Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

CSE4CI - CYBERSECURITY ECOSYSTEM FOR CRITICAL INFRASTRUCTURES

ESTUDANTE PEDRO MIGUEL MACHADO MAGALHÃES

Leiria, Setembro de 2023

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Cibersegurança e Informática Forense

CSE4CI - CYBERSECURITY ECOSYSTEM FOR CRITICAL INFRASTRUCTURES

ESTUDANTE PEDRO MIGUEL MACHADO MAGALHÃES
Número: 2202272

Dissertação realizada sob orientação do Professor Doutor Carlos Manuel Gonçalves Antunes (carlos.antunes@ipleiria.pt) e Professor Doutor Leonel Filipe Simões Santos (leonel.santos@ipleiria.pt).

Leiria, Setembro de 2023

1

INTRODUÇÃO

1.1 PROBLEMA E MOTIVAÇÃO

Com o aumento constante das ameaças cibernéticas e a crescente dependência das organizações em relação à tecnologia, a segurança da informação e a proteção dos ativos digitais tornaram-se preocupações essenciais. Neste contexto, a implementação de uma framework de cibersegurança eficaz é fundamental para garantir a confidencialidade, integridade e disponibilidade das informações, bem como para minimizar os riscos cibernéticos.

Diversas organizações e entidades desenvolveram frameworks de referência que estabelecem diretrizes e boas práticas para a implementação de controlos de segurança. Entre as principais enunciadas destacam-se o CIS CSC v8, COBIT 2019, CSA CCM, ENISA Technical Guideline of Security Measures, ISO 22301:2019, ISO 27001, ISO 27002:2022, ISO 27108:2014, ISO/IEC 27701:2019, ISO 29100, ISO 31000, ISO 31010, NIST Privacy Framework v1.0, NIST 800-37 rev2, NIST 800-53 rev 5, NIST Cybersecurity Framework v1.1 (Abr 19), OSAWP Top 10 v2017, Lei de Proteção de Dados Pessoais, Regulamento relativo à Segurança e à Integridade das Redes e Serviços de Comunicações Eletrónicas e o Regime Jurídico da Segurança do Ciberespaço.

No entanto, a diversidade destas frameworks pode levar a desafios na seleção e implementação dos controlos de segurança adequados. A falta de integração entre as frameworks também pode resultar em lacunas na proteção dos sistemas, além de dificultar a adoção de uma abordagem global e eficiente para a cibersegurança.

1.2 OBJETIVOS E CONTRIBUTOS

Perante estes desafios, esta dissertação visa desenvolver uma framework de cibersegurança integrada que abranja os controlos propostos pelas diversas frameworks mencionadas. A proposta é fornecer às organizações que gerem infraestruturas críticas uma estrutura unificada para a implementação de medidas de segurança, permitindo uma abordagem global e eficaz para proteger os seus ativos digitais.

Considerando as linhas orientadoras apresentadas pelas frameworks reconhecidas na área de cibersegurança o objetivo principal desta dissertação é explorar as diferentes frameworks de cibersegurança mencionadas, identificar as suas áreas de sobreposição e complementaridade, e propor um framework integrada que leve em consideração as melhores práticas e diretrizes de cada uma delas. Através de uma revisão bibliográfica das frameworks selecionadas e uma análise comparativa, pretende-se demonstrar a viabilidade e os benefícios de um framework de cibersegurança unificada.

1.3 ESTRUTURA DO DOCUMENTO

Ao concluir a leitura desta dissertação, o leitor deve obter um conhecimento aprofundado sobre as diversas frameworks de cibersegurança, as suas diretrizes e controlos propostos. Além disso, o leitor deve compreender a importância e os benefícios de um framework de cibersegurança unificada, capaz de simplificar a seleção e implementação de controlos de segurança, fortalecer a resiliência das organizações e proteger os seus ativos digitais contra ameaças cibernéticas cada vez mais sofisticadas.

Neste contexto, esta dissertação está estruturado da seguinte forma: no Capítulo 2, serão apresentados os fundamentos teóricos da cibersegurança nomeadamente uma análise detalhada das frameworks de cibersegurança de referência. O Capítulo 3 abordará a metodologia de pesquisa utilizada para identificar as áreas de sobreposição e complementaridade entre as frameworks e a respetiva apresentação da proposta de framework de cibersegurança, destacando as suas principais características e benefícios. Por fim, no Capítulo 4, discutiremos as conclusões da prova de conceito e as recomendações para a implementação eficaz da framework proposta.

Esta estrutura visa fornecer ao leitor uma visão abrangente e organizada do conteúdo desta dissertação, facilitando a compreensão e a utilização das informações aqui apresentadas.

2

TRABALHO RELACIONADO

Este capítulo tem o intuito de oferecer uma visão alargada e abrangente das diferentes frameworks de referência, amplamente adotadas no cenário de segurança cibernética, como as desenvolvidas por organizações líderes em segurança da informação.

Iremos explorar essas frameworks para entender as suas abordagens, princípios e diretrizes, analisando a forma como as mesmas foram concebidas para abordar os desafios da cibersegurança. Esta análise permitirá uma compreensão aprofundada das frameworks existentes, as suas áreas de atuação e como podem ser aplicadas em organizações que gerem infraestruturas críticas.

Ao longo deste capítulo, serão destacadas as práticas, princípios e abordagens que emergem dessas frameworks, de forma a mapear as necessidades de conformidade com as mesmas.

2.1 NORMA ISO 27001 - INFORMATION SECURITY MANAGEMENT STANDARD

Os sistemas de segurança da informação são frequentemente considerados pelas organizações como simples listas de verificação ou políticas e procedimentos que necessitam de uma atenção redobrada. Normalmente, as organizações evitam construir adequadamente um SGSI (Sistema de Gestão de Segurança da Informação) [1] [2] e atingir todo o potencial, quer seja no desempenho operacional e financeiro, quer seja na reputação da imagem da organização.

Existem vastas frameworks [3] no mercado que permitem ajudar as organizações a lidar com os requisitos globais de segurança e a construção de um Sistema de Gestão de Segurança da informação entre elas a ISO 27001:2013 [4] [5] [6], emitidas pela Organização Internacional de Normalização.

Independentemente de estar acoplado a outro sistema de gestão, como por exemplo a ISO 9001 (Qualidade), ISO 14001 (Meio Ambiente) [7], ou OHSAS 18001 (Saúde e Segurança Operacional), o padrão ISO 27001:2013 fornece orientação e foco incidindo nas funcionalidades de como uma organização, independentemente do seu tamanho e setor, deve gerir a segurança da informação e, com este resultado, lidar com os riscos de segurança da informação. Esta ação pode trazer imensos benefícios, não

apenas para a própria organização, mas também para os clientes, fornecedores e outras partes interessadas.

Mas para as organizações que não estão familiarizadas com os padrões ISO ou conceitos de segurança da informação, a ISO 27001 pode tornar-se bastante confusa e de difícil compreensão sem enquadramento.

2.1.1 *Impacto de Conformidade*

A conformidade com a norma ISO 27001:2013 é obrigatória para obter uma certificação de segurança, mas a conformidade por si só não garante a capacidade de uma organização proteger as suas informações e mitigar possíveis ameaças que possam ocorrer. É necessário criar um vinculo robusto entre requisitos, políticas, objetivos, desempenho e ações. É por esta necessidade que uma abordagem minuciosa ao processo de construção de um SGSI é extremamente útil. A figura 1 apresenta os requisitos necessários para a conformidade com a ISO 27001. Esta demonstra uma abordagem ao processo de forma a que seja possível organizar e gerir os indicadores de segurança da informação para criar um valor acrescentado para a organização e outras partes interessadas.

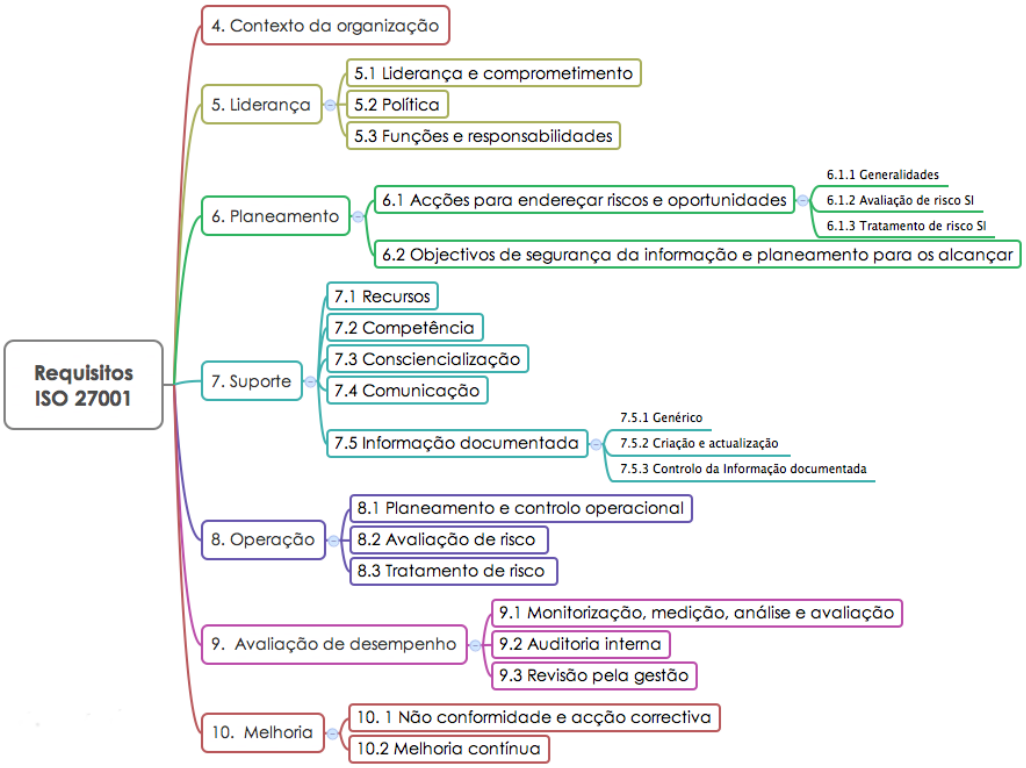

Figura 1: Requisitos da ISO 27001 (Fonte: www.27001.pt)

Assim, ao adotar uma abordagem processual para a gestão da segurança da informação, uma organização pode ter uma visão mais alargada de como cada etapa contribui para os objetivos principais relacionados com a proteção da informação, permitindo identificar rapidamente os pontos problemáticos na execução do processo.

2.1.2 *O ciclo Plan-Do-Check-Act*

Uma vez que qualquer organização está em constante evolução, sofrendo alterações derivado ás influências internas e externas, é necessário que o Sistema de Gestão da Segurança da Informação também seja capaz de se ajustar (por exemplo, a inclusão de objetivos e procedimentos) para acompanhar as mudanças do negócio e permanecer relevante e útil. A norma ISO 27001:2013 garante que esta condição seja alcançada através da adoção de um ciclo "Plan-Do-Check-Act"(PDCA) [8], que é apresentado na figura 2 e que na sua estrutura pode ser descrito da seguinte forma:

- Planear a definição de políticas, objetivos, metas, controlos e procedimentos, bem como a execução da gestão dos riscos que apoiam e disponibilizam a segurança da informação alinhada com o *core business* da organização.
- Executar a implementação e operação dos processos planeados.
- Verificar a monitorização, medição, avaliação e revisão dos resultados em relação à segurança da informação, políticas e objectivos, para que acções correctivas e/ou de melhoria possam ser determinadas e posteriormente autorizadas
- Atuar na realização das ações autorizadas para garantir que a segurança da informação seja entregue e os seus resultados possam ser melhorados.

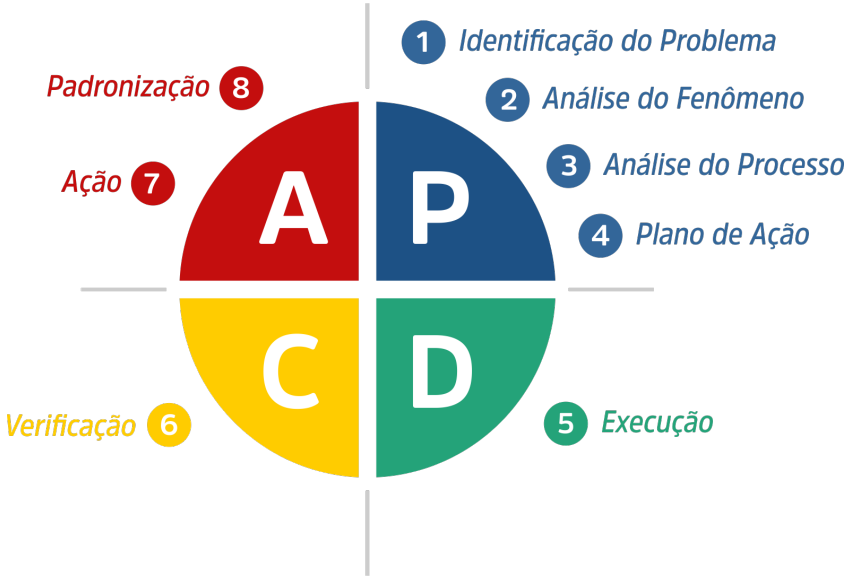

Figura 2: Ciclo PDCA (Fonte: https://www.voitto.com.br/)

É importante referir que o ciclo PDCA é uma metodologia para um sistema de gestão generalizado reconhecida e utilizada em vários sistemas de gestão de negócios, mas a sua utilização é obrigatória e extremamente benéfica dentro da ISO 27001:2013.

2.1.3 *Importância da Norma ISO 27001*

A norma não apenas fornece às empresas o *know-how* necessário para proteger os seus ativos mais valiosos, permitindo também obter a certificação ISO 27001 e dessa forma demonstrar para os seus clientes e parceiros que protege os seus dados de forma eficiente. Por ser um padrão internacional, a ISO 27001 é facilmente reconhecida em todo o mundo, por isso aumenta as oportunidades de negócios quer para as organizações quer para os seus profissionais.

2.1.4 *Como funciona a Norma ISO 27001*

O foco principal da ISO 27001 é proteger a confidencialidade, integridade e disponibilidade das informações de uma organização. Isso é feito descobrindo quais são as potenciais vulnerabilidades dos métodos de gestão da informação (avaliação de risco) e, em seguida, definindo os procedimentos de mitigação dessas respetivas vulnerabilidades (mitigação de risco). Portanto, a principal filosofia da ISO 27001 é baseada num processo de gestão de risco: descobrir onde estão os riscos, e então tratá-los sistematicamente através da implementação de controlos de segurança. A ISO 27001 exige que uma empresa efetue uma lista de todos os controlos que devem

ser implementados num documento denominado de Declaração de Aplicabilidade (*Statement of Applicability*).

2.1.5 *Requisitos da Norma ISO 27001*

Os requisitos obrigatórios da ISO 27001 são definidos nas suas cláusulas 4 a 10, isto significa que todos esses requisitos devem ser implementados numa organização se a mesma quiser estar em conformidade com a norma. Os controlos do Anexo A da ISO 27001 devem ser implementados somente se descritos como aplicáveis na Declaração de Aplicabilidade.

- Cláusula 4 – Contexto da organização

Esta cláusula define os requisitos para a compreensão de problemas externos e internos, partes interessadas e as suas necessidades, define também o objetivo do SGSI.

- Cláusula 5 – Liderança

Define as responsabilidades da administração de topo da organização, definindo as funções e responsabilidades, assim como o conteúdo da Política de Segurança da Informação do nível superior.

- Cláusula 6 – Planeamento

São definidos os requisitos para a avaliação de risco, tratamento de risco, declaração de aplicabilidade, plano de tratamento de risco e definição dos objetivos de segurança da informação na cláusula 6 da ISO 27001.

- Cláusula 7 – Suporte

Define os requisitos de disponibilidade de recursos, competências, comunicação e controlo de documentos e registos.

- Cláusula 8 – Operação

Define a implementação da avaliação e tratamento de riscos, bem como os controlos e outros processos necessários para atingir os objetivos de segurança da informação.

- Cláusula 9 – Avaliação de desempenho

São definidos os requisitos para monitorização, medição, analise, avaliação, auditoria e analise critica pela direção da organização.

- Cláusula 10 – Melhorias

Define os requisitos para não conformidades, correção, ações de correção e inovação de melhorias.

2.1.6 *Domínios da Norma ISO 27001*

Podemos encontrar catorze domínios listados no Anexo A da ISO 27001, organizados em secções A.5 até á A.18. As secções abordam vários parâmetros que serão descritos nos próximos tópicos.

- A.5 – Políticas de Segurança da Informação

Os controlos nesta secção descrevem como lidar com as políticas de segurança da informação.

- A.6 – Organização da Segurança da Informação

Nesta secção os controlos fornecem a estrutura básica para a implementação e operação da segurança da informação, definindo a sua organização interna (por exemplo, funções, responsabilidades e outras), por meio dos aspetos organizacionais da segurança da informação, como a gestão de projetos, o uso de dispositivos móveis e o teletrabalho.

- A.7 – Segurança dos Recursos Humanos

Os controlos nesta secção garantem que as pessoas que estão sobre o controlo da organização sejam contratadas, formadas e geridas de forma segura. Também são referidos os princípios de ação disciplinar e rescisão dos acordos estabelecidos.

- A.8 – Gestão de Ativos

Aqui, garantindo que, através dos controlos, os ativos de segurança da informação (por exemplo, informações, dispositivos de processamento, dispositivos de armazenamento, e outros) sejam identificados, que as responsabilidades pela sua segurança sejam designadas e que as pessoas tenham conhecimento de como lidar com eles de acordo com os níveis de classificação predefinidos.

- A.9 – Controlo de Acesso

Os controlos nesta secção limitam o acesso a informações e ativos de informação de acordo com as necessidades reais da organização. Estes controlos são tanto para acesso físico como acesso lógico.

- A.10 – Criptografia

Nesta secção os controlos fornecem a base para o uso adequado de soluções de criptografia para proteger a confidencialidade, autenticidade e/ou integridade das informações.

- A.11 – Segurança Física e Ambiental

Os controlos neste parâmetro evitam o acesso não autorizado a áreas físicas e protegem os equipamentos e instalações de serem comprometidos por intervenção humana ou natural.

- A.12 – Segurança de Operações

Nesta secção são descritos os controlos que os sistemas de TI [9], incluindo sistemas operativos e software, necessitam para estarem seguros e protegidos contra a perda de dados. Além disso, os controlos nesta secção requerem meios para registar eventos e gerar evidências, verificações periódicas de vulnerabilidades e tomar precauções para evitar que as atividades de auditoria afetem as operações.

- A.13 – Segurança das Comunicações

Neste parâmetro os controlos protegem a infraestrutura e os serviços de rede, bem como as informações que passam por estes meios.

- A.14 – Aquisição, Desenvolvimento e Manutenção do Sistema

Os controlos nesta secção garantem que a segurança da informação seja levada em consideração quer nos cadernos de encargos para futuras aquisições de sistemas e/ou soluções tecnológicas, quer nos processos de atualização dos existentes.

- A.15 – Relacionamento com Fornecedores

É referido que os controlos garantem que as atividades terceirizadas que sejam realizadas por fornecedores ou parceiros também usem controlos de segurança da informação apropriados e que descrevam como monitorizar o desempenho da segurança de terceiros.

- A.16 – Gestão de Incidentes de Segurança da Informação

Os controlos nesta secção fornecem uma estrutura para garantir a comunicação e o tratamento adequado de eventos e incidentes de segurança, para que possam ser resolvidos em tempo útil. Eles também definem como se devem preservar as evidências, bem como aprender com os incidentes para prevenir a sua recorrência.

- A.17 – Aspetos de Segurança da Informação e Continuidade de Negócio

É descrito nesta secção os controlos que garantem a continuidade da gestão de segurança da informação durante interrupções de funcionamento e a disponibilidade dos mesmos.

- A.18 – Conformidade

Os controlos nesta secção fornecem uma estrutura para prevenir as violações legais, estatais, regulamentares e contratuais, auditar se a segurança da informação está implementada e é eficaz de acordo com as políticas, procedimentos e requisitos definidos na norma ISO 27001.

2.1.7 *Documentos importantes para a ISO 27001*

A ISO 27001 especifica um conjunto mínimo de políticas, procedimentos, planos, registos e outro tipo de informações importantes para que se torne compatível.

A ISO 27001 requere os seguintes documentos preenchidos:

- Âmbito do SGSI (clausula 4.3)
- Política e Objetivos de Segurança da Informação (clausula 5.2 e 6.2)
- Avaliação de Risco e Metodologia de Tratamento de Risco (clausula 6.1.2)
- Declaração de Aplicabilidade (6.1.3)
- Plano de Tratamento de Risco (clausula 6.1.3 e 6.2)
- Relatório de Avaliação de Risco (clausula 8.2)
- Definição de Funções e Responsabilidades de Segurança (controlos A.7.1.2 e A.13.2.4)
- Inventário de Ativos (controlo A.8.1.1)
- Uso Aceitável de Ativos (controlo A.8.1.3)
- Política de Controlo de Acesso (controlo A.9.1.1)
- Procedimentos Operacionais para a Gestão de TI (controlo A.12.1.1)
- Princípios de Engenharia de um Sistema Seguro (controlo A.14.2.5)
- Políticas de Segurança do Fornecedor (controlo A.15.1.1)
- Procedimento de Gestão de Incidentes (controlo A.16.1.5)
- Procedimentos de Continuidade de Negócios (controlo A.17.1.2)
- Requisitos Governamentais, Regulamentares e Contratuais (controlo A.18.1.1)

Para além dos documentos que têm de estar preenchidos, a norma ISO 27001 define como obrigatórios os seguintes registos:

- Registo de aprendizagem, habilidades, experiência e qualificações (clausula 7.2)
- Resultados de Monitorização e Medição (clausula 9.2)

- Programa de Auditoria Interna (clausula 9.2)
- Resultados da Análise Critica da Gestão (clausula 9.3)
- Resultados das Ações Corretivas (clausula 10.1)
- Registos de Atividade do Utilizador, Exceções e Eventos de Segurança (controlos A.12.4.1 e A.12.4.3)

2.1.8 *Norma ISO 27002*

Assim como a parte governamental e a gestão de risco, a gestão de segurança da informação é um tópico amplo com ramificações em todas as organizações. A segurança da informação, e, portanto, ISO/IEC 27002 [10], é relevante para todo o tipo de organizações, incluindo empresas comerciais de variados tamanhos, organizações sem fins lucrativos, instituições de caridade, departamentos do governo e qualquer tipo de organização autónoma que depende de informações. Os requisitos específicos de risco e controlo de informações podem diferir em detalhes, mas existem muitos pontos em comum, por exemplo, a maioria das organizações necessita de abordar os riscos de informações relativamente aos funcionários, além dos contratados, consultores e fornecedores externos de serviços de informação. A norma foca-se na segurança da informação, ou seja, a segurança de todas as formas de informação (por exemplo, dados do computador, documentação, conhecimento e propriedade intelectual).

2.1.9 *Estrutura e formato da Norma ISO 27002*

A ISO/IEC 27002 é um código de práticas, em suma um documento para consulta genérico, não é uma especificação formal como a ISO 27001. Ele recomenda que exista controlo relativamente á segurança da informação e que sejam abordados os objetivos sobre o controlo de segurança da informação decorrentes de riscos relativamente à confidencialidade, integridade e disponibilidade da informação. O padrão é estruturado logicamente em torno de grupos de controlos de segurança interligados. Muitos controlos poderiam ter sido colocados em várias secções, mas, para evitar a duplicação e conflitos, eles foram arbitrariamente atribuídos a uma secção ou através de referência cruzada de outro local. Por exemplo, um sistema de controlo de acesso por cartão numa sala com um computador ou cofre pode ser tanto um *access-control*, como um controlo físico que envolve tecnologia, a sua gestão ou administração, procedimentos e políticas de uso associadas.

2.1.10 *Conteúdo da Norma ISO 27002*

Com mais detalhe, de seguida será apresentada uma análise resumida das dezanove secções ou capítulos da norma atual ISO 27002. Nafigura 3 podemos verificar os títulos do conteúdo da ISO 27002, nomeadamente os controlos do Anexo A.

Figura 3: Controlos Anexo A, ISO 27002 (Fonte: https://www.27001.pt/)

- Secção 0 – Introdução

Esta secção descreve o histórico e menciona as três origens dos requisitos de segurança da informação. É possível observar que a norma oferece orientações genéricas e potencialmente incompletas que devem ser interpretadas no contexto da organização. Menciona também os ciclos de vida de um sistema de informação.

- Secção 1 – Finalidade

A norma fornece recomendações para as pessoas que são responsáveis por selecionar, implementar e gerir a segurança da informação. Esta norma pode ser ou não utilizada para apoiar um SGSI que está explicito na ISO/IEC 27001 apresentada anteriormente.

- Secção 2 – Referências Normativas

A ISO/IEC 27000 é a única norma considerada absolutamente indispensável para o uso da ISO/IEC 27002. No entanto, são várias as outras normas referenciadas na ISO/IEC 27002.

- Secção 3 – Estrutura da Norma

Neste momento, todos os termos e definições específicos estão definidos na ISO/IEC 27000 e a maioria aplica-se a toda a família de normas ISO27k.

- Secção 4 – Termos e Definições

Em relação à cláusula de controlo de segurança, existem 21 secções ou capítulos da norma. Destas, 14 especificam os objetivos de controlo e indicando o nome de cláusulas de controlo de segurança. Existe uma estrutura padrão dentro de cada cláusula de controlo, uma ou mais subsecções de primeiro nível, cada uma incidindo num objetivo de controlo e cada objetivo de controlo é apoiado, por sua vez, por um ou mais controlos declarados. Cada controlo segue a orientação de implementação associada e, em alguns casos, notas explicativas adicionais.

A quantidade de objetivos de controlo tem o valor de 35, ou seja, a ISO/IEC 27002 especifica cerca de 35 objetivos de controlo (um por cada categoria de controlo de segurança) sobre a necessidade de proteger a confidencialidade, integridade e disponibilidade da informação. Os objetivos de controlo estão num nível bastante alto e, na verdade, compreendem uma especificação de requisitos funcionais genéricos para a arquitetura da gestão de segurança da informação de uma organização. É importante referir que poucos profissionais iriam contestar seriamente a validade dos objetivos de controlo ou, dito por outra forma, seria difícil argumentar que uma organização não precisa de satisfazer os objetivos de controlo declarados na generalidade. No entanto, alguns objetivos de controlo não são aplicáveis em todos as situações e a sua formulação genérica é sobretudo improvável que reflita os requisitos

precisos de cada organização, especialmente dada a ampla gama de organizações e setores aos quais o padrão se aplica. É por isso que a ISO/IEC 27001 requer o SoA (*Statement of Applicability*) para estabelecer de forma inequívoca quais os controlos de segurança que são ou não exigidos pela organização, bem como o seu estado de implementação.

Cada um dos objetivos de controlo é suportado por, pelo menos, um dos controlos, perfazendo assim, um total de 114 controlos. No entanto, o número é um pouco enganador, uma vez que a orientação de implementação recomenda ter vários controlos reais inseridos nos detalhes. O objetivo do controlo que incide na subsecção 9.4.2 "*Secure log-on procedure*s"(ou procedimentos de autenticação seguros) pode ser, por exemplo, suportado pelas seguintes verificações:

- Escolher, implementar e utilizar técnicas de autenticação adequadas;
- Não divulgar informações confidencias no momento do *login*;
- Validação de entrada de dados;
- Proteção contra ataques de força bruta (*brute force*);
- Não transmitir palavras-passe pela rede;
- Tempo limite de inatividade em cada sessão;
- Restrições de tempo de acesso.

Para além dos controlos listados, podem ser utilizados outros, como políticas e procedimentos, conscientização e treino, avaliação de conformidade e aplicação, supervisão, garantia, entre outros.

Podemos argumentar que a ISO/IEC 27002 recomenda literalmente centenas de controlos distintos de segurança da informação, embora alguns ofereçam suporte a objetivos de controlo variados, ou seja, alguns controlos têm diversos propósitos. Além disso, o texto completo da norma afirma claramente ou implica que este não é um conjunto totalmente abrangente. Uma organização pode ter objetivos de controlo de segurança da informação ligeiramente diferentes ou completamente novos, exigindo assim outros controlos nesse lugar ou além daqueles declarados na norma. Uma sala de cirurgia de um hospital, por exemplo, não é o lugar ideal para se estar a alterar constantemente os métodos de autenticação, palavras-passe e todos esses métodos de proteção. Os riscos e a segurança da informação dependem muito do contexto onde estamos a colocar o nosso foco. De entre estas secções, destacam-se:

- Secção 5 – Políticas de Segurança da Informação

É importante que a administração da organização defina um conjunto de políticas e suporte para esclarecer todas as pessoas que estejam diretamente ligadas á

segurança da informação naquele local. No nível superior, deve existir uma política de segurança da informação generalizada, conforme especificado na ISO/IEC 27001 secção 5.2.

- Secção 6 – Organização da Segurança da Informação

Na gestão interna, a organização deve definir as funções e responsabilidades pela segurança da informação e distribuí-las às pessoas mais indicadas nessa área. Quando for relevante, as funções devem ser segregadas entre as mesmas e entre as pessoas responsáveis para evitar conflitos de interesse e atividades inadequadas. Deve existir contacto com autoridades externas relevantes. A segurança da informação deve ser parte integrante da gestão de todos os tipos do projeto. Em relação aos dispositivos móveis e teletrabalho, deve haver políticas e controlos de segurança para dispositivos móveis (como *laptops*, *tablets*, dispositivos IoT [11], *smartphones*, dispositivos USB e outros) e teletrabalho (trabalho em casa ou remoto).

- Secção 7 – Segurança de Recursos Humanos

Antes do recrutamento para o emprego, as responsabilidades de segurança da informação devem ser levadas em consideração ao recrutar novos colaboradores permanentemente ou temporariamente. Para efetuar esta ação, por exemplo podemos elaborar descrições de emprego mais sucintas, triagens na pré-contratação e incluir todos os requisitos de segurança necessários nos termos e condições do contrato, ou outros acordos assinados, definindo com isto funções, responsabilidades de segurança e obrigações de conformidade. Ao longo do desempenho das funções no emprego, os aspetos de segurança da saída de uma pessoa da organização ou mudanças significativas de funções dentro dela, devem ser geridos de forma a que seja possível devolver informações corporativas e equipamentos que estejam em sua posse. Contudo, também é necessário atualizar os seus direitos de acesso e relembrar os mesmos das suas obrigações continuas em relação à privacidade e propriedade intelectual.

- Secção 8 – Gestão de Ativos

Na responsabilidade pelos ativos da organização, estes devem ser inventariados e os proprietários identificados para serem responsáveis pela sua segurança. As políticas de uso aceitável (*Acceptable use*) devem ser definidas e os ativos devem ser devolvidos quando as pessoas abandonarem a organização ou alterarem funções que assim o obriguem. Em relação á classificação da informação, esta devem ser classificada e rotulada pelos seus proprietários de acordo com a proteção de segurança que seja necessária e as mesmas devem ser tratadas de forma adequada. Ao utilizar ferramentas de media, os meios de armazenamento de informações devem ser geridos, controlados, movidos ou descartados de forma a que o conteúdo da informação não seja comprometido.

- Secção 9 – Controlo de Acesso

Nos requisitos comerciais de controlo de acesso, estes são necessários para controlar o acesso aos ativos de informação e que sejam claramente documentados numa política e procedimentos de controlo de acesso. O acesso à rede e às interligações devem ser restritos. Na gestão de acesso do utilizador, a atribuição de direitos de acesso deve ser controlada desde o registo inicial do utilizador até á eliminação do direito de acesso quando forem sobretudo não mais necessários. Devem-se incluir restrições especiais para os direitos de acesso privilegiado e para a gestão de palavras-passe, além de análises regulares às atualizações de direitos de acesso ao sistema. As responsabilidades do utilizador indicam que estes devem estar cientes das suas obrigações em manter os controlos de acesso eficazes. Escolher palavras-passe fortes e guardar as mesmas de forma confidencial. Na área dos sistemas e controlo de acesso das aplicações, o acesso ás informações deve ser restrito de acordo com as políticas de controlo de acesso. Por exemplo por meio de autenticação segura, gestão de palavras-passe, controlo sobre utilitários que tenham privilégios e acesso restrito ao código fonte do programa.

- Secção 10 – Criptografia

Nos controlos criptográficos, deve existir uma política relacionada com o uso de criptografia, além da autenticação criptográfica e controlos de integridade. Como exemplo, temos assinaturas digitais e códigos de autenticação de mensagens e gestão de chaves criptográficas.

- Secção 11 – Segurança Física e de Infraestruturas

Ao nível das infraestruturas ou perímetros físicos, estes devem ser definidos com controlos de entrada física e procedimentos de controlo. Devem proteger as instalações, escritórios, salas, áreas de entregas ou carregamentos contra o acesso não autorizado. É importante procurar aconselhamento especializado em relação á proteção contra incêndios, inundações, terramotos ou, até mesmo, ataques terroristas. Em relação aos equipamentos, nomeadamente equipamentos de TI e utilitários de suporte dos mesmos, estes devem ser protegidos e bem conservados. Equipamentos e a informação não devem ser levados para fora das instalações, a menos que seja autorizado, no entanto devem ser protegidos adequadamente quer estejam dentro ou fora das instalações. A informação deve ser destruída antes dos equipamentos de armazenamento serem descartados ou reutilizados.

- Secção 12 – Operações de Segurança

Em relação aos procedimentos operacionais e as suas responsabilidades, estes devem ser bem documentados e descritos. As mudanças nas instalações e sistemas de TI devem ser controladas. A capacidade e desempenho devem ser bem geridos,

os sistemas de desenvolvimento e de testes operacionais devem estar separados. Na proteção contra malware [12] [13], são necessários controlos dos mesmos, incluindo a conscientização do utilizador. As cópias de segurança (*backups*) devem ser feitos de forma apropriada e mantidos de acordo com uma política de *backup*. No registo e monitorização das atividades do utilizador do sistema e do administrador/operador, verificamos que exceções, falhas e eventos de segurança da informação devem ser registados e protegidos. É importante que os relógios sejam sincronizados. O controlo de *software* [14] operacional foca-se na instalação de software em sistemas operativos e estes devem ser controlados. Na gestão de vulnerabilidades técnicas, estas devem ser corrigidas e devem existir regras em vigor que administrem a instalação de *software* pelos utilizadores. As considerações de auditoria aos sistemas de informação devem ser planeadas e controladas para minimizar os efeitos adversos nos sistemas de produção ou o acesso inadequado aos dados.

- Secção 13 – Comunicações Seguras

Em relação á gestão da segurança de redes, as redes e serviços devem ser protegidos. Como exemplo, podemos verificar a proteção por segregação. Ao nível das transferências de informações devem existir políticas, procedimentos e acordos (por exemplo acordos de não divulgação) relativos á transferência de informações de ou para terceiros, incluindo mensagens eletrónicas.

- Secção 14 – Aquisição, Desenvolvimento e Manutenção do Sistema

Os requisitos de segurança da informação indicam que convém que estes requisitos de controlo de segurança sejam analisados e especificados, incluindo aplicações e transações na *WEB*. A segurança no processo de desenvolvimento e suporte foca- se nas regras que regem o desenvolvimento de *software*/sistemas seguros que devem ser definidos como uma política. As alterações nos sistemas (aplicações e sistemas operativos) devem ser controladas. Idealmente, os pacotes de *software* não devem ser modificados e os princípios de engenharia de um sistema seguro devem ser considerados. O ambiente de desenvolvimento deve ser protegido e o desenvolvimento terceirizado deve ser controlado. A segurança do sistema deve ser testada e os critérios de aceitação definidos para incluir os aspetos de segurança. Na área de testes de dados, os dados devem ser cuidadosamente selecionados ou gerados e, por fim, controlados.

- Secção 15 – Relação com Fornecedores

Na parte da segurança da informação na relação com fornecedores devem existir políticas, procedimentos, conscientização para proteger as informações da organização que são acessíveis aos terceirizados na área de TI e outros fornecedores externos que estejam presentes na cadeia de abastecimento, acordados nos contratos ou nos acordos. A gestão de entrega de serviços do fornecedor, indica que esta entrega de

serviços por fornecedores externos deve ser monitorizada e revista/auditada em foco nos contratos/acordos. As mudanças de serviço devem ser controladas, é importante referir que o mesmo ponto se aplica a serviços prestados por fornecedores internos.

- Secção 16 – Gestão de Incidentes

Nesta secção apenas existe a subsecção referente á gestão de incidentes e melhorias de segurança da informação. Esta subsecção refere que devem existir responsabilidades e procedimentos para gerir (relatar, avaliar, responder e aprender) eventos, incidentes e fragilidades de segurança da informação de forma consistente e eficaz, com o objetivo de adquirir evidências forenses.

- Secção 17 – Aspetos de Segurança da Informação e Gestão da Continuidade de Negócio

Na área de continuidade da segurança da informação esta deve ser planeada, implementada e revista como parte integrante dos sistemas de gestão da continuidade de negócios da organização. Em relação ás redundâncias, as instalações de TI devem ter redundância suficiente para satisfazer os requisitos de disponibilidade.

- Secção 18 – Conformidade

A conformidade com os requisitos legais e contratuais é importante, a organização deve identificar e documentar as suas obrigações com autoridades externas e outros em relação á segurança da informação. Deve ser incluído a propriedade intelectual, registos, privacidade/informação de identificação pessoal e criptografia. A revisão de segurança da informação indica que as alterações de segurança da informação na organização devem ser analisadas de forma independente e reportadas aos seus superiores. Estes superiores também devem rever regularmente a conformidade dos seus funcionários e sistemas com as políticas de segurança, procedimentos e outros. É importante iniciar ações corretivas quando necessário.

2.1.11 *Implementação de um SGSI*

As organizações podem beneficiar significativamente com a implementação de um SGSI, podendo assim alcançar a conformidade com a ISO 27001 e ISO 27002 [15]. Com isto, é possível não só garantir a segurança dos ativos de informação, mas também uma implementação completa, assim como um processo de formação, ambos necessários para tirar partido de todos os benefícios proporcionados por um SGSI. De seguida, apresentam-se os principais passos para a implementação de um SGSI.

- Passo 1 – Identificação e Avaliação de Ativos

O primeiro passo para implementar um SGSI é identificar os ativos que devem ser protegidos e determinar o seu valor relativo para a organização. É importante relembrar que um SGSI baseado em risco leva em consideração a importância relativa de diferentes tipos de dados e dispositivos e com isto os protege adequadamente. Neste passo, as organizações adquirem dados da documentação para identificar os ativos de TI críticos para os negócios e a sua importância relativamente á organização.

É importante que as organizações criem uma Declaração de Sensibilidade (*SoS – Statement of Sensitivity*) que atribua uma classificação a cada um dos ativos de TI em três dimensões distintas (confidencialidade, integridade e disponibilidade) como apresentado de seguida:

- Confidencialidade – garantia que as informações estejam acessíveis exclusivamente ás pessoas autorizadas;
- Integridade – garante que as informações a serem protegidas sejam precisas e completas, e que as informações e métodos de processamento possam ser protegidos;
- Disponibilidade – aqui é possível garantir que as pessoas autorizadas tenham acesso ás informações e ativos seguros quando necessário, bem como os métodos e metodologias corretas de o fazer.

As organizações devem encontrar um equilíbrio entre proteger os ativos e torná-los acessíveis a pessoas autorizadas que podem precisar dos dados para efetuar o seu trabalho.

- Passo 2 – Efetuar uma Avaliação de Risco

Uma vez que a identificação e avaliação de ativos foi concluída e a organização formulou um SoS , é altura de efetuar uma avaliação de risco detalhada que irá formar a produção do SGSI. Uma análise de avaliação de risco inclui quatro etapas importantes para determinar como os ativos de TI devem ser protegidos, essas etapas são enunciadas da seguinte forma:

- Ameaças – a organização deve analisar as ameaças a cada um dos ativos ao documentar quaisquer eventos indesejados que possam resultar em uso indevido ou acidental, perda ou dano nos ativos.
- Vulnerabilidades – as ameaças são uma descrição concreta do que pode acontecer, e as vulnerabilidades são uma medida de quão suscetível o ativo de TI pode ser ás ameaças identificadas na primeira parte da análise. Aqui é feita a diferenciação entre os diferentes tipos de ativos, embora um ataque de *software* malicioso seja uma ameaça para servidores, computadores ou *smartphones*, podemos indicar neste ponto que os *smartphones* são mais vulneráveis á ame-

aça porque podem ser utilizados remotamente e ainda conectados a várias redes externas.

- Impacto e probabilidade – A organização nesta área pode avaliar a probabilidade de certo tipo de violações ocorrerem num conjunto com a magnitude do potencial dano que pode ser causado através desta violação de dados. As organizações podem utilizar uma análise de custo-benefício para ajudá-las a visar as violações que sejam potencialmente mais prejudiciais.
- Mitigação – Por fim, a organização propõe um conjunto de métodos, técnicas e metodologias para minimizar as ameaças, vulnerabilidades e impactos reconhecidos por meio das políticas e procedimentos no SGSI.
- Passo 3 – Estabelecer o SGSI

Agora que a organização identificou os ativos a serem protegidos e conduziu uma avaliação de risco completa, esta pode avançar para a fase seguinte e definir as políticas e procedimentos reais que compõem o SGSI. As organizações devem estabelecer o SGSI em conformidade com a ISO 27001 e a ISO 27002 se desejam obter uma certificação relacionada com as melhores práticas em gestão da segurança de informação.

Um exemplo a assinalar é o caso dos equipamentos móveis pedidos ou extraviados. Esta situação deve ser reportada ao departamento de TI, num prazo máximo de 8 horas, como especificado nos documentos das normas de segurança. A equipa de TI deve ter capacidade de monitorizar, apagar ou inutilizar remotamente o acesso à informação ou dados de um equipamento móvel que seja propriedade da empresa. É importante que por exemplo um *smartphone* seja protegido por uma autenticação biométrica, reconhecimento facial ou leitura de retina entre outras formas de autenticação.

Este conjunto de políticas e procedimentos minimiza a possibilidade de que uma violação de dados aconteça caso exista uma perda do equipamento. A exigência de uma autenticação biométrica aumenta significativamente o nível de sofisticação necessária para obter o acesso não autorizado. Os requisitos do relatório introduzem responsabilidade adicional ao utilizador do equipamento e a equipa de TI, com vista a dispor de capacidade de remover ou impedir o acesso aos dados confidenciais de qualquer equipamento que esteja em falta.

2.2 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - CYBERSECURITY FRAMEWORK(NIST CSF)

O *National Institute of Standards and Technology* desenvolveu uma metodologia de segurança no âmbito dos sistemas de informação conhecida como "The Framework for Improving Critical Infrastructure Cybersecurity"[16], para fortalecer a segurança de infraestruturas críticas. O objetivo da NIST é estabelecer um conjunto comum de padrões, objetivos e tipos de linguagem para aumentar a segurança da informação e melhorar a capacidade de remediar e mitigar possíveis ataques informáticos. Uma abordagem comum permite capacitar melhor as equipas de segurança de informação nas decisões a tomar. Qualquer organização que tenha uma metodologia semelhante nos vários setores enquadra todos os processos de mitigação e erradicação de ataques informáticos como, por exemplo, esquemas de phishing e *ransomware*.

Esta metodologia foi lançada em 2014 sobre a ordem executiva do presidente Barack Obama e atualizada em 2018, a NIST CSF tornou-se um recurso inestimável na gestão de risco para organizações do setor privado e do setor público.

A NIST CSF foca-se em 3 tipos de componentes, os componentes fundamentais da sua estrutura, camadas de implementação e perfis. Os componentes principais são divididos em 5 áreas de segurança informática:Identificar, Proteger, Detectar, Responder e Recuperar.

Cada uma destas áreas inclui atividades de nível inferior para mitigar os riscos de segurança informática e são divididas em categorias e subcategorias, que incluem descrições das principais práticas de segurança da informação e planos de resposta a incidentes, bem como métodos para obter uma recuperação de ataques bem-sucedida, como por exemplo ataques de *ransomware* [17].

2.2.1 *As Cinco Principais Funções - NIST CSF (Cybersecurity Framework)*

A Framework da NIST focada na segurança informática (NIST CSF), permite aumentar a resiliência das infraestruturas críticas e a sua ciberdefesa. Esta *framework* consiste em três principais componentes: camadas de implementação, núcleo da estrutura e o respetivo perfil da estrutura.

A estrutura central do documento identifica cinco funções sobre a segurança da informação. Cada função compreende várias categorias, 23 no total, que por sua vez incluem 108 categorias que permitem mapear requisitos e controlos a serem cumpridos, bem como referências informativas. É importante referir que a NIST CSF não se destina a ser uma estrutura única para todo o tipo de organizações.

Cada organização deve decidir quais as funções, categorias e subcategorias que irá cumprir. As funções, com as suas respetivas categorias e subcategorias, são:

1. Identificar
    a) Gestão de Ativos (ID.AM)
        i. A organização identifica os dados, pessoais, dispositivos, sistemas e instalações necessárias para os seus serviços no âmbito de negócios críticos.
        ii. A organização prioriza esses ativos com base na sua criticidade e a respetiva estratégia de risco da empresa.
        iii. A organização gere os seus ativos de acordo com a prioridade definida. Esta ação significa que a organização atingiu os seguintes objetivos:
            A. Inventário de ativos, constituído por todos os equipamentos físicos;
            B. Identificação de todas as plataformas de *software* e aplicações;
            C. Mapear os fluxos de comunicação e acesso a dados;
            D. Registo dos sistemas de informação externos;
            E. Priorizar os recursos (*hardware*, dados, tempo, pessoal e *software*) de acordo com a classificação, nível de importância (criticidade) e valor comercial;
            F. Estabelece as funções e responsabilidades de segurança informática em toda a organização e para as todas as partes externas intervenientes(fornecedores, clientes, parceiros).
    b) Ambiente do Negócio (ID.BE)
        i. Ás equipas é dado o conhecimento das suas responsabilidades, os objetivos, as partes interessadas e as atividades da organização, conforme identificado na política;
        ii. As equipas utilizam essas informações para relatar as acções, responsabilidades e decisões de gestão dos riscos de segurança informática. após este passo significa que estão identificados os seguintes tópicos:
            A. Identificação e comunicação do papel da organização no setor onde está inserida;
            B. Identificação e comunicação da organização como infraestrutura crítica referente ao seu setor de indústria;
            C. Estabelecer e comunicar as prioridades para a missão, objetivos de negócio e atividades;

D. Mapear as dependências e as funções críticas para a entrega de serviços críticos;

E. Estabelecer requisitos de resiliência para apoiar a entrega de serviços críticos durante as operações diárias, bem como durante um ataque ou sob coação e durante a recuperação

c) Governança (ID.GV)

Os gestores de risco de cibersegurança de uma organização conhecem, compreendem e utilizam as políticas, procedimentos e processos de segurança para gerir e monitorizar os requisitos regulatórios, legais, ambientais e operacionais da organização.

i. As equipas compreendem as suas responsabilidades, os objetivos, as partes interessadas e as atividades da organização, conforme identificado;

ii. As equipas utilizam essas informações para relatar as funções, responsabilidades e decisões de gestão dos riscos de segurança informática. Desta forma estão identificados os seguintes tópicos:

A. Política de Segurança Informática da organização deve ser estabelecida e comunicada;

B. As funções e responsabilidades de segurança informática devem ser coordenadas e alinhadas quer internamente quer com parceiros externos;

C. Os requisitios legais e regulamentares relativos à segurança informática, incluindo obrigações de privacidade são compreendidas e geridas;

D. Endereçamento dos processos de governança e gestão de riscos de cibersegurança.

d) Avaliação de Risco (ID.RA)

i. A organização entende o risco de segurança informática para as suas operações (incluindo a missão, funções, imagem ou reputação), ativos e pessoas.

A. Foram identificadas e documentadas as vulnerabilidades nos ativos;

B. Obtenção de inteligência sobre ameaças informáticas em fóruns e fontes de partilha de informações externas;

C. Identificação e documentação do ambiente no âmbito das ameaças informáticas, que são os vetores de ataque internos ou externos;

D. Identificação dos potenciais impactos de riscos e ameaças nos negócios da organização, bem como a probabilidade da sua ocorrência;

E. Determinar o risco geral com foco nas vulnerabilidades, ameaças e probabilidades anteriormente identificadas;

F. Identificação e priorização da resposta aos riscos.

e) Estratégia de Gestão do Risco (ID.RM)

i. A organização estabelece as suas prioridades, restrições, tolerâncias de risco e suposições utilizando as mesmas para apoiar em decisões finais no âmbito do risco operacional.

A. Foi estabelecido e gerido ativamente um processo de gestão de risco, com o acordo das partes interessadas;

B. Determinação clara da tolerância ao risco da organização;

C. A empresa ao determinar a tolerância ao risco, considerou o papel da empresa na categoria de infraestrutura crítica e considerou as análises de risco do setor onde está inserida.

f) Gestão de Risco na Cadeia de Abastecimento (ID.SC)

i. A empresa definiu prioridades, restrições, tolerâncias de risco e suposições e também definiu processos para identificar, avaliar e gerir os riscos referentes à cadeia de abastecimento.

A. Estabelecer, identificar e avaliar processos de gestão de risco na cadeia de abastecimento e gerir as mesmas com o acordo das partes interessadas.

B. Identificar, priorizar e avaliar os fornecedores e parceiros com foco nos sistemas de informação, componentes e serviços utilizados no processo de avaliação de risco da cadeia de abastecimento.

C. Utilização de contratos com fornecedores e parceiros para ajudar a cumprir os objetivos do programa de segurança informático da empresa e também da sua gestão da cadeia de fornecimento.

D. Avaliações de rotina aos fornecedores e parceiros, por exemplo através de auditorias, resultados de testes ou outro tipo de avaliações que permitam confirmar se estes cumprem as suas obrigações contratuais.

E. Planeamento e testes dos procedimentos de resposta e recuperação em conjunto com os fornecedores e parceiros.

2. Proteger

a) Gestão de Identidade, Autenticação e Controlo de Acessos (PR.AC)

   i. Apenas os utilizadores, processo e dispositivos autorizados podem obter acesso aos ativos físicos e lógicos e as respetivas instalações associadas. Como é gerido o acesso depende dos riscos associados ao acesso não autorizado.

      A. Emitir, gerir, verificar, revogar e auditar as entidades e credenciais para os dispositivos, utilizadores e processos autorizados;

      B. Gerir e proteger o acesso físico aos ativos;

      C. Gerir o acesso remoto;

      D. Gerir as permissões de acesso a contas de utilizadores com privilégios administrativos utilizando a norma de menor privilégio necessário para efetuar o trabalha segregando funções;

      E. Proteger a integridade da rede utilizando meios como a segregação e segmentação da rede, bem como a utilização de *software* de proteção contra vírus e *backups* de dados;

      F. Elucidar e vincular identidades a credencias singulares, permitindo que estas sejam confirmadas num conjunto de iterações;

      G. Autenticação dos utilizadores, dispositivos e outros ativos proporcionais ao risco de cada alteração.

b) Consciencialização e Treino (PR.AT)

   i. Os parceiros da organização recebem instruções sobre a consciencialização relacionada com a segurança informática e são instruídos para desempenhar as suas funções e responsabilidades com foco nas tecnologias de informação de acordo com as políticas,procedimentos e acordos efetuados com ambas as partes.

      A. Os utilizadores são informados e treinados no âmbito da segurança da informação;

      B. Os utilizadores privilegiados compreendem as suas funções e responsabilidades;

      C. As partes interessadas (por exemplo fornecedores, clientes e parceiros) compreendem as suas funções e responsabilidades.

      D. A administração, mais propriamente os executivos seniores compreendem as suas funções e responsabilidades.

      E. Os colaboradores da área de segurança física e de segurança informática compreendem as suas funções e responsabilidades.

c) Segurança de Dados (PR.DS)

i. A organização deve gerir os dados de acordo com a sua estratégia de risco para proteger a confidencialidade, integridade e disponibilidade das informações.

A. Os dados armazenados deverão estar protegidos contra acessos indevidos;

B. Os dados devem ser protegidos durante a sua transferência;

C. A organização deve gerir os ativos conforme a sua alteração e/ou eliminação;

D. A organização deve manter uma capacidade de armazenamento adequada para garantir que os seus dados estejam sempre disponíveis.

E. Existe proteção contra perdas de dados e planos estabelecidos para a recuperação dos mesmos;

F. A organização verifica o *software*, o *firmware* e a integridade da informação.

G. Os ambientes da empresa no âmbito do desenvolvimento e testes devem ser separados do ambiente de produção

d) Processos e Procedimentos de Proteção de Informações (PR.IP)

i. A organização deve utilizar políticas de segurança que tratam o âmbito, funções, responsabilidades e compromisso na gestão da coordenação organizacional, incluindo processos e procedimentos que permitam a proteção de sistemas e ativos de informação.

A. A empresa tem uma configuração básica referente á tecnologia de informação / sistemas de controlo industriais que incorporem os princípios de segurança (o conceito de menor funcionalidade);

B. A organização deve ter um ciclo de vida de desenvolvimento de sistemas para gerir os mesmos de forma correta;

C. Existência de processos para o controlo de alterações nas configurações dos sistemas;

D. São executados e mantidos backups de informações com regularidade;

E. O ambiente funcional físico para os ativos da organização devem atender ás políticas e regulamentos em vigor;

F. A organização destrói os dados de acordo com as políticas anteriormente definidas;

G. São melhorados ou adequados os processos relativos à proteção de dados sempre que se verificar a sua necessidade;

H. A empresa deve partilhar a eficácia das tecnologias inerentes à proteção dos sistemas de informação;

I. Existência de planos de resposta e recuperação que a organização gere;

J. São testados regularmente os planos de resposta e recuperação;

K. A empresa incluí medidas de segurança informática nas práticas de recursos humanos, como a triagem de colaboradores;

L. A organização deve ter um plano de gestão de vulnerabilidades.

e) Manutenção (PR.MA)

i. A organização deve manter e reparar os ativos da empresa e registar essas atividades, com a utilização de ferramentas credenciadas e controladas para o efeito.

ii. A manutenção remota dos ativos deve ser aprovada, registada e executada de maneira a evitar o acesso não autorizado.

f) Tecnologias de Proteção (PR.PT)

i. São geridas as soluções de segurança técnica para garantir que os sistemas e ativos sejam seguros, resilientes, consistentes com as políticas, procedimentos e acordos definidos na organização.

A. Documentação e análise dos registos de auditorias de acordo com as políticas identificadas;

B. A organização protege todos os sistemas de armazenamento amovível e restringe a sua utilização de acordo com as políticas definidas;

C. A configuração dos sistemas deve assegurar que cada utilizador apenas tem acesso ao que necessita (baseado no modelo de menor funcionalidade);

D. As comunicações e o controlo de rede devem estar protegidas;

E. Utilização de mecanismos "*failover*", balanceamento de carga e "*hot swap*", implementando uma maior resiliência a falhas.

3. Detetar

a) Eventos e Anomalias (DE.AE)

i. A organização deve reconhecer quando as atividades maliciosas ocorrem nos seus sistemas.

A. Manter e gerir um guia com base nas operações de rede e nos fluxos de dados constituídos pelas ações esperadas pelos utilizadores e sistemas presentes na organização;

B. A empresa deve analisar os eventos detetados para compreender os alvos e os métodos de ataque caso existam;

C. Os sistemas devem recolher e correlacionar os dados de todos os eventos referente ás várias fontes e sensores presentes no parque informático;

D. Devem ser conhecidos os impactos dos eventos de segurança informática;

E. É necessário estabelecer limites nos alertas de incidentes.

b) Monitorização Continua de Segurança (DE.CM)

i. A organização deve efetuar uma monitorização continua dos seus sistemas de informação e ativos para identificar eventos de segurança informática e verificar a eficácia das mediadas de proteção. A monitorização deve incluir as seguintes áreas:

A. A rede empresarial;

B. O ambiente físico;

C. A atividade dos prestadores de serviços externos;

D. A atividade dos colaboradores;

E. A monitorização deve verificar também anomalias (código malicioso, acessos não autorizados, vulnerabilidade entre outros).

c) Processo de Deteção (DE.DP)

i. A organização deve manter e testar os seus processos e procedimento de deteção para garantir que estejam cientes de possíveis eventos anómalos.

A. Devem ser definidas funções e responsabilidade na ótica de deteção de eventos;

B. As atividades de deteção devem estar em conformidade com os requisitos estabelecidos pela organização;

C. A organização deve testar os seus processos de deteção;

D. As informações de deteção de eventos devem ser comunicadas aos responsáveis pela área da empresa identificada;

E. Devem ser efetuadas melhorias continuas aos processo de deteção.

4. Responder

a) Planeamento de Respostas (RS.RP)

i. A organização deve desenvolver processos e procedimentos para responder a incidentes de segurança informática.

A. A organização deve seguir o seu plano de resposta durante ou após um incidente.

b) Comunicações (RS.CO)

i. A organização deve coordenar as atividades de resposta com as partes interessadas internas e externas, incluindo agências de aplicação da lei.

A. Os colaboradores devem conhecer as suas funções e a ordem das operações quando uma resposta é necessária;

B. Os incidentes são relatados de acordo com os critérios definidos;

C. As equipas compartilham informações consistentes com os seus planos de resposta.

D. A organização coordena com as partes interessadas de acordo com os seus planos de resposta;

E. São oferecidas informações sobre os incidentes de segurança com as partes interessadas externas, para uma maior conscientização.

c) Análises (RS.AN)

i. A organização deve analisar e responder aos incidentes de segurança da informação para aumentar a resiliência ao suporte das atividades de recuperação.

A. A organização investiga as notificações dos sistemas;

B. A equipa da organização percebe o impacto de cada incidente;

C. As equipas partilham informação através dos planos de resposta a incidentes;

D. A organização deve voluntariamente informar sobre os incidentes ás partes interessadas.

d) Mitigação (RS.MI)

i. A organização deve trabalhar para prevenir a expansão de eventos, mitigar os eventos afetos e resolver os incidentes.

A. Os incidentes devem ser contidos;

B. Os incidentes devem ser mitigados;

C. A organização deve identificar com antecedência as vulnerabilidades ou documentar a aceitação dos riscos.

e) Melhorias (RS.IM)

i. A organização trabalha na ótica da resposta a ameaças de segurança, eventos, e incidentes incorporando as lições aprendidas de atividades de deteção/resposta atuais ou passadas.

A. Os planos de resposta devem incorporar as lições aprendidas;

B. As estratégias de resposta devem ser atualizadas consoante as necessidades.

5. Recuperar

a) Plano de Recuperação (RC.RP)

i. A organização deve manter os procedimentos e os processos de recuperação dos ativos em caso de incidente de cibersegurança.

A. A organização deve seguir o plano de recuperação durante ou após um incidente de cibersegurança;

b) Melhorias (RC.IM)

i. A organização deve efetuar melhorias nos processos e no plano de recuperação incorporando as lições aprendidas.

A. Os planos de recuperação devem incorporar as lições aprendidas;

B. A organização deve efetuar uma atualização das suas estratégias de recuperação constantemente.

c) Comunicações (RC.CO)

i. A organização deve coordenar as atividades internas ou externas de recuperação, incluindo a coordenação de centros operacionais, ISP's, vitimas, equipas de resposta a incidentes.

A. A organização deve gerir as relações após um incidente;

B. A empresa deve reparar a sua reputação após um incidente;

C. Devem ser notificas as partes interessada, internas ou externas sobre as atividades de recuperação.

2.3 NIS - EU NETWORK AND INFORMATION SECURITY

Como parte da estratégia de segurança dos sistemas de informação da União Europeia, a comissão da UE propôs pela primeira vez a Diretiva de Segurança de Redes e Informações [18] (NIS) em 2016, que foi a primeira parte que permite legislar a segurança informática em toda a União Europeia.

Esta diretiva tornou-se aplicável a partir de 9 de maio de 2018 e todos os Estados-Membros da UE devem adotar a legislação nacional que siga ou transponha a diretiva.

As diretivas da UE permitem alguma flexibilidade de modo a considerar as circunstâncias nacionais de cada país, incluindo a capacidade de reutilizar as estruturas organizacionais existentes ou de alinhar com a legislação nacional existente. O objetivo da diretiva NIS é criar níveis de resiliência superiores nas nações europeias.

A diretiva NIS foca-se em 3 partes essenciais:

a) Capacidades Nacionais : Os Estados-Membros da UE devem ter determinadas capacidades nacionais de cibersegurança nos respetivos países (por exemplo devem ter um CSIRT [19] nacional, realizar exercícios regulares no âmbito da segurança da informação, entre outras atividades importantes);

b) Colaboração Transfronteiriça: Deve existir uma colaboração ativa entre os vários países da UE (por exemplo, a rede operacional do CSIRT Europeu, o grupo Estratégico de cooperação no âmbito da presente diretiva, entre outros);

c) Supervisão dos Setores Críticos Nacionais: Supervisionar as medidas de segurança dos setores críticos nacionais (energia, transporte, água, saúde, infraestruturas digitais e financeiras).

2.3.1 *Aplicabilidade e Penalidades sob a Diretiva NIS*

A presente Diretiva aplica-se a prestadores de serviços digitais e operadores de serviços essenciais que operam nos Estados-Membros da UE. Os prestadores de serviços digitais incluem entidades que fornecem serviços digitais, como mecanismos de pesquisa, mercados online e serviços de *cloud*. Os operadores de serviços essenciais incluem quaisquer organização que se envolva em atividades sociais ou económicas críticas, cujas operações seriam muito afetadas no caso de uma violação de segurança informática. Esta categoria incluí os setores

como operadores de energia, fornecedores de transportes e fornecedores de alimentação e água.

Tanto os operadores de serviços essenciais como os prestadores de serviços digitais são responsáveis por relatar grandes incidentes de segurança ás equipa de resposta a incidentes de segurança informática (CSIRTs), mesmo que subcontratem a manutenção dos seus sistema de informação. A diretiva NIS estabelece que as penalidades por não conformidade devem ser eficazes, proporcionais e dissuasoras. No entanto, os Estados Membros individuais e não a UE em conjunto, determinam, em última análise as sanções especificas em caso de incumprimento. No Reino Unido, por exemplo, as organizações que não implementarem medidas eficazes de segurança informática podem ser multados em 17 milhões de libras ou 4 por cento da sua faturação global.

2.3.2 *Melhores Práticas - Conformidade com a Diretiva NIS*

Os requisitos de segurança da Diretiva NIS incluem medidas técnicas especificas que gerem os riscos de violações de segurança informática de uma maneira preventiva. Um dos melhores exemplos de como aplicar estes controlos técnicos é a orientação da framework Cyber Assessment (CAF) [20], lançada em 2018 pelo National Cyber Security Center (NCSC), do Reino Unido. Centra-se em indicadores específicos de boas práticas ao abrigo da Diretiva NIS, incluindo quatro objetivos e 14 princípios:

a) Gestão de Riscos de Segurança: As organizações devem garantir que as estruturas, políticas e processos apropriados estejam implementados para entender, avaliar e gerir sistematicamente os riscos de segurança para as redes e os sistemas de informação que suportam funções essenciais.

   Os Principios sobre este objetivo incluem:

   i. Governança - Garantir que as políticas e processos de gestão apropriados estejam a ser implementados para controlar a segurança da rede e dos sistemas de informação.

   ii. Gestão de Riscos - As organizações devem identificar, avaliar e compreender os riscos de segurança informática para a rede e os sistemas de informação que suportam a operação de funções essenciais.

   iii. Gestão de Ativos - Tudo o que é necessário para entregar, manter ou apoiar a operação das funções essenciais é determinado e compreendido. Isto incluí dados, pessoas e sistemas, bem como qualquer infraestrutura de suporte.

iv. Cadeia de Abastecimento - A organização deve entender e gerir os riscos de segurança para a operação de funções essenciais que surgem como resultado de dependências de fornecedores externos, incluindo a garantia de que medidas apropriadas sejam aplicadas quando os serviços de terceiros são utilizados.

b) Proteção contra Ataques Informáticos: As organizações devem garantir que as medidas de segurança sejam proporcionais e estejam em vigor para proteger a rede e os sistemas de informação que suportam funções essenciais contra ataques informáticos.

Os Princípios deste objetivo incluem:

i. Proteção e Políticas de Serviço - Uma organização deve definir, implementar, comunicar e aplicar políticas e processos apropriados que direcionem a sua abordagem geral para proteger os sistemas e dados que suportam a operação de funções essenciais.

ii. Controlo de Identidades de Acesso - A organização deve entender, documentar e gerir o acesso a redes e sistemas de informação e suportar a operação de funções essenciais. Os utilizadores (ou funções automatizadas) que possam aceder a dados ou serviços devem ser devidamente verificados, autenticados e autorizados.

iii. Segurança dos Dados - Os dados armazenados ou transmitidos eletronicamente devem ser protegidos de ações como o acesso não autorizado, modificação ou exclusão que possam causar um impacto adverso em funções essenciais.

iv. Segurança dos Sistemas - Os sistemas críticos para a operação de funções essenciais devem ser protegidos contra ataques cibernéticos, utilizando medidas de segurança de proteção robustas e confiáveis para limitar efetivamente as oportunidades de os invasores comprometerem as redes e os sistemas.

v. Redes e Sistemas Resilientes - Uma organização deve construir resiliência contra ataques cibernéticos no projeto, na implementação, na operação e na gestão de sistemas que suportam a operação de funções essenciais.

vi. Consciencialização e Treino - A equipa de colaboradores tem de ter consciência, conhecimento e habilidades adequadas para desempenhar as suas funções organizacionais de forma eficaz em relação à segurança da rede e dos sistemas de informação que suportam a operação de funções essenciais.

c) Deteção de Incidentes de Segurança Informática:

A organização deve garantir que as defesas de segurança possam detetar eventos de segurança cibernética que afetem, ou que tenham potencial de afetar, as funções essenciais.

Os princípios sob este objetivo incluem:

i. Monitorização de Segurança - A organização deve monitorizar o estado da segurança das redes e sistemas que suportam as funções essenciais para detetar possíveis problemas de segurança e analisar a eficácia contínua das medias de segurança e proteção.

ii. Segurança Pro ativa e Descoberta de Eventos - A organização deve detetar, dentro das redes e dos sistemas de informação, atividades maliciosas que afetam, ou com potencial de afetar, a operação de funções essenciais, mesmo quando a atividade não seja linear e não seja detetada através das soluções padrão baseadas em assinaturas.

d) Minimizar o Impacto dos Incidentes de Segurança:

A organização deve garantir que pode minimizar o impacto adverso de um incidente de segurança informática na operação de funções essenciais, incluindo a restauração dessas funções quando necessário.

Os princípios sob este objetivo incluem:

i. Planeamento de Resposta e Recuperação - A organização deve ter processos de gestão de incidentes bem definidos e testados, que visam garantir a continuidade das funções essenciais em caso de falha do sistema ou serviço. As atividades de mitigação planeadas para conter ou mitigar o impacto do comprometimento de ativos devem estar em vigor na organização.

ii. Lições Aprendidas - Quando ocorre um incidente, uma organização deve tomar medidas para entender as suas causas raiz e garantir que a ação de remediação apropriada seja tomada.

2.4 REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO

O Decreto-Lei n.º 65/2021 [21], aprovado pelo Conselho de Ministros Português, vem responder à necessidade de se estabelecerem regras sobre os requisitos de segurança das redes e sistemas de informação ligados à *internet* e para notificação de incidentes, previstas na Lei n.º 46/2018.

O Decreto-Lei n.º 65/2021 tem como âmbito de aplicabilidade a Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais, previstos nas alíneas a) a d) do nº 1 do artigo 2.º do Regimes Jurídico da Segurança do Ciberespaço (Lei nº 46/2018).

Requisitos do Decreto-Lei N.º 65/2021

Como necessidade de futuras auditorias e entrega de relatórios anuais que estejam em conformidade com o Decreto de Lei, de seguida estão explícitos os requisitos regulamentares do decreto:

a) Identificar e comunicar ao CNCS o Ponto de Contacto Permanente;

b) Identificar e comunicar ao CNCS o Responsável de Segurança

c) Inventariar todos os ativos essenciais e comunicar a lista de ativos ao CNCS;

d) Realizar uma Análise de Risco aos ativos que garantem a continuidade do funcionamento das redes e dos sistemas de informação e a prestação dos serviços;

e) Elaborar e manter atualizado um Plano de Segurança;

f) Notificar o CNCS de todos os incidentes com impacto relevante ou substancial;

g) Elaborar um relatório anual com a descrição das atividades realizadas, informação e estatísticas de incidentes e recomendações de melhoria.

3

FRAMEWORK CSE4CI

Neste tópico, será apresentada uma framework de cibersegurança abrangente e inovadora, meticulosamente elaborada com base nas normas mais reconhecidas da indústria (ISO 27001, NIST CSF, CIS, COBIT, entre outras). A crescente sofisticação das ameaças cibernéticas torna a segurança da informação uma prioridade crítica nas organizações que operam infraestruturas críticas. Esta framework representa uma abordagem proativa e altamente eficaz para proteger os sistemas e dados sensíveis. Ela foi desenvolvida com base numa extensa pesquisa, incorporando as melhores práticas da indústria, bases regulatórias e normas internacionalmente reconhecidas na área da cibersegurança.

Esta framework de cibersegurança que será proposta neste capítulo tem como objetivo fornecer uma estrutura sólida e adaptável para abordar os desafios emergentes de segurança cibernética. Ao alinhar-se com as normas amplamente reconhecidas, ela procura estabelecer um alicerce sólido para a proteção de informações críticas e a preservação da integridade dos sistemas. Além disso, será abordada a implementação prática dessa framework, incluindo metodologias de avaliação de riscos, estratégias de mitigação e integração em ambientes organizacionais.

3.1 OBJETIVOS DE SEGURANÇA

A *Framework* CSE4CI (CyberSecurity Ecosystem For Critical Infrastructures) A Framework CSE4CI disponibiliza e descreve um conjunto de medidas de segurança e respetivos controlos específicos para as organizações. São referenciados exemplos processuais e técnicos que permitem sistematizar os processos de conformidade, procedimentos e respetivas ferramentas, cuja a aplicação permita atingir os objetivos definidos. Através desta *framework* é possível analisar o estado atual relativo à proteção do perímetro interno e externo de uma organização, referente aos seus processos lógicos e técnicos que permitam mitigar problemas atuais na infraestrutura tecnológica e humana. Na figura 4 são evidenciados os objetivos principais da *framework*.

A utilização da *framework* CSE4CI deve ser efetuada numa perspetiva inicial de conformidade com as regulamentações nacionais e internacionais na área de

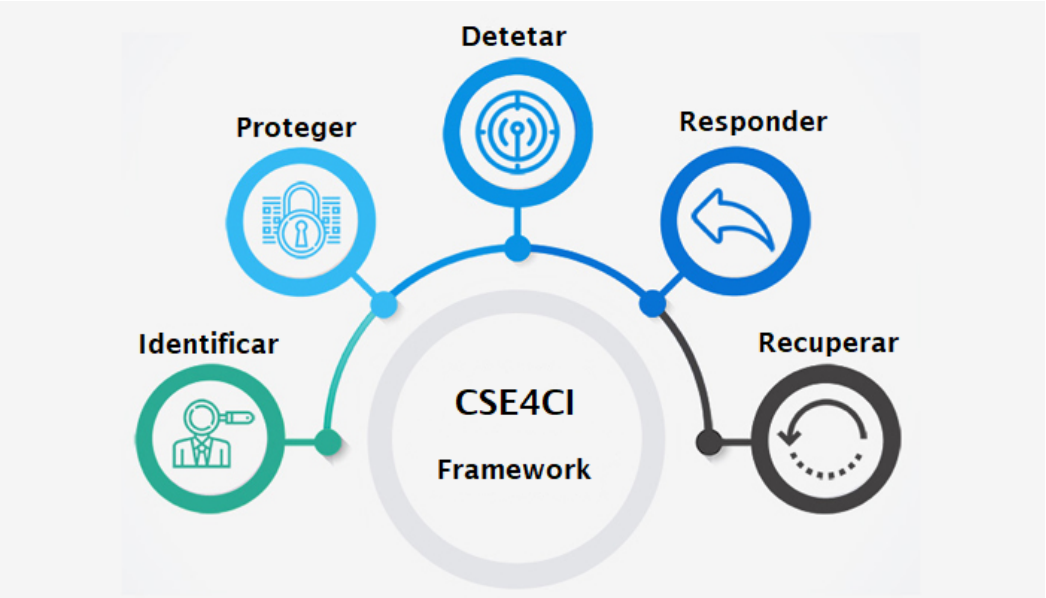

Figura 4: Conteúdo da CSE4CI

segurança da informação, com foco no aumento da resiliência da infraestrutura crítica a proteger.

No quadro seguinte são apresentados os objetivos principais de segurança propostos:

Objetivos de Segurança	Descrição do Objetivo
Identificar	Perceção do contexto e o plano de negócios da organização, dos ativos de informação que suportam todos os processos críticos da atividade e os riscos associados que possam comprometer o bom funcionamento da organização. Esta compreensão da organização permite que seja possível definir e priorizar os recursos e investimentos a efetuar futuramente para alcançar um nível de maturidade elevada em questões de segurança informática.
Proteger	Implementação das medidas destinadas a proteger os processos da organização e os respetivos ativos críticos, independentemente da tipologia dos ativos. Nesta categoria são descritas e colocadas em prática todas as medidas orientadas à proteção da organização com foco nas áreas de recursos humanos, processos organizacionais e tecnologias.
Detetar	Consolidação e implementação de medidas endereçadas a identificar de forma preventiva os incidentes que possam ocorrer ao longo do tempo, ou seja, a deteção de eventos anómalos na segurança das redes e sistemas de informação.
Responder	Categorização e definição de medidas que, através da deteção de um incidente, permitam uma maior agilidade de processos na mitigação dos incidentes. As medidas propostas neste ponto pretendem reduzir o impacto e os respetivos efeitos adjacentes dos mesmos.
Recuperar	Planos e atividades de recuperação que permitam gerir a recuperação de sistemas e aplicações afetados devido a um incidente de cibersegurança. As medidas pretendem assegurar a resiliência e as lições aprendidas após um incidente e o seu tratamento.

Tabela 1: Principais Objetivos de Segurança Propostos

3.2 DOMÍNIOS DE SEGURANÇA

Neste capítulo, serão apresentados os diversos domínios de segurança que desempenham um papel fundamental na proteção de ativos de informação e na garantia da confidencialidade, integridade e disponibilidade dos dados. Ao examinar estes domínios, podemos adquirir uma visão mais clara das complexidades e desafios associados à segurança da informação, bem como das estratégias e melhores práticas que podem ser adotadas para fortalecer a postura de segurança de uma organização. Cada domínio representa uma faceta única e essencial do campo da segurança da informação, contribuindo para um panorama abrangente da gestão de riscos e proteção de dados num ambiente tecnológico em constante evolução. Estes domínios permitem mapear as categorias essenciais da *framework*, revelando as estratégias e abordagens necessárias para garantir a segurança da informação num mundo digital interconectado e dinâmico.

Como estrutura principal da framework, de seguida, serão apresentados os domínios de segurança da CSE4CI constituídos pelo seu objetivo e intenção de principio:

- 01. Governação de Segurança e Privacidade (GSP)

  Objetivo: Especificar o desenvolvimento de programas de segurança e privacidade de uma organização, incluindo critérios para medir o sucesso.

  Intenção de Princípio: Garantir o envolvimento contínuo da liderança e a gestão de riscos.

- 02. Gestão de Ativos (GAT)

  Objetivo: Garantir que os ativos tecnológicos são corretamente geridos ao longo do ciclo de vida do ativo, desde a aquisição até a eliminação.

  Intenção de Princípio: Autorizar o acesso à infraestrutura da organização apenas a dispositivos previamente validados, protegendo os dados, tanto em trânsito como em repouso.

- 03. Continuidade de Negócios e Recuperação de Desastres (CRD)

  Objetivo: Estabelecer processos que ajudarão a organização a recuperar de situações adversas com o mínimo impacto nas operações.

  Intenção de Princípio: Fornecer a capacidade de *e-discovery* e garantir a resiliência do negócio.

- 04.Capacidade e Planeamento de Desempenho (CPD)

  Objetivo: Mitigar interrupções de negócios evitáveis causadas por limitações de capacidade e desempenho.

Intenção de Princípio: Manter a conscientização sobre a situação atual e futura, garantindo a escalabilidade.

- 05. Gestão de Mudanças (GDM)

  Objetivo: Garantir que tanto a tecnologia como a liderança organizacional gerem proativamente a mudança.

  Intenção de Princípio: Evitar impactos negativos nas operações e facilitar a resolução de problemas.

- 06. Segurança na Cloud (SNC)

  Objetivo: Gerir eficazmente o uso de ambientes de *cloud* pública e privada para gerir os riscos associados.

  Intenção de Princípio: Mitigar riscos associados a terceiros e decisões arquitetónicas na adoção de *cloud*.

- 07. Conformidade (COF)

  Objetivo: Garantir que os controlos estão em vigor para cumprir as obrigações legais, regulamentares e contratuais.

  Intenção de Princípio: Alinhar com as normas internas da organização e manter a conformidade.

- 08. Gestão de Configuração (GDC)

  Objetivo: Estabelecer e manter a integridade dos sistemas, com controlos de gestão de configuração documentados.

  Intenção de Princípio: Evitar irregularidades de processamento e execução de código malicioso.

- 09. Monitorização Contínua (MOC)

  Objetivo: Estabelecer e manter a consciencialização da situação em toda a organização, recolhendo e revisando os registos de eventos.

  Intenção de Princípio: Evitar comprometimento do sistema, exfiltração de dados e indisponibilidade de recursos.

- 10. Proteções Criptográficas (PCR)

  Objetivo: Garantir a confidencialidade dos dados da organização através da implementação de tecnologias criptográficas adequadas.

  Intenção de Príncipio: Utilização de tecnologias criptográficas.

- 11. Classificação e Tratamento de Dados (CTD)

  Objetivo: Garantir que os ativos tecnológicos são devidamente classificados e que as medidas são implementadas para proteger os dados da organização.

Intenção de Princípio: Proteger a confidencialidade, integridade e disponibilidade dos dados.

- 12. Segurança Endpoint (SEN)

  Objetivo: Garantir que os *endpoints* estejam devidamente protegidos contra ameaças à segurança do dispositivo e os seus dados.

  Intenção de Princípio: Garantir a confidencialidade, integridade, disponibilidade e segurança dos *endpoints*.

- 13. Segurança de Recursos Humanos (SRH)

  Objetivo: Criar uma equipa de trabalho na área de segurança e privacidade num ambiente propício à inovação.

  Intenção de Princípio: Considerar cultura, recompensa e colaboração.

- 14. Identificação e Autenticação (IAT)

  Objetivo: Implementar o conceito de "menor privilégio"limitando o acesso apenas aos utilizadores autorizados.

  Intenção de Princípio: Garantir acesso controlado a sistemas e dados.

- 15. Resposta a Incidentes (RAI)

  Objetivo: Estabelecer e manter a capacidade de orientar a resposta da organização a incidentes de segurança ou privacidade.

  Intenção de Princípio: Formar os utilizadores para a deteção e comunicação de incidentes.

- 16. Garantia de Informação (GDI)

  Objetivo: Assegurar que a segurança e os controlos adequados estão presentes nos ambientes de desenvolvimento e produção.

  Intenção de Princípio: Manter a integridade dos sistemas ao longo do seu ciclo de vida.

- 17. Manutenção (MNT)

  Objetivo: Assegurar que os ativos tecnológicos são mantidos adequadamente para garantir um bom desempenho contínuo.

  Intenção de Princípio: Verificar a segurança em ativos no fim de vida ou término de suporte.

- 18. Gestão de Dispositivos Móveis (GEM)

  Objetivo: Regular os riscos associados a dispositivos móveis, independentemente de serem propriedade da organização.

Intenção de Princípio: Gerir práticas de acesso a armazenamento de dispositivos móveis.

- 19. Segurança da Rede (SDR)

  Objetivo: Garantir controlos de segurança suficientes para proteger a infraestrutura de rede da organização.

  Intenção de Princípio: Preservar a confidencialidade, integridade e disponibilidade dos recursos de rede.

- 20. Segurança Física e Ambiental (SFA)

  Objetivo: Minimizar o acesso físico aos sistemas e dados da organização, abordando os controlos de segurança física e ambiental.

  Intenção de Princípio: Proteger equipamentos contra ameaças ambientais.

- 21. Privacidade (PRI)

  Objetivo: Alinhar decisões de engenharia de privacidade com a estratégia de privacidade global da organização.

  Intenção de Princípio: Implementar o conceito de privacidade por *design* e por padrão.

- 22. Projeto e Gestão de Recursos (PGR)

  Objetivo: Garantir que projetos relacionados com segurança têm apoio de gestão de recursos e projetos/programas.

  Intenção de Princípio: Execução bem-sucedida de projetos de segurança.

- 23. Gestão dos Riscos (GDR)

  Objetivo: Garantir que riscos de segurança e privacidade são visíveis e compreendidos pelas unidades responsáveis pelos ativos/processos.

  Intenção de Princípio: Proprietários de risco são unidades de negócio e partes interessadas chave.

- 24. Engenharia Segurança e Arquitetura (ESA)

  Objetivo: Alinhar decisões de engenharia de cibersegurança com a estratégia arquitetónica e tecnológica da organização.

  Intenção de Princípio: Garantir ambientes de rede seguros.

- 25. Operações de Segurança (ODS)

  Objetivo: Garantir recursos adequados e uma estrutura de gestão para a prestação de serviços de segurança e privacidade.

  Intenção de Princípio: Prestação eficaz de serviços de cibersegurança.

- 26. Consciência de Segurança e Formação (CSF)

  Objetivo: Desenvolver uma força de trabalho de segurança e privacidade através de atividades teóricas e práticas.

  Intenção de Princípio: Melhorar a formação existente.

- 27. Desenvolvimento Tecnológico e Aquisição (DTA)

  Objetivo: Garantir que princípios de segurança e privacidade são implementados em produtos/soluções desenvolvidos ou adquiridos.

  Intenção de Princípio: Incorporar conceitos de "menor privilégio"e "menor funcionalidade".

- 28. Gestão de Terceiros (GDT)

  Objetivo: Minimizar riscos de segurança e privacidade associados a terceiros e sustentar operações em caso de comprometimento de terceiros.

  Intenção de Princípio: Lidar com riscos relacionados a terceiros.

- 29. Gestão de Ameaças (GDA)

  Objetivo: Estabelecer capacidade para identificar e gerir proativamente ameaças à segurança e privacidade.

  Intenção de Princípio: Identificar e gerir ameaças tecnológicas.

- 30. Gestão de Vulnerabilidades & Patch (GVP)

  Objetivo: Gerir riscos associados à gestão de vulnerabilidades técnicas e práticas de gestão de atualizações.

  Intenção de Princípio: Garantir a segurança através de gestão de vulnerabilidades.

- 31. Segurança Web (SWB)

  Objetivo: Abordar os riscos associados a tecnologias acessíveis à Internet, endurecer dispositivos e monitorizar a integridade de arquivos de sistema.

  Intenção de Princípio: Auditoria e monitorização de atividades maliciosas.

3.3 CONTROLOS E CONFORMIDADE CSE4CI

Nesta secção, vão ser enunciados diversas variedades de controlos de segurança essenciais que formam a base da estrutura da *framework* CS4ECI. Estes controlos permitem abranger uma ampla gama de áreas e considerações, contribuindo para a proteção geral dos ativos de informação.

À medida que exploramos os detalhes destes controlos, podemos examinar as suas implicações práticas, benefícios e como podem ser implementados efetivamente num ambiente empresarial. Os seguintes controlos são projetados para abordar ameaças diversas, desde ataques cibernéticos sofisticados até incidentes internos não intencionais. Além disso, eles permitem ajudar as organizações a cumprir regulamentações e padrões de segurança cada vez mais rigorosos.

Este estudo não apenas fornece uma visão técnica dos controlos de segurança, mas também destaca a sua importância para a continuidade dos negócios, a gestão de riscos e cooperação com entidades externas. A segurança da informação é um esforço contínuo e colaborativo que requer a atenção de todos os níveis de uma organização. Ao entender e aplicar estes controlos, as organizações podem fortalecer as suas defesas cibernéticas, protegendo-se de ameaças em constante evolução num mundo digital, altamente conectado.

3.3.1 *Governação de Segurança e Privacidade*

GSP-01 | Programa de Governação de Segurança e Privacidade

Descrição: Mecanismos para facilitar a implementação dos controlos de cibersegurança e de governação da privacidade.

Implementação: As métricas são utilizadas para avaliar a eficácia do programa de governação, com base em tendências históricas. Deve existir um programa formal de governação tanto para a segurança como para a privacidade. Uma equipa de Governação, Risco e Conformidade (GRC) ou função semelhante, deve proporcionar a supervisão de governação para a implementação das obrigações legais, regulamentares e contratuais de cibersegurança e privacidade aplicáveis que facilitam a implementação de práticas seguras para proteger a confidencialidade, integridade, disponibilidade e segurança das aplicações, sistemas, serviços e dados da organização.A função de governação deve ser formalmente atribuída com funções definidas e responsabilidades associadas. Os requisitos de conformidade para a segurança e privacidade devem ser identificados e documentados. Os controlos são atribuídos a ativos sensíveis para aderir a requisitos específicos de conformidade.

Questão de Controlo: Os colaboradores da organização operam de forma a governar centralmente os controlos de cibersegurança e privacidade?

Evidências:

1. Comité de Segurança e Conformidade;
2. Programa de Direção de Segurança Digital (DSP);
3. Programa de Cibersegurança e Proteção de Dados (CDPP).

GSP-02 | Documentação de Segurança e Privacidade

Descrição: Mecanismos para estabelecer, manter e divulgar políticas de cibersegurança e privacidade, normas e procedimentos.

Implementação: Políticas e procedimentos de cibersegurança alinhados com as regulamentações nacionais e internacionais nomeadamente ISO 27001, NIST CSF, NIS2, QNRCS entre outros. A documentação deve ser transmitida a todos os colaboradores internos. Os procedimentos devem ser mapeados para os respetivos responsáveis.

Questão de Controlo: A organização estabelece, mantém e divulga políticas de cibersegurança e privacidade, normas e procedimentos?

Evidências:

1. Programa de Direção de Segurança Digital (DSP);
2. Programa de Cibersegurança e Proteção de Dados (CDPP);
3. Ferramenta de governação, solução de risco e conformidade (GRC) (Ostendio, ZenGRC, RequirementONE, Allgress, Archer, RSAM, Metric, etc.).

GSP-03 | Análise e Atualização Periódica de Segurança e Privacidade

Descrição: Mecanismos para rever o programa de cibersegurança e privacidade, incluindo políticas, normas e procedimentos, em intervalos planeados ou se ocorrerem alterações significativas para garantir a sua adequação e eficácia contínuas.

Implementação: O processo formal de revisão deve ser realizado numa base anual. Este processo de revisão deve incluir o âmbito das obrigações legais, regulamentares e contratuais aplicáveis. As recomendações para as edições devem ser submetidas para revisão e são tratadas de acordo com os processos de controlo da alteração de documentação aplicável na organização. A versão atualizada deve ser publicada pelo menos anualmente, com base no processo de revisão. As pessoas afetadas pelas alterações devem ser notificadas das alterações efetuadas.

Questão de Controlo: A organização revê as políticas de cibersegurança e privacidade, padrões e procedimentos em intervalos previstos ou se ocorrerem alterações significativas para garantir a sua adequação e eficácia contínuas?

Evidências:

1. Plano de revisão ;
2. Ferramenta de governação, solução de risco e conformidade (GRC) (Ostendio, ZenGRC, RequirementONE, Allgress, Archer, RSAM, Metric, etc.).

GSP-04 | Atribuição de Responsabilidades de Segurança e Privacidade

Descrição: Mecanismos para atribuir um indivíduo qualificado com a missão e recursos para gerir, coordenar, desenvolver, implementar e manter um programa de cibersegurança e privacidade em toda a organização.

Implementação: Devem existir mecanismos para atribuir um indivíduo qualificado com a missão e recursos para gerir, coordenar, desenvolver, implementar e manter um programa de cibersegurança e privacidade em toda a organização.

Questão de Controlo: A organização atribui a um indivíduo qualificado a missão e recursos para gerir centralmente a coordenação, desenvolver, implementar e manter um programa de cibersegurança e privacidade em toda a organização?

Evidências:

1. Chefe de Segurança da Informação (CISO);
2. Responsável de Segurança (DL 65/2021, Reg 303/ANACOM).

GSP-05 | Principais Indicadores de Desempenho (KPI's)

Descrição: Mecanismos para desenvolver, reportar e monitorizar os principais indicadores de desempenho (KPI's) para ajudar a gestão organizacional na monitorização de desempenho e análise de tendências do programa de cibersegurança e privacidade.

Implementação: Devem existir processos para recolher métricas detalhadas que sejam capazes de fornecer uma compreensão quantitativa das capacidades dos processos e uma melhor forma de prever o desempenho expectável. Uma equipa de Governação, Risco e Conformidade ou função semelhante, deve proporcionar uma supervisão de governação para a implementação das obrigações legais, regulamentares e contratuais de cibersegurança e privacidade aplicáveis que facilitam a implementação de práticas seguras para proteger a confidencialidade, integridade, disponibilidade e segurança das aplicações, sistemas, serviços e dados da organização. A administração da organização mantém um processo formal de revisão objetiva e de resposta aos KPI's (por exemplo, revisão mensal ou trimestral).

Questão de Controlo: A organização desenvolve, reporta e monitoriza os Principais Indicadores de Desempenho (KPI's) para ajudar a gestão organizacional na monitorização de desempenho e análise de tendências do programa de cibersegurança e privacidade?

Evidências:

1. Principais Indicadores de Desempenho (KPI's).

GSP-06 | Principais Indicadores de Risco (KRIs)

Descrição: Mecanismos para desenvolver, reportar e monitorizar os principais indicadores de risco (KR) para ajudar as equipas de gestão na monitorização de desempenho e análise de tendências do programa de cibersegurança e privacidade.

Implementação: Devem existir processos para recolher métricas detalhadas que sejam capazes de fornecer uma compreensão quantitativa das capacidades dos processos e uma melhor capacidade de prever o desempenho. Uma equipa de Governação, Risco e Conformidade ou função semelhante, proporciona a supervisão de governação para a implementação das obrigações legais, regulamentares e contratuais de cibersegurança e privacidade aplicáveis que facilitam a implementação de práticas seguras para proteger a confidencialidade, integridade, disponibilidade e segurança das aplicações, sistemas, serviços e dados da organização. A administração da organização mantém um processo formal de revisão objetiva e resposta a KRIs (por exemplo, revisão mensal ou trimestral).

Questão de Controlo: A organização desenvolve, reporta e monitoriza indicadores-chave de risco (KRIs) para ajudar a equipa de gestão na monitorização de desempenho e análise de tendências do programa de cibersegurança e privacidade?

Evidências:

1. Principais indicadores de risco (KRIs).

GSP-07 | Contactos com as Autoridades

Descrição: Mecanismos para identificar e documentar contactos adequados com as autoridades responsáveis pela aplicação da lei e com os organismos reguladores.

Implementação: Os colaboradores da equipa de resposta a incidentes identifica e mantém informações de contacto com as autoridades locais e nacionais (por exemplo, CNCS, PJ) em caso de incidentes de cibersegurança que exijam envolvimento da aplicação da lei. Estas informações de contacto devem ser verificadas e atualizadas pelo menos anualmente.

Questão de Controlo: A organização identifica e documenta os contactos adequados dentro das autoridades policiais e regulamentares competentes?

Evidências:

1. Equipa de Inteligência de Ameaças;
2. Equipa de Resposta a Incidentes de Segurança (CSIRT);
3. Ponto de Contacto Permanente.

GSP-08 | Gestão de Dados

Descrição: Mecanismos para facilitar a gestão de dados para supervisionar as políticas, normas e procedimentos da organização, de modo a que os dados sensíveis sejam efetivamente geridos e mantidos de acordo com as obrigações legais, regulamentares e contratuais aplicáveis.

Implementação: Os requisitos de conformidade para a segurança e privacidade são identificados e documentados. Os controlos são atribuídos a ativos sensíveis para cumprir com os requisitos de conformidade específicos.

Questão de Controlo: A organização estabelece a governação de dados em toda a organização?

3.3.2 *Gestão de Ativos*

GAT-01 | Governação de Ativos

Descrição: Mecanismos para facilitar a criação de um programa de Gestão de Ativos de TI (ITAM) para implementar e gerir controlos de gestão de ativos.

Implementação: Os requisitos de gestão de ativos de TI para segurança e privacidade devem ser identificados e documentados. Os controlos devem ser atribuídos aos ativos sensíveis para cumprir os requisitos específicos de conformidade para a gestão de ativos. A gestão de ativos tem de ser formalmente atribuída como um dever adicional aos colaboradores da área de TI ou cibersegurança. O inventário dos ativos físicos deve abranger os dispositivos comuns (por exemplo, computadores portáteis, estações de trabalho e servidores). O inventário deve ser realizado/revisto pelo menos anualmente.

Questão de Controlo: A organização facilita a implementação de controlos de gestão de ativos?

Evidências:

1. Princípios Contabilísticos (GAAP);
2. ITIL - Base de Dados de Gestão de Configurações (CMDB);
3. Programa de Gestão de Ativos de TI (ITAM).

GAT-02 | Dependência de Serviços sobre Ativos

Descrição: Mecanismos para identificar e avaliar a segurança dos ativos tecnológicos que suportam mais do que uma função empresarial crítica.

Implementação: Devem ser desenvolvidas métricas que fornecem supervisão de gestão para garantir que as dependências críticas dos serviços de ativos sejam identificadas e geridas para minimizar o risco. Um programa de *IT Asset Management* (ITAM) ou função semelhante, deve ser implementado para regular a gestão de ativos que garante o cumprimento dos requisitos para a governação de ativos. O ITAM deve alavancar uma Base de Dados de Gestão de Configurações (CMDB), ou uma ferramenta semelhante. A função ITAM tem de ser formalmente atribuída com funções definidas e responsabilidades associadas. O processo de compra, a atualização, reparação e alienação de ativos deve estar integrada nos processos ITAM. O inventário dos ativos de TI deve cobrir os ativos físicos e virtuais para criar uma visibilidade holística sobre os ativos da organização. Os inventários têm de ser configurados para serem digitalizados recorrentemente. A CMDB, ou ferramenta similar, deve ser combinado com outras soluções para identificar dependências de serviços de ativos que podem impactar a segurança dos mesmos.

Questão de Controlo: A organização identifica e avalia a segurança dos ativos tecnológicos que suportam mais do que uma função empresarial crítica?

GAT-03 | Inventário de Ativos

Descrição: Mecanismos para a realização de inventários de ativos tecnológicos que devem refletir com precisão os sistemas, aplicações e serviços atuais em uso.

Inventário de Ativos: Informação mínima necessária:

- ID Inventário - único;
- Nome do ativo;
- Modelo / Versão do Equipamento / Fabricante;
- Data da Implementação;
- Número de Série;
- Coordenadas Geográficas;
- Endereço(s) IP/IPs - Opcional;
- Endereço de Hardware (MAC Address) - Caso se aplique;
- Nome do Responsável , Contacto do Responsável e Departamento do Responsável;;
- Classificação do ativo (Físico ou Lógico);
- Criticidade (Alta, Média ou Baixa);
- Serviço Suportado (Cliente, Plataforma, Acesso, etc);
- Dependências Físicas (Fontes de Alimentação, Rede, AVAC entre outras);
- Dependências Lógicas (Licenciamento, plataformas entre outras);
- Medidas, controlos e registos do ativo;
- Registo de violações ou perdas de integridade;
- Registo de alterações.

Implementação: Os inventários devem ser predominantemente automatizados e cobrir os ativos físicos e lógicos da organização. A configuração deve ser efetuada com base numa ferramenta *IT Asset Management* (ITAM). Esta lista de ativos deve ser revista regularmente.

Questão de Controlo: A organização cria um inventário de ativos de tecnologia que reflete com precisão o seu ecossistema digital?

Evidências:

1. Inventário de ativos;
2. Programa de Gestão de Ativos de TI (ITAM).

GAT-04 | Deteção automatizada de componentes não autorizados

Descrição: Mecanismos automatizados para detetar e alertar após a deteção de componentes de *hardware*, *software* e *firmware* não autorizados.

Implementação: Deve existir um programa de Gestão de Ativos de TI (ITAM) ou função semelhante, que rege a gestão de ativos para garantir o cumprimento dos requisitos para a gestão de ativos. Deve ser efetuada uma verificação contínua para identificar os ativos não autorizados.

Questão de Controlo: A organização utiliza mecanismos automatizados para detetar e alertar após a identificação de componentes de *hardware*, *software* e *firmware* não autorizados?

GAT-05 | Controlo de Acesso à Rede (NAC)

Descrição: Mecanismos automatizados para implementar o Controlo de Acesso à Rede (NAC), ou uma tecnologia semelhante, capaz de detetar dispositivos não autorizados e desativar o acesso à rede a esses dispositivos não autorizados.

Implementação: As tecnologias NAC devem ser implementadas em segmentos de rede e/ou dispositivos de ponto final para impedir comunicações de rede não autorizadas. As tecnologias NAC devem ser configuradas para alertar a equipa de cibersegurança para possíveis incidentes (por exemplo, Os registos NAC devem ser direcionados para um SIEM).

Questão de Controlo: A organização implementa o Network Access Control (NAC), ou uma tecnologia similar, capaz de detetar dispositivos não autorizados e desativar o acesso à rede a esses dispositivos não autorizados?

GAT-06 | Base de Dados de Gestão de Configuração (CMDB)

Descrição: Mecanismos para implementar e gerir uma Base de Dados de Gestão de Configuração (CMDB), ou tecnologia semelhante, para monitorizar e gerir informações específicas do ativo tecnológico.

Implementação: A atualização, reparação e alienação de ativos deve estar integrada nos processos do ITAM. O inventário dos ativos de TI deve cobrir ativos físicos e virtuais para criar uma visibilidade holística nos ativos da organização.

Questão de Controlo: A organização implementa e gere uma Base de Dados de Gestão de Configuração (CMDB), ou tecnologia semelhante, para monitorizar e gerir informações específicas de ativos?

GAT-07 | Atribuição da Propriedade de Ativos

Descrição: Mecanismos para atribuir responsabilidades de propriedade de ativos a um departamento, equipa ou indivíduo para estabelecer uma compreensão comum dos requisitos para a proteção dos bens.

Implementação: Os inventários devem ser predominantemente automatizados, mas podem ter alguns componentes manuais (por exemplo, ativos baseados na *cloud* que estão fora de alcance para análises automatizadas de inventário). O inventário dos ativos de TI cobre ativos físicos e virtuais para criar uma visibilidade holística nos ativos da organização nomeadamente as equipas e/ou colaborador responsável.

Questão de Controlo: A organização atribui responsabilidades de propriedade de ativos a um departamento, equipa ou indivíduo para estabelecer uma compreensão comum dos requisitos para a proteção de bens?

GAT-08 | Origem dos Sistemas

Descrição: Mecanismos para acompanhar a origem, desenvolvimento, propriedade, localização e alterações nos sistemas, componentes do sistema e dados associados.

Implementação: É necessário um procedimento bem definido para acompanhar a origem, desenvolvimento, propriedade, localização e alterações a um sistema, componentes do sistema e dados associados.

Questão de Controlo: A organização rege a cronologia da origem, desenvolvimento, propriedade, localização e alterações a um sistema, componentes do sistema e dados associados?

GAT-09 | Diagramas de rede e diagramas de fluxo de dados (DFDs)

Descrição: Mecanismos para manter os diagramas de arquitetura em rede que devem conter detalhes suficientes para avaliar a segurança da arquitetura da rede, refletir a arquitetura atual do ambiente de rede e documentar todos os fluxos de dados sensíveis.

Implementação: Os responsáveis de aplicações/sistema/processos devem categorizar os dados de acordo com as políticas e normas organizacionais. Os proprietários de aplicações/sistema/processos, em conjunto com o pessoal de TI e cibersegurança, devem documentar onde os dados pessoais são armazenados, transmitidos e tratados de forma a documentar os fluxos de dados sensíveis. Os responsáveis de aplicações/sistemas/processos, em conjunto com o pessoal de TI e cibersegurança, devem criar diagramas de fluxo de dados (DFDs) e diagramas de rede. Este processo deve ser revisto no mínimo, anualmente, ou após qualquer mudança de processo/sistema.

Questão de Controlo: A organização mantém diagramas de arquitetura de rede que:

- Contém detalhes suficientes para avaliar a segurança da arquitetura da rede
- Reflete a arquitetura atual do ambiente de rede
- Documenta todos os fluxos de dados sensíveis/regulados

GAT-10 | Segurança dos Ativos Digitais

Descrição: Mecanismos para manter um controlo rigoroso sobre a distribuição interna ou externa de qualquer tipo de suporte sensível/regulamentado.

Implementação: Os responsáveis de aplicações/sistemas/processos devem categorizar os dados de acordo com as políticas e normas organizacionais. Os responsáveis de aplicações/sistema/processos, em conjunto com o pessoal de TI e cibersegurança, devem documentar a localização onde os dados pessoais são armazenados, transmitidos e tratados de forma a documentar os fluxos de dados sensíveis e as respetivas ameaças.

Questão de Controlo: A organização mantém um controlo rigoroso sobre a distribuição interna ou externa de qualquer tipo de suporte sensível/regulamentado?

Evidências:

1. ITIL - Base de Dados de Gestão de Configurações (CMDB);
2. Biblioteca de Software (DSL)

GAT-11 | Equipamento de Endpoint sem Supervisão

Descrição: Mecanismos para implementar medidas de proteção reforçadas para sistemas sem vigilância para proteger contra adulteração e acesso não autorizado.

Implementação: Devem ser efetuadas inspeções físicas periodicamente para validar a integridade dos sistemas não contextualizados. As políticas organizacionais e as normas devem abranger os requisitos de segurança para sistemas não supervisionados (por exemplo, quiosques, caixas multibanco, etc.). As configurações dos sistemas de modo *hardening* devem ser utilizadas para sistemas sem vigilância com o intuito de impor o princípio da "menor funcionalidade"removendo contas, aplicações e serviços desnecessários.

Questão de Controlo: A organização implementa medidas de proteção reforçadas para sistemas não supervisionados para proteger contra adulteração e acesso não autorizado?

Evidências:

1. Monitorização da Integridade do Ficheiro (FIM);
2. Verificador de alterações (NNT);
3. Fita de deteção (Tamper);

GAT-12 | Eliminação Segura

Descrição: Mecanismos para eliminar, destruir ou reutilizar de forma segura componentes do sistema utilizando técnicas e métodos definidos pela organização para evitar a recuperação de informações destes componentes.

Implementação: A equipa de Sistemas de Informação deve recolher os ativos tecnológicos e meios de comunicação para destruição quando já não são necessários por razões empresariais ou legais. A equipa de Sistemas de Informação deve realizar a destruição dos ativos tecnológicos e dos meios de comunicação de forma segura ou subcontrata a destruição a terceiros especializados em ativos tecnológicos e destruição dos meios de comunicação. As políticas organizacionais e as normas devem abranger os requisitos para os utilizadores conseguirem descartar, destruir ou reutilizar componentes do sistema quando já não for necessário por razões comerciais ou legais.

Questão de Controlo: A organização elimina, destrói ou reutiliza de forma segura componentes do sistema utilizando técnicas e métodos definidos pela organização para impedir que tais componentes entrem no mercado ilícito?

Evidências:

1. Ferramenta de destruição de dados lógicos,
2. Política de Destruição e reutilização de ativos tecnológicos.

GAT-13 | Devolução de Ativos

Descrição: Mecanismos para garantir que os trabalhadores e utilizadores externos devolvam todos os ativos organizacionais na sua posse aquando da cessação do contrato.

Implementação: A equipa responsável pelos sistemas de informação da organização deve recolher os bens dos ex-colaboradores . Os dispositivos devem ser "*escrowed*", armazenados por um período de tempo antes de serem limpos e atribuídos a outro utilizador. Os ativos não devolvidos devem ser reportados como um incidente de segurança, com base nos dados que podem existir no(s) dispositivos.

Questão de Controlo: A organização assegura que os colaboradores e utilizadores externos devolvem todos os ativos organizacionais na sua posse após cessação de contrato?

Evidências:

1. Lista de Rescisão de colaboradores anual;
2. Procedimento de análise de Sistemas de Operativos e respetivos dispositivos que os suportam.

GAT-14 | Extinção de Ativos

Descrição: Mecanismos para autorizar, controlar e rastrear os ativos tecnológicos que entram e saem das instalações organizacionais.

Implementação: As políticas organizacionais e as normas devem cobrir os requisitos para a aprovação de instalação de *software* nos ativos da organização, ou alteração de algum *software* já instalado. Devem também estes ativos ser rastreados ao longo do seu ciclo de vida.

Questão de Controlo: A organização autoriza, controla e rastreia os ativos tecnológicos que entram e saem das instalações organizacionais?

Evidências:

1. *Software* de Gestão de Ativos;
2. Marcação de ativos através de RFID;
3. Sensores de proximidade em vários pontos de acesso.

GAT-15 | Utilização de Dispositivos Pessoais

Descrição: Mecanismos para restringir a posse e utilização de dispositivos tecnológicos de propriedade pessoal dentro de instalações controladas pela organização.

Implementação: O *software Mobile Device Management* (MDM) deve ser utilizado para restringir os dados que residem em dispositivos pessoais. As políticas e padrões organizacionais devem abranger o uso de dispositivos pessoais (por exemplo, *Bring Your Own Device* (BYOD), como parte de comportamentos aceitáveis e inaceitáveis.

Questão de Controlo: A organização restringe a posse e o uso de dispositivos tecnológicos de propriedade pessoal dentro de instalações controladas pela organização?

Evidências:

1. Política BYOD;

GAT-16 | Parâmetros de Utilização

Descrição: Existem mecanismos para monitorizar e impor parâmetros de utilização que limitam os potenciais danos causados pela alteração não autorizada ou não intencional das configurações do sistema.

Implementação: Deve existir um Gestor de Eventos de Incidentes de Segurança (SIEM) para alertar a equipa de cibersegurança sobre possíveis incidentes relacionados com comportamentos anómalos. A monitorização do desempenho da rede deve ser utilizada para efetuar uma triagem do tráfego de rede "normal"que pode ser utilizado para identificar comportamentos anómalos. Os servidores que contêm dados sensíveis devem ter monitorização ativa de CPU, RAM, ficheiros alterados/eliminados e sessões de acesso.

Questão de Controlo: A organização monitoriza e aplica parâmetros de utilização que limitam os potenciais danos causados pela alteração não autorizada ou não intencional dos parâmetros do sistema?

Evidências:

1. Política de Monitorização de Ativos;

GAT-17 | Proteção Tamper

Descrição: Mecanismos para verificar as configurações lógicas e a integridade física dos ativos tecnológicos ao longo do seu ciclo de vida

Implementação: O Monitor de Integridade de Ficheiros (FIM) deve ser implementado em sistemas que armazenam, processam ou transmitem dados sensíveis para monitorizar a integridade dos ficheiros críticos com o intuito de detetar qualquer adulteração. O Sistema de Prevenção de Intrusões (HIPS) deve ser implementado nos ativos para identificar e bloquear atividades maliciosas. Devem ser realizadas inspeções físicas para validar a integridade dos sistemas sensíveis. As configurações dos sistemas devem ser robustas nos sistemas sensíveis para impor o princípio da "menor funcionalidade", removendo contas, aplicações e serviços desnecessários.

Questão de Controlo: A organização verifica as configurações lógicas e a integridade física dos ativos de tecnologia crítica ao longo do seu ciclo de vida?

Evidências:

1. Monitorização da Integridade do Ficheiro (FIM);
2. Sistema de Prevenção de Intrusão em *endpoints* (HIPS).

3.3.3 *Continuidade de Negócio e Recuperação de Desastres*

CRD-01 | Sistema de Gestão de Continuidade de Negócios (BCMS)

Descrição: Mecanismos para facilitar a implementação de controlos de planeamento de contingência para ajudar a garantir a resiliência dos ativos e serviços.

Implementação: A equpa de TI deve desenvolver planos de recuperação de desastres (PDR) para recuperar sistemas e serviços críticos de negócio.- As partes interessadas devem desenvolver planos de continuidade de negócios (BCPs) para garantir que as funções empresariais são sustentáveis durante e após um incidente.

Questão de Controlo: A organização facilita a implementação de controlos de planeamento de contingência?

Evidências:

1. Plano de Continuidade de Negócio (BCP);
2. Plano de Recuperação de Desastres (PDDR);
3. Plano de Continuidade de Operações (COOP);
4. Análise de Impacto Empresarial (BIA).

CRD-02 | Coordenação com Planos Relacionados

Descrição: Mecanismos para coordenar o desenvolvimento do plano de contingência com elementos internos e externos responsáveis pelos planos conexos.

Implementação: O programa formal de recuperação de desastres (DR) deve existir tanto para a segurança como para a privacidade. A função DR é formalmente atribuída com funções definidas e responsabilidades associadas, incluindo papéis críticos que requerem despedimentos e/ou formação. Os Requisitos de DR para a segurança e privacidade devem ser identificados e documentados. Os controlos devem ser atribuídos a ativos sensíveis para cumprir com os requisitos específicos de DR para facilitar as operações de recuperação de acordo com os Objetivos de Tempo de Recuperação (RTOs) e Objetivos de Ponto de Recuperação (RPOs). Numa base anual, a equipa de DR deve executar exercícios no mundo real para validar os planos de recuperação e contingência de desastres e de viabilidade.A equipa de DR deve trabalhar com as partes interessadas (organizações) para identificar os sistemas e serviços críticos de negócio, incluindo planos relacionados (por exemplo, resposta a incidentes, notificação de violação, etc.). A equipa de TI deve desenvolver os planos de recuperação de desastres (PDR) para recuperar sistemas e serviços críticos do negócio. As partes interessadas das organizações devem desenvolver Planos de Continuidade de Negócios (BCPs) para garantir que as funções empresariais são sustentáveis durante e após um incidente.

Questão de Controlo: A organização coordena o desenvolvimento do plano de contingência com elementos internos e externos responsáveis por planos relacionados?

Evidências:

1. Plano de Resposta a Incidentes de Cibersegurança (IIRP).

CRD-03 | Identificação de Ativos Críticos

Descrição: Mecanismos para identificar e documentar os sistemas, aplicações e serviços críticos que suportam missões essenciais e funções empresariais.

Implementação: A Recuperação de Desastres (DR) deve ser formalmente atribuída como um dever adicional para com a equipa de TI ou de cibersegurança existente.As equipas devem trabalhar com as partes interessadas empresariais para identificar sistemas e serviços críticos do negócios

Questão de Controlo: A organização identifica e documenta os sistemas, aplicações e serviços críticos que suportam missões essenciais e funções empresariais?

Evidências:

1. Análise de Impacto Empresarial (BIA);
2. Avaliações de criticidade.

CRD-04 | Testes e Exercícios do Plano de Contingência

Descrição: Mecanismos para a realização de testes e/ou exercícios para avaliar a eficácia do plano de contingência e a disponibilidade da organização para executar o plano.

Implementação: A equipa de DR deve trabalhar com as partes interessadas empresariais para identificar os sistemas e serviços críticos de negócio, incluindo planos relacionados (por exemplo, resposta a incidentes, notificação de violação, etc.). A equipa de TI deve desenvolver planos de recuperação de desastres (PDR) para recuperar sistemas e serviços críticos do negócio. As partes interessadas das organizações devem desenvolver Planos de Continuidade de Negócios (BCPs) para garantir que as funções empresariais são sustentáveis durante e após um incidente.

Questão de Controlo: A organização realiza testes e/ou exercícios para avaliar a eficácia do plano de contingência e a disponibilidade da organização para executar o plano?

Evidências:

1. Desastres simulados / emergências.

CRD-05 | Testes e Exercícios do Plano de Contingência

Descrição: Mecanismos para coordenar os testes do plano de contingência com elementos internos e externos responsáveis por planos conexos.

Implementação: Pelo menos anualmente, a equipa de DR deve realizar exercícios para validar os planos de recuperação de desastres e planos de contingência. A equipa de DR deve trabalhar com as partes interessadas das organizações para identificar sistemas e serviços críticos de negócio, incluindo equipas internas e prestadores de serviços de terceiros. A equipa de TI deve desenvolver planos de recuperação de desastres (DRP) para recuperar sistemas e serviços críticos de negócio, incluindo equipas internas e prestadores de serviços de terceiros. As partes interessadas devem desenvolver planos de continuidade de negócios (BCPs) para garantir que as funções empresariais são sustentáveis durante e após um incidente.

Questão de Controlo: A organização coordena os testes do plano de contingência com elementos internos e externos responsáveis por planos relacionados?

Evidências:

1. Playbooks;
2. Plano de Continuidade de Operações (COOP).

CRD-06 | Análise da Causa Raiz do Plano de Contingência (RCA) e Lições Aprendidas

Descrição: Mecanismos para a realização de uma atividade de Análise de Causa Raiz (RCA) e "lições aprendidas"sempre que o plano de contingência é ativado.

Implementação: Deve ser realizada uma análise formal da causa-raiz (RCA) que documenta as conclusões num relatório para a gestão técnica e empresarial da liderança.

Questão de Controlo: A organização realiza uma atividade de Análise de Causa Raiz (RCA) e "lições aprendidas"sempre que o plano de contingência é ativado?

Evidências:

1. Procedimentos Operacionais Normalizados (SOP);
2. Plano de Recuperação de Desastres (PDDR);
3. Plano de Continuidade Empresarial (BCP);
4. Plano de Continuidade de Operações (COOP).

CRD-07 | Planeamento de Contingência e Atualizações

Descrição: Mecanismos para manter os planos de contingência atuais com as necessidades da organização, alterações tecnológicas e feedback das atividades de teste do plano de contingência.

Implementação: O programa de recuperação de desastres (DR) deve existir tanto para a segurança como para a privacidade. Os requisitos de Segurança e Privacidade devem ser identificados e documentados. Os controlos devem ser atribuídos a ativos sensíveis para cumprir os requisitos específicos de DR para facilitar as operações de recuperação de acordo com os Objetivos de Tempo de Recuperação (RTOs). Pelo menos numa base anual, a equipa de DR deve realizar exercícios para validar os planos de recuperação e contingência de desastres. A equipa de DR deve trabalhar com as partes interessadas empresariais para identificar sistemas e serviços críticos de negócios, incluindo equipas internas e prestadores de serviços . A equipa de TI deve desenvolver planos de recuperação de desastres (PDR) para recuperar sistemas e serviços críticos do negócio, incluindo equipas internas e prestadores de serviços . As partes interessadas devem desenvolver Planos de Continuidade de Negócios (BCPs) para garantir que as funções empresariais são sustentáveis durante e após um incidente.

Questão de Controlo: A organização mantém os planos de contingência atuais com necessidades empresariais, mudanças tecnológicas e feedback das atividades dos testes do plano de contingência?

Evidências:

1. Documentação offline /offsite;

CRD-08 | Medidas alternativas de segurança

Descrição: Mecanismos para implementar controlos alternativos ou compensatórios para satisfazer funções de segurança quando o principal meio de implementação da função de segurança estiver indisponível ou comprometido.

Implementação: Deve ser identificado e documentado um local de armazenamento alternativo e dedicado. Devem existir tecnologias para realizar cópias de segurança completas, incrementais ou diferenciais (por exemplo, fita/disco, cloud híbrida ou cloud privada). A equipa de TI deve utilizar uma metodologia de backup para armazenar backups separadas do local de armazenamento primário.

Questão de Controlo: A organização implementa controlos alternativos ou compensatórios para satisfazer funções de segurança quando o principal meio de implementação da função de segurança está indisponível ou comprometido?

Evidências:

1. Análise de Impacto Empresarial (BIA);
2. Avaliações de criticidade.

CRD-09 | Disponibilidade de serviços de telecomunicações

Descrição: Mecanismos para reduzir a probabilidade de um único ponto de falha com os serviços primários de telecomunicações.

Implementação: Os responsáveis de aplicações/sistema/processos devem realizar uma Análise de Impacto empresarial (BIA) pelo menos anualmente, ou após qualquer alteração de tecnologia ou processo importante, para identificar pontos únicos de falha. Os responsáveis de aplicações/sistema/processos devem categorizar os dados de acordo com as políticas e normas organizacionais.Os responsáveis de aplicações/sistema/processos, devem, em conjunto com o pessoal de TI e cibersegurança, documentar onde os dados pessoais são armazenados, gerir os diagramas de fluxo de dados (DFDs) e diagramas de rede para documentarem o fluxo de dados com o intuito de criar e manter um mapa de sistemas onde os dados pessoais são armazenados, transmitidos ou tratados. Pelo menos numa base anual, ou após qualquer alteração importante da tecnologia ou do processo, os responsáveis de aplicação/sistema/processo devem atualizar a documentação.

Questão de Controlo: A organização reduz a probabilidade de um único ponto de falha com os serviços primários de telecomunicações?

Evidências:

1. Contrato com fornecedores de telecomunicações (ISP's);

CRD-10 | Backups de dados

Descrição: Mecanismos para criar cópias de segurança recorrentes de dados, software e/ou sistema, bem como verificar a integridade destas cópias de segurança, para garantir a disponibilidade dos dados em prol da satisfação dos Objetivos de Tempo de Recuperação (RTOs) e Objetivos do Ponto de Recuperação (RPOs).

Implementação: A Recuperação de Desastres (DR) deve ser formalmente atribuída como um dever adicional para a equipa de TI ou cibersegurança existente. Pelo menos anualmente, a equipa de DR deve conduzir exercícios para validar planos de recuperação de desastres e planos de contingência. Uma amostragem aleatória de backups deve ser testada pelo menos uma vez ao ano.

Questão de Controlo: A organização cria cópias de segurança recorrentes de dados, software e/ou imagens do sistema, bem como verifica a integridade destas cópias de segurança, para garantir a disponibilidade dos dados para satisfazer os Objetivos de Tempo de Recuperação (RTOs) e Objetivos de Ponto de Recuperação (RPOs)?

Evidências:

1. Tecnologias de Backups;
2. Procedimentos de Backups.

CRD-11 | Proteção Criptográfica

Descrição: Mecanismos criptográficos para impedir a divulgação não autorizada e/ou modificação de informações.

Implementação: Devem existir tecnologias para conduzir plenamente, as cópias de segurança incrementais ou diferenciais. As cópias de segurança devem estar protegidas criptograficamente para impedir a divulgação não autorizada e modificação de informações.

Questão de Controlo: São utilizados mecanismos criptográficos para impedir a divulgação e/ou modificação não autorizadas de informações?

Evidências:

1. Procedimentos de criptografia de informação;
2. Tecnologias de criptografia.

CRD-12 | Sistema Secundário Redundante

Descrição: Mecanismos para manter sistemas contra falhas, que não estão agregados ao sistema primário, aplicação e/ou serviço, que pode ser ativado com pouca ou nenhuma perda de informação ou perturbação nas operações.

Implementação: A equipa de TI deve configurar os sistemas críticos para terem um sistema contra falhas que não esteja agregado com o sistema primário e que possa ser ativado sem qualquer perturbação das operações.

Questão de Controlo: A organização mantém sistemas de failover, que não estão agregados com o sistema primário, aplicação e/ou serviço, que pode ser ativados com pouca ou nenhuma perda de informação ou perturbação nas operações?

Evidências:

1. Arquitetura do Sistema/Serviço.

3.3.4 *Capacidade e Planeamento de Desempenho*

CPD-01 | Planeamento de Capacidades

Descrição: Mecanismos para realizar o planeamento das capacidades, de modo a que exista capacidade necessária para o processamento da informação, telecomunicações e apoio ambiental durante as operações de contingência.

Implementação: A equipa das infraestruturas de TI deve criar e manter um modelo de desempenho da infraestrutura para compreender as necessidades atuais dos recursos.

Questão de Controlo: A organização realizou um planeamento de capacidades para que as necessidade referentes ao processamento de informação, telecomunicações e apoio ambiental existisse durante as operações de contingência?

Evidências:

1. Planeamento das capacidades;

CPD-02 | Monitorização de Desempenho

Descrição: Existem mecanismos automatizados para monitorizar e alertar centralmente sobre o estado operacional e o estado de saúde dos sistemas, aplicações e serviços críticos.

Implementação: A equipa de TI deve trabalhar com as partes interessadas das organizações para identificar os sistemas e serviços críticos do negócio. A equipa de infraestruturas de TI deve criar e manter um modelo de desempenho da infraestrutura para compreender as necessidades atuais dos recursos.

Questão de Controlo: A organização monitoriza e alerta centralmente sobre o estado operacional e o estado de saúde dos sistemas, aplicações e serviços críticos?

Evidências:

1. Ferramenta de monitorização de sistemas e serviços;
2. Relatórios mensais dos problemas identificados pelas plataformas de monitorização.

3.3.5 *Gestão de Mudanças*

GDM-01 | Programa de Gestão de Alterações

Descrição: Mecanismos para facilitar a implementação dos controlos de gestão da mudança.

Implementação: Deve existir um Conselho Consultivo para a Mudança (CAB), ou estrutura semelhante, para reger alterações aos sistemas/aplicações/serviços para garantir a sua estabilidade, fiabilidade e previsibilidade. As alterações devem ser monitorizadas através de uma solução tecnológica centralizada para submeter, rever, aprovar e atribuir Pedidos de Mudança (RFC). Antes de serem feitas alterações, os RFCs devem ser revistos. O controlo de acessos deve ser rígido para limitar a capacidade dos não administradores de fazerem alterações de configuração nos sistemas/aplicações/serviços.

Questão de Controlo: A organização facilita a implementação de controlos de gestão de alterações?

Evidências:

1. Ferramenta de monitorização de alterações;
2. Lista de controlos aplicados nos sistemas/serviços.

GDM-02 | Proibição de alterações

Descrição: Mecanismos para proibir alterações não autorizadas, a menos que sejam recebidos pedidos de alteração aprovados pela organização.

Implementação: Antes de serem efetuadas alterações, os RFCs devem ser revistos na ótica da cibersegurança e privacidade. O controlo de acesso deve ser regido para limitar a capacidade dos não administradores de fazerem alterações de configuração nos sistemas/aplicações/serviços.

Questão de Controlo: A organização proíbe alterações não autorizadas, a menos que sejam recebidos pedidos de alteração aprovados pela organização?

Evidências:

1. Pedidos de alteração aprovados;

GDM-03 | Teste Validação e Alteração

Descrição: Mecanismos para testar e documentar adequadamente as alterações propostas num ambiente de não produção antes de serem implementadas alterações num ambiente de produção.

Implementação: A equipa de TI deve utilizar um ambiente de teste dedicado para implementar alterações. Os controlos de segurança de TI devem ser testados após a alteração ser implementada para garantir que os controlos estão a funcionar corretamente. Os resultados das alterações de teste devem ser documentados.

Questão de Controlo: A organização testa e documenta adequadamente as alterações propostas num ambiente de não produção antes de serem implementadas alterações num ambiente de produção?

Evidências:

1. Procedimento de Testes não produção;

GDM-04 | Análise de impacto de segurança para alterações

Descrição: Mecanismos para analisar as alterações propostas para potenciais impactos de segurança, antes da implementação da alteração.

Implementação: As alterações devem ser monitorizadas através de uma solução tecnológica centralizada para submeter, rever, aprovar e atribuir Pedidos de Mudança (RFC). Antes de serem efetuadas alterações, os RFCs devem ser revistos na ótica da cibersegurança e privacidade.

Questão de Controlo: A organização analisa as alterações propostas para potenciais impactos de segurança, antes da implementação da alteração?

Evidências:

1. Procedimento de alteração;
2. Software de registo de alterações e monitorização.

GDM-05 | Verificação de Funcionalidades de Segurança

Descrição: Mecanismos para verificar a funcionalidade dos controlos de segurança quando são descobertas anomalias.

Implementação: Após a implementação do RFC, a equipa deve implementar os testes de alteração para garantir que os controlos de segurança (antimalware), estão em conformidade e funcionam corretamente.

Questão de Controlo: A organização verifica a funcionalidade dos controlos de segurança quando são descobertas anomalias?

Evidências:

1. Programa de Garantia de Informação (IAP);
2. Teste de Segurança e Avaliação (STE).

3.3.6 *Segurança na Cloud*

SNC-01 | Verificação de Funcionalidades de Segurança

Descrição: Mecanismos para facilitar a implementação de controlos de gestão de cloud para garantir que as instâncias na cloud sejam seguras e estejam em conformidade com as práticas da indústria.

Implementação: Os requisitos para a cloud em relação à segurança e privacidade devem ser identificados e documentados. As tecnologias devem existir para apoiar uma arquitetura segura, incluindo uma zona de segurança gerida para servir de repositório de ferramentas de segurança e privacidade. As instâncias da cloud não devem ser tratadas de forma diferente dos ativos da rede local, ou seja, deve existir um processo de governação de cloud dedicado.

Questão de Controlo: A organização facilita a implementação de controlos de gestão de cloud para garantir que as situações de cloud são seguras e em linha com as práticas da indústria? ?

Evidências:

1. Avaliação de Impacto da Proteção de Dados (DPIA).

SNC-02 | Arquitetura de Segurança da Cloud

Descrição: Mecanismos para garantir que a arquitetura de segurança na cloud apoia a estratégia tecnológica da organização para projetar, configurar a cloud de forma segura.

Implementação: As funções, responsabilidades e requisitos específicos da cloud para arquitetos e engenheiros de segurança devem ser identificados e documentados.

Questão de Controlo: A organização garante que a arquitetura de segurança na cloud apoia a estratégia tecnológica da organização para conceber, configurar a cloud de forma segura?

Evidências:

1. Conselho de Revisão;
2. Plano de Segurança do Sistema (SSP);
3. Procedimento de arquitetura de segurança.

SNC-03 | Sub-rede de gestão de segurança

Descrição: Mecanismos para acolher tecnologias específicas de segurança numa sub-rede dedicada.

Implementação: Os requisitos de cibersegurança para a segurança e privacidade de sub-redes devem ser identificados e documentados. Devem existir tecnologias para apoiar uma infraestrutura segura.

Questão de Controlo: A organização acolhe tecnologias específicas de segurança numa sub-rede dedicada?

Evidências:

1. Sub-rede de gestão de segurança;

SNC-04 | Imagens de máquinas virtuais

Descrição: Mecanismos para garantir a integridade das imagens de máquinas virtuais em todos os momentos.

Implementação: Os requisitos na cloud para segurança e privacidade das máquinas virtuais devem ser identificados e documentados. Devem existir tecnologias para apoiar a integridade das imagens virtuais.

Questão de Controlo: A organização garante sempre a integridade das imagens de máquinas virtuais?

Evidências:

1. Procedimento de gestão de máquinas virtuais;
2. Ferramenta de verificação de integridade.

SNC-05 | Ambientes Multi-Tenant

Descrição: Mecanismos para garantir que os ativos detidos ou geridos multi-tenant (físicos e virtuais) sejam concebidos e regidos de modo a que o acesso do utilizador ao fornecedor e ao cliente seja devidamente segmentado.

Implementação: Os requisitos na cloud para a segurança e privacidade de bens detidos ou geridos multi-tenant devem ser identificados e documentados. Devem existir tecnologias para apoiar a integridade dos ativos detidos ou geridos por vários clientes.

Questão de Controlo: A organização garante que os ativos multi-tenant ou geridos (físicos e virtuais) são projetados e regidos de modo a que o acesso ao utilizador do fornecedor e cliente seja devidamente segmentado ?

Evidências:

1. Revisão da arquitetura de segurança;
2. Processos definidos para segmentar redes, aplicações e camadas de bases de dados.

SNC-06 | Tratamento de Dados e Portabilidade

Descrição: Mecanismos para garantir que os fornecedores de cloud utilizam protocolos seguros para a importação, exportação e gestão de dados em serviços baseados na cloud.

Implementação: Os requisitos na cloud para o tratamento de dados e portabilidade devem ser identificados e documentados. Devem existir tecnologias para apoiar o tratamento de dados e portabilidade.

Questão de Controlo: A organização garante que os fornecedores de cloud utilizam protocolos seguros para a importação, exportação e gestão de dados em serviços baseados na cloud?

Evidências:

1. Avaliação de Impacto da Proteção de Dados (DPIA);
2. Transferência de dados encriptadas (por exemplo, TLS ou VPNs).

SNC-07 | Ponto de Acesso à Cloud (CAP)

Descrição: Mecanismos para garantir que os fornecedores de cloud utilizem protocolos seguros para a importação, exportação e gestão de dados em serviços baseados na cloud.

Implementação: Os requisitos na cloud para o tratamento de dados e portabilidade devem ser identificados e documentados. Devem existir tecnologias para apoiar o tratamento de dados e portabilidade.

Questão de Controlo: A organização garante que os fornecedores de cloud utilizam protocolos seguros para a importação, exportação e gestão de dados em serviços baseados na cloud?

Evidências:

1. Avaliação de Impacto da Proteção de Dados (DPIA);
2. Transferência de dados encriptadas (por exemplo, TLS ou VPNs).

3.3.7 *Conformidade*

COF-01 | Conformidade Legal Regulamentar e Contratual

Descrição: Mecanismos que facilitam a identificação e implementação de controlos estatutários, regulamentares e contratuais relevantes.

Implementação: A função de segurança na área de TI deve utilizar um processo estruturado para reger obrigações legais, regulamentares e contratuais em prol da conformidade. Esta função de TI deve executar uma revisão anual dos requisitos de conformidade existentes e efetuar pesquisas sobre a evolução ou novos requisitos que não estejam no âmbito já existente. Aos gestores dos ativos devem ser atribuídos papéis e responsabilidades que abordam os requisitos técnicos de conformidade.

Questão de Controlo: A organização facilita a implementação de controlos estatutários, regulamentares e contratuais relevantes?

Evidências:

1. Ferramenta de governação, risco e conformidade (GRC);
2. Comissão de Gestão de Risco.

COF-02 | Supervisão de Controlos de Segurança e Privacidade

Descrição: Mecanismos para fornecer uma função de supervisão de controlo de segurança e privacidade que reporta à administração da organização.

Implementação: Deve ser realizada uma supervisão semestral sobre os controlos de segurança e privacidade e reportada esta informação à administração da organização.

Questão de Controlo: A organização fornece uma função de supervisão de controlo de segurança e privacidade que reporta à administração da organização?

Evidências:

1. Ferramenta de governação, risco e conformidade (GRC);
2. Plano de Supervisão dos controlos de segurança e privacidade.

COF-03 | Função de Auditoria Interna

Descrição: Mecanismos para implementar uma função de auditoria interna capaz de fornecer à administração das organizações informações sobre a adequação dos processos de gestão tecnológica da organização.

Implementação: É necessário definir um processo para implementar uma função de auditoria interna capaz de fornecer informações sobre a adequação dos processos de gestão tecnológica da organização.

Questão de Controlo: A organização implementa uma função de auditoria interna capaz de fornecer à direção da organização informações sobre a adequação dos processos de gestão de tecnologia da organização?

Evidências:

1. Plano de Auditorias Internas;

COF-04 | Avaliações de Segurança

Descrição: Mecanismos para garantir que os gestores revejam regularmente os processos e procedimentos documentados no âmbito da sua área de responsabilidade para aderir às políticas, normas e procedimentos de segurança.

Implementação: A equipa de segurança deve gerar um relatório formal para cada avaliação de segurança que documente a avaliação dos controlos de segurança para determinar o risco aceitável.

Questão de Controlo: A organização garante que os gestores revejam regularmente os processos e procedimentos documentados dentro da sua área de responsabilidade para aderir às políticas de segurança, normas e procedimentos aplicáveis?

Evidências:

1. Programa de Garantia de Informação (IAP);
2. Teste de Avaliação e Segurança (STE).

COF-05 | Revisão Funcional dos Controlos de Segurança

Descrição: Mecanismos para rever regularmente os ativos tecnológicos para a adesão às políticas e padrões de cibersegurança e privacidade da organização.

Implementação: A equipa de cibersegurança deve utilizar um processo estruturado para reger obrigações legais, regulamentares e contratuais na ótica da conformidade. Esta equipa deve executar uma revisão anual dos requisitos de conformidade existentes e pesquisar novos requisitos que não estejam no âmbito atual. Deve ser utilizado um conjunto de controlos adequados para realizar avaliações de segurança e controlo de privacidade, tal como definido pelos requisitos legais, regulamentares e contratuais aplicáveis. Numa base anual, deve ser realizada uma avaliação dos controlos de segurança e privacidade aplicáveis. Por fim, a equipa de cibersegurança deve gerar um relatório formal para cada avaliação de segurança que documenta a avaliação dos controlos de segurança e privacidade para determinar o risco aceitável.

Questão de Controlo: A organização revê regularmente os ativos tecnológicos para aderir às políticas e padrões de cibersegurança e privacidade da organização?

Evidências:

1. Procedimentos de revisão operacional;
2. Procedimento de revisão anual de políticas e procedimentos.

COF-06 | Notificações de Pedido de Investigação Forense

Descrição: Mecanismos para notificar os clientes sobre notificações de pedidos de investigação, a menos que a base legal aplicável para a ação de uma agência governamental proíba a notificação (por exemplo, um potencial processo penal).

Implementação: Os pedidos de investigação devem ser tratados de acordo com um Plano de Resposta a Incidentes (IRP). A representação legal deve ser consultada se necessário.

Questão de Controlo: A organização notifica os clientes sobre notificações de pedidos de investigação, a menos que a base legal aplicável para a ação de uma agência governamental proíba a notificação (por exemplo, potencial processo penal)?

Evidências:

1. Procedimento de notificação de pedidos de Investigação Forenses.

3.3.8 *Gestão de Configuração*

GDC-01 | Programa de Gestão de Configuração

Descrição: Mecanismos para facilitar a implementação dos controlos de gestão de configuração.

Implementação: A equipa de cibersegurança deve utilizar um processo estruturado para conceber, construir e manter configurações seguras para ambientes de teste, desenvolvimento e produção. Devem ser utilizadas as orientações de configuração seguras adequadas para responder aos requisitos legais, regulamentares e contratuais aplicáveis. Para além das linhas de base do sistema operativo das estações de trabalho e servidores, a gestão da configuração deve ser descentralizada. As configurações devem corresponder maioritariamente às normas reconhecidas pela indústria (por exemplo, testes do CIS ou guias de segurança OEM), incluindo proteções criptográficas para dados sensíveis. Deve ser realizada uma revisão anual das configurações existentes para garantir que os objetivos de segurança ainda estão a ser cumpridos. Devem ser mantidas versões históricas de configurações para resolução de problemas e objetivos forenses. Devem ser criadas configurações de base especiais para ambientes de "alto risco"ou para sistemas /aplicações/serviços que armazenam, processam ou transmitem dados sensíveis. Os desvios às configurações de base devem ser necessários para ter uma avaliação de risco e o proprietário do processo de negócio deve aceitar o risco(s) associado ao desvio. As alterações de configuração não autorizadas devem ser respondidas de acordo com a configuração não autorizada.

Questão de Controlo: A organização facilita a implementação de controlos de gestão de configuração?

Evidências:

1. Base de Dados de Gestão de Configuração;
2. Programa de Garantia de Informação (IAP);
3. Teste de Segurança e Avaliação.

GDC-02 | Menor funcionalidade

Descrição: Mecanismos de configuração de sistemas que apenas fornecem capacidades essenciais, proibindo ou restringindo especificamente a utilização de portos, protocolos e/ou serviços.

Implementação: A equipa de segurança de TI deve utilizar as orientações de configuração seguras adequadas para responder aos requisitos legais, regulamentares e contratuais aplicáveis. Para além das linhas de base do sistema operativo relacionadas com a estação de trabalho e servidores, deve existir uma verificação mensal dos sistemas perimétricos (Firewalls, Balanceadores) na óticas das regras e permissões de acesso aos sistemas internos, quer via rede exterior, quer via rede interna. Devem ser documentadas as regras aplicadas, os utilizadores com acesso administrativo. Os privilégios dos utilizadores devem ser auditados, e apenas conter as permissões necessárias à sua função laboral.

Questão de Controlo: A organização configura sistemas para fornecer apenas capacidades essenciais, proibindo ou restringindo especificamente o uso de portos, protocolos e/ou serviços?

Evidências:

1. Listagem de regras das Firewalls;
2. Relatório de auditoria mensal aos sistemas (utilizadores privilegiados);
3. Testes de Segurança e Avaliação.

GDC-03 |Software Instalado pelo Utilizador

Descrição: Mecanismos para restringir a capacidade de utilizadores não privilegiados de instalarem software não autorizado.

Implementação: Regras de comportamento aceitável devem abordar a exigência de que os utilizadores cumpram os requisitos de utilização do software aplicáveis e as leis de direitos de autor. As tecnologias baseadas na rede devem bloquear ficheiros com extensões de execuções conhecidas (.exe, .msi, .bin). As tecnologias baseadas no host devem bloqueiar extensões e tipos de ficheiros conhecidos ou bloquear totalmente os meios de comunicação amovíveis. O controlo de acesso deve ser imposto para proibir os utilizadores não administrativos de poderem instalar software não autorizado.

Questão de Controlo: A organização restringe a capacidade de utilizadores não privilegiados instalarem software não autorizado?

Evidências:

1. Gestão de Conta Privilegiada (PAM).

3.3.9 *Monitorização Contínua*

MOC-01 | Monitorização Contínua

Descrição: Mecanismos para facilitar a implementação dos controlos de monitorização a nível organizacional.

Implementação: As configurações de base do sistema devem gerar registos que contêm informações suficientes para estabelecer as indicações necessárias de atividade e que permitam efetuar uma análise forense. As configurações de base do sistema devem impor o registo que interliga o acesso do sistema a utilizadores individuais ou contas de serviço que utilizam uma capacidade de não-repúdio para proteger contra um indivíduo que nega falsamente ter realizado uma determinada ação. As configurações de base do sistema devem armazenar registos localmente e reencaminhar os mesmos para um repositório de logs centralizado para fornecer uma capacidade de auditoria alternativa em caso de falha na capacidade de auditoria primária (local). As configurações de base do sistema devem restringir o acesso à gestão de registos de eventos a utilizadores privilegiados com uma necessidade específica de proteger os dados sobre eventos e ferramentas de auditoria de acesso não autorizado. As configurações de base do sistema devem manter os registos de auditoria por um período de tempo consistente com os requisitos de retenção de registos para fornecer apoio a investigações de incidentes de segurança e para satisfazer os requisitos legais, regulamentares e de retenção contratual. Os registos de funções privilegiadas (por exemplo, administrador ou ações de sistema) devem ser revistos para comprovativo de atividades não autorizadas. Um agregador de registos, ou uma ferramenta automatizada semelhante, deve monitorizar sistemas críticos para atividades não autorizadas. Um agregador de registos, ou uma ferramenta automatizada semelhante, deve fornecer uma capacidade de geração de relatórios de eventos para ajudar na deteção e avaliação de atividades anómalas em sistemas críticos.

Questão de Controlo: A organização facilita a implementação de controlos de monitorização a nível organizacional?

Evidências:

1. Ferramenta SIEM (Splunk,QRadar, FortiSiem,OSSEC, LogPoint entre outras);
2. Relatório de registo de eventos mensais de alterações a sistemas críticos.

MOC-02 | Sistemas de Deteção e Prevenção de Intrusões (IDS e IPS)

Descrição: Mecanismos para implementar tecnologias de Deteção/Prevenção de Intrusões (IDS/ IPS) em sistemas críticos, segmentos de rede chave e pontos de interligação de redes internas com redes externas.

Implementação: Os flows de rede devem ser registados a fim de identificar atividades proibidas e ajudar os analistas de segurança a identificar sistemas potencialmente comprometidos. Devem ser ativadas as tecnologias IDS e IPS com interligação a um repositório de IoCs, para efetuar o bloqueio de ficheiros, ligações a endereços IP maliciosos e domínios através da rede interna.

Questão de Controlo: A organização implementa tecnologias de Deteção/Prevenção de Intrusões (IDS/ IPS) em sistemas críticos, segmentos de rede chave e interligações de redes internas com redes externas?

Evidências:

1. IDS/IPS;
2. Repositório de IoCs;
3. Logs dos sistemas de deteção ou prevenção de intrusão de rede.

MOC-03 | Ferramentas Automatizadas para Análise em Tempo Real

Descrição: Mecanismos para utilizar um Gestor de Eventos de Segurança (SIEM), ou uma ferramenta automatizada semelhante, para suportar a análise em tempo real de incidentes.

Implementação: Implementação e configuração de um Gestor de Eventos de Segurança, ou ferramenta semelhante, que consiga ingerir logs dos vários sistemas de rede e os correlacione de forma adequada. Configuração dos casos de uso para alertar em caso de deteção de um incidente.

Questão de Controlo: A organização utiliza um Gestor de Eventos de Segurança (SIEM), ou uma ferramenta automatizada semelhante, para suportar a análise em tempo real incidentes?

Evidências:

1. SIEM;
2. Listagem dos casos de uso introduzidos no SIEM.

MOC-04 | Tráfego de Comunicações de Entrada e Saída

Descrição: Mecanismos para monitorizar continuamente o tráfego de comunicações de entrada e saída para atividades ou condições incomuns ou não autorizadas.

Implementação: Implementação e configuração de Netflow ou sFlow, para monitorizar os fluxos de rede. Pode ser implementada a monitorização da rede e a respetiva análise através de soluções de análise de pacotes (Ex: Zeek). Configuração de casos de uso nas ferramentas de monitorização para detetar tráfego anómalo.

Questão de Controlo: A organização monitoriza continuamente o tráfego de comunicações de entrada e saída para atividades ou condições incomuns ou não autorizadas?

Evidências:

1. Flows de tráfego com retenção de 60 dias, no mínimo;
2. Listagem dos Equipamentos que contêm a configuração de análise e monitorização de tráfego.

MOC-05 | Alertas Automatizados

Descrição: Mecanismos automatizados para alertar a equipa de resposta a incidentes de atividades inadequadas ou incomuns que tenham implicações em incidentes de segurança.

Implementação: Implementação e configuração de fluxos de ações, em caso de deteção de um incidente, quais os membros da equipa de resposta a incidentes que devem ser contactadas. Casos de uso, para detetar e alertar em tempo real as equipas responsáveis pelos sistemas de informação. Utilização e implementação de ferramentas que permitam interligar vários sistemas entre si, unificando o acesso central aos incidentes e às notificações. (Ex: SOAR integrado com um SIEM e comunicando os alertas via webhooks ao Slack).

Questão de Controlo: A organização tem sistemas de alerta para a equipa de resposta a incidentes sobre atividades inadequadas ou incomuns que têm implicações em incidentes de segurança?

Evidências:

1. Registo dos alertas de segurança anuais;
2. Ferramenta SOAR;
3. Ferramenta unificada de receção de alertas (MS Teams, Slack, PagerDuty entre outros).

MOC-06 | Monitorização dos Indicadores de Compromisso (IOC)

Descrição: Mecanismos automatizados para identificar e alertar sobre os Indicadores de Compromisso (IoC).

Implementação: Uma ferramenta SIEM, ou uma ferramenta automatizada semelhante, deve monitorizar as atividades não autorizadas, contas, ligações, dispositivos e software de acordo com os indicadores de compromisso específicos da organização (IoC), incluindo feeds de scanners de vulnerabilidade. Deve existir também um repositório interno de IoC's que permita a ingestão destes dados por parte dos equipamentos ativos, nomeadamente firewalls, EDR/XDR, WAF's entre outros, para bloqueaream os indicadores de compromisso automaticamente.

Questão de Controlo: A organização tem sistemas de alerta para a equipa de resposta a incidentes sobre atividades inadequadas ou incomuns que têm implicações em incidentes de segurança?

Evidências:

1. SIEM;
2. Plataforma de TIP (Threat Intel) com interligações a feeds exteriores de confiança;

MOC-07 | Comportamento Anómalo

Descrição: Mecanismos para detetar e responder a comportamentos anómalos que possam indicar o compromisso da conta ou outras atividades maliciosas.

Implementação: Os registos de funções privilegiadas (por exemplo, administrador ou ações de sistema) devem ser revistos para comprovar as atividades não autorizadas. Um agregador de registos, ou uma ferramenta automatizada semelhante, deve monitorizar os sistemas críticos na ótica de atividades não autorizadas. Um agregador de registos, ou uma ferramenta automatizada semelhante, deve fornecer uma capacidade de geração de relatório de eventos para ajudar na deteção e avaliação de atividades anómalas em sistemas críticos. Os pedidos de ligação à Internet devem ser registados a fim de identificar atividades proibidas e ajudar a equipa de resposta a incidentes a identificar sistemas potencialmente comprometidos.

Questão de Controlo: A organização deteta e responde a comportamentos anómalos que possam indicar o compromisso da conta ou outras atividades maliciosas?

Evidências:

1. SIEM;
2. Relatórios semanais de funções privilegiadas e respetivos acessos.

3.3.10 *Proteções Criptográficas*

PCR - 01 | Utilização de Controlos Criptográficos

Descrição: Mecanismos para facilitar a implementação de controlos de proteções criptográficas utilizando normas públicas conhecidas e tecnologias criptográficas fidedignas.

Implementação: As configurações devem estar em conformidade com as normas de segurança reconhecidas pela indústria (por exemplo, STIGs DISA, CIS Benchmarks ou guias de segurança OEM) para ambientes de teste, desenvolvimento e produção, incluindo a implementação de controlos de proteções criptográficas utilizando normas públicas conhecidas e tecnologias criptográficas fidedignas para proteger a confidencialidade e integridade dos dados.Todos os casos de acesso administrativo não-consola devem utilizar mecanismos criptográficos para proteger a confidencialidade e integridade dos dados que estão a ser transmitidos. Todas as bases de dados que contenham dados sensíveis devem utilizar um mecanismo criptográfico para impedir a divulgação não autorizada de informações presente na base de dados (por exemplo, Encriptação de Dados Transparente (TDE), etc.). Todas as comunicações de rede que contenham dados sensíveis devem utilizar um mecanismo criptográfico para impedir a divulgação não autorizada de informações durante o trânsito (por exemplo, SSH, TLS, VPN, etc.). A equipa de TI ou função semelhante, deve implementar e manter uma infraestrutura de chaves públicas internas (PKI) ou obter os serviços de PKI através de um prestador de serviços. A função de gestão de PKI deve facilitar a implementação de controlos de gestão de chaves criptográficas para proteger a confidencialidade, integridade e disponibilidade das chaves.

Questão de Controlo: A organização facilita a implementação de controlos criptográficos utilizando padrões públicos conhecidos e tecnologias criptográficas confiáveis?

Evidências:

1. Ferramenta de Gestão de Chaves e Certificados;
2. Procedimentos de encriptação de dados em trânsito e gestão de chaves e certificados.

PCR - 02 | Confidencialidade da Comunicação

Descrição: Mecanismos criptográficos para proteger a confidencialidade e a integridade dos dados que estão a ser transmitidos.

Implementação: Devem ser utilizados protocolos de comunicação segura para a transmissão de dados e com autenticação forte. As comunicações devem ser cifradas de modo a proteger a confidencialidade e integridade dos dados.

Questão de Controlo: Os mecanismos criptográficos são utilizados para proteger a confidencialidade dos dados que estão a ser transmitidos?

Evidências:

1. Utilização do Protocolos SSL /TLS;
2. Túneis IPSec;
3. Configurações de túneis encriptados MPLS;
4. Procedimento de encriptação de dados em trânsito.

PCR - 03 | Encriptação de dados em Repouso

Descrição: Mecanismos criptográficos para impedir a divulgação não autorizada de dados em repouso.

Implementação: Devem ser utilizados mecanismos de proteção de dados em repouso, com criptografia forte. Devem ser aplicados controlos de acesso com o principio de privilégio mínimo.

Questão de Controlo: Os mecanismos criptográficos são utilizados em sistemas para impedir a divulgação não autorizada de dados em repouso?

Evidências:

1. Ferramentas de proteção de dados;
2. Política de Gestão de dados em repouso;
3. Procedimento de gestão de dados em repouso.

PCR - 04 | Gestão de Chaves Criptográficas

Descrição: Mecanismos para facilitar os controlos de gestão de chaves criptográficas para proteger a confidencialidade, integridade e disponibilidade de chaves.

Implementação: A equipa de TI, ou função semelhante, deve implementar e manter uma infraestrutura de chaves públicas interna (PKI) ou obter este serviço de PKI através de um prestador de serviços. A infraestrutura de PKI deve assegurar a disponibilidade de informação em caso de perda de chaves criptográficas por utilizadores individuais. A infraestrutura de PKI deve facilitar a distribuição segura de chaves criptográficas simétricas e assimétricas utilizando tecnologia e processos de gestão de chaves reconhecidos pela indústria. Todas as chaves criptográficas devem estar ligadas a identidades individuais.

Questão de Controlo: A organização facilita os controlos de gestão de chaves criptográficas para proteger a confidencialidade, integridade e disponibilidade de chaves?

Evidências:

1. Ferramentas de gestão de chaves e certificados (Microsoft Active Directory Certificate Services, Digitcert, Comodo, ...);

3.3.11 *Classificação e Tratamento de Dados*

CTD - 01 | Proteção de Dados

Descrição: Mecanismos para facilitar a implementação dos controlos de proteção de dados.

Implementação: Os controlos físicos, processos administrativos e tecnologias devem focar-se na proteção de Ativos de Alto Valor (HVAs), incluindo ambientes onde os dados sensíveis são armazenados, transmitidos e processados. Os controlos de proteção de dados devem ser principalmente de natureza administrativa e preventiva (por exemplo, políticas e normas) para classificar, proteger e eliminar sistemas e dados. A gestão de dados deve ser descentralizada onde se espera que os proprietários dos processos empresariais tomem a iniciativa de trabalhar com os Responsáveis pela Proteção de Dados (DPOs) para garantir a aplicação da lei. As obrigações regulamentares e contratuais devem ser devidamente abordadas, incluindo o armazenamento, transmissão e tratamento de dados sensíveis.

Questão de Controlo: A organização facilita a implementação de controlos de proteção de dados?

Evidências:

1. N/D.

CTD - 02 | Sanitização de Dados Pessoais (PD)

Descrição: Mecanismos para facilitar a higienização dos Dados Pessoais (PD).

Implementação: Deve existir um programa de IT Asset Management (ITAM) ou função similar, que categoriza os ativos de acordo com os dados que os ativos armazenam, transmitem e/ou processam e aplica os controlos tecnológicos adequados para proteger os dados de acordo com os requisitos de classificação e tratamento de dados da organização. O ITAM, ou função semelhante, deve garantir que as ações de saneamento e eliminação dos meios de comunicação são documentadas e verificadas. Uma ITAM, ou função semelhante, deve garantir que os equipamentos e procedimentos de saneamento são testados para verificar se o resultado pretendido é alcançado. Um ITAM, ou função semelhante, deve facilitar a destruição de Dados Pessoais (PD). Devem existir processos administrativos e tecnologias para armazenar de forma segura meios digitais e não digitais em áreas controladas utilizando medidas de segurança definidas pela organização e por fim proteger os meios de comunicação do sistema até que os meios sejam destruídos ou higienizados utilizando equipamentos, técnicas e procedimentos aprovados.

Questão de Controlo: A organização facilita a higienização dos Dados Pessoais (PD)?

Evidências:

1. Procedimento de Higienização de Dados Pessoais.

CTD - 03 | Sistemas / Componentes / Dispositivos não Organizacionais

Descrição: Mecanismos para restringir a utilização de sistemas de informação não pertencentes à organização, componentes ou dispositivos do sistema para processar, armazenar ou transmitir informações organizacionais.

Implementação: Deve existir um programa de gestão de Ativos de TI (ITAM) ou função semelhante, que regula a gestão de ativos para garantir o cumprimento dos requisitos para a gestão de ativos. O ITAM deve alavancar uma Base de Dados de Gestão de Configuração (CMDB), ou uma ferramenta similar. A função de ITAM deve ser formalmente atribuída com funções definidas e responsabilidades associadas, incluindo a definição de critérios de Controlo de Acesso à Rede (NAC), como parte de comportamentos aceitáveis e inaceitáveis.

Questão de Controlo: A organização restringe a utilização de sistemas de informação não pertencentes a organizações, componentes ou dispositivos de sistema para processar, armazenar ou transmitir informações organizacionais?

Evidências:

1. Controlo de Acesso à Rede (NAC);
2. ITAM.

CTD - 04 | Eliminação de Informações

Descrição: Mecanismos para eliminar, destruir ou apagar informações de forma segura.

Implementação: A equipa de Governação, Risco e Compliance (GRC) ou função semelhante, deve garantir que as obrigações legais, regulamentares e contratuais de cibersegurança e privacidade para a proteção de dados são devidamente endereçadas.O programa de Gestão de Ativos de TI (ITAM), ou função semelhante, deve categorizar os ativos de acordo com os dados que os ativos armazenam, transmitem e/ou processam e devem aplicar os controlos tecnológicos adequados para proteger os dados de acordo com os requisitos de classificação e tratamento de dados da organização. Os processos e tecnologias administrativas devem reter meios e dados de acordo com as obrigações legais, regulamentares e contratuais aplicáveis. Os processos administrativos e as tecnologias devem proteger os dados armazenados de acordo com as obrigações legais, regulamentares e contratuais aplicáveis. Os controlos físicos, processos administrativos e tecnologias devem ter possibilidade para destruir ou apagar informação de forma segura. Os processos e tecnologias administrativas devem eliminar seguramente os meios de comunicação quando já não são necessários, utilizando procedimentos estabelecidos pela organização.

Questão de Controlo: A organização elimina, destrói ou apaga informação de forma segura?

Evidências:

1. Solução Shred-it (Eliminação Segura);
2. Procedimento de eliminação de dados.

CTD - 05 | Eliminação Mascaramento Encriptação Hashing ou Substituição de Identificadores Diretos

Descrição: Mecanismos para remover, mascarar, encriptar, colocar hashs ou substituir identificadores diretos num conjunto de dados.

Implementação: Uma Avaliação de Impacto de Proteção de Dados (DPIA) deve ser utilizada para ajudar a garantir a proteção de informações sensíveis processadas, armazenadas ou transmitidas em sistemas externos, de modo a que os controlos de segurança e privacidade sejam implementados de acordo com as obrigações legais, regulamentares e contratuais aplicáveis. Os processos e tecnologias administrativas devem remover Dados Pessoais (PD) do conjuntos de dados. Os processos administrativos e tecnologias devem selecionar os dados no conjunto após a recolha, não recolhendo dados pessoais. Os processos e tecnologias administrativos devem proteger os dados armazenados de acordo com as obrigações legais, regulamentares e contratuais aplicáveis. Os processos e tecnologias administrativas devem abster-se de armazenar elementos de Dados Pessoais (PD) se esses elementos não forem necessários após o arquivo do conjunto de dados. Os processos e tecnologias administrativas devem remover os elementos de Dados Pessoais (PD) de um conjunto de dados antes da sua libertação se esses elementos não precisarem de fazer parte da libertação de dados.

Questão de Controlo: A organização remove, mascara, encripta, aplica hashs ou substitui identificadores diretos num conjunto de dados?

Evidências:

1. Avaliação de Impacto da Proteção de Dados (DPIA).

3.3.12 *Segurança de Endpoint*

SEN - 01 | Segurança de Endpoint

Descrição: Mecanismos para facilitar a implementação dos controlos de segurança nos endpoints.

Implementação: As alterações de configuração não autorizadas devem ser respondidas de acordo com o Plano de Resposta a Incidentes (IRP) para determinar se qualquer configuração não autorizada é de natureza maliciosa. O departamento de segurança da informação, ou uma função semelhante, deve garantir que os sistemas, aplicações e processos estão em conformidade com os padrões reconhecidos pela indústria para o endurecimento das configurações (por exemplo, DISA STIGs, CIS Benchmarks ou guias de segurança OEM) para ambientes de teste, desenvolvimento e produção. Isto inclui a criação de requisitos especiais de endurecimento para atividades de Ativos de Alto Valor (HVAs). O centro de Operações de Segurança (SOC), ou função semelhante, deve gerir centralmente tecnologias anti-malware e anti-phishing, de acordo com práticas reconhecidas pela indústria para atividades de Prevenção, Deteção e Resposta (PDR). Uma Gestão de Identidade e Acesso (IAM), ou função similar, deve gerir permissões e implementar soluções com o minímo privilégio necessário.

Questão de Controlo: A organização facilita a implementação de controlos de segurança em endpoints?

Evidências:

1. Políticas de Grupo (GPOs);
2. Solução EDR/XDR;
3. Firewalls de software.

SEN - 02 | Proibir Instalações sem Estatuto Privilegiado

Descrição: Mecanismos para proibir a instalação de software por parte do utilizador sem o estatuto privilegiado explicitamente atribuído.

Implementação: Deve ser implementada uma política de configuração para todos os sistemas, onde inicialmente o utilizador não terá acesso administrativo, só em caso desse utilizador ser um utilizador privilegiado. A administração dos sistemas deve só ser possível através de contas de utilizador nominais administrativas.

Questão de Controlo: A organização facilita a implementação de controlos de segurança em endpoints?

Evidências:

1. Políticas de Grupo (GPOs);
2. Sistema de Gestão de Contas Privilegiadas (PAM).

SEN - 03 | Proteção de Código Malicioso (Anti-Malware)

Descrição: Mecanismos para utilizar tecnologias antimalware para detetar e erradicar código malicioso.

Implementação: Deve ser implementada e disponibilizada uma solução de proteção contra código malicioso nos sistemas da organização (EDR/XDR).

Questão de Controlo: A organização utiliza tecnologias antimalware para detetar e erradicar código malicioso?

Evidências:

1. Solução para proteção contra código malicioso (EDR/XDR).

SEN - 04 | Atualizações Automáticas

Descrição: Mecanismos para atualizar automaticamente as tecnologias antimalware, incluindo definições de assinatura.

Implementação: Deve ser implementada uma política e automatismos para efetuar as atualizações de todas as bases de dados de indicadores de compromisso e assinaturas das tecnologias antimalware.

Questão de Controlo: A organização atualiza automaticamente as tecnologias antimalware, incluindo definições de assinatura?

Evidências:

1. Solução para proteção contra código malicioso (EDR/XDR)
2. Configuração de atualizações automáticas nos sistemas antimalware.

SEN - 05 | Software Firewall

Descrição: Mecanismos para utilizar software de firewall baseado no host, ou uma tecnologia semelhante, em todos os sistemas de informação, sempre que tecnicamente exequível.

Implementação: Deve ser implementada configurada uma firewall de software em cada host, se possível.

Questão de Controlo: A organização utiliza software de firewall baseado no host, ou uma tecnologia similar, em todos os sistemas de informação, onde tecnicamente viável?

Evidências:

1. Firewal de software.

SEN - 06 | Verificações de Integridade

Descrição: Mecanismos para validar configurações através da verificação de integridade de software e firmware.

Implementação: Deve ser implementada e configurada a tecnologia do Monitor de Integridade de Ficheiros (FIM) para detetar e reportar alterações não autorizadas em ficheiros e configurações críticas dos sistemas.

Questão de Controlo: A organização valida configurações através da verificação de integridade de software e firmware?

Evidências:

1. Monitor de Integridade de Ficheiros (FIM).

SEN - 07 | Proteção de Phishing e Spam

Descrição: Mecanismos para utilizar tecnologias anti-phishing e de proteção de spam para detetar e tomar medidas em mensagens não solicitadas transportadas por correio eletrónico.

Implementação: Deve ser implementada e configurada uma proteção contra Phishing e Spam nos sistemas de correio eletrónico da organização.

Questão de Controlo: A organização utiliza tecnologias de proteção anti-phishing e spam para detetar e tomar medidas em mensagens não solicitadas transportadas por correio eletrónico?

Evidências:

1. Tecnologias anti-phishing e proteção de spam.

3.3.13 *Segurança de Recursos Humanos*

SRH - 01 | Gestão de Segurança de Recursos Humanos

Descrição: Mecanismos para garantir que todos os utilizadores que acedam a um sistema que processa, armazena ou transmita informações sensíveis são limpos e regularmente treinados para lidar com a informação em causa.

Implementação: A equipa de RH, ou função semelhante, deve gerir o risco de segurança dos colaboradores, atribuindo uma designação de risco a todas as posições e estabelecendo critérios de análise para indivíduos que preenchem essas posições.A equipa de HR, ou função semelhante, deve garantir que todos os utilizadores que acedam a um sistema que processa, armazena ou transmite informações sensíveis são limpos e regularmente treinados em práticas adequadas de tratamento de dados.

Questão de Controlo: A organização garante que todos os utilizadores que acedam a um sistema que processa, armazena ou transmite informações sensíveis são limpos e regularmente treinados para lidar com a informação em causa?

Evidências:

1. N/D.

SRH - 02 | Utilizadores com Privilégios Elevados

Descrição: Mecanismos para facilitar a implementação dos controlos de segurança dos colaboradores.

Implementação: A equipa de RH, em conjunto com a equipa de GRC, deve definir termos de contrato, regras aceitáveis e inaceitáveis de comportamento para o uso de tecnologias, incluindo consequências para comportamentos inaceitáveis. A equipa de GRC deve facilitar a implementação de controlos de segurança e privacidade com ois proprietários dos ativos/processos.Um sistema de Gestão de Identidade e Acesso (IAM), ou função similar, deve gerir centralmente permissões e implementar práticas de "menos privilégios"para a gestão dos utilizadores, contas de grupo e sistema, incluindo contas privilegiadas.

Questão de Controlo: A organização garante que todos os utilizadores que acedam a um sistema que processa, armazena ou transmite informações sensíveis são limpos e regularmente treinados para lidar com a informação em causa?

Evidências:

1. N/D.

SRH - 03 | Papéis e Responsabilidades

Descrição: Mecanismos para definir responsabilidades de cibersegurança para todos os colaboradores.

Implementação: Os processos administrativos devem exigir que todos os colaboradores apliquem princípios de segurança e privacidade no seu trabalho diário. Os processos administrativos devem educar formalmente os utilizadores sobre os seus deveres para proteger dados sensíveis e confidenciais.

Questão de Controlo: A organização define responsabilidades de cibersegurança para todos os colaboradores?

Evidências:

1. N/D.

SRH - 04 | Contratos de Acesso

Descrição: Mecanismos para exigir que os utilizadores internos e terceiros assinem acordos de acesso antes de terem possibilidade de aceder.

Implementação: Deve ser assinado um acordo/contrato de acesso entre os colaboradores internos ou externos antes de os mesmos terem acesso aos locais ou sistemas presentes no âmbito.

Questão de Controlo: A organização exige que os utilizadores internos e de terceiros assinem acordos de acesso adequados antes de terem possibilidade de aceder?

Evidências:

1. N/D.

SRH - 05 | Acordos de Confidencialidade

Descrição: Mecanismos para exigir acordos de não-divulgação (NDA) ou acordos de confidencialidade semelhantes que reflitam as necessidades de proteger dados e detalhes operacionais, ou tanto os colaboradores internos como externos.

Implementação: Deve ser assinado um acordo de não divulgação (NDA), sempre que existir informação ou dados sensíveis/confidenciais presentes no âmbito da função/funções a executar.

Questão de Controlo: A organização requer acordos de não-divulgação (NDAs) ou acordos de confidencialidade semelhantes que reflitam as necessidades de proteger dados e detalhes operacionais, ou os colaboradores internos como externos?

Evidências:

1. Acordos de Não-Divulgação.

3.3.14 *Identificação e Autenticação*

IAT - 01 | Gestão de Identidade e Acesso (IAM)

Descrição: Mecanismos para facilitar a implementação dos controlos de identificação e gestão de acessos.

Implementação: Um sistema de Gestão de Identidades e Acesso (IAM), ou função semelhante, deve facilitar a implementação de controlos de gestão de identificação e acesso dos colaboradores internos ou externos. Um IAM, ou função semelhante, deve gerir as permissões e implementar práticas de "menor privilégio"na gestão de contas de utilizador, grupo e sistema, incluindo contas privilegiadas. Deve ser utilizado um Diretório ativo (AD), ou uma tecnologia similar, para gerir centralmente identidades e permissões.

Questão de Controlo: A organização facilita a implementação de controlos de gestão de identificação e acesso?

Evidências:

1. N/D.

IAT - 02 | Identificação e Autenticação para Colaboradores Internos

Descrição: Mecanismos para identificar e centralmente autenticar, autorizar e auditar utilizadores internos .

Implementação: A equipa de IT, ou uma função semelhante, deve implementar e manter um sistema de Gestão de Identidade e Acesso (IAM) para todos os utilizadores. Os controlos IAM devem ser principalmente de natureza administrativa e preventiva (por exemplo, políticas e normas) para gerir contas e permissões.

Questão de Controlo: A organização identifica e autentica exclusivamente utilizadores internos?

Evidências:

1. N/D.

IAT - 03 | Identificação e Autenticação para Colaboradores Externos

Descrição: Mecanismos para identificar e centralmente autenticar, autorizar e auditar utilizadores externos.

Implementação: Um sistema de Gestão de Identidade e Acesso (IAM), ou semelhante, deve facilitar a implementação de controlos de gestão de identificação e acesso. O IAM, ou função semelhante, deve gerir as permissões e implementar práticas de "menor privilégio"na gestão de contas de utilizador, grupo e sistema, incluindo contas privilegiadas. Deve existir um Active Directory (AD), ou uma tecnologia similar, para gerir centralmente identidades e permissões.

Questão de Controlo: A organização autentica, autorizar e auditar utilizadores externos?

Evidências:

1. N/D.

IAT - 04 | Identificação e Autenticação para Dispositivos

Descrição: Mecanismos para identificar e centralmente autenticar, autorizar e auditar dispositivos antes de estabelecer uma ligação.

Implementação: A Active Directory (AD), ou uma tecnologia similar, deve ser utilizada para gerir centralmente identidades e permissões. As tecnologias devem ser configuradas para identificar e autenticar dispositivos de forma única antes de estabelecer uma ligação. Os processos e tecnologias administrativas devem identificar e autenticar sistemas e serviços de terceiros.

Questão de Controlo: A organização identifica, autoriza e audita dispositivos antes de estes estabelecerem uma ligação ?

Evidências:

1. Active Directory (AD) e Kerberos.

IAT - 05 | Autenticação multi-factor (MFA)

Descrição: Mecanismos automatizados para impor a autenticação multi-factor (MFA) para: Acesso remoto à rede; Sistemas, aplicações e/ou serviços de terceiros; e/ou Acesso não-consola a sistemas ou sistemas críticos que armazenam, transmitem e/ou processam dados sensíveis.

Implementação: Deve ser implementada a autenticação multi-fator em todos os sistemas críticos e sensiveis da organização. Devem ser desenvolvidas métricas que forneçam uma supervisão de gestão para garantir que o processo de Autenticação Multi-Factor (MFA) está a funcionar corretamente

Questão de Controlo: A organização necessita de autenticação multi-factor (MFA) para acesso remoto à rede e sistemas críticos?

Evidências:

1. Autenticação multi-factor (MFA) : Yubico, Duo entre outros.

IAT - 06 | Gestores de Passwords

Descrição: Mecanismos para proteger e armazenar senhas através de uma ferramenta de gestão de passwords.

Implementação: As credenciais pessoais e administrativas devem ser guardadas numa plataforma de gestão de passwords encriptada. Esta plataforma deve ter a possibilidade de auditar as credenciais na ótica de reutilização das mesmas e a exposição pública (base de dados de utilizadores expostas).

Questão de Controlo: A organização protege e armazena palavras-passe através de uma ferramenta de gestão de passwords?

Evidências:

1. Plataforma de gestão de passwords.

IAT - 07 | Gestão de Conta Privilegiada (PAM)

Descrição: Mecanismos para restringir e controlar os direitos de acesso privilegiados para os utilizadores e serviços.

Implementação: Deve ser implementada uma solução de Gestão de Acesso Privilegiado (PAM), com vários decisores de aprovação para cada credencial/chave de acesso aos sistemas críticos.

Questão de Controlo: A organização restringe e controla direitos de acesso privilegiados para utilizadores e serviços?

Evidências:

1. Plataforma PAM (Delinea, CyberArk, entre outros).

IAT - 08 | Revisão Periódica dos Privilégios do Utilizador

Descrição: Mecanismos para rever periodicamente os privilégios atribuídos aos utilizadores para validar a necessidade de tais privilégios; e retribuir ou remover privilégios, se necessário, para refletir corretamente a missão organizacional e as necessidades empresariais.

Implementação: Os processos administrativos e as tecnologias devem documentar todas as contas privilegiadas e validar que cada pessoa com privilégios elevados é autorizada pelo nível adequado de gestão organizacional. Devem existir processos administrativos para rever periodicamente os privilégios atribuídos aos utilizadores para validar a necessidade de tais privilégios e retribuir ou remover privilégios, se necessário, para refletir corretamente a missão organizacional e as necessidades empresariais.

Questão de Controlo: A organização revê periodicamente os privilégios atribuídos aos utilizadores para validar as necessidades de tais privilégios; e retribuir ou remover privilégios, se necessário, para refletir corretamente a missão organizacional e as necessidades empresariais?

Evidências:

1. N/D.

IAT - 09 | Máquinas Administrativas Dedicadas

Descrição: Mecanismos para restringir a execução de tarefas administrativas ou tarefas que exijam um acesso privilegiado através de uma máquina administrativa dedicada.

Implementação: Os acessos administrativos aos sistemas de informação da organização devem apenas ser permitidos através de uma máquina dedicada .

Questão de Controlo: A organização restringe a execução de tarefas administrativas ou tarefas que exijam acesso elevado através de uma máquina dedicada?

Evidências:

1. Máquina dedicada (Jump Machine).

IAT - 10 | Bloqueio de Conta

Descrição: Mecanismos para impor um limite para tentativas de login inválidas por um utilizador durante um período de tempo definido pela organização e o bloqueio automático da conta quando o número máximo de tentativas falhadas é ultrapassado.

Implementação: Deve existir em cada sistema uma configuração de autenticação com o limite mínimo de 3 tentativas consecutivas falhas acionando de seguida o bloqueio de conta.

Questão de Controlo: A organização impõe um limite para tentativas de login inválidas consecutivas por um utilizador durante um período de tempo definido pela organização e bloqueia automaticamente a conta quando o número máximo de tentativas falhadas é ultrapassado?

Evidências:

1. N/D.

3.3.15 *Resposta a Incidentes*

RAI - 01 | Tratamento de Incidentes

Descrição: Mecanismos para abranger a preparação, deteção automatizada ou a admissão de relatórios de análises de contenção, erradicação e recuperação.

Implementação: Uma Equipa Integrada de Resposta a Incidentes de Segurança (CSIRT), ou função semelhante, deve existir para contituir um grupo de colaboradores representantes na área de cibersegurança, nomeadamente colaboradores da área de TI, privacidade e empresarial . Esta equipa deve ter capacidade para gerir operações coordenadas de resposta a incidentes. O CSIRT, ou função similar, deve desenvolver e manter um plano de Resposta a Incidentes (IRP) que fornece uma orientação operacional e tática que permite regular as operações de cibersegurança e resposta a incidentes. O CSIRT, ou função semelhante, deve incorporar as lições aprendidas com a análise e resolução de incidentes de cibersegurança e privacidade para reduzir a probabilidade ou impacto de futuros incidentes.

Questão de Controlo: Os processos de tratamento de incidentes da organização abrangem a preparação, deteção e análise, contenção, erradicação e recuperação?

Evidências:

1. Plano de Resposta a Incidentes (IRP).

RAI - 02 | Desativação Automática do Sistema

Descrição: Mecanismos para desativar automaticamente os sistemas, após a deteção de um possível incidente que satisfaça os critérios organizacionais e que permita que seja efetuada uma análise forense.

Implementação: A organização deve elaborar uma arquitetura de resiliência, com a dependência de cada sistema para o caso de ser necessário desativar um sistema após a descoberta de um incidente nesse equipamento perimitindo assim uma rápida análise pela equipa de CSIRT. Deve ser possível automaticamente através de ferramentas de repsosta a incidentes encerrar qualquer sistema infetado/comprometido num incidente de segurança.

Questão de Controlo: A organização desativa automaticamente os sistemas envolvidos num incidente após a sua deteção?

Evidências:

1. Plano de Resposta a Incidentes (IRP).

RAI - 03 | Indicadores de Compromisso (IOC)

Descrição: Mecanismos para definir indicadores específicos de compromisso (IOC) para identificar os sinais de potenciais eventos de cibersegurança.

Implementação: A organização deve definir várias fontes confiavéis de repositórios de indicadores de compromisso. Deve existir uma plataforma TIP (Threat Intelligence Plataforma) para analisar e recolher indicadores de compromisso oriundos de diversas plataformas (SIEM, Firewalls, EDR/XDR) ou entidades (AlienVault, RiskIQ, Recorded Future, Centro Nacional de Cibersegurança, Rede Nacional de CSIRTS)

Questão de Controlo: A organização define indicadores específicos de compromisso (IOC) que identificam o impacto potencial de eventos de cibersegurança?

Evidências:

1. Lista de Indicadores de Compromisso,
2. Plataforma de Inteligência de Ameaças (TIP).

RAI - 04 | Plano de Resposta a Incidentes (IRP)

Descrição: Mecanismos para manter e disponibilizar um plano de resposta a incidentes (IRP) atual e viável a todas as partes interessadas.

Implementação: Deve ser criado um Plano de Resposta a Incidentes que contenha os seguintes tópicos

1. Preparação: Plano definido com tarefas e elementos a acionar em caso de incidente;
2. Deteção e análise: descrição do incidente, a sua origem, a sua causa, severidade e o tipo;
3. Contenção e erradicação: ações a executar para interromper o incidente;
4. Recuperação: Lista de lições aprendidas.

Questão de Controlo: A organização mantém e disponibiliza um plano de resposta a incidentes (IRP) atual e viável para todas as partes interessadas?

Evidências:

1. Plano de Resposta a Incidentes (IRP).

RAI - 05 | Testes de Resposta a Incidentes

Descrição: Mecanismos para testar formalmente as capacidades de resposta a incidentes através de exercícios realistas para determinar a eficácia operacional dessas capacidades.

Implementação: O CSIRT, ou função semelhante, trabalha com as partes interessadas para realizar formação e exercícios de resposta a incidentes regularmente. Estes exercícios devem ser o mais aproximados à realidade possível, por exemplo executar um exercício de resposta a um ataque de ransomware.

Questão de Controlo: A organização testa formalmente as capacidades de resposta a incidentes através de exercícios realistas para determinar a eficácia operacional dessas capacidades?

Evidências:

1. Exercícios Red Team vs Blue Team.

RAI - 06 | Equipa de Resposta a Incidentes de Segurança (CSIRT)

Descrição: Mecanismos para criar uma equipa integrada de cibersegurança que seja capaz de abordar questões de cibersegurança e de resposta a incidentes.

Implementação: Deve ser criada uma equipa de Resposta a Incidentes de Segurança (CSIRT), que incluí membros da equipa de TI, como da equipa de GRC e comité de administração caso exista. Esta equipa de CSIRT deve ter pelo menos os seguintes tipos de elementos:

1. Gestor ou Líder de equipa
2. Operador NSOC
3. Analista de Incidentes
4. Analista de Vulnerabilidades
5. Analista de Artefatos
6. Especialistas e arquitetos de soluções, nomeadamente SIEM e SOAR.

Questão de Controlo: A organização tem uma equipa de cibersegurança que é capaz de abordar operações de cibersegurança e resposta a incidentes ?

Evidências:

1. N/D.

RAI - 07 | Cadeia de Custódia Forense

Descrição: Mecanismos para realizar perícias digitais e manter a integridade da cadeia de custódia, de acordo com as leis, regulamentos e boas práticas reconhecidas pela indústria.

Implementação: Deve ser criado um conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica de qualquer artefato obtido ou rastreado a partir do seu reconhecimento até à sua eliminação. Recomenda-se que seja elaborado a partir do processo de aquisição o propósito de manter o registo de cadeia da custódia para possibilitar a identificação, acesso e movimento da evidência em qualquer altura.
O registo deve conter no mínimo os seguintes elementos:

1. Identificador único da evidência;
2. Quem acedeu à evidência e o espaço temporal e local em que ocorreu;
3. Quem verificou a evidência internamento ou externamente e quando o mesmo ocorreu;
4. Quais foram as alterações inevitáveis que ocorreram.

Questão de Controlo: A organização efetua provas forenses digitais e mantém a integridade da cadeia de custódia?

Evidências:

1. Procedimento da cadeia de custódia;
2. Conjunto de ferramentas Forenses (FTK Imager, Autopsy, Cellebrite entre outros).

RAI - 08 | Análise de Causa De Raiz (RCA) e Lições Aprendidas

Descrição: Mecanismos para incorporar lições aprendidas com a análise e resolução de incidentes de cibersegurança e privacidade para reduzir a probabilidade ou o impacto de futuros incidentes.

Implementação: Após a resolução de cada incidente, deve ser criado um relatório de incidente que contenha as lições aprendidas durante a mitigação do mesmo. Essas lições aprendidas devem constar no relatório anual de segurança para incluir no plano de ação de aprendizagem da equipa de cibersegurança e tecnologias de informação.

Questão de Controlo: A organização incorpora lições aprendidas com a análise e resolução de incidentes de cibersegurança e privacidade para reduzir a probabilidade ou o impacto de futuros incidentes?

Evidências:

1. N/D.

RAI - 09 | Contactos Regulatórios e Aplicação da Lei

Descrição: Mecanismos para manter os contactos de resposta a incidentes com as autoridades reguladoras e de aplicação da lei aplicáveis.

Implementação: Deve ser criado um documento que permita identificar o ponto de contacto permanente, nomeadamente todos os interlocutores principais da organização em caso de incidente de segurança. Deve contar não só os contactos principais como os alternativos (número de telefone, número de telemóvel e email).

Questão de Controlo: A organização mantém contactos de resposta a incidentes com as agências reguladoras?

Evidências:

1. Ponto de Contato Permamente.

3.3.16 *Garantia de Informação*

GDI - 01 | Avaliações

Descrição: Mecanismos para avaliar formalmente a cibersegurança e os controlos de privacidade em sistemas, aplicações e serviços para determinar até que ponto os controlos são executados corretamente.

Implementação: A equipa de segurança informática deve identificar a proteção de dados e os controlos de privacidade adequados para responder aos requisitos legais, regulamentares e contratuais aplicáveis para testes de segurança e controlo de privacidade pré-produção. Devem ser avaliados os controlos de modo a verificar a sua real aplicação.

Questão de Controlo: A organização avalia formalmente os controlos de cibersegurança e privacidade em sistemas, para determinar até que ponto os controlos são executados corretamente?

Evidências:

1. Programa de Garantia da Informação (IAP).

GDI - 02 | Autorização de Segurança

Descrição: Mecanismos para garantir que os sistemas, projetos e serviços sejam oficialmente autorizados antes de irem para um ambiente de produção.

Implementação: Os controlos de segurança devem ser principalmente de natureza administrativa e preventiva (por exemplo, políticas e procedimentos) para gerir controlos técnicos para requisitos de segurança e privacidade. Estes controlos devem-se focar na proteção de Ativos de Alto Valor (HVAs), incluindo ambientes onde os dados sensíveis são armazenados, transmitidos e processados.

Questão de Controlo: A organização garante que os sistemas, projetos e serviços são oficialmente autorizados antes de irem para um ambiente de produção?

Evidências:

1. Programa de Garantia da Informação (IAP).

3.3.17 *Manutenção*

MNT - 01 | Operações de Manutenção

Descrição: Mecanismos para desenvolver, divulgar, rever e atualizar procedimentos para facilitar a implementação de controlos de manutenção em toda a organização.

Implementação: Uma equipa de Governação, Risco e Compliance (GRC) ou função semelhante, desenvolve, divulga, analisa as atualizações e orientações para facilitar a implementação segura e atempada dos controlos de manutenção em toda a organização, incluindo operações de manutenção preventiva e reativa.

Questão de Controlo: A organização desenvolve, divulga, analisa e atualiza os procedimentos para facilitar a implementação de controlos de manutenção em toda a organização?

Evidências:

1. N/D.

MNT - 02 | Manutenção Controlada

Descrição: Mecanismos para a realização de atividades de manutenção controladas ao longo do ciclo de vida do sistema, aplicação ou serviço.

Implementação: Devem existir processos e tecnologias administrativas para realizar atividades de manutenção controladas e oportunas ao longo do ciclo de vida do sistema, aplicação ou serviço.

Questão de Controlo: A organização realiza atividades de manutenção controladas ao longo do ciclo de vida do sistema, aplicação ou serviço?

Evidências:

1. N/D.

MNT - 03 | Ferramentas de Manutenção

Descrição: Mecanismos para a realização de atividades de manutenção controladas ao longo do ciclo de vida do sistema, aplicação ou serviço.

Implementação: As operações de manutenção devem ser centralizadas em termos de gestão de alterações, mas descentralizadas em termos de execução. Uma equipa responsável pelo controlo de alterações, ou função semelhante, deve gerir centralmente o processo de operações de manutenção para reduzir as possibilidades de interrupções de negócio. Um programa de Gestão de Ativos (ITAM) ou função semelhante, deve categorizar os dispositivos de acordo com os dados que os ativos armazenam, transmitem e/ou processam e aplicar os controlos tecnológicos adequados para proteger o ativo e os respetivos dados.

Questão de Controlo: A organização controla e monitoriza a utilização de ferramentas de manutenção do sistema?

Evidências:

1. N/D.

3.3.18 *Segurança da Rede*

SDR - 01 | Gestão de Segurança de Rede

Descrição: Mecanismos para desenvolver, governar e atualizar procedimentos para facilitar a implementação dos controlos de segurança da rede.

Implementação: A equipa de tecnologias de informação, ou função semelhante, deve facilitar a implementação de controlos de segurança de rede em toda a organização. A equipa de cibersegurança deve trabalhar com a equipa de tecnologias de informação para implementar uma arquitetura de rede de "defesa em camadas"que permita facilitar uma abordagem de defesa aprofundada proporcionando uma redução de riscos de segurança.

Questão de Controlo: A organização desenvolve, governa e atualiza os procedimentos para facilitar a implementação dos controlos de segurança da rede?

Evidências:

1. Diagramas de Rede.

SDR - 02 | Arquitetura Zero Trust (ZTA)

Descrição: Mecanismos para tratar todos os utilizadores e dispositivos como potenciais ameaças e impedir o acesso a dados e recursos até que os utilizadores possam ser devidamente autenticados e o seu acesso autorizado.

Implementação: O acesso à rede corporativa deve ser limitada através da criação de um acesso lógico baseado na identidade do utilizador e no contexto da ação. O acesso às aplicações e serviços da organização devem ser controlados através de políticas e controlos de segurança limitando assim a superfície de ataque.

Questão de Controlo: A organização trata todos os utilizadores como potenciais ameaças e impede o acesso aos dados e recursos até que os utilizadores possam ser devidamente autenticados e o seu acesso autorizado?

Evidências:

1. N/D.

SDR - 03 | Proteção de Negação de Serviço (DoS)

Descrição: Mecanismos automatizados para proteger ou limitar os efeitos de ataques de negação de serviço.

Implementação: As tecnologias utilizadas pela organização devem ser configuradas para proteger ou limitar os efeitos dos ataques de Negação de Serviço (DoS).

Questão de Controlo: A organização protege contra ou limita os efeitos dos ataques de Negação de Serviço (DoS) ?

Evidências:

1. N/D.

SDR - 04 | Pontos de Acesso à Rede

Descrição: Mecanismos para limitar os pontos de acesso à rede.

Implementação: As tecnologias de proteção de perímetro devem monitorizar e controlar as comunicações na fronteira externa da rede e nos principais limites internos dentro da rede da organização.

Questão de Controlo: A organização limita o número de ligações de rede externas que um sistema irá simultaneamente aceitar?

Evidências:

1. N/D.

SDR - 05 | Sub-rede separada para ligação a diferentes Domínios de Segurança

Descrição: Mecanismos para implementar endereços de rede separados (por exemplo, diferentes sub-redes) para interligar a sistemas em domínios de segurança distintos.

Implementação: Deve existir segmentação da rede para implementar endereços de rede separados (por exemplo, diferentes sub-redes) para interligar sistemas em domínios de segurança distintos.

Questão de Controlo: A organização implementa endereços de rede separados (por exemplo, diferentes sub-redes) para interligar sistemas em domínios de segurança distintos?

Evidências:

1. N/D.

SDR - 06 | Segmentação da Rede

Descrição: Mecanismos para segregar logicamente ou fisicamente os fluxos de informação para realizar a segmentação da rede.

Implementação: Devem existir processos administrativos e tecnologias logicamente ou fisicamente que segregam os fluxos de informação para realizar a segmentação da rede.

Questão de Controlo: A organização segmenta os fluxos de informação logicamente ou fisicamente para realizar a segmentação da rede?

Evidências:

1. Sub-redes;
2. VLANs;
3. VRFs.

SDR - 07 | Separação da Rede Local Virtual (VLAN)

Descrição: Mecanismos que permitem que as redes de área local virtual (VLANs) limitem a capacidade dos dispositivos numa rede de comunicar diretamente com outros dispositivos na sub-rede e limitar a capacidade do intruso de se mover lateralmente para comprometer os sistemas vizinhos.

Implementação: Devem existir processos e tecnologias administrativas quem permitem ás Redes de Área Local Virtual (VLANs) limitar a capacidade dos dispositivos numa rede de comunicar diretamente com outros dispositivos na sub-rede e limitar um limite a um dispositivo na sub-rede e limitar um limite a um dispositivo capacidade do atacante de mover lateralmente para comprometer sistemas vizinhos.

Questão de Controlo: A organização permite que as Redes de Área Local Virtual (VLANs) limitem a capacidade dos dispositivos numa rede de comunicação direta com outros dispositivos na sub-rede e limitem a capacidade de um intruso de se mover lateralmente para comprometer sistemas vizinhos?

Evidências:

1. VLANs.

SDR - 08 | Sistemas de Deteção/ Prevenção de Intrusões na Rede (NIDS / NIPS)

Descrição: Mecanismos para implementar sistemas de deteção/prevenção de intrusões de rede (NIDS/NIPS) para detetar e/ou prevenir incidentes de segurança.

Implementação: Devem existir sistemas de deteção/prevenção de intrusões de Rede (NIDS/NIPS) para detetar e/ou prevenir incidentes de segurança.

Questão de Controlo: Os sistemas de deteção/prevenção de intrusões em Rede (NIDS/NIPS) são utilizados para detetar e/ou prevenir incidentes de segurança ?

Evidências:

1. NIDS/NIPS.

SDR - 09 | Redes DMZ

Descrição: Mecanismos para exigir segmentos de rede de zonas desmilitarizadas (DMZ) para separar redes não fidedignas de redes fidedignas.

Implementação: Os processos administrativos devem requerer segmentos de rede de Zona Desmilitarizada (DMZ) para separar redes não fidedignas de redes fidedignas (Por exemplo, separação de serviços expostos ao público e serviços privados da organização).

Questão de Controlo: A organização requer segmentos de rede de Zonas Desmilitarizadas (DMZ) para separar redes não confiáveis de redes fidedignas?

Evidências:

1. Plano de Segurança para Sistemas (SSP).

SDR - 10 | Sistema de Nome de Domínio (DNS)

Descrição: Mecanismos para garantir que a resolução do Sistema de Nome de Domínio (DNS) é projetada, implementada e gerida para proteger a segurança da resolução do nome/endereço.

Implementação: As tecnologias devem ser configuradas para realizar a autenticação de origem de dados e verificação da integridade dos dados nas respostas de resolução do Sistema de Nome de Domínio (DNS), sendo estas recebidas de fontes autoritárias quando solicitadas pelos sistemas cliente.

Questão de Controlo: A organização garante que a resolução do Sistema de Nome de Domínio (DNS) é projetada, implementada e gerida para proteger a segurança da resolução de nome/endereço?

Evidências:

1. N/D.

SDR - 11 | Quadro Político do Remetente (SPF)

Descrição: Mecanismos para validar a legitimidade das comunicações de e-mail através da configuração de um registo do Sender Policy Framework (SPF) do Serviço de Nomeação de Domínio (DNS) para especificar os endereços IP e/ou os nomes de anfitriões autorizados a enviar e-mails a partir do domínio especificado.

Implementação: Devem ser aplicados mecanismos para validar a legitimidade das comunicações de email através da configuração de um registo de Sender Policy Framework e validada a configuração posteriormente.

Questão de Controlo: A organização valida a legitimidade das comunicações de e-mail através da configuração de um registo do Sender Policy Framework (SPF) do Serviço de Nomeação de Domínio (DNS) para especificar os endereços IP e/ou os nomes de anfitriões autorizados a enviar e-mails do domínio especificado?

Evidências:

1. N/D.

SDR - 12 | Acesso Remoto

Descrição: Mecanismos para definir, controlar e rever métodos de acesso remoto protegidos e aprovados pela organização.

Implementação: Os processos e tecnologias administrativas devem reger o acesso remoto a sistemas e dados para trabalhadores remotos. Estes processos e tecnologias administrativas devem controlar e monitorizar proactivamente as contas de terceiros utilizadas para aceder, apoiar ou manter componentes do sistema através de acesso remoto. Os Processos e tecnologias administrativas devem validar as versões de software e controlar os dispositivos remotos ligados a redes corporativas ou a executar determinadas funções, como o armazenamento e acesso a informações da organização. Os processos e tecnologias administrativas devem proporcionar a capacidade de desligar ou desativar rapidamente a sessão de acesso remoto de um utilizador.

Questão de Controlo: A organização define, controla e revê métodos de acesso remoto seguros e aprovados pela organização ?

Evidências:

1. N/D.

SDR - 13 | Trabalho em Remoto (WFA)

Descrição: Mecanismos para definir práticas seguras de teletrabalho e reger o acesso remoto a sistemas e dados para trabalhadores remotos.

Implementação: Devem ser transmitidas as boas práticas de segurança aos colaboradores em teletrabalho. Devem também ser disponibilizados materiais de informação regulares sobre a segurança dos dados e acessos aos sistemas da organização (webinares, reuniões entre outros).

Questão de Controlo: A organização define práticas seguras de teletrabalho e rege o acesso remoto a sistemas e dados para trabalhadores remotos?

Evidências:

1. N/D.

SDR - 14 | Intranets

Descrição: Mecanismos para estabelecer relações de confiança com outras organizações proprietárias, operacionais permitindo que os indivíduos autorizados acedam à intranet a partir desses sistemas externos e possam processar, amazenar, transmitar informações controladas pela organização através de sistemas externos.

Implementação: Os processos administrativos e tecnologias devem estabelecer relações de confiança com outras organizações proprietárias, operacionais, e/ou mantendo sistemas intranet, permitindo que indivíduos autorizados acedam à intranet a partir de plataformas externas.

Questão de Controlo: A organização estabelece relações de confiança com outras organizações proprietárias, operacionais permitindo que os indivíduos autorizados acedam à intranet a partir desses sistemas externos e possam processar, amazenar, transmitir informações controladas pela organização através de sistemas externos?

Evidências:

1. N/D.

SDR - 15 | Prevenção da Perda de Dados (DLP)

Descrição: Mecanismos automatizados para implementar a Prevenção de Perda de Dados (DLP) para proteger informações sensíveis à medida que são armazenadas, transmitidas e processadas.

Implementação: As tecnologias devem ser configuradas para implementar técnicas de Prevenção de Perdas de Dados (DLP) para proteger informações sensíveis à medida que são armazenadas, transmitidas e processadas.

Questão de Controlo: A Prevenção de Perda de Dados (DLP) é utilizada para proteger informações sensíveis à medida que são armazenadas, transmitidas e processadas?

Evidências:

1. Prevenção de Perdas de Dados (DLP).

SDR - 16 | Filtragem de Conteúdos

Descrição: Mecanismos para forçar o tráfego de rede ligado à internet através de um dispositivo proxy para filtragem de conteúdos (URL e DNS) para limitar a capacidade de um utilizador de se ligar a sites de internet maliciosos ou proibidos.

Implementação: As tecnologias e sistemas devem ser configuradas para encaminhar o tráfego de comunicações internas para redes externas através de servidores proxy aprovados pela organização .

Questão de Controlo: A organização força o tráfego de rede ligado à internet através de um dispositivo proxy para filtragem de conteúdos URL e filtragem de DNS para limitar a capacidade de um utilizador de se ligar a sites de internet maliciosos ou proibidos?

Evidências:

1. N/D.

3.3.19 *Segurança Física e Ambiental*

SFA - 01 | Proteções Físicas e Ambientais

Descrição: Mecanismos para facilitar o funcionamento dos controlos de proteção física e ambiental.

Implementação: A equipa de Governação, Risco e Compliance (GRC) ou função semelhante, deve garantir que as obrigações legais, regulamentares e contratuais são devidamente direcionadas para facilitar a implementação de uma segurança física adequada.

Questão de Controlo: A organização facilita o funcionamento dos controlos de proteção física e ambiental?

Evidências:

1. N/D.

SFA - 02 | Autorizações de Acesso Físico

Descrição: Mecanismos de controlo de acesso físico para manter uma lista atual de colaboradores com acesso autorizado a instalações organizacionais (exceto as áreas dentro da instalação oficialmente designadas como acessíveis ao público).

Implementação: Os controlos e tecnologias físicas devem ser configurados para impor autorizações de acesso a todos os pontos de acesso físico (incluindo pontos de entrada/saída definidos) às instalações (excluindo as áreas dentro da instalação oficialmente designadas como acessíveis ao público).

Questão de Controlo: A organização mantém uma lista atual de colaboradores com acesso autorizado a instalações organizacionais (exceto as áreas dentro das instalações oficialmente designadas como acessíveis ao público)?

Evidências:

1. Lista de colaboradores autorizados.

SFA - 03 | Equipamentos de Monitorização e Acesso Físico

Descrição: Mecanismos de controlo de acesso físico para monitorizar alarmes de intrusão física e equipamentos de vigilância.

Implementação: Os controlos físicos devem ser implementados para escritórios, salas e gabinetes técnicos. Os processos administrativos, controlos físicos e tecnologias devem garantir que apenas os colaboradores autorizados têm permissão de acesso ás áreas seguras. Os controlos e tecnologias físicas devem estar configuradas para monitorizar, detetar e responder a incidentes de segurança física. Os processos administrativos, controlos físicos e tecnologias devem monitorizar os alarmes de intrusão física e os equipamentos de vigilância.

Questão de Controlo: A organização monitoriza os alarmes de intrusão física e os equipamentos de vigilância?

Evidências:

1. Controlo de acessos (leitor biométrico, RFID entre outros);
2. CCTV.

SFA - 04 | Monitorização e Rastreio de Ativos

Descrição: Mecanismos de segurança física para implementar tecnologias de localização de ativos que rastreiam e monitorizam a localização e o movimento dos ativos pela organização nas respetivas áreas organizacionais.

Implementação: Processos administrativos e controlos físicos devem utilizar tecnologias de localização de ativos para monitorizar a localização e o movimento de ativos definidos pela organização nas respetivas áreas organizacionais.

Questão de Controlo: A organização implementa tecnologias de localização de ativos que rastreiam e monitorizam a localização e movimento de ativos definidos pela organização em áreas controladas pela organização?

Evidências:

1. Marcação RFID.

3.3.20 *Privacidade*

PRI - 01 | Encarregado de Proteção de Dados (DPO)

Descrição: Mecanismos para nomear um Encarregado de Proteção de Dados (DPO), com especial função de estar encarregue da gestão de dados pessoais e da sua proteção.

Implementação: Os Encarregados de Proteção de Dados (DPOs) devem ser designados para trabalhar em colaboração com unidades de negócio e equipas de projeto para garantir que os princípios de privacidade são adequadamente concebidos e implementados. Devem existir processos administrativos para garantir que o DPO esteja envolvido em todas as questões relacionadas com a proteção de dados.

Questão de Controlo: A organização nomeia um Encarregado de Proteção de Dados (DPO) ?

Evidências:

1. Encarregado de Proteção de Dados (DPO).

PRI - 02 | Segurança de Dados Pessoais

Descrição: Mecanismos para garantir que os Dados Pessoais (PD) sejam protegidos de forma segura e adequadas para salvaguardar a confidencialidade e integridade do dados pessoais.

Implementação: Os Encarregados de Proteção de Dados (DPOs) devem ser designados para trabalhar em colaboração com unidades de negócio e equipas de projeto para garantir que os princípios de privacidade são adequadamente concebidos e implementados. Devem existir processos administrativos para garantir que o DPO esteja envolvido em todas as questões relacionadas com a proteção de dados.

Questão de Controlo: A organização garante que os Dados Pessoais (PD) estão protegidos adequadamente com foco na salvaguarda da confidencialidade e integridade dos dados pessoais?

Evidências:

1. N/D.

PRI - 03 | Retenção e Eliminação de Dados Pessoais

Descrição: Mecanismos para:

- Reter dados pessoais (PD), incluindo metadados, durante um período de tempo definido pela organização para cumprir as finalidades identificadas conforme exigido por lei;
- Eliminar, destruir, apagar e/ou anonimizar a memória, independentemente do método de armazenamento;
- Utilizar técnicas ou métodos definidos pela organização para garantir a supressão ou destruição segura de dados., incluindo originais, cópias e arquivos.

Implementação: Os processos e tecnologias administrativas devem reter os dados pessoais, incluindo metadados, durante um período de tempo definido pela organização para cumprir os fins identificados nos termos da lei. Os processos administrativos e tecnologias devem eliminar, destruir, apagar e/ou anonimizar o PI, independentemente do método de armazenamento.

Questão de Controlo: A organização retém dados pessoais (PD), incluindo metadados, por um período de tempo definido pela organização conforme exigido por lei, elimina, destrói, apaga e/ou anonimiza o PI, independentemente do método de armazenamento e utiliza técnicas ou métodos definidos pela organização para garantir a supressão ou destruição segura de dados.

Evidências:

1. N/D.

3.3.21 *Projeto e Gestão de Recursos*

PGR - 01 | Plano Estratégico e Objetivos

Descrição: Mecanismos para estabelecer um plano estratégico de cibersegurança e o conjunto de objetivos para alcançar esse plano.

Implementação: O Chief Information Officer (CIO), ou função semelhante, deve analisar a estratégia de negócio da organização e priorizar os objetivos da função de segurança, com base nos requisitos empresariais. A equipa de TI e/ou cibersegurança deve desenvolver planos para implementar objetivos relacionados com a segurança, com base em níveis de maturidade.

Questão de Controlo: A organização estabelece um plano estratégico de cibersegurança e um conjunto de objetivos para atingir esse plano?

Evidências:

1. Plano Estratégico de Cibersegurança.

PGR - 02 | Níveis de Maturidade da Capacidade de Serviços Críticos

Descrição: Mecanismos para definir e identificar os níveis de maturidade da capacidade de serviços críticos.

Implementação: A equipa de TI em conjunto com a equipa de cibersegurança devem identificar os níveis de maturidade dos serviços críticos e posteriormente defini-los de forma segregada. Estes níveis de maturidade devem ser apresentados por tipologia de ativos (equipamento de rede, servidor, firewall entre outros).

Questão de Controlo: A organização define e identifica os níveis de maturidade da capacidade dos serviços críticos?

Evidências:

1. N/D.

PGR - 03 | Definição de Requisitos de Segurança e Privacidade

Descrição: Mecanismos para identificar componentes e funções críticas do sistema através da realização de uma análise extensa para sistemas críticos, componentes do sistema ou serviços em pontos de decisão pré-definidos no Ciclo de Vida de Desenvolvimento Seguro (SDLC).

Implementação: Devem existir processos administrativos para identificar componentes e funções críticas do sistema, através da realização de uma análise extensa dos sistemas críticos, componentes ou serviços do sistema em pontos de decisão pré-definidos no SDLC.

Questão de Controlo: A organização identifica componentes e funções críticas do sistema através da realização de uma análise extensa para sistemas críticos, componentes do sistema ou serviços em pontos de decisão pré-definidos no Ciclo de Vida de Desenvolvimento Seguro (SDLC)?

Evidências:

1. Ciclo de Vida de Desenvolvimento Seguro (SDLC).

3.3.22 *Gestão de Riscos*

GDR - 01 | Programa de Gestão de Riscos

Descrição: Mecanismos para facilitar a implementação dos controlos de gestão dos riscos.

Implementação:A equipa de GRC desenvolve e implementa um Programa de Gestão de Riscos (RMP) a nível empresarial que fornece orientação operacional sobre a forma como o risco é consistentemente identificado, avaliado, remediado e reportado.

Questão de Controlo: A organização facilita a implementação de controlos de gestão de risco?

Evidências:

1. Programa de Gestão de Riscos (RMP).

GDR - 02 | Análise de Impacto Empresarial (BIA)

Descrição: Mecanismos para a realização de uma Análise de Impacto Empresarial (BIA).

Implementação: A equipa de GRC deve apoiar os proprietários de processos empresariais a realizar uma Análise de Impacto Empresarial (BIA) para identificar e remediar riscos relacionados com o processo de negócio.

Questão de Controlo: A organização realiza uma Análise de Impacto Empresarial (BIA)?

Evidências:

1. Programa de Gestão de Riscos (RMP);
2. Avaliação de Impacto de Proteção de Dados (DPIA);
3. Avaliação do Impacto da Privacidade (PIA).

GDR - 03 | Plano de Gestão de Risco da Cadeia de Abastecimento (SCRM)

Descrição: Mecanismos para desenvolver um plano de Gestão de Risco da Cadeia de Abastecimento (SCRM) associado ao desenvolvimento, aquisição, manutenção e eliminação de sistemas, componentes e serviços do , incluindo documentar ações de mitigação e monitorizar o desempenho associados a esses planos.

Implementação: A equipa de GRC, em conjunto com a equipa de compras e os proprietários de processos empresariais, devem reger os riscos da cadeia de fornecimento associados ao desenvolvimento, aquisição, manutenção e eliminação de sistemas, componentes e serviços.

Questão de Controlo: A organização desenvolve um plano de Gestão de Risco da Cadeia de Abastecimento (SCRM) associado ao desenvolvimento, aquisição, manutenção e eliminação de sistemas, componentes e serviços, incluindo documentar ações de mitigação selecionadas e monitorizar o desempenho associados a esses planos?

Evidências:

1. Programa de Gestão de Riscos (RMP).

GDR - 04 | Avaliação de Impacto da Proteção de Dados (DPIA)

Descrição: Mecanismos para a realização de uma Avaliação de Impacto de Proteção de Dados (DPIA) em sistemas, aplicações e serviços para avaliar as implicações da privacidade.

Implementação: A equipa de GRC, em conjunto com os proprietários de processos empresariais e encarregados de proteção de dados (DPOs), deve realizar uma Avaliação de Impacto de Proteção de Dados (DPIA) em todos os sistemas, aplicações e serviços que potencialmente armazenam, processam ou transmitem Dados Pessoais (PD) para avaliar as implicações da privacidade.

Questão de Controlo: A organização realiza uma Avaliação de Impacto de Proteção de Dados (DPIA) em sistemas, aplicações e serviços para avaliar as implicações de privacidade?

Evidências:

1. Avaliação de Impacto de Proteção de Dados (DPIA);
2. Avaliação do Impacto da Privacidade (PIA).

GDR - 05 | Monitorização de Riscos

Descrição: Mecanismos para garantir a monitorização do risco como parte integrante da estratégia de monitorização contínua que inclui o acompanhamento da eficácia dos controlos de segurança e privacidade, a conformidade e a gestão da mudança.

Implementação: A equipa de GRC deve manter um registo do risco centralizado para refletir a monitorização e identificação do risco associado a cada ativo. O registo de risco deve identificar e atribuir um ranking de risco a vulnerabilidades definidas pela organização com foco nas campanhas atuais de ataque cibernético. A monitorização do risco deve ser efetuada a cada 6 meses, ou a cada entrada de uma tipologia de ativo nova.

Questão de Controlo: A organização garante a monitorização de riscos como parte integrante da estratégia de monitorização contínua que inclui a monitorização da eficácia dos controlos de segurança e privacidade, conformidade e gestão de alterações?

Evidências:

1. N/D.

3.3.23 *Engenharia e Arquitetura Segura*

ESA - 01 | Arquitetura de Defesa em Profundidade (DiD)

Descrição: Mecanismos para implementar funções de segurança como uma estrutura de segurança em camadas minimizando as interações entre as diversas áreas tecnológicas da organização evitando qualquer dependência entre elas.

Implementação: A equipa de segurança, ou uma função semelhante, deve facilitar a implementação de práticas de segurança e privacidade reconhecidas pela indústria na especificação, conceção, desenvolvimento, implementação e modificação de sistemas e serviços. Esta equipa deve garantir que os dispositivos de rede estão em conformidade com as normas reconhecidas pela indústria para o fortalecimento das configurações (por exemplo, STIGs DISA, Referências CIS ou guias de segurança OEM) para ambientes de teste, desenvolvimento e produção. Isto inclui a criação de requisitos especiais de fortalecimento para ativos de alto valor (HVAs).

Questão de Controlo: A organização implementa funções de segurança como uma estrutura em camadas minimizando as interações entre as diversas áreas tecnológicas da organização?

Evidências:

1. N/D.

ESA - 02 | Análise Previsível de Falhas

Descrição: Mecanismos para determinar o Tempo Médio de Falha (MTTF) para componentes do sistema em ambientes específicos de funcionamento.

Implementação: A equipa responsável pelas aquisições de serviços, ou função semelhante, deve determinar o Tempo Médio de Falha (MTTF) para componentes dos sistemas em ambientes específicos de operação.

Questão de Controlo: A organização determina o Tempo Médio para A Falha (MTTF) para componentes do sistema em ambientes específicos de funcionamento?

Evidências:

1. Tempo Médio para Falha (MTTF).

ESA - 03 | Gestão do Ciclo de Vida da Tecnologia

Descrição: Mecanismos para gerir os ciclos de vida utilizáveis dos sistemas

Implementação: A organização deve gerir os ciclos de vida dos sistemas de modo a que se mitiguem falhas desnecessárias dos sistemas.

Questão de Controlo: A organização gere os ciclos de vida dos sistemas?

Evidências:

1. Programa de Ciclo de Vida Computacional (CLP).

ESA - 04 | Atualizações de Fontes Fidedignas

Descrição: Mecanismos para garantir que o software e os dados necessários para as componentes do sistema de informação e respetivas atualizações de serviço são obtidos a partir de fontes fidedignas.

Implementação: A organização deve configurar em cada sistema o respetivo repositório de atualizações seguro, preferencialmente um repositório local onde sejam definidos todas as tipologias de atualizações necessárias para os diversos equipamentos/software. Os sistemas da organizações e o software devem estar configurados para aceder apenas aos repositórios locais da organização.

Questão de Controlo: A organização garante que o software e os dados necessários para a componente do sistema de informação e as respetivas atualizações de serviço são obtidos a partir de fontes fidedignas?

Evidências:

1. Repositório Local de Atualizações.

ESA - 05 | HoneyPots

Descrição: Mecanismos para utilizar honeypots especificamente concebidos para serem alvo de ataques maliciosos com o propósito de detetar, desviar e analisar os respetivos ataques.

Implementação: A organização deve implementar e configurar honeypots em diversas áreas tecnológicas da organização, para detetar, desviar e e analisar ataque maliciosos que possa ocorrer na infraestrutura da organização.

Questão de Controlo: A organização utiliza honeypots especificamente concebidos para serem alvo de ataques maliciosos com o propósito de detetar, desviar e analisar os respetivos ataques?

Evidências:

1. N/D.

ESA - 06 | Sincronização do Relógio

Descrição: Mecanismos para utilizar a tecnologia de sincronização temporal para sincronizar todos os relógios críticos do sistema.

Implementação: As tecnologias/sistemas devem ser configuradas para utilizar a tecnologia de sincronização do temporal para sincronizar todos os relógios críticos do sistema.

Questão de Controlo: A organização utiliza a tecnologia de sincronização temporal para sincronizar todos os relógios críticos do sistema?

Evidências:

1. Protocolo de Tempo de Rede (NTP).

3.3.24 *Operações de Segurança*

ODS - 01 | Centro de Operações de Segurança (SOC)

Descrição: Mecanismos para estabelecer e manter um Centro de Operações de Segurança (SOC) que permite uma capacidade de resposta 24x7.

Implementação: O SOC deve ser capaz de detetar e responder a potenciais incidentes através de uma plataforma de tickets relacionados com a segurança. Deve monitorizar os registos dos ativos tecnológicos e analisar os feeds de inteligência de ameaças. O SOC deve responder a incidentes de cibersegurança e privacidade de acordo com os procedimentos implementados na organização. O SOC deve manter um repositório de documentação (base de conhecimento) para ajudar nas operações do SOC. Deve ser atribuída aos colaboradores do SOC funções e responsabilidades adequadas para ajudar a Equipa de Resposta a Incidentes de Segurança (CSIRT) nas operações de resposta a incidentes.

Questão de Controlo: A organização tem um Centro de Operações de Segurança (SOC) interno ou subcontratado que permite uma capacidade de resposta 24x7?

Evidências:

1. Colaboradores da Equipa do SOC;
2. Repositório de documentação do SOC.

ODS - 02 | Diretrizes de Práticas Seguras

Descrição: Mecanismos para fornecer orientações e recomendações para a utilização segura de produtos e/ou serviços para ajudar na configuração, instalação e utilização do produto e/ou serviço.

Implementação: A organização deve fornecer orientações e recomendações para a utilização segura das ferramentas e serviços presentes no portfólio da organização. Devem existir procedimentos e guias de utilização nomeadamente para as plataformas que gerem dados críticos e/ou confidenciais.

Questão de Controlo: A organização fornece orientações e recomendações para a utilização segura de produtos e/ou serviços para ajudar na configuração, instalação e utilização do produto e/ou serviço?

Evidências:

1. N/D.

3.3.25 *Consciência de Segurança e Formação*

CSF - 01 | Exercícios Práticos

Descrição: Mecanismos para incluir exercícios práticos na formação em segurança e privacidade que reforcem os objetivos estratégicos de aprendizagem.

Implementação: Devem existir processos administrativos, controlos físicos e tecnologias para simular ciberataques reais através de exercícios práticos que reforçam os objetivos de formação dos colaboradores.

Questão de Controlo: A organização inclui exercícios práticos na formação em segurança e privacidade que reforçam os objetivos estratégicos de aprendizagem?

Evidências:

1. N/D.

CSF - 02 | Utilizadores Privilegiados

Descrição: Mecanismos para fornecer formação específica para utilizadores privilegiados para garantir que os utilizadores privilegiados compreendam os seus papéis e responsabilidades.

Implementação: A equipa de GRC, ou função semelhante, deve fornecer formação específica para utilizadores privilegiados para garantir que os utilizadores privilegiados compreendam os seus papéis e responsabilidades.

Questão de Controlo: A organização fornece formação específica para utilizadores privilegiados para garantir que os utilizadores privilegiados compreendam os seus papéis e responsabilidades ?

Evidências:

1. N/D.

CSF - 03 | Registos de Formação em Segurança

Descrição: Mecanismos para documentar, reter e monitorizar as atividades de formação individual, incluindo a formação de sensibilização para a segurança básica, a formação em curso de sensibilização e a formação em sistemas específicos. Plano de ações de formação em segurança da informação.

Implementação: A equipa de GRC, ou função semelhante, deve fornecer formação específica para utilizadores privilegiados para garantir que os utilizadores privilegiados compreendam os seus papéis e responsabilidades.

Questão de Controlo: A organização documenta, retém e monitoriza as atividades de formação individual, incluindo a formação básica de sensibilização para a segurança, formação em curso de sensibilização e formação em sistemas específicos?

Evidências:

1. Lista de formações por colaborador.

3.3.26 *Desenvolvimento Tecnológico e Aquisição*

DTA - 01 | Mecanismos de Integridade para Atualizações de Software / Firmware

Descrição: Mecanismos para utilizar métodos de validação da integridade para atualizações de segurança.

Implementação: Devem existir processos administrativos e as tecnologias devem ser configuradas para executar mecanismos de validação de integridade nos binários a executar pela organização.

Questão de Controlo: A organização utiliza mecanismos de validação de integridade para atualizações de segurança?

Evidências:

1. Procedimento de validação de checksum.

DTA - 02 | Testes de Malware

Descrição: Mecanismos para utilizar pelo menos uma (1) ferramenta de deteção de malware para identificar se existe algum malware conhecido nos binários do produto ou da atualização de segurança.

Implementação: Existem processos administrativos para utilizar pelo menos uma (1) ferramenta de deteção de malware para identificar se existe algum malware conhecido nos binários de qualquer produto ou atualização de segurança

Questão de Controlo: A organização utiliza pelo menos uma (1) ferramenta de deteção de malware para identificar se existe algum malware conhecido nos binários do produto ou da atualização de segurança?

Evidências:

1. Ferramentas de deteção de Malware.

DTA - 03 | Requisitos de Segurança

Descrição: Mecanismos para incluir especificações técnicas e funcionais, explícitas ou por referência, em aquisições de sistemas baseadas numa avaliação do risco.

Implementação: A equipa responsável pela aquisição de serviços e produtos, ou função semelhante, deve facilitar a obtenção de especificações técnicas e funcionais, explícitas ou por referência, em aquisições do sistema com base numa avaliação do risco.

Questão de Controlo: A organização inclui especificações técnicas e funcionais, explícitas ou por referência, em aquisições de sistemas com base numa avaliação do risco?

Evidências:

1. N/D.

DTA - 04 | Portos Protocolos e Serviços Em Uso

Descrição: Mecanismos para exigir que os desenvolvedores de sistemas, componentes ou serviços do sistema identifiquem precocemente no Ciclo de Vida de Desenvolvimento Seguro (SDLC), as funções, portas, protocolos e serviços destinados a serem utilizados.

Implementação: Os contratos de aquisição devem exigir que os desenvolvedores de sistemas, componentes ou serviços do sistema identifiquem precocemente no Ciclo de Vida de Desenvolvimento Seguro (SDLC), as funções, portas, protocolos e serviços destinados a serem utilizados. Estes portos e serviços devem ser avaliados pela equipa de cibersegurança ou função semelhante em termos de risco e exposição para a organização.

Questão de Controlo: A organização exige que os desenvolvedores de sistemas, componentes ou serviços do sistema identifiquem precocemente no Ciclo de Vida de Desenvolvimento Seguro (SDLC), as funções, portas, protocolos e serviços destinados a serem utilizados?

Evidências:

1. Identificação dos Serviços e respetivas portas de rede.

DTA - 05 | Configurações de Segurança Pré-Estabelecidas

Descrição: Mecanismos para garantir que os fornecedores/fabricantes de software:

- Entreguem o sistema, componente ou serviço com configurações de segurança pré-estabelecidas pela organização;
- Utilizem as configurações de segurança pré-estabelecidas pela organização para qualquer sistema, componente ou reinstalação de serviço .

Implementação: A organização deve definir as configurações padrão para a instalação, atualização de um serviço ou sistema via entidades externas. As entidades externas devem assegurar o cumprimento das configurações pré-estabelecidas pela organização.

Questão de Controlo: A organização assegura fornecedores/fabricantes de software entreguem o sistema, componente ou serviço com configurações de segurança pré-estabelecidas pela organização e utilizem as configurações de segurança pré-estabelecidas pela organização para qualquer sistema, componente ou reinstalação de serviço ?

Evidências:

1. N/D.

DTA - 06 | Análise de Código Estático

Descrição: Mecanismos para exigir que os desenvolvedores de sistemas, componentes do sistema ou serviços utilizem ferramentas estáticas de análise de códigos para identificar e remediar falhas e documentar os resultados da respetiva análise.

Implementação: Os desenvolvedores de sistemas, componentes ou serviços do sistema devem ser obrigados a utilizar ferramentas estáticas de análise de código para identificar e remediar falhas efetuando a documentação dos resultados da análise antes de a aplicação ser introduzida nos sistemas de produção.

Questão de Controlo: A organização exige que os desenvolvedores de sistemas, componentes ou serviços do sistema utilizem ferramentas estáticas de análise de código para identificar e remediar falhas e documentar os resultados da respetiva análise?

Evidências:

1. N/D.

DTA - 07 | Análise Dinâmica do Código

Descrição: Mecanismos para exigir que os desenvolvedores de sistemas, componentes do sistema ou serviços utilizem ferramentas dinâmicas de análise de códigos para identificar e remediar falhas efetuando a documentação dos resultados da análise.

Implementação: Os desenvolvedores de sistemas, componentes ou serviços de sistema devem utilizar ferramentas dinâmicas de análise de código para identificar e remediar falhas, procedendo à documentação dos resultados da análise antes de a aplicação entrar em produção.

Questão de Controlo: A organização exige que os desenvolvedores de sistemas, componentes ou serviços do sistema utilizem ferramentas dinâmicas de análise de códigos para identificar e remediar falhas efetuando a documentação dos resultados da análise?

Evidências:

1. N/D.

3.3.27 *Gestão de Terceiros*

GDT - 01 | Serviços de Terceiros

Descrição: Mecanismos para mitigar os riscos associados ao acesso de terceiros aos sistemas e dados da organização.

Implementação: A equipa de GRC em conjunto com a equipa de de TI, devem mitigar os riscos associados ao acesso de terceiros aos sistemas e dados da organização.

Questão de Controlo: A organização atenua os riscos associados ao acesso de terceiros aos sistemas e dados da organização?

Evidências:

1. Avaliação de Risco antes da aquisição de serviços;
2. Políticas e Procedimentos de prestação de serviços.

GDT - 02 | Requisitos Contratuais de Terceiros

Descrição: Mecanismos para identificar, rever e documentar regularmente a confidencialidade de terceiros, acordos de não-divulgação (NDAs) e outros contratos que reflitam as necessidades da organização de proteger sistemas e dados.

Implementação: Os contratos de aquisição devem identificar a necessidade, rever regularmente e documentar a confidencialidade de terceiros, os Acordos de Não-Divulgação (NDAs) e outros contratos que reflitam as necessidades da organização de proteger sistemas e dados.

Questão de Controlo: A organização identifica, revê e documenta regularmente confidencialidade de terceiros, Acordos de Não-Divulgação (NDAs) e outros contratos que reflitam as necessidades da organização para proteger sistemas e dados?

Evidências:

1. Acordos de Não Divulgação (NDAs).

3.3.28 *Gestão de Ameaças*

GDA - 01 | Programa de Inteligência de Ameaças

Descrição: Mecanismos para implementar um programa de inteligência de ameaças que inclui uma capacidade de partilha de informação entre organizações que pode influenciar o desenvolvimento do sistema e arquiteturas de segurança, seleção de soluções de segurança, monitorização, procura de ameaças, resposta e recuperação.

Implementação: A equipa de Cibersegurança deve definir um programa de inteligência de ameaças, constituída pela partilha de IoCs entre várias organizações externas do setor onde esta se incluí.

Questão de Controlo: A organização implementa um programa de sensibilização para ameaças que inclui uma capacidade de partilha de informação entre organizações?

Evidências:

1. Programa de Inteligência de Ameaças.

GDA - 02 | Indicadores de Exposição (IOE)

Descrição: Mecanismos para desenvolver indicadores de exposição (IOE) para entender os potenciais vetores de ataque que os utilizadores maliciosos poderiam utilizar para atacar a organização.

Implementação: O SOC, ou função semelhante, deve facilitar o desenvolvimento de Indicadores de Exposição (IOE) para entender os potenciais vetores de ataque que os utilizadores maliciosos poderiam utilizar para atacar a organização.

Questão de Controlo: A organização desenvolve Indicadores de Exposição (IOE) para entender os potenciais vetores de ataque que os atacantes poderiam usar para atacar a organização?

Evidências:

1. Indicadores de Exposição (IoE).

GDA - 03 | Feeds de Inteligência de Ameaças

Descrição: Mecanismos para manter a consciência da situação das ameaças em evolução, aproveitando o conhecimento das táticas, técnicas e procedimentos dos atacantes para facilitar a implementação de controlos preventivos.

Implementação: Um Centro de Operações de Segurança (SOC), ou função semelhante, deve facilitar as operações de gestão de incidentes que cobrem a preparação, deteção e análise, contenção, erradicação e recuperação, incluindo monitorização de feeds de inteligência de ameaças. Devem existir processos administrativos para que o SOC mantenha a consciência da situação das ameaças em evolução na atualidade. Deve ser criado um feed de inteligência de ameaças que permita a partilha de indicadores de compromisso, para inserir nos equipamentos ativos (Firewalls, DNS, EDR entre outros), para o bloqueio automático dos IoCs, com o intuito de estes não acederem à infraestrutura da organização.

Questão de Controlo: A organização mantém a consciência da situação das ameaças em evolução?

Evidências:

1. Feeds de Inteligência de Ameaças.

GDA - 04 | Programa de Divulgação de Vulnerabilidades (VDP)

Descrição: Mecanismos para estabelecer um Programa de Divulgação de Vulnerabilidades (VDP) para ajudar no desenvolvimento e manutenção segura de produtos e serviços que recebem informações não solicitadas do público sobre vulnerabilidades em sistemas organizacionais, serviços e processos.

Implementação: A organização deve estabelecer um programa de vulnerabilidades para ajudar na identificação e mitigação de vulnerabilidades com foco no ecossistema digital da organização.

Questão de Controlo: A organização estabelece um Programa de Divulgação de Vulnerabilidades (VDP) para ajudar no desenvolvimento e manutenção segura de produtos e serviços que recebem informações não solicitadas do público sobre vulnerabilidades em sistemas organizacionais, serviços e processos?

Evidências:

1. Programa bug bounty (hackerone entre outras plataformas).

3.3.29 *Gestão de Vulnerabilidades e Atualizações*

GVP - 01 | Programa de Divulgação de Vulnerabilidades (VDP)

Descrição: Mecanismos para facilitar a implementação e a supervisão dos controlos de gestão da vulnerabilidade.

Implementação: Um SOC, ou função similar, deve gerir centralmente o processo de remediação de falhas como parte do programa de gestão de atualizações e vulnerabilidades das organizações em geral (VPMP), incluindo a supervisão dos controlos de gestão de vulnerabilidades em toda a organização.

Questão de Controlo: A organização facilita a implementação e monitorização dos controlos de gestão de vulnerabilidades?

Evidências:

1. Programa de Gestão de Vulnerabilidades e Atualizações.

GVP - 02 | Processo de Remediação de Vulnerabilidades

Descrição: Mecanismos para garantir que as vulnerabilidades sejam devidamente identificadas, rastreadas e remediadas.

Implementação: Um SOC, ou função semelhante, deve facilitar a identificação, acompanhamento e mitigação de vulnerabilidades.

Questão de Controlo: A organização garante que as vulnerabilidades são devidamente identificadas, rastreadas e remediadas?

Evidências:

1. Procedimento de identificação e remediação de vulnerabilidades.

GVP - 03 | Ranking de Vulnerabilidade

Descrição: Mecanismos para identificar e atribuir um ranking de risco a vulnerabilidades de segurança recentemente descobertas utilizando fontes externas fidedignas para informações de vulnerabilidade de segurança.

Implementação: Um SOC, ou função semelhante, deve identificar e atribuir um ranking de risco a vulnerabilidades de segurança recentemente descobertas utilizando fontes externas fidedignas para informações de vulnerabilidade de segurança.

Questão de Controlo: A organização identifica e atribui um ranking de risco a vulnerabilidades de segurança recentemente descobertas utilizando fontes externas fidedignas para informações de vulnerabilidade de segurança?

Evidências:

1. Procedimento de classificação de vulnerabilidades através de CVSS (Common Vulnerability Scoring System).

GVP - 04 | Atividades de Remediação Contínua de Vulnerabilidades

Descrição: Mecanismos para enfrentar novas ameaças e vulnerabilidades numa base contínua e garantir que os ativos são protegidos contra ataques conhecidos.

Implementação: Um SOC, ou função semelhante, deve abordar novas ameaças e vulnerabilidades numa base contínua e garantir que os ativos são protegidos contra ataques conhecidos.

Questão de Controlo: A organização aborda novas ameaças e vulnerabilidades numa base contínua e garante que os ativos estão protegidos contra ataques conhecidos?

Evidências:

1. N/D.

GVP - 05 | Correções de Software e Firmware

Descrição: Mecanismos para realizar correções de software para todos os sistemas operativos, aplicações e firmware implementados.

Implementação: Devem existir processos administrativos e as tecnologias devem ser configuradas para os gestores de ativos realizarem correções de software para todos os sistemas operativos, aplicações e firmware implementados.

Questão de Controlo: A organização realiza correções de software para todos os sistemas operativos, aplicações e firmware implementados?

Evidências:

1. Ferramenta e gestões de correções (Patching).

GVP - 06 | Análises Internas de Vulnerabilidades

Descrição: Mecanismos para realizar análises trimestrais de vulnerabilidades internas, que incluem todos os segmentos da rede interna da organização.

Implementação: Deve ser efetuada uma verificação completa de vulnerabilidades na organização com o intuito de detetar vulnerabilidades e erros de configuração de sistemas, aplicações e serviços em toda a organização. Esta verificação deve ser efetuada trimestralmente.

Questão de Controlo: A organização realiza análises trimestrais de vulnerabilidade interna, que inclui todos os segmentos da rede interna da organização?

Evidências:

1. Relatórios Trimestrais de Vulnerabilidades.

GVP - 07 | Testes de Intrusão

Descrição: Mecanismos para realizar testes de penetração em sistemas e aplicações web.

Implementação: Um SOC, ou função semelhante, deve organizar e executar os testes de penetração em sistemas e aplicações web com periodicidade semestral.

Questão de Controlo: A organização realiza testes de penetração em sistemas e aplicações web?

Evidências:

1. Relatórios Semestrais dos testes de intrusão.

3.3.30 *Segurança Web*

SWB - 01 | Firewall de Aplicação Web (WAF)

Descrição: Mecanismos para implementar firewalls de aplicação web (WAFs) para fornecer proteção em profundidade para ameaças específicas da aplicação.

Implementação: As proteções da fronteira da organização anível aplicacional devem utilizar firewalls de aplicações web (WAFs) para fornecer proteção em profundidade para ameaças específicas das aplicações.

Questão de Controlo: A organização implementa firewalls de aplicação web (WAFs) para fornecer proteção em profundidade para ameaças específicas da aplicação?

Evidências:

1. Firewall de aplicação web (WAF).

3.4 SÍNTESE DA FRAMEWORK

Por forma a sintetizar todo o trabalho realizado, é apresentado seguidamente o quadro que enuncia todos os domínios e questões de controlo em conformidade com a framework CSE4CI.

Nos domínios, estão referidas as áreas específicas dentro da estrutura de cibersegurança que posteriormente serão avaliadas. Os domínios geralmente representam aspetos fundamentais da segurança informática, como a gestão, proteção de dados, deteção de ameaças, resposta a incidentes, entre outros. Cada domínio aborda um conjunto específico de desafios e melhores práticas de segurança.

Na coluna relacionada com as questões de controlo, aqui são listadas as perguntas específicas relacionadas ao domínio em questão. Essas perguntas são formuladas para avaliar se a organização está a cumprir com os requisitos e padrões de segurança estabelecidos pela estrutura apresentada ao longo deste documento. Estas questões de controlo servem como critérios para determinar o nível de conformidade da organização. Na figura 5 é possível verificar um excerto da síntese dos controlos com base nas questões associadas aos mesmos.

É importante salientar que a proteção criptográfica, a classificação e o tratamento de dados, juntamente com a segurança de endpoints e dos recursos humanos, são pilares fundamentais para prevenir e mitigar os riscos associados a ataques

Domínio CSE4CI	Questão de controlo (CSE4CI)
Governação de Segurança e Privacidade	Os colaboradores da organização operam de forma a governar centralmente os controlos de cibersegurança e privacidade?
Governação de Segurança e Privacidade	A organização estabelece, mantém e divulga políticas de cibersegurança e privacidade, normas e procedimentos?
Governação de Segurança e Privacidade	A organização revê as políticas de cibersegurança e privacidade, padrões e procedimentos em intervalos previstos ou se ocorrerem alterações significativas para garantir a sua adequação, adequação e eficácia contínuas?
Governação de Segurança e Privacidade	A organização atribui a um indivíduo qualificado a missão e recursos para gerir centralmente a coordenação, desenvolver, implementar e manter um programa de cibersegurança e privacidade em toda a empresa?
Governação de Segurança e Privacidade	A organização desenvolve, reporta e monitoriza os Principais Indicadores de Desempenho (KPI's) para ajudar a gestão organizacional na monitorização de desempenho e análise de tendências do programa de cibersegurança e privacidade?
Governação de Segurança e Privacidade	A organização desenvolve, reporta e monitoriza indicadores-chave de risco (KRIs) para ajudar a gestão sénior na monitorização de desempenho e análise de tendências do programa de cibersegurança e privacidade?
Governação de Segurança e Privacidade	A organização identifica e documenta os contactos adequados dentro das autoridades policiais e regulamentares competentes?
Governação de Segurança e Privacidade	A organização estabelece a governação de dados em toda a organização?
Gestão de Ativos	A organização facilita a implementação de controlos de gestão de ativos?
Gestão de Ativos	A organização identifica e avalia a segurança dos ativos tecnológicos que suportam mais do que uma função empresarial crítica?
Gestão de Ativos	A organização de inventário de ativos de tecnologia que: ▪ Reflete com precisão o sistema atual; ▪ Encontra-se ao nível da granularidade considerada necessária para o rastreio e a comunicação; ▪ Inclui informações definidas pela organização consideradas necessárias para obter uma responsabilização efetiva da propriedade; e ▪ está disponível para revisão e auditoria por funcionários organizacionais designados?
Gestão de Ativos	A organização utiliza mecanismos automatizados para detetar e alertar após a deteção de componentes de hardware, software e firmware não autorizados?

Figura 5: Excerto da Tabela Síntese da Framework (Tabela completa presente no Apêndice B)

cibernéticos direcionados. A identificação e autenticação adequadas garantem que apenas os utilizadores autorizados tenham acesso aos sistemas e informações sensíveis, enquanto a resposta a incidentes permite uma ação rápida e eficaz diante de eventos de segurança adversos.

A garantia de informação assegura a integridade e confiabilidade dos dados, enquanto a manutenção adequada dos sistemas e a gestão de dispositivos móveis fortalecem a segurança em todas as plataformas. A segurança da rede é fundamental para proteger a infraestrutura de comunicação e prevenir ataques de rede, enquanto a segurança física e ambiental garante a proteção dos ativos físicos e infraestrutura crítica.

A privacidade, considerada um direito fundamental, requer medidas de segurança robustas para proteger os dados pessoais e evitar violações de privacidade. O projeto e gestão de recursos abrange a seleção e implementação de soluções tecnológicas seguras, enquanto a gestão de riscos identifica e avalia os riscos potenciais e desenvolve estratégias para mitigá-los.

A engenharia de segurança e arquitetura estabelece os fundamentos para a construção de sistemas e redes seguras desde o início, enquanto as operações de segurança garantem a manutenção contínua das medidas de segurança e a resposta efetiva a incidentes em tempo real. A consciência de segurança e a formação são componentes vitais para criar uma cultura de segurança em toda a organização, capacitando os indivíduos a se tornarem defensores proativos da segurança cibernética.

A gestão de ameaças e vulnerabilidades, juntamente com a segurança web, fecha o círculo, fornecendo uma abordagem abrangente para identificar, avaliar e mitigar os riscos associados a ataques cibernéticos e ameaças emergentes.

Por fim, o desenvolvimento tecnológico e a aquisição de soluções de segurança adequadas são essenciais para acompanhar as rápidas mudanças tecnológicas e garantir que as medidas de segurança sejam atualizadas e eficazes. A gestão de terceiros desempenha um papel crítico na garantia da segurança de parceiros, fornecedores e prestadores de serviços externos, pois a segurança de uma organização é tão forte quanto a sua cadeia de fornecimento mais fraca.

4

PROVA DE CONCEITO

Com vista a validar a framework desenvolvida, foi elaborada uma prova de conceito com a avaliação da aplicação da framework num caso real. A recolha de dados foi realizada através de um processo cuidadosamente planeado e delineado com a organização selecionada, que foi mantida em sigilo por motivos de segurança.

Foi elaborado um quadro de excel que contém a lista detalhada dos controlos de cibersegurança, cada um identificado por um nome único e acompanhado por uma descrição concisa das medidas de segurança que representava. Além disso, o quadro em excel incluí uma coluna designada para atribuir valores numéricos que quantificassem o grau de implementação e eficácia de cada controlo, com os valores genéricos para a importância dos mesmos nas diversas organizações que gerem infraestruturas críticas. Relembrar que estes valores referentes a cada controlo podem ser alterados, pois em diferentes setores de atividade podem exigir outra quantificação dos mesmos.

Para recolher os dados, utilizando o quadro de valores de maturidade de implementação nos domínios da CSE4CI, o CISO de uma organização de relevo público efetuou vários passos que se encontram descritos nas secções abaixo.

4.1 IDENTIFICAÇÃO DOS DOMÍNIOS RELEVANTES

Inicialmente, o CISO identificou quais os domínios da CSE4CI eram relevantes para a organização. Com base nessa seleção, concentrou-se em recolher dados e documentação sobre cada um desses domínios, com vista ao preenchimento da tabela previamente elaborada, tal como apresentado na tabela apresentada no Apêndice B.

4.2 DEFINIÇÃO DOS CRITÉRIOS DE MATURIDADE

Para cada domínio selecionado, o CISO definiu critérios claros da organização em relação à maturidade da framework em que deferiram as opções: "Não implementado"ou "Implementado", para cada um dos domínios. Esses critérios serviram como uma escala de avaliação para determinar o nível de implementação dos controlos em cada domínio.

Os valores numéricos atribuídos a cada controlo foram determinados com base na criticidade para a gestão e operação de infraestruturas críticas, sendo que foram considerados vários fatores. Esses fatores incluíam a extensão da implementação do controlo, a sua conformidade com normas de segurança relevantes, a eficácia na proteção da organização, e a sua contribuição potencial para a redução de riscos. Este valor pode ser alterado em cada controlo ou, para casos específicos, onde os mesmos sejam impossíveis de aplicar.

Os resultados da avaliação da maturidade foram sintetizados em percentagem, calculado a soma dos valores atribuídos a cada controlo, sintetizando a percentagem de maturidade por cada domínio da framework e o respetivo resultado do valor de maturidade. Esses valores advém da multiplicação do peso do controlo com a implementação ou não implementação (Implementado = 1 , Não Implementado = 0).

4.3 AVALIAÇÃO DA IMPLEMENTAÇÃO E PREENCHIMENTO DA CALCULADORA DE MATURIDADE

O CISO conduziu avaliações detalhadas em cada domínio, examinando a implementação dos controlos específicos definidos na CSE4CI. Ele recolheu evidências e informações relevantes que ajudaram a determinar se cada controlo estava ou não implementado, de acordo com os critérios definidos.

O CISO preencheu o quadro com os valores de maturidade de implementação para cada domínio. Isso envolveu a atribuição de um dos dois valores: "Não implementado", "Implementado", tal como apresentado na figura 6.

Domínio CSE4CI	Questão de controlo (CSE4CI)	Resposta	Controlo Ponderado	Valor Controlo	Peso do Controlo (1-10)	Grupo
Governação de Segurança e Privacidade	Os colaboradores da organização	Implementado	10	1	10	Identify
Governação de Segurança e Privacidade	A organização estabelece, mantém e divulga	Não implementado		0	10	Identify
Governação de Segurança e Privacidade	A organização revê as políticas de	Implementado	7	1	7	Identify
Governação de Segurança e Privacidade	A organização atribui a um indivíduo	Implementado	10	1	10	Identify
Governação de Segurança e Privacidade	A organização desenvolve, reporta e monitoriza os	Não implementado		0	6	Protect
Governação de Segurança e Privacidade	A organização desenvolve, reporta e	Implementado	6	1	6	Protect
Governação de Segurança e Privacidade	A organização identifica e documenta os	Implementado	5	1	5	Identify
Governação de Segurança e Privacidade	A organização estabelece a governação de	Implementado	10	1	10	Protect

Figura 6: Excerto da Calculadora de maturidade CSE4CI

4.4 ANÁLISE FINAL DOS RESULTADOS

Após a recolha dos dados em todos os domínios da CSE4CI, o CISO realizou uma análise abrangente dos resultados. O quadro partilhado com o CISO permitiu calcular automaticamente o estado da organização em cada domínio e apresentou um gráfico geral das áreas que estão em conformidade, assim como as que necessitam de melhorias. Os dados recolhidos por via deste processo foram utilizados como base para o caso de uso desta dissertação. Eles forneceram uma avaliação concreta da postura de segurança da organização em relação aos padrões e controlos da CSE4CI. Ao seguir este processo, o CISO conseguiu recolher dados precisos e significativos sobre a implementação de controlos de segurança em cada domínio da CSE4CI, fornecendo uma base sólida para a sua pesquisa e análise de segurança na organização onde se encontra.

A análise dos resultados permitiu identificar áreas de destaque na organização, onde os controlos de cibersegurança estavam bem implementados e tinham contribuído significativamente para a maturidade geral. Isto incluí controlos que demonstraram uma implementação completa, e conformidade com os padrões de segurança descritos pela CSE4CI. Por outro lado, também foi possível identificar áreas que requerem melhorias substanciais, onde os controlos não estavam totalmente implementados ou não estão a atingir completamente os parâmetros necessários em cada controlo. Através dos resultados obtidos, podemos verificar que a organização necessita de melhorar os domínios de Segurança Física e Ambiental, Consciência de Segurança e Formação, Gestão de Vulnerabilidades e Atualizações, Manutenção e

Classificação e Tratamento de Dados. Estes domínios não foram além dos 60 por cento de execução, o que para uma organização e na ótica da framework é uma percentagem muito baixa.

Nos pontos positivos, temos os domínios Capacidade e Planeamento de Desempenho, Segurança na Cloud, Monitorização Contínua, Proteções Criptográficas, Garantia da Informação, Operações de Segurança, Gestão de Terceiros e Segurança Web. Estes domínios tiveram uma percentagem de 100 por cento de execução na análise efetuada pelo CISO. O respetivo gráfico dos resultado pode ser visualizado na figura 7, e os resultados finais na figura 8.

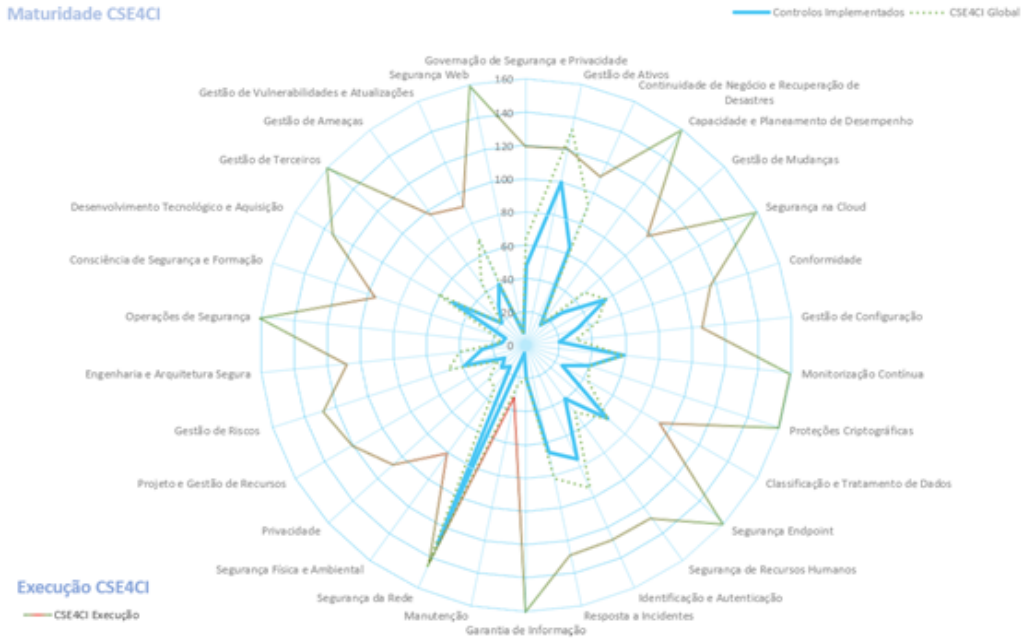

Figura 7: Gráfico dos resultados do Caso de Uso

Domínio CSE4CI	Controlos Implementados	CSE4CI Global	CSE4CI Execução
Governação de Segurança e Privacidade	48	64	75%
Gestão de Ativos	100	132	76%
Continuidade de Negócio e Recuperação de Desastres	64	92	70%
Capacidade e Planeamento de Desempenho	15	15	100%
Gestão de Mudanças	29	47	62%
Segurança na Cloud	55	55	100%
Conformidade	33	45	73%
Gestão de Configuração	20	30	67%
Monitorização Contínua	59	59	100%
Proteções Criptográficas	40	40	100%
Classificação e Tratamento de Dados	25	43	58%
Segurança Endpoint	66	66	100%
Segurança de Recursos Humanos	40	50	80%
Identificação e Autenticação	75	94	80%
Resposta a Incidentes	66	82	80%
Garantia de Informação	20	20	100%
Manutenção	5	25	20%
Segurança da Rede	131	147	89%
Segurança Física e Ambiental	16	32	50%
Privacidade	20	30	67%
Projeto e Gestão de Recursos	15	20	75%
Gestão de Riscos	39	49	80%
Engenharia e Arquitetura Segura	27	40	68%
Operações de Segurança	15	15	100%
Consciência de Segurança e Formação	13	22	59%
Desenvolvimento Tecnológico e Aquisição	51	61	84%
Gestão de Terceiros	20	20	100%
Gestão de Ameaças	28	46	61%
Gestão de Vulnerabilidades e Atualizações	40	70	57%
Segurança Web	8	8	100%

Figura 8: Resultados do Caso de Uso por domínio

4.5 CONCLUSÃO DOS RESULTADOS OBTIDOS

Em resumo, a análise de maturidade dos controlos de cibersegurança revelou informações valiosas sobre o estado atual da postura de segurança da organização, ao qual o CISO efetuou a análise. Os resultados identificaram tanto áreas que demonstraram solidez em termos de segurança quanto áreas que precisam de melhorias.

Os resultados desempenham um papel crucial na definição das prioridades de segurança da organização. Eles fornecem uma base objetiva para a alocação de recursos, investimentos e esforços de melhoria. As áreas fortes podem ser reconhecidas e consolidadas, enquanto as áreas com necessidade de melhoria podem ser alvo de estratégias de correção e otimização. Além disso, os resultados influenciam diretamente nas decisões de segurança a serem tomadas no futuro, garantindo que a organização esteja em constante evolução para enfrentar os desafios num cenário de ameaças em constante mudança.

O CISO, efetuou, por fim o seguinte comentário, relativamente à ferramenta de cálculo de maturidade e execução da framework CSE4CI: "Esta framework apresenta um novo referencial de cibersegurança para Infraestruturas Críticas (IC) que é mais abrangente e holístico do que os referenciais existentes, permitindo uma avaliação dos desafios e lacunas dos para IC's, considerando diferentes aspetos da cibersegurança aplicada às IC's, incluindo segurança da informação, segurança da infraestrutura física e a segurança da operação. Contudo existem algumas oportunidades para melhoria, nomeadamente uma análise de implementação de forma a demonstrar a viabilidade do referencial proposto, assim como propostas de mitigação automáticas para os controlos não implementados, controlos mais específicos na área de segurança web e criptografia quântica".