventos;<br>• Os efeitos do impacto de um evento são aferidos. | • Documentos de apoio ao processo de gestão de eventos;<br>• Metodologias de avaliação do impacto de um evento. |
| **3 – Avançado** | • A gestão de incidentes é acionada a partir da gestão de eventos. | • Registos que interliguem eventos detetados a registos na gestão de incidentes. |

## DE.AE-5 - Devem ser definidos os limites de alerta para 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os incidentes são abertos sem limite formal definido para o número de eventos relacionados. | • Registos ocasionais de incidentes de segurança, sem consistência no número de eventos necessários à constituição formal de incidente. |
| **2 – Intermédio** | • Está estabelecido um processo de gestão de eventos;<br>• Está estabelecida a definição de incidentes de segurança no contexto da organização. | • Documentos de apoio ao processo de gestão de eventos;<br>• Registo da taxonomia de incidentes e das suas prioridades no tratamento. |
| **3 – Avançado** | • Os incidentes são analisados e avaliados com base no risco percebido;<br>• O tratamento de incidentes é realizado conforme o seu nível de complexidade e impacto. | • Ferramentas de correlação de eventos;<br>• Limites a serem considerados para a determinação de um incidente, ainda que sendo resultado de eventos isolados;<br>• Critérios de elevação/decréscimo de eventos em uma escala. |

## 1.5.2 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A monitorização é realizada sem um sistema automático de deteção ou com deteção manual. | • Registos ocasionais de deteções manuais. |
| **2 – Intermédio** | • É realizada a monitorização e proteção face a comportamentos anómalos na rede, que possam representar um incidente. | • Implementação de sistemas de monitorização e proteção da rede (ex.: WAF, IDS/IPS, etc.). |
| **3 – Avançado** | • É realizada a associação de eventos de segurança de origens distintas;<br>• Os acessos a ativos conhecidos são restringidos;<br>• A gestão de incidentes é suportada por uma equipa dedicada. | • Implementação de sistema de gestão e correlação e eventos;<br>• Regras de acesso às infraestruturas e sistemas apenas para dispositivos cadastrados e registados;<br>• Existência na organização de uma equipa dedicada à gestão de incidentes. |

## DE.MC-2 - O ambiente físico deve ser monitorizado para se detetar potenciais incidentes de segurança

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os acessos físicos são monitorizados;<br>• A deteção de incidentes de intrusão física é manual;<br>• São produzidos registos de auditoria de acessos físicos. | • Registos ocasionais de deteção de incidentes de segurança física. |
| **2 – Intermédio** | • Estão estabelecidos controlos de monitorização de áreas seguras;<br>• É gerada alarmística para tentativas de acessos não autorizados. | • Suporte da gestão de acessos para segurança física;<br>• Instalação de sistemas de CCTV;<br>• Suporte de sistemas de monitorização para alarmísticas. |
| **3 – Avançado** | • Os acessos físicos são revistos em intervalos regulares. | • Registos de auditorias nos controlos de acesso e monitorização dos ambientes físicos;<br>• Pontos de auditorias e eventos registados são correlacionados na gestão de incidentes. |

## 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A atividade dos colaboradores é monitorizada;<br>• Os incidentes são detetados manualmente. | • Registos ocasionais de incidentes originados na deteção manual, baseados no comportamento digital dos colaboradores. |
| **2 – Intermédio** | • Os eventos de segurança levam em conta as ações dos colaboradores;<br>• Estão estabelecidos padrões fiáveis de monitorização de colaboradores. | • Suporte dos registos de eventos que identificam o responsável;<br>• Formalizar padrões e métricas que sirvam de referencial para a monitorização das atividades dos colaboradores;<br>• Sistema central de armazenamento e gestão de eventos. |
| **3 – Avançado** | • Os eventos dispersos são analisados em contexto;<br>• Existe a capacidade de antecipar incidentes de segurança a partir da análise de tendências. | • Utilização da correlação de eventos para a monitorização e registo de incidentes;<br>• Alertas preditivos. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A deteção da presença de código malicioso na infraestrutura é reativa. | • Implementar ferramentas de antivírus nas estações de trabalho e servidores. |
| **2 – Intermédio** | • Estão estabelecidas regras formais de avaliação de códigos maliciosos;<br>• As verificações periódicas de códigos maliciosos são realizadas periodicamente. | • Apoio de políticas de antivírus;<br>• Sistemas de antivírus configurados para pesquisas periódicas e recorrentes. |
| **3 – Avançado** | • Estão estabelecidos procedimentos de resposta integrada a incidentes;<br>• A eficiência dos sistemas de antivírus é avaliada;<br>• É realizada a análise técnica de ameaças. | • Integração do sistema de antivírus com o sistema central de gestão de eventos de segurança;<br>• Integração do sistema de análise comportamental com o sistema central de gestão de eventos de segurança;<br>• Realizar auditorias aos sistemas de antivírus;<br>• Registo de atividades de análise de código;<br>• Registo de atividades de análise forense;<br>• Registo de atividades para engenharia reversa de 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As aplicações em dispositivos móveis da organização são monitorizadas;<br>• A deteção de aplicações não autorizadas é manual. | • Registo ocasional de incidentes de segurança, com origem na deteção manual de aplicações não autorizadas. |
| **2 – Intermédio** | • Estão definidas as aplicações permitidas nas redes e sistemas;<br>• O comprometimento do colaborador em não utilizar sistemas não autorizados é garantido. | • Estabelecimento de *whitelists* e/ou *blacklists* de aplicações e sistemas;<br>• Termo de responsabilidade dos utilizadores sobre a utilização dos equipamentos. |
| **3 – Avançado** | • A gestão do parque de dispositivos móveis é feita de forma centralizada;<br>• O sistema de gestão de dispositivos móveis está integrado com o sistema de gestão de eventos de segurança;<br>• Existe a capacidade de correlacionar os eventos de segurança com dispositivos móveis;<br>• A gestão de ativos é realizada de forma integrada. | • Gestão dos sistemas de forma a ser capaz de monitorizar aplicações instaladas nos equipamentos;<br>• Instalação de sistema central de gestão de dispositivos móveis;<br>• Registos de incidentes de segurança, com origem na deteção automática de aplicações não autorizadas. |

## DE.MC-6 - As atividades dos prestadores de serviços externos devem ser monitorizadas para deteção de incidentes

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As atividades dos prestadores de serviços externos são monitorizadas;<br>• A deteção de incidentes é manual e não sistematizada. | • Registos ocasionais de incidentes de segurança, com origem em atividades suspeitas, por prestadores de serviços externos, detetadas manualmente. |
| **2 – Intermédio** | • Os pedidos de acesso remoto são identificados e avaliados;<br>• Estão estabelecidas formalmente regras de acesso remoto para prestadores de serviços externos. | • Adoção de sistemas de deteção e prevenção de intrusões;<br>• Suporte de políticas, normas e procedimentos para a interação com prestadores de serviços externos;<br>• Gestão de acessos dos prestadores de serviços externos. |
| **3 – Avançado** | • É realizada a avaliação dos eventos relativos aos acessos externos;<br>• Os acessos e permissões concedidas a prestadores de serviços externos são avaliados regularmente. | • Integração com sistemas de correlação de eventos;<br>• Suporte de atividades de auditoria de segurança na revisão e avaliação dos acessos de prestadores de serviços externos;<br>• Registos de incidentes de segurança, com origem em atividades suspeitas detetadas automaticamente, por prestadores de serviços externos. |

## DE.MC-7 - Deve ser efetuada a monitorização de acessos não autorizados de colaboradores, conexões, dispositivos e software

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os acessos são monitorizados e analisados manualmente. | • Não aplicável. |
| **2 – Intermédio** | • Os pedidos de acesso às infraestruturas e servidores são monitorizados;<br>• Os dados dispersos são recolhidos e centralizados para análise de anomalias. | • Implementação de sistemas de deteção e prevenção de intrusões;<br>• Registos de eventos de acesso aos servidores e sistemas. |
| **3 – Avançado** | • Os eventos de acesso e incidentes relacionados são tratados. | • Sistema de correlação de eventos;<br>• Relatórios de incidentes. |

## DE.MC-8 - Devem ser efetuados rastreamentos de vulnerabilidades

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A pesquisa por vulnerabilidades nos sistemas e redes de comunicação é feita pontualmente. | • Relatórios ocasionais de vulnerabilidades. |
| **2 – Intermédio** | • As vulnerabilidades identificadas nos sistemas e redes de comunicação são analisadas regularmente. | • Estabelecer um plano de análise de vulnerabilidades;<br>• Implementar uma ferramenta de análise de vulnerabilidades;<br>• Registos de suporte à análise e avaliação das vulnerabilidades. |
| **3 – Avançado** | • A análise de vulnerabilidades está integrada com outros processos da organização;<br>• As vulnerabilidades identificadas são geridas. | • Integrar a análise de vulnerabilidades com processos de testes e análises de segurança em sistemas e aplicações;<br>• Registo de planos de ação para o tratamento das vulnerabilidades. |

## 1.5.3 DE.PD Processos de Deteção

### DE.PD-1 - Devem ser definidos os papéis e responsabilidades na deteção de eventos anómalos

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As responsabilidades na deteção de eventos são definidas informalmente. | • Não aplicável. |
| **2 – Intermédio** | • Os responsáveis pelo tratamento de eventos anómalos são identificados;<br>• Os colaboradores são esclarecidos sobre a deteção de eventos anómalos. | • Comunicados, nomeações ou qualquer outro elemento de suporte na identificação do responsável pelo tratamento dos eventos anómalos;<br>• Material de apoio e de registo das sessões de consciencialização. |
| **3 – Avançado** | • Estão estabelecidas as responsabilidades no processo de deteção de eventos anómalos;<br>• Os agentes externos envolvidos estão comprometidos na deteção de eventos anómalos. | • Documentação de suporte ao estabelecimento de responsabilidades (ex.: RACI, definições de perfis funcionais, etc.);<br>• Acordos de prestação de serviços que apresentam termos sobre a responsabilização na deteção de eventos anómalos. |

### DE.PD-2 - As atividades de deteção devem cumprir com todos os requisitos aplicáveis

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As atividades de deteção seguem um processo *ad hoc*. | • Não aplicável. |
| **2 – Intermédio** | • Os incidentes são detetados e identificados a partir dos eventos registados;<br>• Os responsáveis por atividades de deteção são identificados. | • Relatórios ou indicadores de utilização de sistema de correlação de eventos;<br>• Matriz RASIC dos envolvidos nas atividades de deteção. |
| **3 – Avançado** | • Estão estabelecidas ações de validação dos controlos;<br>• A integridade dos dados coletados é garantida por aplicação de controlos. | • Registos de suporte a auditorias internas;<br>• Utilização de soluções de *hashing* na assinatura de registos. |

## DE.PD-3 - Os processos de deteção devem ser testados

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os processos de deteção são medidos de forma *ad hoc*. | • Registos ocasionais de testes aos serviços de deteção. |
| **2 – Intermédio** | • Existe um processo sistemático de analise aos processos de deteção;<br>• Os processos de deteção são medidos regularmente. | • Planos de teste para os processos de deteção;<br>• Resultados da análise aos processos de deteção. |
| **3 – Avançado** | • A integridade e fiabilidade dos processos de deteção é avaliada. | • Resultados de testes de integridade aos processos de deteção;<br>• Resultados e análise da fiabilidade dos processos de deteção;<br>• Aplicação de metodologias de melhoria contínua. |

## DE.PD-4 - Informações sobre deteções de eventos devem ser comunicadas

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os eventos de segurança são reportados internamente e de forma informal. | • Relatórios ou emails ocasionais de deteções de eventos e respetivas comunicações internas. |
| **2 – Intermédio** | • Está estabelecido internamente um canal de comunicação adequado;<br>• Os incidentes detetados são registados adequadamente. | • Documentos de suporte à gestão de incidentes;<br>• Registo de eventos detetados que resultam em incidentes. |
| **3 – Avançado** | • Está definida a gestão centralizada e otimizada da deteção dos incidentes. | • Estabelecer uma plataforma centralizada de resposta a 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os processos de deteção são melhorados de forma não sistematizada. | • Atualizações isoladas dos processos de deteção. |
| **2 – Intermédio** | • Existem mecanismos de medição e avaliação dos processos de deteção. | • Resultados da avaliação dos processos de deteção quanto à eficiência. |
| **3 – Avançado** | • Os resultados da avaliação são usados para informar o processo de melhoria;<br>• Os processos de deteção são melhorados regularmente. | • Registo de tratamento dos planos de ação de melhorias. |

# RESPONDER

## 1.6.1 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**

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • São implementados procedimentos *ad hoc* de resposta a incidentes, de forma reativa. | • Registos de execução de atividades relacionadas com resposta a incidentes. |
| **2 – Intermédio** | • Os processos de reposta a incidentes são sistematizados e incluem as fases de contenção e erradicação, bem como a identificação dos diversos responsáveis e o escalonamento. | • Documentos de suporte ao tratamento de incidentes (ex.: políticas, procedimentos, padrões, etc.). |
| **3 – Avançado** | • É garantida a integridade das evidências analisadas;<br>• A resposta a incidentes é dada conforme o nível de escalonamento. | • Registos de validação de integridade das evidências;<br>• Documentos com os critérios de escalonamento de incidentes. |

## 1.6.2 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Deve existir o conhecimento informal e não estruturado das funções de cada interveniente da organização. | • Conhecimento informal evidenciado (p. ex. por realização de entrevistas aos colaboradores). |
| **2 – Intermédio** | • Os colaboradores têm conhecimento sobre os procedimentos e responsabilidades;<br>• Estão estabelecidos os guiões de resposta a incidentes. | • Documentos de suporte à resposta a incidentes;<br>• Registo das sessões de formação em segurança e respostas a incidentes;<br>• Estabelecer guiões de tratamento e resposta a incidentes. |
| **3 – Avançado** | • Deve existir envolvimento das partes externas relevantes na resposta a incidentes. | • Mapa das partes externas relevantes;<br>• Estabelecimento dos papéis e responsabilidades. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Deve existir o conhecimento informal e não estruturado dos canais de reporte dos incidentes. | • Conhecimento informal evidenciado (p. ex. por realização de entrevistas aos colaboradores). |
| **2 – Intermédio** | • A capacidade de reporte de incidentes deve estar garantida;<br>• Estão estabelecidos critérios de reporte de incidentes. | • Definição dos canais de reporte de incidentes;<br>• Documentos de suporte na orientação de como reportar incidentes;<br>• Registo de divulgação dos critérios de reporte de incidentes. |
| **3 – Avançado** | • Estão estabelecidos critérios para envolver as partes interessadas externas no tratamento dos incidentes;<br>• O reporte de incidentes é realizado de maneira integrada. | • Registo de reporte de incidentes, envolvendo equipas externas;<br>• Plataforma de resposta a incidentes. |

**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.

## RS.CO-3 - As informações devem ser partilhadas de acordo com o plano de resposta

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A identificação das partes interessadas para a comunicação de incidentes é informal e não estruturada. | • Registo das partes interessadas, internas e externas, na comunicação de incidentes. |
| **2 – Intermédio** | • A comunicação de um incidente é do conhecimento de todos os envolvidos. | • Plano de comunicação de incidentes;<br>• Registos de formação e consciencialização sobre a partilha de informação no plano de resposta a incidentes. |
| **3 – Avançado** | • Estão estabelecidos canais seguros de comunicação de incidentes;<br>• As partes externas interessadas no tratamento dos incidentes estão envolvidas na resposta. | • Procedimentos de comunicação de incidentes documentados através de canais seguros;<br>• Registo de comunicação às partes externas 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Não aplicável. | • Não aplicável. |
| **2 – Intermédio** | • Existe coordenação com partes externas interessadas. | • Identificação das partes interessadas externas;<br>• Documentos de apoio ao plano de comunicação de incidentes com partes externas. |
| **3 – Avançado** | • Estão estabelecidos níveis de responsabilização na resposta a incidentes;<br>• A comunicação de incidentes é avaliada. | • Registo da definição de responsabilidades no âmbito da resposta a incidentes;<br>• Análise e avaliação dos registos de comunicação quanto aos critérios estabelecidos. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Mesmo que de forma informal e não estruturada, a informação relacionada com um incidente é partilhada voluntariamente. | • Observação de comunicação informal através de entrevista aos colaboradores. |
| **2 – Intermédio** | • As partes interessadas externas relevantes são identificadas. | • Registo atualizado de parceiros, fornecedores e demais partes externas relevantes. |
| **3 – Avançado** | • Está estabelecido um plano de comunicação coerente com as necessidades da organização. | • Documentos de apoio do plano de comunicação voluntária de incidentes. |

## 1.6.3 RS.AN Análise

### RS.AN-1 - As notificações dos sistemas de deteção devem ser investigadas

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • O registo de notificações de eventos elevados a incidentes existe, mesmo que não estruturado;<br>• Existem orientações sobre a ativação da gestão de incidentes. | • Registos das orientações para a ativação da gestão de incidentes;<br>• Registos de notificações elevadas a incidentes. |
| **2 – Intermédio** | • Estão estabelecidas práticas de acompanhamento aos eventos detetados;<br>• Existe um plano de resposta a incidentes e é cumprido. | • Evidências do tratamento dos eventos identificados como incidentes. |
| **3 – Avançado** | • As notificações dos sistemas são avaliadas transversalmente. | • Implementar uma plataforma de gestão e correlação de eventos. |

### RS.AN-2 - O impacto do incidente deve ser avaliado

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • O impacto dos incidentes é avaliado, de forma informal e não estruturada. | • Observação da avaliação do impacto, por entrevista aos colaboradores. |
| **2 – Intermédio** | • Os incidentes de segurança são categorizados pelo nível de impacto percebido. | • Definição de padrões para categorias de incidentes;<br>• Taxonomia de impacto de incidentes. |
| **3 – Avançado** | • O risco dos incidentes é avaliado;<br>• Estão estabelecidas métricas relativas às respostas e tratamento de incidentes. | • Registos da avaliação de riscos de incidentes;<br>• Documentação de apoio ao processo de gestão e correlação de eventos;<br>• Métricas relativas a tempos de resposta, resolução, níveis de alertas e prioridades 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Não aplicável. | • Não aplicável. |
| **2 – Intermédio** | • Estão definidos procedimentos de identificação, coleta e aquisição de registos e informação;<br>• Estão definidos procedimentos para a captura dos dados no seu formato original, para análise forense. | • Documentos de suporte aos processos de coleta de dados e garantia da cadeia de custódia;<br>• Formação dos colaboradores sobre procedimentos de análise forense. |
| **3 – Avançado** | • É garantida a integridade e cadeia de custódia das evidências recolhidas;<br>• Existem meios específicos para a realização de análises forenses. | • Adoção de *software* de captura de dados para fins forenses;<br>• Sistema de integração da coleta de dados forenses com a gestão e correlação de eventos. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A categorização dos incidentes é definida de formal informal e pouco estruturada. | • Observação da categorização dos incidentes, obtida por entrevista a colaboradores. |
| **2 – Intermédio** | • Está estabelecida uma taxonomia de categorização de incidentes;<br>• A categorização do incidente está presente no momento da resposta. | • Documentação de apoio na taxonomia de categorização de incidentes;<br>• Inclusão da categorização de incidentes nos planos de resposta. |
| **3 – Avançado** | • Estão estabelecidas metodologias de tratamento para cada tipo de incidente detetado. | • Documentos de suporte ao tratamento de incidentes;<br>• Registo das categorizações de 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A submissão de vulnerabilidades é realizada através de processos *ad hoc*. | • Observação de submissão de vulnerabilidades por entrevista a colaboradores. |
| **2 – Intermédio** | • Existem múltiplos mecanismos para que a organização seja informada sobre vulnerabilidades, quer seja de forma interna ou externa;<br>• Estão estabelecidos processos de tratamento às vulnerabilidades sobre as quais a organização é informada. | • Documento de suporte ao processo de gestão de vulnerabilidades;<br>• Formas de se informar sobre vulnerabilidades estabelecidas e divulgadas;<br>• Registo de receção das comunicações das vulnerabilidades;<br>• Critérios de classificação das vulnerabilidades, de forma a direcionar um tratamento adequado. |
| **3 – Avançado** | • As vulnerabilidades registadas são analisadas e avaliadas sistematicamente. | • Documentos de suporte aos procedimentos de análise e avaliação de vulnerabilidades;<br>• Registos do controlo e acompanhamento das análises das vulnerabilidades identificadas. |

## 1.6.4 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A resposta aos incidentes de segurança é realizada de forma não sistematizada. | • Registo de resposta no tratamento de incidentes. |
| **2 – Intermédio** | • Estão estabelecidos processos de resposta aos incidentes. | • Procedimentos de resposta a incidentes de segurança;<br>• Documentos de suporte ao tratamento de incidentes;<br>• Elaboração de recomendações de tratamentos de incidentes. |
| **3 – Avançado** | • As causas para a origem de incidentes são analisadas e avaliadas. | • Registos de investigação e análises forenses sobre as causas dos incidentes;<br>• Indicação de melhorias para a mitigação dos incidentes conhecidos. |

## RS.MI-2 - Os incidentes devem ser mitigados

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • O tratamento dos incidentes é efetuado de forma reativa e não estruturada. | • Ações de contenção imediata de incidentes (p. ex. bloqueio de contas, interrupção de acessos, etc.). |
| **2 – Intermédio** | • Estão estabelecidas práticas para a redução do impacto dos incidentes;<br>• Os procedimentos sobre o tratamento de incidentes são documentados. | • Disponibilização de infraestrutura alternativa;<br>• Separação da rede em zonas protegidas por *firewalls*, etc.;<br>• Documentos de suporte à mitigação dos incidentes (p. ex. procedimentos, padrões, etc.). |
| **3 – Avançado** | • Os incidentes são erradicados;<br>• É feita uma análise do tratamento dos incidentes para efeitos de melhoria contínua. | • Remoção de ameaças nas infraestruturas;<br>• Uso ou melhoria dos sistemas de proteção (p. ex. antivírus);<br>• Repositório de incidentes anteriores com os respetivos planos de ação corretivos. |

## RS.MI-3 - As novas vulnerabilidades identificadas devem ser mitigadas ou documentadas como riscos aceites

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • O tratamento das vulnerabilidades é avaliado de forma não estruturada. | • Observação da avaliação das vulnerabilidades, por entrevista aos colaboradores. |
| **2 – Intermédio** | • Está estabelecido um processo de gestão de vulnerabilidades;<br>• As vulnerabilidades são mitigadas de acordo com critérios definidos. | • Registo de execução do processo de gestão das vulnerabilidades. |
| **3 – Avançado** | • O processo de análise de risco das vulnerabilidades é definido;<br>• A aceitação das vulnerabilidades, onde seja aplicável, é formalizada. | • Resultados das análises de risco;<br>• Registo da aceitação das vulnerabilidades. |

## 1.6.5 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Não aplicável. | • Não aplicável. |
| **2 – Intermédio** | • Não aplicável. | • Não aplicável. |
| **3 – Avançado** | • Os procedimentos de reposta a incidentes são melhorados através da análise de *lições aprendidas*. | • Documentos de suporte ao plano de resposta a incidentes;<br>• Registos de reuniões e demais interações, no contexto da melhoria contínua;<br>• Registo do tratamento de vulnerabilidades resultantes de incidentes ocorridos. |

**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.

### RS.ME-2 - As estratégias de resposta a incidentes devem ser atualizadas

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Não aplicável. | • Não aplicável. |
| **2 – Intermédio** | • Os procedimentos são atualizados periodicamente, mas não se limitando às tecnologias e sistemas utilizados. | • Registo de atualização de procedimentos para a reposta a incidentes, num determinado período de análise. |
| **3 – Avançado** | • Estão estabelecidos processos de melhoria contínua dos planos de resposta a incidentes;<br>• Os planos de resposta a incidentes são avaliados. | • Registo dos testes de validação dos procedimentos de resposta a incidentes. |

# RECUPERAR

## 1.7.1 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**

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • As cópias de segurança são realizadas de forma *ad hoc*. | • Relatórios de execução de cópias de segurança e restauro. |
| **2 – Intermédio** | • Estão estabelecidos regras e procedimentos para a recuperação de incidentes;<br>• Está estabelecido um processo de gestão de cópias de segurança. | • Registo documental de procedimentos, políticas e padrões dedicados ao tema da recuperação de incidentes;<br>• Relatórios de utilização de plataforma de cópias de segurança e restauro. |
| **3 – Avançado** | • São implementadas ações preditivas para dar respostas adequadas;<br>• Existe uma equipa dedicada ao tratamento e monitorização de ameaças, planeamento e resposta a incidentes (ex.: CSIRT). | • Registo de recuperação de incidentes;<br>• Registos de constituição, com descrição de funções dos elementos da equipa de resposta a incidentes. |

## 1.7.2 RC.ME Melhorias

### RC.ME-1 - Os planos de recuperação devem incorporar as lições aprendidas

**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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Não aplicável. | • Não aplicável. |
| **2 – Intermédio** | • Existem e são avaliadas métricas relativas aos planos de recuperação;<br>• As fragilidades nos planos anteriores são identificadas. | • Registos dos indicadores e resultados analíticos de avaliação de resultados de ações, relativas aos planos de recuperação. |
| **3 – Avançado** | • São identificadas as oportunidades de melhoria que possam ser implementadas;<br>• Os planos de recuperação são atualizados com as melhorias encontradas. | • Documentos com atualização dos planos;<br>• Documentos de suporte à execução das análises. |

### 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.

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • Os procedimentos *ad hoc*, de análise da operação da organização, incluem pontos de discussão relativos à recuperação de incidentes. | • Registos de discussão dos procedimentos *ad hoc* de recuperação (p. ex. atas ou notas de reuniões). |
| **2 – Intermédio** | • Estão estabelecidos procedimentos de revisão e atualização da documentação e dos processos pertinentes à recuperação;<br>• As equipas afetas à recuperação de incidentes são geridas. | • Registo de atualização dos procedimentos e atualização dos métodos empregues como estratégias de recuperação;<br>• Registo de formação ou atualização das equipas internas e/ou externas envolvidas. |
| **3 – Avançado** | • Estão estabelecidos procedimentos de revisão periódica das estratégias de recuperação, por parte da gestão de topo. | • Registo de revisão de estratégias de recuperação e estratégias complementares (p. ex. gestão de incidentes, plano de continuidade de negócio, gestão das vulnerabilidades, etc.). |

## 1.7.3 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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A comunicação às partes interessadas sobre eventos de segurança é reativa.<br>• A comunicação é efetuada, mesmo que de forma pouco estruturada e dispersa. | • Registos de comunicações realizadas conforme as ocorrências. |
| **2 – Intermédio** | • Está estabelecido um plano de comunicação sobre eventos de segurança;<br>• As partes interessadas relevantes estão identificadas. | • Documento de suporte ao plano de comunicação;<br>• Registo de partes interessadas conforme o tema a ser comunicado. |
| **3 – Avançado** | • A comunicação é efetuada através de ações de consciencialização e de forma proativa. | • Plano de comunicações periódicas sobre segurança da informação, para as diversas audiências no âmbito;<br>• Registos de comunicações. |

**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

| NÍVEIS | DESCRIÇÃO | EVIDÊNCIAS |
|---|---|---|
| **1 – Básico** | • A comunicação é efetuada de forma reativa e não estruturada. | • Registos das comunicações efetuadas. |
| **2 – Intermédio** | • Está estabelecido um plano de comunicação consoante o seu propósito;<br>• Para cada objetivo a ser comunicado, é efetuada a identificação de audiência adequada e respetivo plano de comunicação. | • Plano de comunicação com o detalhe do objetivo a ser comunicado e identificação de audiência. |
| **3 – Avançado** | • Está estabelecida uma estratégia de comunicação adequada para as equipas executivas e de gestão;<br>• Os processos de aprovação das comunicações estão definidos. | • Registos de comunicações para equipas executivas e de gestão;<br>• Registos dos processos de aprovação das comunicações;<br>• Avaliação da mensagem para cada audiência. |

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