

QUADRO DE AVALIAÇÃO DE CAPACIDADES DE CIBERSEGURANÇA

Centro Nacional de Cibersegurança



QUADRO DE AVALIAÇÃO DE CAPACIDADES DE CIBERSEGURANÇA

Centro Nacional de Cibersegurança

Versão 1.0

Janeiro de 2020

ÍNDICE

1	Níveis de Capacidade	4
1.1	Introdução	4
1.2	Definições e Abreviaturas	5
1.2.1	Definições	5
1.2.2	Abreviaturas	8
1.3	Identificar	9
1.3.1	ID.GA - Gestão de Ativos	10
1.3.2	ID.AO – Ambiente da Organização	15
1.3.3	ID.GV – Governação	20
1.3.4	ID.AR – Avaliação do Risco	22
1.3.5	ID.GR – Estratégia de Gestão do Risco	27
1.3.6	ID.GL – Gestão do Risco da Cadeia Logística	29
1.4	Proteger	34
1.4.1	PR.GA – Gestão de Identidades, Autenticação e Controlo de Acessos	35
1.4.2	PR.FC – Formação e Sensibilização	42
1.4.3	PR.SD – Segurança de Dados	46
1.4.4	PR.PI – Procedimentos e Processos de Proteção da Informação	53
1.4.5	PR.MA – Manutenção	63
1.4.6	PR.TP – Tecnologia de Proteção	65
1.5	Detetar	70
1.5.1	DE.AE – Anomalias e Eventos	71
1.5.2	DE.MC – Monitorização Contínua de Segurança	75
1.5.3	DE.PD – Processos de Detecção	82
1.6	Responder	85
1.6.1	RS.PR – Planeamento da Resposta	86
1.6.2	RS.CO – Comunicações	87
1.6.3	RS.AN – Análise	90
1.6.4	RS.MI – Mitigação	93
1.6.5	RS.ME – Melhorias	95
1.7	Recuperar	96
1.7.1	RC.PR – Plano de Recuperação	97
1.7.2	RC.ME – Melhorias	98
1.7.3	RC.CO – Comunicações	99

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 cumprimento 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 <i>ad-hoc</i> , 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 <i>software</i> , 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 <i>software</i> 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 <i>Internet</i> 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	<i>Computer Security Incident Response Team</i> – Equipa de Resposta a Incidentes de Segurança Informática.
ENSC	Estratégia Nacional de Segurança do Ciberespaço 2019-2023.
IDS	<i>Intrusion Detection System</i> – Sistema de deteção de intrusões.
IP	<i>Internet Protocol</i> – Protocolo de comunicações.
IPS	<i>Intrusion Prevention System</i> – Sistema de prevenção de intrusões.
ISO	<i>International Organization for Standardization</i> – Organização internacional de normalização.
ISO/IEC	<i>International Organization for Standardization/International Electrotechnical Commission</i> – Organização internacional de normalização/ Comissão eletrotécnica internacional.
QNRCS	Quadro Nacional de Referência para a Cibersegurança.
RASIC	<i>Responsible</i> – Responsável, <i>Accountable</i> – Aprovador, <i>Supports</i> – Suporte, <i>Consulted</i> – Consultado e <i>Informed</i> – Informado. Matriz de atribuição de Responsabilidades.
SOC	<i>Security Operations Center</i> – Centro de Operações de Segurança.
SWOT	<i>Strengths</i> – Forças, <i>Weaknesses</i> – Fraquezas, <i>Opportunities</i> – Oportunidades e <i>Threats</i> – Ameaças.
VPN	<i>Virtual Private Network</i> – Rede privada virtual.
TI	Tecnologias de Informação.
UPS	<i>Uninterruptible Power Source</i> – Unidade de alimentação ininterrupta.
WAF	<i>Web Application Firewall</i> – 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	<ul style="list-style-type: none"> Os ativos da organização são registados de forma isolada e pouco sistémica; Existem algumas iniciativas isoladas de identificação dos responsáveis pelos ativos; Alguns setores da organização já conseguem manter o seu inventário, ainda que isoladamente. 	<ul style="list-style-type: none"> Ficheiros isolados de registo dos ativos com alguma informação sobre os ativos; Alguma identificação de responsáveis por ativos.
2 – Intermédio	<ul style="list-style-type: none"> Os ativos são registados sistematicamente com informação completa e pertinente a cada ativo; Os ativos são identificados individualmente na organização; A cada ativo corresponde a associação de um único responsável; Existe uma política formalmente divulgada de inventário dos ativos. 	<ul style="list-style-type: none"> Ferramentas/aplicações de gestão integrada de ativos; Políticas de inventário de ativos; Registos de endereços IP, número de inventário, dados do equipamento, etc.; Associação de nome e contacto do colaborador responsável pelo ativo; Classificação dos ativos quanto à sua criticidade.
3 – Avançado	<ul style="list-style-type: none"> O inventário é monitorizado e acompanhado recorrentemente; A gestão de ativos é integrada com a gestão de alterações; Ocorrem revisões periódicas no inventário dos ativos para atestar a sua efetividade; São propostas e avaliadas melhorias no processo de gestão dos inventários. 	<ul style="list-style-type: none"> Indicadores e registos de acompanhamento dos inventários; Sistemas de monitorização dos inventários; Sistema de identificação automatizada de novos ativos ou alterações dos ativos existentes; 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	<ul style="list-style-type: none"> Os sistemas da organização são registados de forma isolada e pouco sistémica; Existem algumas iniciativas isoladas de identificação dos responsáveis pelos sistemas; Alguns setores da organização já conseguem manter um inventário de sistemas utilizados, ainda que isoladamente; Os inventários são registados em controlos pouco sistémicos. 	<ul style="list-style-type: none"> Ficheiros isolados de registo dos sistemas com alguma informação; Alguma identificação de responsáveis pelos sistemas utilizados na organização.
2 – Intermédio	<ul style="list-style-type: none"> As aplicações e plataformas são registadas sistematicamente com informação completa e pertinente; As aplicações e plataformas são identificadas individualmente na organização; A cada aplicação e plataforma tem-se a associação de um único responsável; Existe uma política formalmente divulgada de inventário dos ativos. 	<ul style="list-style-type: none"> Ferramentas/aplicações de gestão integrada de sistemas; Políticas de inventário de ativos; Associação de nome e contacto de colaborador responsável pelo sistema; Classificação dos sistemas quanto à sua criticidade.
3 – Avançado	<ul style="list-style-type: none"> O inventário é monitorizado e acompanhado regularmente; A gestão de sistemas é integrada com a gestão de alterações; Ocorrem revisões periódicas no inventário de sistemas para atestar a sua efetividade; São propostas e avaliadas melhorias no processo de gestão dos inventários. 	<ul style="list-style-type: none"> Indicadores e registos de acompanhamento dos inventários; Sistemas de monitorização dos inventários; Sistema de descoberta automatizada de novos sistemas ou alterações dos ativos existentes; Avaliações e auditorias dos sistemas e processos de inventário de sistemas.

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os ativos de redes de comunicações são identificados; Existe uma percepção sobre a topologia de rede. 	<ul style="list-style-type: none"> Registo dos ativos de redes; Esquema da rede com identificação das zonas.
2 – Intermédio	<ul style="list-style-type: none"> Os ativos de redes de comunicações são identificados e inventariados; A topologia de rede é registada com identificação de zonas, endereços IP e identificação de ativos críticos; Identificação do fluxo de comunicação entre os sistemas internos e externos; Existe uma política e grupo de procedimentos que definem regras de inventários. 	<ul style="list-style-type: none"> Mapa de endereços IP; Mapa da topologia da rede; Mapa de fluxo de comunicações; Procedimentos que tratam do mapeamento de rede; Documento que identifique o fluxo seguro de dados.
3 – Avançado	<ul style="list-style-type: none"> O inventário de rede de comunicação é mantido com ferramentas automáticas de descoberta; São mantidas métricas de acompanhamento dos ativos; O inventário é revisto periodicamente para garantir a sua atualização e melhoria contínua nos processos. 	<ul style="list-style-type: none"> Uso de ferramenta/aplicações automatizadas de descoberta de ativos de rede; Indicadores relacionados com o inventário de rede de comunicação; 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	<ul style="list-style-type: none"> Os ativos de rede localizados externamente são identificados de maneira <i>ad hoc</i>. 	<ul style="list-style-type: none"> Identificação dos ativos de rede em ambientes externos.
2 – Intermédio	<ul style="list-style-type: none"> Os ativos de rede localizados externamente possuem dados completos de identificação; Existe um registo georeferencial de onde os equipamentos se encontram; Existem equipas dedicadas no acompanhamento e manutenção destes ativos; Existem políticas e procedimentos para a segurança destes ativos e da informação que suportam. 	<ul style="list-style-type: none"> Registo do ativo contendo endereço IP, inventário, tipologia do ativo, responsável, geolocalização, etc.; Política de segurança para ativos em ambientes externos.
3 – Avançado	<ul style="list-style-type: none"> Os ativos são monitorizados e geridos remotamente; É efetuada uma monitorização dos indicadores de performance; Os ativos são vistoriados periodicamente para fins preventivos. 	<ul style="list-style-type: none"> Inventário automatizado dos ativos de rede em ambientes externos; Relatórios de acompanhamento dos indicadores de performance; 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	<ul style="list-style-type: none"> Os ativos são classificados de forma <i>ad hoc</i>; Só alguns dos responsáveis pelos ativos estão identificados. 	<ul style="list-style-type: none"> Registos possivelmente incompletos com classificação de ativos.
2 – Intermédio	<ul style="list-style-type: none"> A organização definiu métodos de classificação dos seus ativos por criticidade e valor percebido; Existe uma política de classificação dos ativos consoante a sua importância percebida para o negócio; Os responsáveis pelos ativos são orientados a classificá-los adequadamente. 	<ul style="list-style-type: none"> Política de classificação de ativos; Formalização dos procedimentos de classificação; Base de corelacionamento entre ativos e responsáveis; Base de identificação dos ativos.
3 – Avançado	<ul style="list-style-type: none"> A classificação dos ativos é revista em períodos regulares; O nível da classificação dos ativos influencia na seleção dos controlos de segurança aplicados; São feitas avaliações periódicas aos critérios e controlos de classificação dos ativos. 	<ul style="list-style-type: none"> Registo atualizado da classificação dos ativos; Mapa de tipos de controlos de segurança por níveis de classificação dos ativos; 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	<ul style="list-style-type: none"> Os fornecedores de cada subgrupo da organização encontram-se identificados, ainda que de forma isolada. 	<ul style="list-style-type: none"> Registo formal de fornecedores por subgrupo da organização.
2 – Intermédio	<ul style="list-style-type: none"> O governo, no relacionamento entre a organização e os seus fornecedores, encontra-se estabelecido e tem o suporte documental necessário; Existem controlos de restrições (ex-: colaboradores, anti branqueamento, etc.); São mantidos registos integrados e de tipificação dos fornecedores em cada âmbito da organização; Os fornecedores são tipificados consoante a sua criticidade para a organização. 	<ul style="list-style-type: none"> Políticas e procedimentos para a relação com fornecedores; Sistema de cadastro integrado dos fornecedores.
3 – Avançado	<ul style="list-style-type: none"> Os contratos são revistos em intervalos regulares; Os fornecedores de serviços críticos para a organização, têm os seus controlos de segurança validados, para atenderem aos requisitos da organização; A tipificação dos fornecedores é revista e avaliada em intervalos regulares. 	<ul style="list-style-type: none"> Relatório da análise e avaliação de riscos na cadeia de fornecedores; 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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A organização tem a sua missão e objetivo definidos e consegue identificar partes interessadas, internas e externas, para o efeito. 	<ul style="list-style-type: none"> Contrato ou estatuto de formação da organização; Relação de fornecedores, parceiros e demais interessados.
2 – Intermédio	<ul style="list-style-type: none"> A política de segurança da informação faz referência à missão, objetivos da organização e às suas partes interessadas; A política de segurança da informação está divulgada e é de conhecimento de todas as partes interessadas; A gestão da organização realizou uma análise de forças, oportunidades, ameaças e fraquezas (SWOT) da sua atividade. 	<ul style="list-style-type: none"> Referência à missão e objetivos da organização na política de segurança; Registos comprovativos da divulgação da política de segurança pelas partes interessadas; Relatório da análise SWOT da organização.
3 – Avançado	<ul style="list-style-type: none"> As políticas e os relacionamentos com as partes interessadas são revistos em intervalos regulares; Ocorrem regularmente ações de sensibilização sobre as políticas de segurança; A relação dos interessados é revista regularmente pela gestão da organização. 	<ul style="list-style-type: none"> Controlo de ações de sensibilização das partes interessadas quanto às políticas de segurança, missão e objetivo da organização; Registos de revisão das relações com partes interessadas; Registo de revisão dos estudos SWOT.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A organização tem a sua missão, visão, valores e objetivos estratégicos definidos e consegue identificar partes interessadas, internas e externas, para o efeito. 	<ul style="list-style-type: none"> Contrato ou estatuto de formação da organização; Relação de fornecedores, parceiros e demais interessados. Plano de negócio ou equivalente que indique as estratégias da organização.
2 – Intermédio	<ul style="list-style-type: none"> A política de segurança da informação faz referência à missão, visão, objetivos e valores da organização e às suas partes interessadas; A política de segurança da informação está divulgada e é de conhecimento de todas as partes interessadas. 	<ul style="list-style-type: none"> Referência à missão e objetivos da organização na política de segurança da informação; Registos comprovativos da divulgação da política de segurança de informação pelas partes interessadas.
3 – Avançado	<ul style="list-style-type: none"> As políticas e a relação com as partes interessadas são revistas em intervalos regulares; Ocorrem regularmente ações de sensibilização sobre as políticas de segurança; O plano de negócio (ou equivalente) é revisto conforme a estratégia da organização; A relação com os interessados é revista regularmente pela gestão da organização. 	<ul style="list-style-type: none"> Controlo de ações de sensibilização das partes interessadas quanto às políticas de segurança, missão e objetivo da organização; Registos de revisão das relações com as partes interessadas.

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

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	<ul style="list-style-type: none"> Os ativos críticos são identificados de forma <i>ad hoc</i>. 	<ul style="list-style-type: none"> Registo possivelmente incompleto dos ativos críticos.
2 – Intermédio	<ul style="list-style-type: none"> Os ativos que suportam os processos críticos são identificados em sistema de gestão de ativos consolidado; É utilizada uma ferramenta/aplicação para a gestão integrada dos ativos da organização; A capacidade produtiva dos ativos de infraestrutura, redes e sistemas é registada e monitorizada de modo a garantir a operação. 	<ul style="list-style-type: none"> Registo em ferramenta de gestão dos ativos críticos de infraestrutura, redes e sistemas da organização; Política de classificação de ativos conforme a sua criticidade; Monitorização e gestão das capacidades produtivas dos ativos críticos.
3 – Avançado	<ul style="list-style-type: none"> Os registos dos ativos são atualizados dinamicamente conforme as alterações realizadas nos ambientes existentes (p. ex. desenvolvimento, qualidade e produção); São realizadas manutenções preventivas planeadas, nos ativos críticos de infraestrutura e redes; São realizadas revisões das capacidades de cada ativo para garantir que atendem às necessidades da organização. 	<ul style="list-style-type: none"> Sistema de descoberta automática de ativos; Registo de manutenções preventivas aos equipamentos de infraestrutura; Planeamento da redundância e estratégias de recuperação e restauro de desastres.

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

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.

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Existem notas <i>ad hoc</i> sobre os requisitos mínimos para prestação de serviços críticos. 	<ul style="list-style-type: none"> Documentação com os requisitos mínimos de infraestrutura para suportar os serviços críticos; Fornecedores críticos identificados.
2 – Intermédio	<ul style="list-style-type: none"> Existe um plano de continuidade registado e testado com estratégias de recuperação; A organização mantém contratos com fornecedores para a manutenção dos serviços críticos; A organização possui procedimentos de recuperação da infraestrutura bem definidos. 	<ul style="list-style-type: none"> Documentação do Plano de Continuidade de Negócio (PCN) e registo de testes efetivos realizados; Registo nos contratos com fornecedores críticos de cláusulas de continuidade; Registo de procedimentos relativos à recuperação das infraestruturas.
3 – Avançado	<ul style="list-style-type: none"> O plano de continuidade é revisto regularmente; Agentes externos em cadeia crítica da organização são auditados quanto às suas capacidades no atendimento à resiliência da organização; A organização mantém um <i>hot site</i> de contingência. 	<ul style="list-style-type: none"> Resultados de simulacros em ambientes de produção; Registos de ações de sensibilização de colaboradores; Relatórios de auditorias de fornecedores e parceiros para o efeito; Capacidade de operação imediata no <i>hot site</i>.

1.3.3 ID.GV

Governança

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

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.

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Existe uma política de segurança estabelecida e divulgada internamente. 	<ul style="list-style-type: none"> Documento com a política da informação; Comunicação interna para disseminação da política de informação.
2 – Intermédio	<ul style="list-style-type: none"> Os colaboradores são informados e participam em ações de sensibilização sobre a existência da política e os seus termos. 	<ul style="list-style-type: none"> Publicação oficial da política de segurança da informação pela gestão de topo; Registo de comprovação de leitura da política pelos colaboradores; Armazenamento da política em local de fácil acesso aos colaboradores.
3 – Avançado	<ul style="list-style-type: none"> 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.); A política é mantida num sistema de Gestão Eletrónica de Documentação (GED) e divulgada pela intranet da organização; A política é revista com regularidade mínima anual. 	<ul style="list-style-type: none"> Acompanhamento de documentos de segurança; Conjunto de políticas de segurança para temas específicos; 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	<ul style="list-style-type: none"> Os colaboradores têm conhecimento informal das leis e regulamentações aplicáveis. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Identificação de leis e regulamentações aplicáveis à organização nas políticas de segurança; Publicação da política relativa à privacidade dos dados. 	<ul style="list-style-type: none"> Secção na política de segurança que faz referência a leis e regulamentações pertinentes; Divulgação e consciencialização sobre a política de privacidade.
3 – Avançado	<ul style="list-style-type: none"> Revisão regular de publicações de novos diplomas legais aplicáveis à organização; Estabelecimento de equipa específica para cumprimento das leis e regulamentações aplicáveis; Auditorias e comités internos de tratamento dos controlos de privacidade. 	<ul style="list-style-type: none"> Registo da execução de procedimento e/ou sistema de monitorização/<i>clipping</i> das publicações de leis pertinentes; Criação de equipa de conformidade interna ou contrato com fornecedor externo para o efeito; Relatórios de auditorias internas e/ou de parceiros, quanto ao cumprimento das leis pertinentes; 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	<ul style="list-style-type: none"> As vulnerabilidades são identificadas, mas não existe processo formal de tratamento; Não existe uma equipa dedicada à gestão de vulnerabilidades. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> As vulnerabilidades são identificadas e tipificadas nos ativos de informação; Existe um processo de gestão de vulnerabilidades que monitoriza os ativos, de acordo com as suas vulnerabilidades atuais e novas; Existe uma equipa dedicada ao acompanhamento de publicações de novas vulnerabilidades. 	<ul style="list-style-type: none"> Relatórios de pesquisa de vulnerabilidades; Classificação das vulnerabilidades por “facilidade de exploração” ou qualquer outro critério definido pela organização.
3 – Avançado	<ul style="list-style-type: none"> Existe um processo formal de revisão e análise recorrente das vulnerabilidades identificadas; As vulnerabilidades são identificadas automaticamente por sistemas de pesquisa de vulnerabilidades dedicados; As vulnerabilidades, em cada ativo de uma cadeia de acesso, são correlacionadas para reduzir o risco de “escalada”. 	<ul style="list-style-type: none"> Relatórios de avaliação e revisão dos processos de análises de vulnerabilidades; Sistema automatizado de deteção de vulnerabilidades; 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	<ul style="list-style-type: none"> São estabelecidos contactos informais com grupos de interesse. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Existem canais de comunicação estabelecidos com grupos de interesse, sobre ameaças e temas de segurança da informação; São identificados responsáveis pela comunicação das vulnerabilidades com os grupos de interesse. 	<ul style="list-style-type: none"> Procedimentos de comunicação de vulnerabilidades; Indicação de responsáveis pela comunicação de vulnerabilidades com os grupos de interesse; Acesso a grupos e fontes públicas ou privadas de dados e listas de distribuição sobre vulnerabilidades e correções; Relação de fontes fiáveis de informações sobre vulnerabilidades pertinentes à organização.
3 – Avançado	<ul style="list-style-type: none"> Os canais de comunicação são otimizados de forma a garantir controlos e métricas de acompanhamento; Todas as comunicações que forem possíveis são sistematizadas em processos automáticos; As comunicações são revistas periodicamente para avaliar a sua assertividade e efetividade. 	<ul style="list-style-type: none"> Registos das comunicações feitas e dos resultados obtidos (ex.: vulnerabilidades tratadas, riscos mitigados, etc.); Sistema de coleta e tratamento de comunicações de vulnerabilidades integrado com os processos de gestão das vulnerabilidades; 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	<ul style="list-style-type: none"> Existe uma lista genérica de ameaças, sem mapeamento ou documentação na metodologia de gestão do risco. 	<ul style="list-style-type: none"> Documento com lista de ameaças.
2 – Intermédio	<ul style="list-style-type: none"> Existe um mapa de ameaças conhecidas, associado a cada tipo de ativo; Existe uma indicação de tratamento de cada ameaça mapeada. 	<ul style="list-style-type: none"> Mapa de ameaças por vulnerabilidade, por ativo; Estratégias de tratamento dos riscos estabelecidas.
3 – Avançado	<ul style="list-style-type: none"> 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; O processo de gestão de riscos é avaliado e testado quanto à sua efetividade; Existe suporte de um sistema de gestão de riscos que permite uma melhor eficiência e garante a integridade do processo. 	<ul style="list-style-type: none"> Registos da análise e avaliação de riscos nos ambientes e ativos da organização; Registo da participação da gestão de topo nas tomadas de decisão sobre o tratamento dos riscos; Relatórios de avaliação do processo de gestão de riscos; Apoio sistémico ao processo e aos <i>workflows</i> 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	<ul style="list-style-type: none"> Existe uma metodologia de gestão do risco estabelecida. 	<ul style="list-style-type: none"> Documento com a metodologia de gestão do risco.
2 – Intermédio	<ul style="list-style-type: none"> Os critérios de probabilidade e impacto dos riscos foram formalmente definidos; As vulnerabilidades e ameaças são categorizadas conforme os critérios de probabilidade e impacto estabelecidos; Existe uma perceção de relevância dos ativos para a organização, estabelecida numa escala própria; As avaliações de risco são associadas a funções para o cálculo, de forma a identificar o nível de risco de cada ativo. 	<ul style="list-style-type: none"> Procedimentos que descrevem as metodologias de análise de riscos; Catálogo das ameaças e vulnerabilidades identificadas na estrutura da organização; Categorização dos ativos quanto à sua relevância para a organização.
3 – Avançado	<ul style="list-style-type: none"> Os ativos têm a sua relevância associada ao grau de importância para o negócio ou têm um valor monetário associado; As avaliações de riscos são suportadas por sistemas específicos para o efeito. 	<ul style="list-style-type: none"> Relatórios de avaliação quantitativa de riscos; Sistema de suporte à avaliação de riscos.

R.N. CIS CSC 4;

COBIT 5

APO12.05,

APO13.02;

ISO/IEC

27001:2013 Cláu-

sula 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	<ul style="list-style-type: none"> Os riscos são tratados, mas de forma não sistematizada. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> A metodologia de riscos estabelece formalmente estratégias para o tratamento dos riscos identificados, de acordo com o apetite ao risco da organização; 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. 	<ul style="list-style-type: none"> Formalização em documentação interna de riscos sobre a metodologia de tratamento de riscos; 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	<ul style="list-style-type: none"> Os riscos são categorizados numa escala de importância para a priorização dos tratamentos; 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. 	<ul style="list-style-type: none"> Revisão periódica das classificações dos riscos e critérios de classificação; 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 Cláu-
sula 6.1.3;
ISO/IEC
27001:2013 Cláu-
se 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	<ul style="list-style-type: none"> As estratégias para a gestão de riscos não estão definidas ou não são consistentes em toda a organização. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Existem estratégias definidas para a gestão de riscos e as estratégias para a gestão de riscos são consistentes em toda a organização; A gestão de risco tem claramente definidos responsáveis pela gestão do processo e pelo tratamento dos riscos identificados (gestão do risco); A gestão de riscos considera o vínculo dos riscos aos ativos e processos produtivos da organização. 	<ul style="list-style-type: none"> Política de gestão de riscos; Exercício de análise e avaliação de riscos transversais à organização; Nomeação formal através de e-mail ou de descritivo de função do responsável pela coordenação da gestão de riscos; Identificação de responsáveis pelo tratamento dos riscos nos resultados das análises; Mapa dos riscos por ativos e processos.
3 – Avançado	<ul style="list-style-type: none"> Existe uma cultura de risco na organização, percebida em diversos níveis; A gestão de riscos é suportada por um sistema dedicado; Existe um registo histórico de revisão dos riscos. 	<ul style="list-style-type: none"> 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; Software ou plataforma de suporte à gestão de riscos em pleno uso; Registo de avaliações dos riscos identificados e reavaliações de controlos implementados.

R.N. COBIT 5
APO12.06;
ISO/IEC
27001:2013 Cláu-
sula 6.1.3, Cláusu-
la 8.3;
NIST SP 800-53
Rev. 4 PM-9.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A tolerância ao risco é decidida arbitrariamente e/ou de forma <i>ad hoc</i>. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> As estratégias de tratamento de riscos são relacionadas ao nível de risco aceite pela organização; Os processos de aprovação dos riscos são definidos e aprovados pela gestão de topo. 	<ul style="list-style-type: none"> Registo formal na documentação da gestão de riscos: <ul style="list-style-type: none"> - da tolerância ao risco aceite; - da estratégia de tratamento de riscos conforme o nível do risco percebido; - dos riscos aceites pela gestão de topo.
3 – Avançado	<ul style="list-style-type: none"> Nas revisões das estratégias de riscos, os indicadores de tolerância ao risco são atualizados. 	<ul style="list-style-type: none"> Evidências de que as estratégias de riscos são revistas, juntamente com seus indicadores de tolerância.

R.N. COBIT 5
APO12.02;
ISO/IEC
27001:2013 Cláu-
sula 6.1.3, Cláusu-
la 8.3;
NIST SP 800-53
Rev. 4 SA-14, PM-
8, PM-9, PM-11.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> O tratamento dos riscos é feito de forma <i>ad hoc</i> e não sistematizada. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> É identificada a estratégia de resposta aos riscos associados aos ativos críticos observados. 	<ul style="list-style-type: none"> Existem registos de riscos indicados, pelo menos para uma das quatro estratégias clássicas (negar, mitigar, transferir ou aceitar).
3 – Avançado	<ul style="list-style-type: none"> Orientações e boas práticas de tratamento de riscos no setor de atuação são consideradas para a seleção da estratégia de tratamento. 	<ul style="list-style-type: none"> Consideram-se resultados de <i>benchmarks</i> 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	<ul style="list-style-type: none"> A cadeia de logística está identificada. 	<ul style="list-style-type: none"> Documento com a identificação dos diferentes fornecedores e parceiros da cadeia logística.
2 – Intermédio	<ul style="list-style-type: none"> A organização aplica a gestão de riscos na sua cadeia logística. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Os fornecedores e parceiros são categorizados de acordo com o nível de risco atribuído após avaliação; A organização avalia regularmente os controlos de segurança dos seus fornecedores críticos. 	<ul style="list-style-type: none"> Existe um mapa de riscos que indica o risco dos fornecedores; 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	<ul style="list-style-type: none"> Os fornecedores da organização, que fazem parte da cadeia de logística de cibersegurança são identificados. 	<ul style="list-style-type: none"> Documento com listagem de fornecedores envolvidos na cadeia de logística de cibersegurança.
2 – Intermédio	<ul style="list-style-type: none"> A política de fornecedores indica controlos específicos para a cadeia logística crítica da organização; Os fornecedores da organização são classificados quanto à sua criticidade. 	<ul style="list-style-type: none"> Os fornecedores são categorizados conforme indicado nos critérios da política de gestão de fornecedores; Os fornecedores críticos e de cibersegurança são categorizados quanto à criticidade que têm para o negócio.
3 – Avançado	<ul style="list-style-type: none"> Existe capacidade de, proativamente, definir controlos de segurança para novos fornecedores; A organização encarrega-se que o impacto na cadeia logística seja evitado. 	<ul style="list-style-type: none"> A organização possui critérios de classificação proativa de risco dos seus fornecedores; 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	<ul style="list-style-type: none"> Existe um processo formal de contratação de fornecedores. 	<ul style="list-style-type: none"> Existem contratos formais com os fornecedores relevantes para a cadeia de logística.
2 – Intermédio	<ul style="list-style-type: none"> A organização garante que o tema da segurança da informação é incluído nos contratos da cadeia logística; A política de fornecedores inclui controlos de segurança na cadeia logística. 	<ul style="list-style-type: none"> Existem cláusulas sobre confidencialidade e privacidade nos contratos e termos de contratação da organização; Os parceiros e fornecedores registam a sua tomada de conhecimento e aceitação das políticas de segurança nas relações com a organização.
3 – Avançado	<ul style="list-style-type: none"> A organização avalia os controlos de segurança dos seus fornecedores, em intervalos regulares. 	<ul style="list-style-type: none"> Indicadores de acompanhamento dos controlos de segurança que dão visibilidade sobre a forma como a cadeia logística atende à gestão de riscos; 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	<ul style="list-style-type: none"> A avaliação dos fornecedores é feita de forma não sistematizada. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> As políticas internas da organização devem prever a possibilidade de os seus fornecedores serem avaliados no âmbito da segurança da informação; Devem existir planos de auditoria orientados pela perceção do risco, que incluam os fornecedores no âmbito. 	<ul style="list-style-type: none"> Referência nas políticas e contratos com fornecedores, sobre a possibilidade de auditorias por parte da organização; Plano anual de auditoria de segurança da informação com a cadeia de fornecedores no âmbito, listados pelo nível de exposição ao risco.
3 – Avançado	<ul style="list-style-type: none"> Mecanismos de acompanhamento e monitorização dos controlos de riscos na cadeia logística; Evidências de tratamento dos pontos identificados nas auditorias aos fornecedores. 	<ul style="list-style-type: none"> Procedimentos e ferramentas de monitorização dos indicadores de segurança na cadeia logística; 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	<ul style="list-style-type: none"> Identificar os fornecedores que suportam os processos críticos da organização. 	<ul style="list-style-type: none"> Registos de fornecedores críticos à organização.
2 – Intermédio	<ul style="list-style-type: none"> Os planos de resposta e recuperação de desastres definidos consideram a cadeia de fornecedores. 	<ul style="list-style-type: none"> Identificação de dependências a fornecedores externos na cadeia crítica da organização; Os planos de resposta a incidentes e recuperação de desastres fazem referência aos fornecedores.
3 – Avançado	<ul style="list-style-type: none"> Validação dos planos de resposta e recuperação de desastres da organização, com a participação ativa de fornecedores críticos envolvidos no âmbito. 	<ul style="list-style-type: none"> Tratamento dos resultados de testes de recuperação e resposta a incidentes com o envolvimento dos fornecedores; 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

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.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A associação de acessos de identidades é feita com base nos acessos atribuídos no passado. 	<ul style="list-style-type: none"> Registo da associação de acessos atribuídos a identidades.
2 – Intermédio	<ul style="list-style-type: none"> Existem políticas de gestão de identidades e acessos; As etapas dos ciclos de acessos são bem definidas e transversais às tecnologias e acessos em geral; Base única de identidades e regras de acessos. 	<ul style="list-style-type: none"> Políticas destinadas à gestão das identidades e dos acessos nos sistemas e acessos em geral; Os procedimentos relativos à gestão de acessos são definidos minimamente para as etapas de emissão, gestão, verificação e revogação dos acessos; Existe um diretório centralizado, pelo qual as identidades e os acessos são geridos.
3 – Avançado	<ul style="list-style-type: none"> Os acessos são estabelecidos e limitados de acordo com perfis funcionais; Os acessos são revistos em intervalos regulares. 	<ul style="list-style-type: none"> Os acessos são geridos conforme o perfil funcional para cada tipo de acesso; Existem controlos que evitam acessos excessivos sem a justificação pelo descritivo funcional; Todos os acessos são revistos e reavaliados em intervalos regulares.

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.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Existem controlos que restringem os acessos físicos às zonas que se pretende proteger; Os acessos são registados de forma a ser possível a identificação individual. 	<ul style="list-style-type: none"> Estão instalados controlos de acessos a áreas físicas, como portas, torniquetes ou qualquer outra barreira semelhante; Existem registos de entrada e saída dos ambientes físicos.
2 – Intermédio	<ul style="list-style-type: none"> Os acessos físicos são integrados com um sistema transversal de gestão de identidades e acessos. 	<ul style="list-style-type: none"> Os acessos físicos são associados a um sistema integrado de identidades e acessos, pelo que as permissões são geridas de forma centralizada.
3 – Avançado	<ul style="list-style-type: none"> Os acessos de pessoas externas são monitorizados; Os acessos físicos são avaliados regularmente. 	<ul style="list-style-type: none"> Os acessos de pessoas externas são monitorizados e acompanhados por colaboradores; Pessoas externas são acompanhadas por um colaborador com autorização de acesso a zonas seguras; Os registos de acessos físicos são revistos regularmente, de acordo com os perfis de acesso; Existem registos das avaliações regulares dos procedimentos para acessos físicos.

R.N. CIS CSC 12;
COBIT 5
APO13.01,
DSS01.04,
DSS05.03;

ISO/IEC
27001:2013
A.6.2.1, A.6.2.2,
A.11.2.6, A.13.1.1,
A.13.2.1;
NIST SP 800-53
Rev. 4 AC-1, AC-
17, AC-19, AC-20,
SC-15.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A organização suporta acessos remotos, mas não controla nem monitoriza os acessos. 	<ul style="list-style-type: none"> Existem soluções de acesso remoto, como por exemplo VPNs, Citrix e <i>Jumpservers</i>.
2 – Intermédio	<ul style="list-style-type: none"> Existem políticas internas que tratam de acessos remotos e teletrabalho; Os acessos remotos são controlados de maneira centralizada e integrada aos sistemas internos; Os acessos remotos são controlados por soluções tecnológicas que apliquem a segurança específica para o efeito. 	<ul style="list-style-type: none"> Registo de aceitação da política de acesso remoto através de VPN; Registo de aceitação da política de teletrabalho pelos colaboradores beneficiados; Sistema de VPN implementado com uso da criptografia adequada na autenticação e no tráfego.
3 – Avançado	<ul style="list-style-type: none"> Bloqueios proativos contra acessos remotos não autorizados; Autenticação federada aos demais sistemas da organização; Autenticação com multi-fatores para acessos remotos; Monitorização dos acessos remotos; Revisão regular dos acessos e tráfego. 	<ul style="list-style-type: none"> Tecnologias de acesso com bloqueio proativo pelas regras de <i>logon</i> interativo, tempo de sessão e/ou origem das ligações; Integração da autenticação externa aos perfis de acessos definidos internamente; Utilização de duplo fator de autenticação para acessos remotos; Registo de monitorização específica dos acessos remotos; Registo de revisões e revalidações dos acessos remotos.

R.N. CIS CSC 3, 5, 12, 14, 15, 16, 18; COBIT 5 DSS05.04;

ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5; NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> São atribuídos acessos de forma nominal e não são partilhados entre múltiplos colaboradores ou entidades; Os acessos são concedidos copiando os acessos anteriores de colaboradores com perfis similares. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Os acessos são concedidos conforme o perfil funcional; Perfis de acessos elevados devem ser atribuídos com critérios de restrição; A política de gestão de acessos prevê o princípio do menor privilégio; Acessos com elevado privilégio (p. ex. administração de sistemas) são atribuídos tendo em conta a restrição por sequenciais, quórum ou geoespacial (ver QNRCS). 	<ul style="list-style-type: none"> Registos de pedidos de acesso por perfil funcional; Registos de pedidos e aprovações apropriadas para acessos privilegiados.
3 – Avançado	<ul style="list-style-type: none"> A definição de funções e níveis de acessos são revistos regularmente; Os acessos concedidos com privilégios elevados são revistos regularmente; Os acessos são monitorizados ao pormenor; Existem controlos complementares para os acessos elevados, tais como férias obrigatórias e <i>job rotation</i>; Utilizadores com acessos elevados são submetidos a controlos compensatórios. 	<ul style="list-style-type: none"> Registos da execução da revisão de acessos; Listagem de acessos removidos, alterados e criados na última revisão; Registos correspondentes aos acessos disponíveis; Alertas de segurança sobre acessos privilegiados; Incidentes de segurança abertos, referentes ao uso indevido de acessos privilegiados.

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> As redes internas encontram-se segregadas conforme a sua finalidade. 	<ul style="list-style-type: none"> Existem <i>routers</i>, <i>firewalls</i> e demais tecnologias de redes de comunicações, que possibilitem a segmentação da rede; Impossibilidade de aceder a qualquer sistema a partir de qualquer zona.
2 – Intermédio	<ul style="list-style-type: none"> A rede tem a sua topologia documentada e regras de acessos definidas; As regras de acesso são documentadas; Qualquer alteração nas regras de conexão é registada. 	<ul style="list-style-type: none"> Documentação que indique as regras permitidas de conexão entre cada segmento da rede; Os equipamentos de segurança de redes produzem registos de eventos de operação e de auditoria; Registos de pedidos de alteração de regras de firewalls ou outros equipamentos para segurança de redes de comunicações.
3 – Avançado	<ul style="list-style-type: none"> São efetuadas revisões das regras de conexão; Monitorização dos equipamentos das redes de comunicações; As alterações são efetuadas após resultados de validações específicas; Testes dos controlos gerais de segurança. 	<ul style="list-style-type: none"> Os registos de eventos dos equipamentos de redes são monitorizados e acompanhados; 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 respectivas credenciais

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os colaboradores têm as suas credenciais e identidades registadas e vinculadas. 	<ul style="list-style-type: none"> Registo da atribuição de credenciais nominais aos colaboradores.
2 – Intermédio	<ul style="list-style-type: none"> Os procedimentos de validação das identidades são registados em políticas; A organização conta com o apoio sistémico na gestão dos acessos e, quando necessário, na validação interativa das credenciais; Existe um processo de gestão de identidades e acessos estabelecido, com base na identificação dos colaboradores. 	<ul style="list-style-type: none"> Documentos com a política e procedimentos que suportam o processo de gestão de identidades e acessos.
3 – Avançado	<ul style="list-style-type: none"> A gestão de acessos é revista e avaliada com recorrência e os resultados são utilizados para a melhoria do processo; Os antecedentes são igualmente revistos com uma determinada periodicidade. 	<ul style="list-style-type: none"> Existem registos de revisão dos procedimentos de concessão de acessos, suportados pela verificação de antecedentes; 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	<ul style="list-style-type: none"> Os mecanismos de autenticação foram definidos de acordo com os sistemas. 	<ul style="list-style-type: none"> Conjunto de soluções de autenticação com palavras-passe, estabelecido consoante o sistema.
2 – Intermédio	<ul style="list-style-type: none"> Existe um sistema de gestão de identidades e acessos estabelecido e que abrange utilizadores, dispositivos e outros ativos de sistemas; A autenticação é implementada através de grupos funcionais; Existe uma política de acessos estabelecida. 	<ul style="list-style-type: none"> Os acessos são concedidos conforme o registo em sistema de autenticação transversal aos sistemas; Os acessos são autenticados consoante a identificação e autorização independente de utilizadores e dispositivos.
3 – Avançado	<ul style="list-style-type: none"> As autenticações são realizadas de forma integrada e transversal entre sistemas; As autenticações são reforçadas para evitar fraudes e/ou falhas em pontos únicos de validação. 	<ul style="list-style-type: none"> São implementados serviços de autenticação federada entre sistemas diversos; São observados múltiplos fatores de autenticação em sistemas críticos.

1.4.2 PR.FC Formação e Sensibilização

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

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.

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os colaboradores apresentam alguma consciência sobre os temas de segurança da informação e como a organização os trata; São realizadas intervenções de consciencialização para o tema de segurança da informação. 	<ul style="list-style-type: none"> Observação do comportamento dos colaboradores perante a temática da segurança da informação; Registos de sessões de formação e consciencialização dos colaboradores sobre o tema.
2 – Intermédio	<ul style="list-style-type: none"> As ações de formação e consciencialização são registadas em planos, procedimentos e metas da organização; As formações são planeadas consoante a audiência. 	<ul style="list-style-type: none"> Formalização de um plano com calendarização de ações de formação estabelecida; Registo das ações de formação às partes interessadas.
3 – Avançado	<ul style="list-style-type: none"> Os resultados das ações de formação e consciencialização são medidos; Ações periódicas de formação. 	<ul style="list-style-type: none"> Registos de avaliação do conhecimento e da absorção das formações e consciencializações; 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	<ul style="list-style-type: none"> Os utilizadores com acessos privilegiados são informalmente notificados das responsabilidades acrescidas, relativas aos acessos providenciados. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Os utilizadores de acessos privilegiados têm formação específica sobre segurança da informação; Existem procedimentos de registo da aceitação de condições especiais de acessos para os utilizadores de acessos privilegiados. 	<ul style="list-style-type: none"> Plano de formação específico para os utilizadores com acessos privilegiados; Conteúdo programático da formação específica para utilizadores com acessos privilegiados; Registo das presenças de utilizadores com acessos privilegiados em ações de formação; Registo do termo de responsabilização sobre a utilização de sistemas com acessos privilegiados.
3 – Avançado	<ul style="list-style-type: none"> São medidos os resultados das ações de formação e consciencialização aos utilizadores com acessos privilegiados; Garantia da atualidade da aceitação das condições especiais de acessos com privilégios elevados; Ações periódicas de formação. 	<ul style="list-style-type: none"> Registos de avaliação do conhecimento e da absorção das formações e consciencializações; Registo da renovação regular dos termos de responsabilidade sobre os sistemas; Evidências da recorrência de ações de formação ou consciencialização específicas, com os utilizadores de acessos privilegiados; Procedimento de ações de consciencialização aquando do encerramento do contrato do colaborador com acessos privilegiados.

R.N. CIS CSC 17;

COBIT 5

APO07.03,

APO07.06,

APO10.04,

APO10.05;

ISO/IEC

27001:2013

A.6.1.1, A.7.2.1,

A.7.2.2;

NIST SP 800-53

Rev. 4 PS-7, SA-9,

SA-16.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Estabelecimento de requisitos mínimos de segurança da informação para a sua cadeia de clientes e fornecedores. 	<ul style="list-style-type: none"> Registo dos requisitos mínimos de segurança, no âmbito de relacionamento com fornecedores, parceiros e clientes.
2 – Intermédio	<ul style="list-style-type: none"> Formação e sensibilização sobre os requisitos de segurança que os clientes, parceiros e fornecedores devem seguir. 	<ul style="list-style-type: none"> Registo de formação para os agentes externos; Material de divulgação dos requisitos de segurança a serem seguidos (p. ex. folhetos, termos em contratos, etc.).
3 – Avançado	<ul style="list-style-type: none"> Os clientes, parceiros e fornecedores têm como dever cumprir os requisitos de segurança definidos; As partes interessadas externas são envolvidas no processo de melhoria contínua. 	<ul style="list-style-type: none"> Registos de termos de compromisso com os requisitos de segurança da organização; 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	<ul style="list-style-type: none"> A gestão de topo tem as suas funções e responsabilidades definidas de forma informal. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Os papéis e responsabilidades da gestão de topo no âmbito da segurança da informação estão estabelecidos. 	<ul style="list-style-type: none"> Matriz “RACI” da segurança da informação, onde se inclua a gestão de topo; Registo de papéis e responsabilidades dos membros da gestão de topo no tema da segurança da informação.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidos o envolvimento e a consciencialização da gestão de topo em temas de segurança da informação. 	<ul style="list-style-type: none"> Registo da participação da gestão de topo em ações de consciencialização; 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 5APO1.06, 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	<ul style="list-style-type: none"> Estão estabelecidas regras de proteção da confidencialidade, integridade e disponibilidade dos ficheiros, documentos e dados. 	<ul style="list-style-type: none"> Políticas de cifras; Evidências de regras para a salvaguarda de ficheiros, consoante o nível de segurança necessário.
2 – Intermédio	<ul style="list-style-type: none"> Está estabelecida a classificação da informação consoante a sua sensibilidade e relevância. 	<ul style="list-style-type: none"> Política, procedimentos e documentos complementares relativos à classificação da informação; Evidência de controlos de proteção da informação ajustados à classificação da mesma.
3 – Avançado	<ul style="list-style-type: none"> Os dados são armazenados consoante os seus níveis de classificação; Os dados <i>offline</i> (p. ex. em cópias de segurança) são geridos consoante a classificação adequada. 	<ul style="list-style-type: none"> Gestão de controlos e sistemas criptográficos; Evidência de armazenamentos adequados consoante o local, tipo de informação armazenada e controlos implementados.

R.N. CIS CSC 13, 14;

COBIT 5
APO01.06,
DSS05.02,
DSS06.06;

ISO/IEC
27001:2013
A.8.2.3, A.13.1.1,
A.13.2.1, A.13.2.3,
A.14.1.2, A.14.1.3;
NIST SP 800-53
Rev. 4 SC-8, SC-11,
SC-12.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Existência de percepção de riscos sobre os dados em circulação; Adoção de controlos genéricos de proteção de dados em circulação. 	<ul style="list-style-type: none"> Evidências de que existe uma percepção de risco sobre alguns tipos de dados mais críticos ao negócio; Utilização da criptografia em casos comuns (p. ex. sítios de internet, formulários de páginas de internet, bancos de dados, etc.).
2 – Intermédio	<ul style="list-style-type: none"> As políticas e os procedimentos que tratam da proteção de dados em circulação são registados formalmente; Adoção de solução criptográfica específica para cada tecnologia/ambiente. 	<ul style="list-style-type: none"> Políticas e procedimentos que enderecem a proteção de dados em circulação (p. ex. criptografia, classificação da informação, transferência da informação, etc.); Utilização estruturada de serviços de criptografia para dados em circulação.
3 – Avançado	<ul style="list-style-type: none"> É adotada a utilização de tecnologias de cifra dedicadas, consoante a classificação da informação; São adotados os controlos compensatórios para situações adversas. 	<ul style="list-style-type: none"> Procedimentos para definição da tecnologia de cifra consoante a classificação da informação; 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	<ul style="list-style-type: none"> Existe o registo informal ou <i>ad hoc</i> dos dados que entram e saem por meio de armazenamento físico; Os dados em suporte amovível são protegidos de forma não sistematizada. 	<ul style="list-style-type: none"> Utilização de <i>software</i> de cifra para componentes amovíveis de forma não padronizada (por exemplo, departamentos diferentes usam ferramentas diferentes).
2 – Intermédio	<ul style="list-style-type: none"> Existe o registo formal dos controlos de dados que entram e saem por meio de armazenamento físico. 	<ul style="list-style-type: none"> Políticas, normas e procedimentos que enderecem o ciclo de vida da informação, armazenada em ativos físicos amovíveis; Registos de responsáveis atribuídos em dispositivos amovíveis que possam conter dados; Adoção de <i>software</i> de cifra para componentes amovíveis.
3 – Avançado	<ul style="list-style-type: none"> Existe a garantia de que a destruição dos dispositivos amovíveis não exporá dados sigilosos; É realizada uma revisão periódica dos procedimentos de descarte de dispositivos de armazenamento amovíveis e destruição definitiva de dados. 	<ul style="list-style-type: none"> Procedimentos de destruição de dispositivos amovíveis; Adoção de <i>software</i> para destruição definitiva de dados; 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	<ul style="list-style-type: none"> A gestão da capacidade é efetuada sem ter em conta métricas bem definidas; Não existe um processo formal para garantir a disponibilidade das redes e dos sistemas de informação. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> As capacidades dos sistemas de informação são monitorizadas. 	<ul style="list-style-type: none"> Procedimentos e documentos de suporte à gestão de capacidades; Sistemas de monitorização das capacidades primárias (armazenamento, memória e processamento e conectividade).
3 – Avançado	<ul style="list-style-type: none"> A partir de indicadores pré-estabelecidos, existe a capacidade de agir pela previsibilidade; A disponibilidade dos recursos de redes e sistemas é garantida; Existe uma gestão pró-ativa da capacidade instalada, com base em modelos de previsão fundamentados na utilização passada e crescimento futuro. 	<ul style="list-style-type: none"> Alarmística estabelecida para indicadores fora do esperado; Estabelecer redundâncias dos recursos de redes e sistemas; Registos das ações de avaliação da gestão de capacidade.

R.N. CIS CSC 13,
COBIT 5
APO01.06,
DSS05.04,
DSS05.07,
DSS06.02;

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Estão formalizados os procedimentos de salvaguarda da informação contra meios de exfiltração. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Os controlos de proteção da informação que mitigue o risco de exfiltração de dados estão implementados; Adoção de controlos com base em avaliação de risco. 	<ul style="list-style-type: none"> Classificação de informação em sistemas de mensagens e troca de emails; Bloqueios preventivos a sistemas não autorizados de partilha de ficheiros.
3 – Avançado	<ul style="list-style-type: none"> Implementação de processos e mecanismos de prevenção contra a perda de informação; Revisão regular dos controlos contra a exfiltração de informação. 	<ul style="list-style-type: none"> Implementação de soluções de <i>Data Loss Protection</i> (DLP); 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	<ul style="list-style-type: none"> Verificação manual ou não sistematizada da integridade dos sistemas de informação, <i>firmware</i> e dados. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> As ações que avaliem e atestem a integridade dos sistemas estão estabelecidas; É avaliada a integridade de bibliotecas desenvolvidas por terceiros, que sejam utilizadas no desenvolvimento ou operação dos sistemas de informação. 	<ul style="list-style-type: none"> Documentos de suporte a processos/procedimentos de verificação da integridade; Resultados dos testes estáticos, dinâmicos e interativos de segurança dos sistemas e infraestrutura.
3 – Avançado	<ul style="list-style-type: none"> É avaliada de forma transversal e regular a integridade dos sistemas e dados e dependências de bibliotecas desenvolvidas por terceiros. 	<ul style="list-style-type: none"> Utilização de algoritmos de verificação de integridade; Sistema de ferramentas centralizadas de verificação de integridade; 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	<ul style="list-style-type: none"> A segregação de ambientes é efetuada de forma <i>ad hoc</i> e não sistematizada. 	<ul style="list-style-type: none"> Registo de alguns sistemas com ambientes de desenvolvimento segregados dos ambientes de produção.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidas zonas distintas para desenvolvimento e produção; Estão estabelecidos normativos internos sobre desenvolvimento seguro. 	<ul style="list-style-type: none"> Documentos de suporte ao desenvolvimento seguro de <i>software</i>; Registo da segregação de todos os diferentes ambientes.
3 – Avançado	<ul style="list-style-type: none"> Os ambientes de produção são protegidos de eventos não planeados; Estão implementadas soluções tecnológicas para a proteção dos dados de teste; É garantido o controlo do acompanhamento da evolução do software em ambiente de produção. 	<ul style="list-style-type: none"> Registos de execução dos processos de gestão de alterações e versões; Soluções para anonimizar dados de produção para fins de testes; Controlo de versionamento de <i>software</i>.

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	<ul style="list-style-type: none"> A integridade do hardware é verificada de forma manual e não sistematizada. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> A integridade do hardware é gerida. 	<ul style="list-style-type: none"> Registo de contrato de manutenção dos equipamentos pelo fabricante ou fornecedor certificado.
3 – Avançado	<ul style="list-style-type: none"> A manutenção preventiva e preditiva é realizada. 	<ul style="list-style-type: none"> Registo de plano de manutenção periódica; Sistemas de monitorização e alarmística para a integridade do hardware.

1.4.4 PR.PI

Procedimentos e Processos de Proteção da Informação

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A definição de uma configuração base de redes e sistemas de informação é feita de forma informal e não sistematizada. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Existem regras que definem a configuração base de redes e sistemas; As configurações base para cada tipo de sistema e/ou para cada finalidade estão estabelecidas. 	<ul style="list-style-type: none"> Criar políticas que definam as configurações base; Estabelecer procedimentos de configurações dos equipamentos conforme requisitos base; Registo da especificação de configurações base para as tecnologias utilizadas.
3 – Avançado	<ul style="list-style-type: none"> As configurações base dos sistemas são monitorizadas; A atualização de segurança dos sistemas é garantida; As regras de configurações base estão integradas em processos contínuos de entrega. 	<ul style="list-style-type: none"> Registo de monitorização contra alterações das configurações base dos sistemas; Sistema de gestão de atualizações de segurança; Sistema de integração/entrega contínua (CI/CD).

R.N. CIS CSC 18;

COBIT 5
APO13.01,
BAI03.01,
BAI03.02,
BAI03.03;

ISO/IEC
27001:2013
A.6.1.5, A.14.1.1,
A.14.2.1, A.14.2.5;
NIST SP 800-53
Rev. 4 PL-8, SA-3,
SA-4, SA-8, SA-10,
SA-11, SA-12, SA-
15, SA-17, SI-12,
SI-13, SI-14, SI-16,
SI-17.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Está definido um conjunto rudimentar de requisitos de segurança mínimos para os projetos de desenvolvimento. 	<ul style="list-style-type: none"> Conjunto rudimentar de medidas de segurança a aplicar para projetos de desenvolvimento.
2 – Intermédio	<ul style="list-style-type: none"> Existe a definição exhaustiva dos requisitos de segurança a seguir nos projetos de desenvolvimento; Existem regras internas para o desenvolvimento seguro. 	<ul style="list-style-type: none"> Registos de análise de riscos de projetos e indicação de requisitos de segurança; Conjunto de políticas, procedimentos e requisitos de segurança para o desenvolvimento seguro.
3 – Avançado	<ul style="list-style-type: none"> Os controlos dinâmicos de segurança nos ciclos de desenvolvimento estão implementados; O código fonte é monitorizado e gerido de maneira segura. 	<ul style="list-style-type: none"> Processos de testes e validações de segurança estabelecidos no ciclo de desenvolvimento; Uso de ferramentas de integração contínua (CI); 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	<ul style="list-style-type: none"> Existe um processo informal para a gestão de alterações. 	<ul style="list-style-type: none"> Evidências <i>ad hoc</i> de alterações passadas.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidas regras internas para a gestão de alterações; Os processos de avaliação e aprovação prévia de alterações estão definidos. 	<ul style="list-style-type: none"> Cria, documenta e mantém procedimentos de gestão de alterações; Estabelecer sistema de controlo de versões; Evidências de análise e avaliação prévia às alterações.
3 – Avançado	<ul style="list-style-type: none"> Os mecanismos técnicos para acompanhar as alterações estão estabelecidos; É realizada a revisão periódica dos procedimentos e registos de alterações. 	<ul style="list-style-type: none"> Adoção de sistema de integração e entrega contínua (CI/CD); Evidência de avaliação dos registos e procedimentos de alterações, conforme procedimentos e aprovações.

R.N. CIS CSC 10;
COBIT 5
APO13.01,
DSS01.01,
DSS04.07;

ISO/IEC
27001:2013
A.12.3.1, A.17.1.2,
A.17.1.3, A.18.1.3;
NIST SP 800-53
Rev. 4 CP-4, CP-6,
CP-9.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> São realizadas cópias de segurança de sistemas e ficheiros. 	<ul style="list-style-type: none"> Evidência da cópia de segurança de sistemas e ficheiros importantes.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidas regras internas formais para a realização das cópias de segurança; A integridade das cópias de segurança é verificada de forma independente em relação ao ambiente protegido. 	<ul style="list-style-type: none"> Documentos de suporte às cópias de segurança (políticas, procedimentos, registos, padrões, etc.); Armazenar as cópias de segurança em local fisicamente separado do ambiente protegido; Realizar testes de restauro das cópias de segurança em ambiente isolado.
3 – Avançado	<ul style="list-style-type: none"> A confidencialidade, integridade e disponibilidade da informação armazenada das cópias de segurança são garantidas; Os procedimentos realizados para as cópias de segurança são verificados. 	<ul style="list-style-type: none"> Utilização de sistemas criptográficos de dados, cuja confidencialidade seja necessária; Estabelecer ciclos de diferentes tipos de restauro e uso das cópias de segurança; Emprego de soluções automatizadas para a validação da integridade das cópias de segurança; 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	<ul style="list-style-type: none"> A proteção de infraestruturas é feita de forma não sistematizada (por exemplo, apenas alguns sistemas são protegidos por UPS). 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> As infraestruturas estão protegidas contra alterações elétricas que causem danos; As alterações no ambiente e que possam afetar os sistemas são monitorizadas e detetadas. 	<ul style="list-style-type: none"> Aplicação de sistemas de proteção contra variações na corrente elétrica, que possam danificar os sistemas; Utilização de sensores de fumo, humidade e temperatura.
3 – Avançado	<ul style="list-style-type: none"> A prevenção contra alterações elétricas que possam causar danos é feita de forma proativa; Existem mecanismos que garantem a constância no fornecimento de energia; A eficácia dos controlos para manter a organização funcional é auditada. 	<ul style="list-style-type: none"> Existência de sistemas de gestão automática do fornecimento de eletricidade; Utilização de fontes alternativas de eletricidade (ex.: geradores); Registo de testes do plano de continuidade, considerando controlos físicos.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os dados são destruídos de forma <i>ad hoc</i>. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> A informação sensível é destruída apropriadamente; Estão documentados procedimentos de destruição de informação sigilosa. 	<ul style="list-style-type: none"> Destruidor de papel; Procedimentos e políticas que tratem da higienização de ficheiros; Sistemas de higienização de ficheiros.
3 – Avançado	<ul style="list-style-type: none"> É realizada a avaliação da eficácia da destruição da informação em meio físico e digital. 	<ul style="list-style-type: none"> Registo de revisão dos mecanismos utilizados para a higienização de ficheiros, tanto físicos quanto digitais; Evidência do comprometimento de parceiros e prestadores de serviços com a higienização de ficheiros compartilhados ou de responsabilidade da organização; Registo das eliminações realizadas.

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os processos de proteção são efetuados de forma não sistematizada. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidos procedimentos e controlos de monitorização e melhoria contínua. 	<ul style="list-style-type: none"> Procedimentos de controlo e monitorização.
3 – Avançado	<ul style="list-style-type: none"> Os procedimentos e controlos são revistos regularmente; São realizadas auditorias internas recorrentes, aos controlos de segurança. 	<ul style="list-style-type: none"> Registos de atualizações dos procedimentos e controlos; Planeamento de auditoria interna; Registo de auditorias internas, realizadas no âmbito da segurança da informação; Planos de ação para tratamento de resultados de auditoria.

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os processos de proteção são melhorados de forma não sistematizada. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> A eficácia das tecnologias de proteção é medida e avaliada; Existe um processo estabelecido de evolução, através de lições aprendidas. 	<ul style="list-style-type: none"> Registos de melhorias aos processos de proteção; KPIs das tecnologias de proteção.
3 – Avançado	<ul style="list-style-type: none"> Os processos de tratamento de incidentes são revistos regularmente; As lições aprendidas são comunicadas às partes relevantes. 	<ul style="list-style-type: none"> Registo de lições aprendidas com eventos de segurança; 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	<ul style="list-style-type: none"> Os planos de resposta são atualizados de forma <i>ad hoc</i>. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Existem processos, formalmente definidos, para as atividades relativas a resposta a incidentes e garantia da resiliência da organização; Os planos de resposta são medidos e avaliados quando executados. 	<ul style="list-style-type: none"> Registo formal de processos e políticas para a resposta a incidentes; Registo formal de processos e políticas para a continuidade de negócio; Estabelecer sessões de consciencialização ou outras formas de divulgação dos planos de continuidade.
3 – Avançado	<ul style="list-style-type: none"> As estratégias e ações para a resposta a incidentes e para a garantia da continuidade da organização são avaliadas regularmente. 	<ul style="list-style-type: none"> Registo de revisão dos planos de continuidade de negócio; 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	<ul style="list-style-type: none"> Os planos de resposta são exercitados de forma não sistematizada. 	<ul style="list-style-type: none"> Registo de exercícios pontuais e isolados.
2 – Intermédio	<ul style="list-style-type: none"> Os planos de continuidade são registados e testados quanto ao âmbito definido. 	<ul style="list-style-type: none"> Registo de exercícios sistematizado (ex.: restauro de ambientes, “<i>table top</i>”, etc.).
3 – Avançado	<ul style="list-style-type: none"> O plano de continuidade é testado pela sua eficiência em âmbito realista. 	<ul style="list-style-type: none"> Registo de simulacros de casos reais em departamentos da organização ou transversais; 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	<ul style="list-style-type: none"> O registo dos colaboradores é realizado. 	<ul style="list-style-type: none"> Dossier dos colaboradores com dados cadastrais identificativos.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidas regras para a seleção, recrutamento e contratação; Estão estabelecidas regras para a cessação da contratação. 	<ul style="list-style-type: none"> Procedimentos e políticas de contratação, mobilidade e cessação de funções de colaboradores.
3 – Avançado	<ul style="list-style-type: none"> Existem perfis funcionais com competências em cibersegurança e segurança da informação, para as contratações; As ações para o tratamento do não cumprimento das normas internas de segurança da informação estão definidas. 	<ul style="list-style-type: none"> Estabelecimento de perfis funcionais com competências em cibersegurança e segurança da informação; Ações disciplinares para casos de infração contra a segurança da informação.

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A pesquisa de vulnerabilidades é executada em intervalos regulares. 	<ul style="list-style-type: none"> Plano de avaliação das vulnerabilidades; Relatório de ferramentas automáticas de pesquisa de vulnerabilidades.
2 – Intermédio	<ul style="list-style-type: none"> As vulnerabilidades são identificadas com equipas de tratamento adequadas; A análise de vulnerabilidades é regular e sistemática; As vulnerabilidades são exploradas, para atestar o seu nível de risco real. 	<ul style="list-style-type: none"> Registo de submissão de vulnerabilidades para serem tratadas por partes interessadas; Registo de análise de vulnerabilidades, realizado regularmente, e do seu devido tratamento; Adoção de ferramenta de pesquisa de vulnerabilidades; Relatório recente (≤ 1 ano) de testes de intrusão nos sistemas e infraestrutura.
3 – Avançado	<ul style="list-style-type: none"> É avaliado regularmente o processo de análise de vulnerabilidades; As partes interessadas, externas, são envolvidas no tratamento das vulnerabilidades; Estão estabelecidos planos de ação formais para o tratamento das vulnerabilidades. 	<ul style="list-style-type: none"> Registo da revisão regular do processo de análise de vulnerabilidades e tratamento de dados; Tratamento das vulnerabilidades com apoio de fornecedores, parceiros e entidades competentes; 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	<ul style="list-style-type: none"> As atividades de manutenção são realizadas sem seguir um processo formal; O registo das atividades não é controlado. 	<ul style="list-style-type: none"> Registos ocasionais de manutenções efetuadas.
2 – Intermédio	<ul style="list-style-type: none"> Os processos de manutenção são realizados formalmente e envolvem as pessoas adequadas; Os colaboradores têm a formação adequada para realizarem a manutenção dos ativos. 	<ul style="list-style-type: none"> Políticas e procedimentos de manutenções; Evidências da consciencialização e formação de colaboradores para realizar as manutenções necessárias; Registo de autorizações de perfis de acessos para fins de manutenção.
3 – Avançado	<ul style="list-style-type: none"> As manutenções realizadas por pessoas externas são acompanhadas adequadamente; O fluxo de trabalho de requisições de manutenção e reparação é automatizado; Estão estabelecidos períodos de manutenção preventiva aos ativos da organização. 	<ul style="list-style-type: none"> Registo de manutenções preventivas planeadas; Ferramenta de gestão de pedidos para acompanhar as manutenções; 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 registradas

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> As manutenções remotas são realizadas sem um processo formal de aprovação. 	<ul style="list-style-type: none"> Registos ocasionais de manutenções remotas.
2 – Intermédio	<ul style="list-style-type: none"> As manutenções remotas são realizadas conforme aprovação; Estão estabelecidos meios seguros para a manutenção remota ser realizada. 	<ul style="list-style-type: none"> Registo dos fluxos de avaliação e aprovação das manutenções remotas, conforme procedimentos definidos; Infraestrutura de conexão e autenticação forte com agentes externos para as manutenções.
3 – Avançado	<ul style="list-style-type: none"> Os controlos de acompanhamento do fluxo de solicitações e aprovações para as manutenções remotas estão automatizados; Estão estabelecidas métricas de acompanhamento e garantia das manutenções; Existe a garantia de que a conexão é encerrada sempre que não for necessária à sua manutenção. 	<ul style="list-style-type: none"> Uso de sistema de gestão de <i>workflow</i> para pedidos e fluxos de aprovação das manutenções; Contratos, SLAs e demais registos que atestem a garantia das manutenções; Registos tecnológicos que indiquem a terminação das conexões sempre que não for necessário estarem ativas.

1.4.6 PR.TP Tecnologia de Proteção

R.N. CIS CSC 1, 3, 5, 6, 14, 15, 16;

COBIT 5
APO11.04,
BAI03.05,
DSS05.04,
DSS05.07,
MEA02.01;

ISO/IEC
27001:2013
A.12.4.1, A.12.4.2,
A.12.4.3, A.12.4.4,
A.12.7.1;

NIST SP 800-53
Rev. 4 família AU.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os registros de auditoria não seguem um processo de gestão formal. 	<ul style="list-style-type: none"> Existência ocasional de registros de auditoria.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidos critérios formais para a auditoria de sistemas; Os registros de eventos para auditorias são geridos de maneira sistêmica; Os formatos e taxonomias de registros estão definidos. 	<ul style="list-style-type: none"> Políticas e normas relativas à coleta e análise de registros de eventos; Execução de procedimentos documentados sobre a coleta e tratamento dos registros de eventos para a análise; Utilização de sistema de coleta, tratamento e análise dos registros de eventos.
3 – Avançado	<ul style="list-style-type: none"> A integridade dos registros de eventos para fins de auditorias deve ser garantida; Os registros de auditorias transversais aos sistemas da organização são geridos centralmente. 	<ul style="list-style-type: none"> Existência de controlos técnicos de integridade dos registros, tais como validação por função <i>hash</i>, sincronização dos relógios e garantia do <i>timestamping</i>. Armazenamento, tratamento e correlação de registros 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	<ul style="list-style-type: none"> Existe uma implementação básica e <i>ad hoc</i> de medidas de proteção aos suportes de dados amovíveis. 	<ul style="list-style-type: none"> <i>Bitlocker</i> ativo em discos amovíveis; Políticas de domínio aplicadas para restrição de acesso a discos amovíveis.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidas regras de uso e boas práticas sobre dispositivos amovíveis; É feita a promoção de ações de sensibilização dos utilizadores sobre os riscos associados aos dispositivos amovíveis; Estão estabelecidos mecanismos técnicos para a proteção de dados em dispositivos amovíveis. 	<ul style="list-style-type: none"> Registar políticas, padrões, normas e boas práticas sobre a utilização de dispositivos amovíveis; Ações de sensibilização sobre a utilização aceitável de dispositivos amovíveis; Utilização de soluções criptográficas para dispositivos amovíveis.
3 – Avançado	<ul style="list-style-type: none"> A utilização de dispositivos amovíveis é bloqueada; É garantida a higienização dos dispositivos amovíveis no momento da sua destruição. 	<ul style="list-style-type: none"> Emprego de bloqueios físicos ou lógicos para o uso de dispositivos amovíveis de armazenamento; Restrição a pessoal autorizado; Procedimentos de descarte seguro de dispositivos amovíveis; 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	<ul style="list-style-type: none"> Os sistemas são configurados com os recursos necessários de forma não sistematizada. 	<ul style="list-style-type: none"> Registos ocasionais e isolados de sistemas configurados apenas com as funcionalidades mínimas necessárias.
2 – Intermédio	<ul style="list-style-type: none"> Os acessos concedidos são os mínimos necessários; São estabelecidas funcionalidades mínimas para cada necessidade de operação. 	<ul style="list-style-type: none"> Integração com gestão de identidades e acessos; Registo formal de políticas e padrões de configurações de recursos mínimos por defeito.
3 – Avançado	<ul style="list-style-type: none"> Os requisitos mínimos são revistos e atualizados periodicamente; Os acessos são condizentes com as necessidades mínimas para as funções. 	<ul style="list-style-type: none"> Registo de revisões periódicas aos padrões e procedimentos de configurações de sistemas; Registo da revisão dos acessos concedidos; Revisão das definições de perfis funcionais por necessidades de acessos.

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.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> As zonas de rede são segregadas de forma não sistematizada; A tecnologia de encriptação é aplicada de forma <i>ad hoc</i>. 	<ul style="list-style-type: none"> Registo de sistemas protegidos com SSL/TLS; Impossibilidade de chegar a qualquer ponto da rede a partir dos postos de trabalho dos colaboradores.
2 – Intermédio	<ul style="list-style-type: none"> As zonas de rede são segmentadas conforme a finalidade; São utilizadas soluções tecnológicas de filtro de fluxo de dados. 	<ul style="list-style-type: none"> Diagrama de redes a indicar a segmentação por zonas; Utilização de IDS/IPS, <i>firewalls</i>, <i>proxies</i>, <i>WAFs</i> e outras soluções tecnológicas para filtro e bloqueio de dados em transmissão.
3 – Avançado	<ul style="list-style-type: none"> São revistas periodicamente as configurações dos sistemas de filtro das conexões; As alterações na rede obedecem a processos de validação sistematizados. 	<ul style="list-style-type: none"> Registo de revisões regulares das definições e dos sistemas de segurança definidos (IDS/IPS, <i>firewalls</i>, <i>proxies</i>, <i>WAFs</i>, etc.); Registo de processos da gestão da alteração.

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.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A incorporação de resiliência nos sistemas e redes de comunicações é aplicada de forma não sistematizada. 	<ul style="list-style-type: none"> Redundância ocasional e isolada de sistemas ou equipamentos de rede de comunicações.
2 – Intermédio	<ul style="list-style-type: none"> Os sistemas críticos são resilientes; Os sistemas são protegidos contra a sobrecarga de acessos. 	<ul style="list-style-type: none"> Redundância dos sistemas críticos; Adoção de soluções de balanceamento de carga.
3 – Avançado	<ul style="list-style-type: none"> A resiliência das infraestruturas às situações adversas é gerida; Existe a garantia de que eventos inesperados não causam negação de serviço das operações. 	<ul style="list-style-type: none"> Garantir a alta disponibilidade dos sistemas críticos; Documentos de suporte ao plano de continuidade de negócios.



DETETAR

1.5.1 DE.AE Anomalias e Eventos

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Não aplicável. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> As alterações nas infraestruturas e fluxos de comunicação são detetadas; Os colaboradores são capazes de tratar e detetar alterações nos modelos de referência estabelecidos; Estão estabelecidos modelos de referência para equipamentos e fluxos de dados. 	<ul style="list-style-type: none"> Utilização de tecnologias de filtro e deteção de requisições anómalas (ex.: <i>firewall, proxy, IDS/IPS</i>); Registo de formação/consciencialização dos colaboradores no tema de deteção de anomalias e eventos de segurança; Registo de padrões e procedimentos padrão para modelos de referências internas.
3 – Avançado	<ul style="list-style-type: none"> É feita, periodicamente, a revisão dos modelos de referência. 	<ul style="list-style-type: none"> Registos de alterações conforme descrito nos procedimentos internos da gestão de alteração.

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> É realizada uma análise <i>ad hoc</i> dos eventos, sem procedimento de tratamento formalizado e implementado. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> As tentativas de ataques e incidentes de segurança são detetadas; Está estabelecido o tratamento apropriado de incidentes de segurança; É realizada a comunicação apropriada de incidentes com as partes interessadas. 	<ul style="list-style-type: none"> Registo de incidentes de segurança, originados pela deteção e monitorização de eventos; Registo de incidentes de segurança, de forma suficiente à sua análise e tratamento; Registo de incidentes a informar as partes interessadas relevantes.
3 – Avançado	<ul style="list-style-type: none"> É realizada a identificação de incidentes de segurança, através da análise dos eventos coletados transversalmente nas infraestruturas; Está estabelecida a resposta apropriada a incidentes detetados. 	<ul style="list-style-type: none"> Implementação de um sistema de correlação de eventos; Registos de incidentes reportados com o devido tratamento.

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.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os eventos são coletados centralmente; Existe correlação <i>ad hoc</i> com fontes não sistematizadas. 	<ul style="list-style-type: none"> Registro de eventos coletados num sistema central.
2 – Intermédio	<ul style="list-style-type: none"> Os eventos de segurança são geridos e analisados; São considerados eventos de diversas fontes internas e externas. 	<ul style="list-style-type: none"> Políticas e procedimento de gestão e correlação de eventos de segurança; Registro de fontes de conhecimento utilizadas para as análises dos eventos; Utilização de sistema de correlação de eventos.
3 – Avançado	<ul style="list-style-type: none"> Existe melhoria contínua dos controlos, a partir do tratamento de eventos anteriores; Estão estabelecidos mecanismos de controlo de um evento de segurança nas suas infraestruturas. 	<ul style="list-style-type: none"> Utilização de registos e tratamentos anteriores como lições aprendidas; Existência da <i>honeypots</i> geridos nas estruturas da organização.

R.N. CIS CSC 4, 6;

COBIT 5
APO12.06,
DSS03.01;

ISO/IEC
27001:2013
A.16.1.4;

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os eventos de segurança são classificados conforme o seu impacto percebido. 	<ul style="list-style-type: none"> Registro dos eventos categorizados.
2 – Intermédio	<ul style="list-style-type: none"> Está estabelecido um processo de gestão de eventos; Os efeitos do impacto de um evento são aferidos. 	<ul style="list-style-type: none"> Documentos de apoio ao processo de gestão de eventos; Metodologias de avaliação do impacto de um evento.
3 – Avançado	<ul style="list-style-type: none"> A gestão de incidentes é acionada a partir da gestão de eventos. 	<ul style="list-style-type: none"> Registos que interliguem eventos detetados a registos na gestão de incidentes.

R.N. CIS CSC 6, 19;
 COBIT 5
 APO12.06,
 DSS03.01;
 ISO/IEC
 27001:2013
 A.16.1.4;
 NIST SP 800-53
 Rev. 4 IR-4, IR-5,
 IR-8.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os incidentes são abertos sem limite formal definido para o número de eventos relacionados. 	<ul style="list-style-type: none"> Registos ocasionais de incidentes de segurança, sem consistência no número de eventos necessários à constituição formal de incidente.
2 – Intermédio	<ul style="list-style-type: none"> Está estabelecido um processo de gestão de eventos; Está estabelecida a definição de incidentes de segurança no contexto da organização. 	<ul style="list-style-type: none"> Documentos de apoio ao processo de gestão de eventos; Registo da taxonomia de incidentes e das suas prioridades no tratamento.
3 – Avançado	<ul style="list-style-type: none"> Os incidentes são analisados e avaliados com base no risco percebido; O tratamento de incidentes é realizado conforme o seu nível de complexidade e impacto. 	<ul style="list-style-type: none"> Ferramentas de correlação de eventos; Limites a serem considerados para a determinação de um incidente, ainda que sendo resultado de eventos isolados; 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	<ul style="list-style-type: none"> A monitorização é realizada sem um sistema automático de deteção ou com deteção manual. 	<ul style="list-style-type: none"> Registos ocasionais de deteções manuais.
2 – Intermédio	<ul style="list-style-type: none"> É realizada a monitorização e proteção face a comportamentos anómalos na rede, que possam representar um incidente. 	<ul style="list-style-type: none"> Implementação de sistemas de monitorização e proteção da rede (ex.: WAF, IDS/IPS, etc.).
3 – Avançado	<ul style="list-style-type: none"> É realizada a associação de eventos de segurança de origens distintas; Os acessos a ativos conhecidos são restringidos; A gestão de incidentes é suportada por uma equipa dedicada. 	<ul style="list-style-type: none"> Implementação de sistema de gestão e correlação e eventos; Regras de acesso às infraestruturas e sistemas apenas para dispositivos cadastrados e registados; Existência na organização de uma equipa dedicada à gestão de incidentes.

R.N. COBIT 5
DSS01.04,
DSS01.05;
ISO/IEC
27001:2013
A.11.1.1, A.11.1.2;
NIST SP 800-53
Rev. 4 CA-7, PE-3,
PE-6, PE-20.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os acessos físicos são monitorizados; A deteção de incidentes de intrusão física é manual; São produzidos registos de auditoria de acessos físicos. 	<ul style="list-style-type: none"> Registos ocasionais de deteção de incidentes de segurança física.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidos controlos de monitorização de áreas seguras; É gerada alarmística para tentativas de acessos não autorizados. 	<ul style="list-style-type: none"> Suporte da gestão de acessos para segurança física; Instalação de sistemas de CCTV; Suporte de sistemas de monitorização para alarmísticas.
3 – Avançado	<ul style="list-style-type: none"> Os acessos físicos são revistos em intervalos regulares. 	<ul style="list-style-type: none"> Registos de auditorias nos controlos de acesso e monitorização dos ambientes físicos; Pontos de auditorias e eventos registados são correlacionados na gestão de 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.

DE.MC-3 - A atividade dos colaboradores deve ser monitorizada para se detetar potenciais incidentes

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A atividade dos colaboradores é monitorizada; Os incidentes são detetados manualmente. 	<ul style="list-style-type: none"> Registos ocasionais de incidentes originados na deteção manual, baseados no comportamento digital dos colaboradores.
2 – Intermédio	<ul style="list-style-type: none"> Os eventos de segurança levam em conta as ações dos colaboradores; Estão estabelecidos padrões fiáveis de monitorização de colaboradores. 	<ul style="list-style-type: none"> Suporte dos registos de eventos que identificam o responsável; Formalizar padrões e métricas que sirvam de referencial para a monitorização das atividades dos colaboradores; Sistema central de armazenamento e gestão de eventos.
3 – Avançado	<ul style="list-style-type: none"> Os eventos dispersos são analisados em contexto; Existe a capacidade de antecipar incidentes de segurança a partir da análise de tendências. 	<ul style="list-style-type: none"> Utilização da correlação de eventos para a monitorização e registo de incidentes; Alertas preditivos.

R.N. CIS CSC4, 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 detecção de código malicioso

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A detecção da presença de código malicioso na infraestrutura é reativa. 	<ul style="list-style-type: none"> Implementar ferramentas de antivírus nas estações de trabalho e servidores.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidas regras formais de avaliação de códigos maliciosos; As verificações periódicas de códigos maliciosos são realizadas periodicamente. 	<ul style="list-style-type: none"> Apoio de políticas de antivírus; Sistemas de antivírus configurados para pesquisas periódicas e recorrentes.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidos procedimentos de resposta integrada a incidentes; A eficiência dos sistemas de antivírus é avaliada; É realizada a análise técnica de ameaças. 	<ul style="list-style-type: none"> Integração do sistema de antivírus com o sistema central de gestão de eventos de segurança; Integração do sistema de análise comportamental com o sistema central de gestão de eventos de segurança; Realizar auditorias aos sistemas de antivírus; Registo de atividades de análise de código; Registo de atividades de análise forense; 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	<ul style="list-style-type: none"> As aplicações em dispositivos móveis da organização são monitorizadas; A deteção de aplicações não autorizadas é manual. 	<ul style="list-style-type: none"> Registo ocasional de incidentes de segurança, com origem na deteção manual de aplicações não autorizadas.
2 – Intermédio	<ul style="list-style-type: none"> Estão definidas as aplicações permitidas nas redes e sistemas; O comprometimento do colaborador em não utilizar sistemas não autorizados é garantido. 	<ul style="list-style-type: none"> Estabelecimento de <i>whitelists</i> e/ou <i>blacklists</i> de aplicações e sistemas; Termo de responsabilidade dos utilizadores sobre a utilização dos equipamentos.
3 – Avançado	<ul style="list-style-type: none"> A gestão do parque de dispositivos móveis é feita de forma centralizada; O sistema de gestão de dispositivos móveis está integrado com o sistema de gestão de eventos de segurança; Existe a capacidade de correlacionar os eventos de segurança com dispositivos móveis; A gestão de ativos é realizada de forma integrada. 	<ul style="list-style-type: none"> Gestão dos sistemas de forma a ser capaz de monitorizar aplicações instaladas nos equipamentos; Instalação de sistema central de gestão de dispositivos móveis; Registos de incidentes de segurança, com origem na deteção automática de aplicações não autorizadas.

R.N. COBIT 5
APO07.06,
APO10.05;
ISO/IEC
27001:2013
A.14.2.7, A.15.2.1;
NIST SP 800-53
Rev. 4 CA-7, PS-7,
SA-4, SA-9, SI-4.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> As atividades dos prestadores de serviços externos são monitorizadas; A deteção de incidentes é manual e não sistematizada. 	<ul style="list-style-type: none"> Registos ocasionais de incidentes de segurança, com origem em atividades suspeitas, por prestadores de serviços externos, detetadas manualmente.
2 – Intermédio	<ul style="list-style-type: none"> Os pedidos de acesso remoto são identificados e avaliados; Estão estabelecidas formalmente regras de acesso remoto para prestadores de serviços externos. 	<ul style="list-style-type: none"> Adoção de sistemas de deteção e prevenção de intrusões; Suporte de políticas, normas e procedimentos para a interação com prestadores de serviços externos; Gestão de acessos dos prestadores de serviços externos.
3 – Avançado	<ul style="list-style-type: none"> É realizada a avaliação dos eventos relativos aos acessos externos; Os acessos e permissões concedidas a prestadores de serviços externos são avaliados regularmente. 	<ul style="list-style-type: none"> Integração com sistemas de correlação de eventos; Suporte de atividades de auditoria de segurança na revisão e avaliação dos acessos de prestadores de serviços externos; Registos de incidentes de segurança, com origem em atividades suspeitas detetadas automaticamente, por prestadores de serviços externos.

R.N. CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16;
 COBIT 5 DSS05.02, DSS05.05;
 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1;
 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os acessos são monitorizados e analisados manualmente. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Os pedidos de acesso às infraestruturas e servidores são monitorizados; Os dados dispersos são recolhidos e centralizados para análise de anomalias. 	<ul style="list-style-type: none"> Implementação de sistemas de deteção e prevenção de intrusões; Registos de eventos de acesso aos servidores e sistemas.
3 – Avançado	<ul style="list-style-type: none"> Os eventos de acesso e incidentes relacionados são tratados. 	<ul style="list-style-type: none"> Sistema de correlação de eventos; Relatórios de incidentes.

R.N. CIS CSC 4, 20;
 COBIT 5 BAI03.10, DSS05.01;
 ISO/IEC 27001:2013 A.12.6.1;
 NIST SP 800-53 Rev. 4 RA-5.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A pesquisa por vulnerabilidades nos sistemas e redes de comunicação é feita pontualmente. 	<ul style="list-style-type: none"> Relatórios ocasionais de vulnerabilidades.
2 – Intermédio	<ul style="list-style-type: none"> As vulnerabilidades identificadas nos sistemas e redes de comunicação são analisadas regularmente. 	<ul style="list-style-type: none"> Estabelecer um plano de análise de vulnerabilidades; Implementar uma ferramenta de análise de vulnerabilidades; Registos de suporte à análise e avaliação das vulnerabilidades.
3 – Avançado	<ul style="list-style-type: none"> A análise de vulnerabilidades está integrada com outros processos da organização; As vulnerabilidades identificadas são geridas. 	<ul style="list-style-type: none"> Integrar a análise de vulnerabilidades com processos de testes e análises de segurança em sistemas e aplicações; Registo de planos de ação para o tratamento das vulnerabilidades.

1.5.3 DE.PD Processos de Detecção

R.N. CIS CSC 19;

COBIT 5
APO01.02,
DSS05.01,
DSS06.03;

ISO/IEC
27001:2013
A.6.1.1, A.7.2.2;
NIST SP 800-53
Rev. 4 CA-2, CA-7,
PM-14.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> As responsabilidades na deteção de eventos são definidas informalmente. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Os responsáveis pelo tratamento de eventos anómalos são identificados; Os colaboradores são esclarecidos sobre a deteção de eventos anómalos. 	<ul style="list-style-type: none"> Comunicados, nomeações ou qualquer outro elemento de suporte na identificação do responsável pelo tratamento dos eventos anómalos; Material de apoio e de registo das sessões de consciencialização.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidas as responsabilidades no processo de deteção de eventos anómalos; Os agentes externos envolvidos estão comprometidos na deteção de eventos anómalos. 	<ul style="list-style-type: none"> Documentação de suporte ao estabelecimento de responsabilidades (ex.: RACI, definições de perfis funcionais, etc.); Acordos de prestação de serviços que apresentam termos sobre a responsabilização na deteção de eventos anómalos.

R.N. COBIT 5
DSS06.01,
MEA03.03,
MEA03.04;

ISO/IEC
27001:2013
A.18.1.4, A.18.2.2,
A.18.2.3;

NIST SP 800-53
Rev. 4 AC-25,
CA-2, CA-7, SA-18,
SI-4, PM-14.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> As atividades de deteção seguem um processo <i>ad hoc</i>. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Os incidentes são detetados e identificados a partir dos eventos registados; Os responsáveis por atividades de deteção são identificados. 	<ul style="list-style-type: none"> Relatórios ou indicadores de utilização de sistema de correlação de eventos; Matriz RASIC dos envolvidos nas atividades de deteção.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidas ações de validação dos controlos; A integridade dos dados coletados é garantida por aplicação de controlos. 	<ul style="list-style-type: none"> Registos de suporte a auditorias internas; Utilização de soluções de <i>hashing</i> na assinatura de registos.

R.N. COBIT 5
APO13.02,
DSS05.02;
ISO/IEC
27001:2013
A.14.2.8;
NIST SP 800-53
Rev. 4 CA-2, CA-7,
PE-3, SI-3, SI-4,
PM-14.

DE.PD-3 - Os processos de detecção devem ser testados

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os processos de detecção são medidos de forma <i>ad hoc</i>. 	<ul style="list-style-type: none"> Registos ocasionais de testes aos serviços de detecção.
2 – Intermédio	<ul style="list-style-type: none"> Existe um processo sistemático de análise aos processos de detecção; Os processos de detecção são medidos regularmente. 	<ul style="list-style-type: none"> Planos de teste para os processos de detecção; Resultados da análise aos processos de detecção.
3 – Avançado	<ul style="list-style-type: none"> A integridade e fiabilidade dos processos de detecção é avaliada. 	<ul style="list-style-type: none"> Resultados de testes de integridade aos processos de detecção; Resultados e análise da fiabilidade dos processos de detecção; Aplicação de metodologias de melhoria contínua.

R.N. CIS CSC 19;
COBIT 5
APO08.04,
APO12.06,
DSS02.05;

ISO/IEC
27001:2013
A.16.1.2, A.16.1.3;
NIST SP 800-53
Rev. 4 AU-6, CA-2,
CA-7, RA-5, SI-4.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os eventos de segurança são reportados internamente e de forma informal. 	<ul style="list-style-type: none"> Relatórios ou emails ocasionais de detecções de eventos e respetivas comunicações internas.
2 – Intermédio	<ul style="list-style-type: none"> Está estabelecido internamente um canal de comunicação adequado; Os incidentes detetados são registados adequadamente. 	<ul style="list-style-type: none"> Documentos de suporte à gestão de incidentes; Registo de eventos detetados que resultam em incidentes.
3 – Avançado	<ul style="list-style-type: none"> Está definida a gestão centralizada e otimizada da detecção dos incidentes. 	<ul style="list-style-type: none"> Estabelecer uma plataforma centralizada de resposta a incidentes.

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.

DE.PD-5 - Os processos de detecção devem ser objeto de melhoria contínua

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os processos de detecção são melhorados de forma não sistematizada. 	<ul style="list-style-type: none"> Atualizações isoladas dos processos de detecção.
2 – Intermédio	<ul style="list-style-type: none"> Existem mecanismos de medição e avaliação dos processos de detecção. 	<ul style="list-style-type: none"> Resultados da avaliação dos processos de detecção quanto à eficiência.
3 – Avançado	<ul style="list-style-type: none"> Os resultados da avaliação são usados para informar o processo de melhoria; Os processos de detecção são melhorados regularmente. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> São implementados procedimentos <i>ad hoc</i> de resposta a incidentes, de forma reativa. 	<ul style="list-style-type: none"> Registos de execução de atividades relacionadas com resposta a incidentes.
2 – Intermédio	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Documentos de suporte ao tratamento de incidentes (ex.: políticas, procedimentos, padrões, etc.).
3 – Avançado	<ul style="list-style-type: none"> É garantida a integridade das evidências analisadas; A resposta a incidentes é dada conforme o nível de escalonamento. 	<ul style="list-style-type: none"> Registos de validação de integridade das evidências; 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	<ul style="list-style-type: none"> Deve existir o conhecimento informal e não estruturado das funções de cada interveniente da organização. 	<ul style="list-style-type: none"> Conhecimento informal evidenciado (p. ex. por realização de entrevistas aos colaboradores).
2 – Intermédio	<ul style="list-style-type: none"> Os colaboradores têm conhecimento sobre os procedimentos e responsabilidades; Estão estabelecidos os guiões de resposta a incidentes. 	<ul style="list-style-type: none"> Documentos de suporte à resposta a incidentes; Registo das sessões de formação em segurança e respostas a incidentes; Estabelecer guiões de tratamento e resposta a incidentes.
3 – Avançado	<ul style="list-style-type: none"> Deve existir envolvimento das partes externas relevantes na resposta a incidentes. 	<ul style="list-style-type: none"> Mapa das partes externas relevantes; 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	<ul style="list-style-type: none"> Deve existir o conhecimento informal e não estruturado dos canais de reporte dos incidentes. 	<ul style="list-style-type: none"> Conhecimento informal evidenciado (p. ex. por realização de entrevistas aos colaboradores).
2 – Intermédio	<ul style="list-style-type: none"> A capacidade de reporte de incidentes deve estar garantida; Estão estabelecidos critérios de reporte de incidentes. 	<ul style="list-style-type: none"> Definição dos canais de reporte de incidentes; Documentos de suporte na orientação de como reportar incidentes; Registo de divulgação dos critérios de reporte de incidentes.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidos critérios para envolver as partes interessadas externas no tratamento dos incidentes; O reporte de incidentes é realizado de maneira integrada. 	<ul style="list-style-type: none"> Registo de reporte de incidentes, envolvendo equipas externas; 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 compartilhadas de acordo com o plano de resposta

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A identificação das partes interessadas para a comunicação de incidentes é informal e não estruturada. 	<ul style="list-style-type: none"> Registro das partes interessadas, internas e externas, na comunicação de incidentes.
2 – Intermédio	<ul style="list-style-type: none"> A comunicação de um incidente é do conhecimento de todos os envolvidos. 	<ul style="list-style-type: none"> Plano de comunicação de incidentes; Registros de formação e conscientização sobre a partilha de informação no plano de resposta a incidentes.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidos canais seguros de comunicação de incidentes; As partes externas interessadas no tratamento dos incidentes estão envolvidas na resposta. 	<ul style="list-style-type: none"> Procedimentos de comunicação de incidentes documentados através de canais seguros; Registro de comunicação às partes externas interessadas.

R.N. CIS CSC 19;
COBIT 5
DSS03.04;
ISO/IEC
27001:2013 Cláu-
sula 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	<ul style="list-style-type: none"> Não aplicável. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Existe coordenação com partes externas interessadas. 	<ul style="list-style-type: none"> Identificação das partes interessadas externas; Documentos de apoio ao plano de comunicação de incidentes com partes externas.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidos níveis de responsabilização na resposta a incidentes; A comunicação de incidentes é avaliada. 	<ul style="list-style-type: none"> Registro da definição de responsabilidades no âmbito da resposta a incidentes; Análise e avaliação dos registros 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	<ul style="list-style-type: none"> Mesmo que de forma informal e não estruturada, a informação relacionada com um incidente é partilhada voluntariamente. 	<ul style="list-style-type: none"> Observação de comunicação informal através de entrevista aos colaboradores.
2 – Intermédio	<ul style="list-style-type: none"> As partes interessadas externas relevantes são identificadas. 	<ul style="list-style-type: none"> Registo atualizado de parceiros, fornecedores e demais partes externas relevantes.
3 – Avançado	<ul style="list-style-type: none"> Está estabelecido um plano de comunicação coerente com as necessidades da organização. 	<ul style="list-style-type: none"> Documentos de apoio do plano de comunicação voluntária de incidentes.

1.6.3 RS.AN

Análise

R.N. CIS CSC 4, 6, 8, 19;

COBIT 5 DSS02.04, DSS02.07;

ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5;

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

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> O registo de notificações de eventos elevados a incidentes existe, mesmo que não estruturado; Existem orientações sobre a ativação da gestão de incidentes. 	<ul style="list-style-type: none"> Registos das orientações para a ativação da gestão de incidentes; Registos de notificações elevadas a incidentes.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidas práticas de acompanhamento aos eventos detetados; Existe um plano de resposta a incidentes e é cumprido. 	<ul style="list-style-type: none"> Evidências do tratamento dos eventos identificados como incidentes.
3 – Avançado	<ul style="list-style-type: none"> As notificações dos sistemas são avaliadas transversalmente. 	<ul style="list-style-type: none"> Implementar uma plataforma de gestão e correlação de eventos.

R.N. COBIT 5 DSS02.02;

ISO/IEC 27001:2013 A.16.1.4, A.16.1.6;

NIST SP 800-53 Rev. 4 CP-2, IR-4.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> O impacto dos incidentes é avaliado, de forma informal e não estruturada. 	<ul style="list-style-type: none"> Observação da avaliação do impacto, por entrevista aos colaboradores.
2 – Intermédio	<ul style="list-style-type: none"> Os incidentes de segurança são categorizados pelo nível de impacto percebido. 	<ul style="list-style-type: none"> Definição de padrões para categorias de incidentes; Taxonomia de impacto de incidentes.
3 – Avançado	<ul style="list-style-type: none"> O risco dos incidentes é avaliado; Estão estabelecidas métricas relativas às respostas e tratamento de incidentes. 	<ul style="list-style-type: none"> Registos da avaliação de riscos de incidentes; Documentação de apoio ao processo de gestão e correlação de eventos; 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	<ul style="list-style-type: none"> Não aplicável. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Estão definidos procedimentos de identificação, coleta e aquisição de registos e informação; Estão definidos procedimentos para a captura dos dados no seu formato original, para análise forense. 	<ul style="list-style-type: none"> Documentos de suporte aos processos de coleta de dados e garantia da cadeia de custódia; Formação dos colaboradores sobre procedimentos de análise forense.
3 – Avançado	<ul style="list-style-type: none"> É garantida a integridade e cadeia de custódia das evidências recolhidas; Existem meios específicos para a realização de análises forenses. 	<ul style="list-style-type: none"> Adoção de <i>software</i> de captura de dados para fins forenses; 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	<ul style="list-style-type: none"> A categorização dos incidentes é definida de formal informal e pouco estruturada. 	<ul style="list-style-type: none"> Observação da categorização dos incidentes, obtida por entrevista a colaboradores.
2 – Intermédio	<ul style="list-style-type: none"> Está estabelecida uma taxonomia de categorização de incidentes; A categorização do incidente está presente no momento da resposta. 	<ul style="list-style-type: none"> Documentação de apoio na taxonomia de categorização de incidentes; Inclusão da categorização de incidentes nos planos de resposta.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidas metodologias de tratamento para cada tipo de incidente detetado. 	<ul style="list-style-type: none"> Documentos de suporte ao tratamento de incidentes; 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	<ul style="list-style-type: none"> A submissão de vulnerabilidades é realizada através de processos <i>ad hoc</i>. 	<ul style="list-style-type: none"> Observação de submissão de vulnerabilidades por entrevista a colaboradores.
2 – Intermédio	<ul style="list-style-type: none"> Existem múltiplos mecanismos para que a organização seja informada sobre vulnerabilidades, quer seja de forma interna ou externa; Estão estabelecidos processos de tratamento às vulnerabilidades sobre as quais a organização é informada. 	<ul style="list-style-type: none"> Documento de suporte ao processo de gestão de vulnerabilidades; Formas de se informar sobre vulnerabilidades estabelecidas e divulgadas; Registo de receção das comunicações das vulnerabilidades; Critérios de classificação das vulnerabilidades, de forma a direccionar um tratamento adequado.
3 – Avançado	<ul style="list-style-type: none"> As vulnerabilidades registadas são analisadas e avaliadas sistematicamente. 	<ul style="list-style-type: none"> Documentos de suporte aos procedimentos de análise e avaliação de vulnerabilidades; 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	<ul style="list-style-type: none"> A resposta aos incidentes de segurança é realizada de forma não sistematizada. 	<ul style="list-style-type: none"> Registo de resposta no tratamento de incidentes.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidos processos de resposta aos incidentes. 	<ul style="list-style-type: none"> Procedimentos de resposta a incidentes de segurança; Documentos de suporte ao tratamento de incidentes; Elaboração de recomendações de tratamentos de incidentes.
3 – Avançado	<ul style="list-style-type: none"> As causas para a origem de incidentes são analisadas e avaliadas. 	<ul style="list-style-type: none"> Registos de investigação e análises forenses sobre as causas dos incidentes; Indicação de melhorias para a mitigação dos incidentes conhecidos.

R.N. CIS CSC 4, 19;
COBIT 5 APO12.06;
ISO/IEC 27001:2013 A.12.2.1, A.16.1.5;
NIST SP 800-53 Rev. 4 IR-4.

RS.MI-2 - Os incidentes devem ser mitigados

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> O tratamento dos incidentes é efetuado de forma reativa e não estruturada. 	<ul style="list-style-type: none"> Ações de contenção imediata de incidentes (p. ex. bloqueio de contas, interrupção de acessos, etc.).
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidas práticas para a redução do impacto dos incidentes; Os procedimentos sobre o tratamento de incidentes são documentados. 	<ul style="list-style-type: none"> Disponibilização de infraestrutura alternativa; Separação da rede em zonas protegidas por <i>firewalls</i>, etc.; Documentos de suporte à mitigação dos incidentes (p. ex. procedimentos, padrões, etc.).
3 – Avançado	<ul style="list-style-type: none"> Os incidentes são erradicados; É feita uma análise do tratamento dos incidentes para efeitos de melhoria contínua. 	<ul style="list-style-type: none"> Remoção de ameaças nas infraestruturas; Uso ou melhoria dos sistemas de proteção (p. ex. antivírus); Repositório de incidentes anteriores com os respetivos planos de ação corretivos.

R.N. CIS CSC 4;
COBIT 5 APO12.06;
ISO/IEC 27001:2013 A.12.6.1;
NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> O tratamento das vulnerabilidades é avaliado de forma não estruturada. 	<ul style="list-style-type: none"> Observação da avaliação das vulnerabilidades, por entrevista aos colaboradores.
2 – Intermédio	<ul style="list-style-type: none"> Está estabelecido um processo de gestão de vulnerabilidades; As vulnerabilidades são mitigadas de acordo com critérios definidos. 	<ul style="list-style-type: none"> Registo de execução do processo de gestão das vulnerabilidades.
3 – Avançado	<ul style="list-style-type: none"> O processo de análise de risco das vulnerabilidades é definido; A aceitação das vulnerabilidades, onde seja aplicável, é formalizada. 	<ul style="list-style-type: none"> Resultados das análises de risco; 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	<ul style="list-style-type: none"> Não aplicável. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Não aplicável. 	<ul style="list-style-type: none"> Não aplicável.
3 – Avançado	<ul style="list-style-type: none"> Os procedimentos de reposta a incidentes são melhorados através da análise de <i>lições aprendidas</i>. 	<ul style="list-style-type: none"> Documentos de suporte ao plano de resposta a incidentes; Registos de reuniões e demais interações, no contexto da melhoria contínua; Registo do tratamento de vulnerabilidades resultantes de incidentes ocorridos.

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

R.N. COBIT 5
BAI01.13;
DSS04.08;
ISO/IEC
27001:2013
A.16.1.6, Cláusula
10;
NIST SP 800-53
Rev. 4 CP-2, IR-4,
IR-8.

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Não aplicável. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Os procedimentos são atualizados periodicamente, mas não se limitando às tecnologias e sistemas utilizados. 	<ul style="list-style-type: none"> Registo de atualização de procedimentos para a reposta a incidentes, num determinado período de análise.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidos processos de melhoria contínua dos planos de resposta a incidentes; Os planos de resposta a incidentes são avaliados. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> As cópias de segurança são realizadas de forma <i>ad hoc</i>. 	<ul style="list-style-type: none"> Relatórios de execução de cópias de segurança e restauro.
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidos regras e procedimentos para a recuperação de incidentes; Está estabelecido um processo de gestão de cópias de segurança. 	<ul style="list-style-type: none"> Registo documental de procedimentos, políticas e padrões dedicados ao tema da recuperação de incidentes; Relatórios de utilização de plataforma de cópias de segurança e restauro.
3 – Avançado	<ul style="list-style-type: none"> São implementadas ações preditivas para dar respostas adequadas; Existe uma equipa dedicada ao tratamento e monitorização de ameaças, planeamento e resposta a incidentes (ex.: CSIRT). 	<ul style="list-style-type: none"> Registo de recuperação de incidentes; Registos de constituição, com descrição de funções dos elementos da equipa de resposta a incidentes.

1.7.2 RC.ME Melhorias

R.N. COBIT 5
APO12.06,
BAI05.07,
DSS04.08;
ISO/IEC
27001:2013
A.16.1.6, Cláusula
10;
NIST SP 800-53
Rev. 4 CP-2, IR-4,
IR-8.

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

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Não aplicável. 	<ul style="list-style-type: none"> Não aplicável.
2 – Intermédio	<ul style="list-style-type: none"> Existem e são avaliadas métricas relativas aos planos de recuperação; As fragilidades nos planos anteriores são identificadas. 	<ul style="list-style-type: none"> Registos dos indicadores e resultados analíticos de avaliação de resultados de ações, relativas aos planos de recuperação.
3 – Avançado	<ul style="list-style-type: none"> São identificadas as oportunidades de melhoria que possam ser implementadas; Os planos de recuperação são atualizados com as melhorias encontradas. 	<ul style="list-style-type: none"> Documentos com atualização dos planos; Documentos de suporte à execução das análises.

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.

RC.ME-2 - As estratégias de recuperação devem ser continuamente revistas e atualizadas

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> Os procedimentos <i>ad hoc</i>, de análise da operação da organização, incluem pontos de discussão relativos à recuperação de incidentes. 	<ul style="list-style-type: none"> Registos de discussão dos procedimentos <i>ad hoc</i> de recuperação (p. ex. atas ou notas de reuniões).
2 – Intermédio	<ul style="list-style-type: none"> Estão estabelecidos procedimentos de revisão e atualização da documentação e dos processos pertinentes à recuperação; As equipas afetas à recuperação de incidentes são geridas. 	<ul style="list-style-type: none"> Registo de atualização dos procedimentos e atualização dos métodos empregues como estratégias de recuperação; Registo de formação ou atualização das equipas internas e/ou externas envolvidas.
3 – Avançado	<ul style="list-style-type: none"> Estão estabelecidos procedimentos de revisão periódica das estratégias de recuperação, por parte da gestão de topo. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> A comunicação às partes interessadas sobre eventos de segurança é reativa. A comunicação é efetuada, mesmo que de forma pouco estruturada e dispersa. 	<ul style="list-style-type: none"> Registos de comunicações realizadas conforme as ocorrências.
2 – Intermédio	<ul style="list-style-type: none"> Está estabelecido um plano de comunicação sobre eventos de segurança; As partes interessadas relevantes estão identificadas. 	<ul style="list-style-type: none"> Documento de suporte ao plano de comunicação; Registo de partes interessadas conforme o tema a ser comunicado.
3 – Avançado	<ul style="list-style-type: none"> A comunicação é efetuada através de ações de consciencialização e de forma proativa. 	<ul style="list-style-type: none"> Plano de comunicações periódicas sobre segurança da informação, para as diversas audiências no âmbito; Registos de comunicações.

RC.CO-2 - As atividades de recuperação devem ser comunicadas às partes interessadas, internas e externas, bem como às equipes executivas e de gestão

NÍVEIS	DESCRIÇÃO	EVIDÊNCIAS
1 – Básico	<ul style="list-style-type: none"> A comunicação é efetuada de forma reativa e não estruturada. 	<ul style="list-style-type: none"> Registos das comunicações efetuadas.
2 – Intermédio	<ul style="list-style-type: none"> Está estabelecido um plano de comunicação consoante o seu propósito; Para cada objetivo a ser comunicado, é efetuada a identificação de audiência adequada e respetivo plano de comunicação. 	<ul style="list-style-type: none"> Plano de comunicação com o detalhe do objetivo a ser comunicado e identificação de audiência.
3 – Avançado	<ul style="list-style-type: none"> Está estabelecida uma estratégia de comunicação adequada para as equipas executivas e de gestão; Os processos de aprovação das comunicações estão definidos. 	<ul style="list-style-type: none"> Registos de comunicações para equipas executivas e de gestão; Registos dos processos de aprovação das comunicações; 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](tel:+351210497400)

