Plano de Segurança para Centro de Investigação e Desenvolvimento

Luís Gonçalves
Nrº 18851

Licenciatura em Engenharia em Sistemas Informáticos
Escola Superior de Tecnologia
Instituto Politécnico do Cávado e do Ave

Índice

1 Introdução **1**

1.1 Objetivo 1

1.2 Mais-Valias 1

1.3 Estrutura do Plano de Segurança 1

1.4 Frameworks, Metodologias e Certificados 2

1.4.1 Framework OCTAVE 2

1.4.2 NIST Cybersecurity Framework 2

1.4.3 ISO/IEC 27001 3

1.4.4 COBIT 3

1.4.5 Certificações de Segurança 3

2 Contextualização **4**

2.1 Descrição do CIDT 4

2.1.1 Espaço Físico 4

2.1.2 Processo de Negócio 4

2.1.3 Organograma 5

2.1.4 Departamento de Recursos Humanos 6

3 Recursos **8**

3.1 Funções e Responsabilidades no CIDT 8

3.2 Mapa de Recursos e Funções 10

3.3 Infraestrutura de Rede 12

4 Gestão dos Sistemas de Informação **13**

4.1 Sistemas de Informação 13

4.2 Suporte do Ciclo de Vida 15

4.3 Restrições de Uso de Software 16

4.4 Software Instalado pelo Utilizador 16

4.5 Serviços Externos do Sistema de Informação 17

4.6 Políticas de Confidencialidade 18

5 Análise e Mitigação de Riscos 19

5.1 Identificação e Categorização dos Riscos 19
5.2 Avaliação e Classificação dos Riscos 20
5.3 Gestão e Mitigação do Risco 20
5.4 Processo Contínuo de Gestão de Riscos 21
5.5 Identificação dos Riscos 22
5.6 Mitigação de Riscos 26

6 Plano de Contingência 30

6.1 Introdução 30
6.2 Objetivos do Plano de Contingência 30
6.3 Plano de Resposta a Incidentes 30
6.4 Plano de Recuperação de Desastres 33
6.5 Plano de Continuidade de Negócios 34
6.6 Monitorização e Revisão do Plano de Contingência 34

7 Formações de Cibersegurança 36

7.1 Objetivos do Plano de Formações 36
7.2 Estrutura do Plano de Formações 36
7.3 Plano de Formação 37
7.3.1 Consciencialização Básica 37
7.3.2 Formação Intermediária 37
7.3.3 Formação Avançada 38
7.4 Métodos de Avaliação 38
7.5 Cronograma de Implementação 39
7.6 Cronograma das Formações 40

8 Auditorias 41

8.1 Objetivos das Auditorias 41
8.2 Estrutura das Auditorias 41
8.3 Plano de Auditorias 42
8.3.1 Auditorias Internas 42
8.3.2 Auditorias Externas 42
8.3.3 Auditorias de Conformidade 43
8.3.4 Auditorias de Vulnerabilidade 43

8.3.5 Auditorias de Segurança Física 44
8.4 Metodologias de Auditoria 44
8.4.1 Metodologia de Auditoria Interna 44
8.4.2 Metodologia de Auditoria Externa 44
8.4.3 Metodologia de Auditoria de Conformidade 45
8.4.4 Metodologia de Auditoria de Vulnerabilidade 45
8.4.5 Metodologia de Auditoria de Segurança Física 45
8.5 Cronograma de Auditorias 45

Figuras

1.1 Esquema da framework OCTAVE 2

2.1 Organograma 6

5.1 Esquema do Processo Contínuo de Gestão de Riscos 29

Tabelas

3.1 Funções e Responsabilidades no CIDT 8
3.2 Mapa de Recursos e Funções 10

4.1 Gestão dos Sistemas de Informação 13
4.1 Gestão dos Sistemas de Informação 14
4.1 Gestão dos Sistemas de Informação 15
4.2 Suporte do Ciclo de Vida 15
4.3 Restrições de Uso de Software 16
4.4 Software Instalado pelo Utilizador 16
4.5 Serviços Externos do Sistema de Informação 17
4.6 Requisitos de Classificação 18

5.1 Categorização dos Riscos no CIDT 19
5.2 Matriz de Avaliação e Classificação dos Riscos no CIDT 20
5.3 Estratégias de Mitigação de Riscos no CIDT 20
5.4 Processo Contínuo de Gestão de Riscos no CIDT 21
5.5 Análise de Riscos no CIDT 22
5.5 Análise de Riscos no CIDT 23
5.5 Análise de Riscos no CIDT 24
5.5 Análise de Riscos no CIDT 25
5.5 Análise de Riscos no CIDT 26
5.6 Mitigação dos Riscos no CIDT 26
5.6 Mitigação dos Riscos no CIDT 27
5.6 Mitigação dos Riscos no CIDT 28

6.1 Plano de Resposta a Incidentes 31
6.1 Plano de Resposta a Incidentes 32
6.1 Plano de Resposta a Incidentes 33
6.2 Plano de Recuperação de Desastres 33

6.3 Plano de Continuidade de Negócios 34
6.4 Monitorização e Revisão do Plano de Contingência 34
6.4 Monitorização e Revisão do Plano de Contingência 35

7.1 Estrutura do Plano de Formações de Cibersegurança 36
7.2 Consciencialização Básica 37
7.3 Formação Intermediária 37
7.4 Formação Avançada 38
7.5 Métodos de Avaliação 39
7.6 Cronograma de Implementação 39
7.7 Cronograma de Formações 40

8.1 Estrutura do Plano de Auditorias 42
8.2 Auditorias Internas 42
8.3 Auditorias Externas 43
8.4 Auditorias de Conformidade 43
8.5 Auditorias de Vulnerabilidade 43
8.6 Auditorias de Segurança Física 44
8.7 Cronograma de Auditorias 45

Siglas & Acrónimos

CEH Certified Ethical Hacker. 3

CIDT Centro de Investigação e Desenvolvimento Tecnológico. vi, 1, 2, 4–10, 12–28, 30, 36, 37, 41, 42, 44

CISA Certified Information Systems Auditor. 3

CISSP Certified Information Systems Security Professional. 3

COBIT Control Objectives for Information and Related Technologies. 3, 41, 44

CRAMM CCTA Risk Analysis and Management Method. 19, 20

DDoS Distributed Denial of Service. 23, 26, 32

DLP Data Loss Prevention. 28

IAM Identity and Access Management. 13

IDS Intrusion Detection System. 13

IEC International Electrotechnical Commission. 3

IP Internet Protocol. 27

ISO International Organization for Standardization. 3, 25, 28

NIST National Institute of Standards and Technology. 2

OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation. 2

RGPD Regulamento Geral de Proteção de Dados. 22, 42, 43

SGSI Sistema de Gestão de Segurança da Informação. 3

SIEM Security Information and Event Management. 14

SQL Structured Query Language. 25

TI Tecnologias da Informação. 3, 4, 10, 13–17, 26, 31, 37, 38, 40, 42, 43, 45

USB Universal Serial Bus. 24, 27, 31

Glossário

Botnet Rede de computadores infectados que podem ser controlados remotamente e forçados a enviar spam, espalhar malware, etc. . 32

certificações Certificação é a declaração formal de comprovação emitida por quem tenha credibilidade ou autoridade legal. Certificação é mais rigorosa que certificado pela exigência de uma prova de credibilidade. . 3

Malware Malware, ou software malicioso, é um termo geral para qualquer tipo de software informático com intenção maliciosa[1]. . 19, 24, 31

Man-in-the-Middle É uma forma criminosa de intercetar a comunicação entre dois hosts e, consequentemente, roubar informações. . 25

patches Atualizações feitas para eliminar bugs. . 27, 31, 32

Phishing Phishing é o crime de ludibriar as pessoas, levando-as a partilhar informações confidenciais, como palavras-passe e números de cartões de crédito. . 23, 31

prepared statements Funcionalidade onde a base de dados pré-compila o código SQL e armazena os resultados, separando-os dos dados. . 28

Ransomware Ransom malware, ou ransomware, é um tipo de malware que impede os utilizadores de aceder ao seu sistema ou ficheiros pessoais e exige-lhes o pagamento de um resgate para devolver o acesso[5]. . 19, 31

Spear phishing Semelhante ao phishing, no entanto visa indivíduos ou organizações específicas. . 25, 31

stored procedures São funções pré-compiladas que ajudam a proteger a base de dados através do controlo de acesso, prevenção de injeção de SQL e validação de entradas, centralizando e restringindo a execução de operações críticas. . 28

1. Introdução

1.1 Objetivo

O objetivo deste plano de segurança é garantir a proteção pessoal, de propriedade intelectual, de equipamentos e de dados sensíveis. Para além disso, procura-se promover um ambiente propício à inovação, onde os investigadores se sintam seguros para explorar novas ideias e desenvolver tecnologias avançadas. Este plano visa estabelecer diretrizes e medidas de segurança que assegurem a integridade das atividades de investigação e desenvolvimento, bem como a proteção dos ativos intelectuais e físicos.

1.2 Mais-Valias

A implementação de um plano de segurança nos Centros de Investigação e Desenvolvimento Tecnológico (CIDT) proporciona diversas mais-valias que contribuem para o sucesso e eficiência das atividades desenvolvidas, como, por exemplo, a proteção de ativos intelectuais, prevenção de perdas materiais, conformidade legal. Além disso, cria na organização uma cultura de segurança e, acima de tudo, dá instruções aos colaboradores de como agir em caso de emergência.

1.3 Estrutura do Plano de Segurança

1. Gestão dos Sistemas de Informação
2. Análise e Mitigação de Riscos
3. Políticas de Segurança
4. Plano de Resposta
5. Plano de Recuperação
6. Plano de Contingência
7. Formação de Colaboradores
8. Auditorias

A estrutura do plano de segurança deve ser flexível o suficiente para se adaptar às mudanças nas ameaças e tecnologias, garantindo assim a proteção contínua dos ativos e operações do CIDT.

O plano deve ser atualizado regularmente adaptando-se a novas ameaças e ferramentas.

1.4 Frameworks, Metodologias e Certificados

Neste plano de segurança, utilizamos diversas frameworks, metodologias e certificados reconhecidos internacionalmente para assegurar a eficácia e abrangência das nossas estratégias de segurança. Estas ferramentas fornecem uma base sólida para a gestão de riscos, segurança da informação e continuidade dos negócios.

1.4.1 Framework OCTAVE

A framework OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) é uma metodologia de gestão de riscos projetada para identificar, avaliar e mitigar riscos de segurança da informação em organizações. A OCTAVE distingue-se pelo seu foco no risco organizacional e pela sua adaptabilidade a qualquer tipo de estrutura organizacional, combinando um enfoque nos objetivos organizacionais com os ativos tecnológicos. A OCTAVE é uma ferramenta equilibrada e abrangente para a gestão de riscos [6].

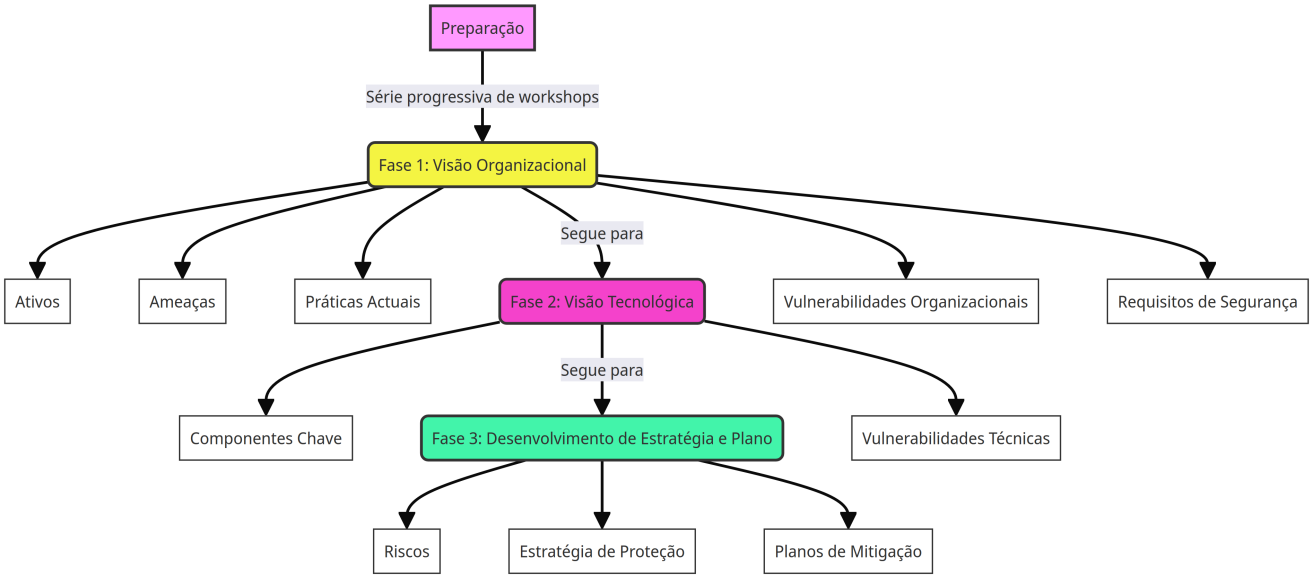

Figure 1.1: Esquema da framework OCTAVE

1.4.2 NIST Cybersecurity Framework

A framework do NIST (National Institute of Standards and Technology) é amplamente reconhecida e utilizada para melhorar a gestão e redução de riscos de cibersegurança. O NIST Cybersecurity Framework proporciona uma abordagem sistemática para identificar, proteger, detetar, responder e recuperar de incidentes de cibersegurança. Esta framework

é valiosa para estabelecer uma base robusta de segurança cibernética alinhada com práticas recomendadas e padrões internacionais[7].

1.4.3 ISO/IEC 27001

A norma ISO/IEC 27001 é um padrão internacional para a gestão de segurança da informação. Ela especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). A conformidade com a ISO/IEC 27001 assegura que a organização implementa práticas eficazes de segurança da informação, protegendo os dados sensíveis e garantindo a continuidade das operações[8].

1.4.4 COBIT

O COBIT (Control Objectives for Information and Related Technologies) é um framework de administração e gestão de TI criado pela ISACA. Ele fornece um conjunto abrangente de melhores práticas, ferramentas e modelos para ajudar as organizações a desenvolver, implementar e monitorizar uma estratégia de administração e gestão de TI. O COBIT assegura que a TI é alinhada com os objetivos empresariais e que os riscos de TI são geridos de maneira eficaz[3, 4].

1.4.5 Certificações de Segurança

Para garantir a competência e a conformidade dos nossos profissionais e processos de segurança, também adotamos diversas certificações de segurança, tais como:

- CISSP (Certified Information Systems Security Professional): Certificação reconhecida internacionalmente para profissionais de segurança da informação.
- CISA (Certified Information Systems Auditor): Certificação focada na auditoria, controlo e segurança de sistemas de informação.
- CEH (Certified Ethical Hacker): Certificação que valida as habilidades de profissionais em identificar e corrigir vulnerabilidades de segurança.

2. Contextualização

2.1 Descrição do CIDT

2.1.1 Espaço Físico

O CIDT está alocado num edifício de três pisos, cada um dedicado a funções específicas que suportam as operações e a eficácia das atividades do centro. A configuração é a seguinte:

- **Piso 0:** Este piso serve como a entrada principal do CIDT, com uma área de receção acolhedora. Inclui também uma sala de reuniões e um auditório, ambos desenhados para facilitar comunicações eficazes e colaborações, tanto internas como externas.
- **Piso 1:** Dedicado à produção, este piso alberga as instalações onde as equipas de desenvolvimento de software trabalham nos sistemas comercializados pela organização. É neste espaço que a teoria se transforma em aplicação prática, com o desenvolvimento e ajuste de produtos destinados ao mercado.
- **Piso 2:** Reservado para a investigação, este piso é o coração da inovação no CIDT. Aqui, os investigadores testam e aprimoram os sistemas existentes, exploram novas tecnologias e conduzem experimentos que podem definir o futuro das tecnologias desenvolvidas pela organização.

Infraestrutura e Recursos Tecnológicos: O CIDT está equipado com tecnologia de ponta, incluindo laboratórios avançados, espaços de co-working tecnologicamente integrados e recursos de simulação de alta fidelidade. A infraestrutura de Tecnologias da Informação (TI) do centro suporta colaborações virtuais globais, permitindo o trabalho remoto e reuniões intercontinentais com eficácia.

2.1.2 Processo de Negócio

O processo de um Centro de Investigação e Desenvolvimento Tecnológico (CIDT) envolve várias etapas e atividades que visam promover a inovação, a investigação e o desenvolvimento de tecnologias avançadas. Entre as principais atividades incluídas nesse processo estão:

– **Identificação de necessidades e oportunidades:** Os CIDTs começam tipicamente por identificar as áreas que são do interesse estratégico para a organização.

- **Definição de objetivos:** Com base nas necessidades identificadas, são estabelecidos objetivos claros e metas mensuráveis para o CIDT. Isso pode incluir o desenvolvimento de novos produtos, a melhoria de processos existentes ou a realização de pesquisas aplicadas.

- **Alocação de recursos:** Os CIDTs requerem recursos financeiros, humanos e materiais para operar. A alocação adequada desses recursos é fundamental para garantir que as atividades de investigação e desenvolvimento sejam realizadas de forma eficaz e eficiente.

- **Execução de projetos de pesquisa:** Os CIDTs conduzem uma variedade de projetos nas suas áreas de investigação. Isso pode incluir a realização de testes, criação de protótipos e análise de dados para promover inovações tecnológicas.

- **Operações:**

  - *Produção:* Foca-se na aplicação prática de tecnologias e conhecimentos desenvolvidos, transformando-os em produtos ou serviços comercializáveis. Envolvendo desenvolvimento de software, ajuste de funcionalidades e garantia de qualidade, esta fase é crucial para gerar receita a partir da inovação.
  - *Investigação:* Orientada para o futuro, explorando novas ideias e tecnologias que podem ter potencial para futuras inovações. Esta área é mais experimental e arriscada, focada na resolução de problemas complexos e na criação de vantagens competitivas a longo prazo.

- **Colaboração e parcerias:** Muitos CIDTs colaboram com outras instituições, universidades e empresas para partilhar recursos, conhecimentos e experiências. A colaboração pode ajudar a potenciar o impacto e a relevância das atividades do CIDT.

- **Patentes:** Nos CIDTs, a questão das patentes desempenha um papel crucial. O objetivo primordial é canalizar os resultados de pesquisa em direção a aplicações práticas no mercado. Este processo pode incluir a identificação de tecnologias passíveis de patenteamento, o licenciamento estratégico de propriedade intelectual e até mesmo a incubação de startups emergentes. A proteção por patentes não apenas salvaguarda as inovações, mas também promove um ambiente propício para o investimento e o desenvolvimento contínuo de novas ideias, incentivando assim a colaboração entre os setores público e privado.

2.1.3 Organograma

Organização Mãe

A Organização Mãe está no topo da hierarquia e mantém a supervisão geral sobre o CIDT, garantindo que suas diretrizes e objetivos estratégicos estejam alinhados com a missão maior da organização.

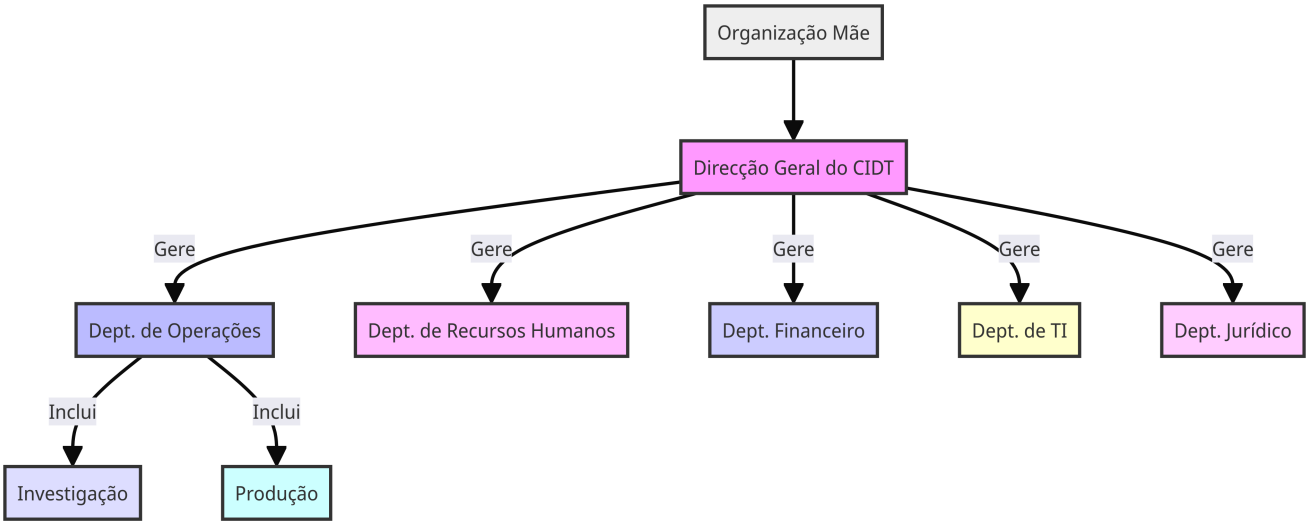

Figure 2.1: Organograma

Direção Geral do CIDT

A Direção Geral atua como o núcleo administrativo e estratégico do CIDT, coordenando todas as atividades internas e assegurando que os projetos estejam em conformidade com as políticas e objetivos organizacionais.

Departamento de Operações

O Departamento de Operações é responsável pela gestão e implementação eficaz das operações diárias dentro do CIDT, incluindo:

- **Investigação**: Conduz investigação de ponta para desenvolver novas tecnologias e inovações.
- **Produção**: Responsável pela produção de protótipos e modelos iniciais baseados nas pesquisas realizadas, essencial para o teste e aprimoramento das inovações desenvolvidas.

2.1.4 Departamento de Recursos Humanos

Este departamento gere todos os aspetos relacionados aos recursos humanos, incluindo recrutamento, formação e desenvolvimento de talentos, crucial para manter uma equipa de alto desempenho.

Departamento Financeiro

Responsável pela gestão financeira do CIDT, garantindo que todos os recursos financeiros sejam alocados eficientemente e que as operações se mantenham dentro do orçamento.

Departamento de TI

O Departamento de Tecnologia da Informação suporta todas as necessidades tecnológicas do centro, desde a infraestrutura de rede até o suporte de software, essencial para a operação contínua das atividades de investigação e desenvolvimento.

Departamento Jurídico

Este departamento lida com todas as questões legais, desde a proteção da propriedade intelectual até o cumprimento de normas regulamentares, assegurando que as inovações do CIDT estejam bem protegidas e legalmente seguras.

3. Recursos

3.1 Funções e Responsabilidades no CIDT

Table 3.1: Funções e Responsabilidades no CIDT

Função	**Responsabilidades**
Diretor Geral Eng. Santos Silva	• Supervisão e liderança estratégica do CIDT. • Decisões de alto nível sobre a direção de investigação e desenvolvimento. • Gestão de relações institucionais e parcerias estratégicas.
Coordenador de Operações (Produção) Eng. Pereira Ferreira	• Gestão das atividades de produção e prototipagem. • Assegurar a eficiência e qualidade dos processos de fabricação. • Supervisão da implementação de melhorias operacionais.

Coordenador de Operações (Investigação) Eng. Costa Oliveira	• Liderança e coordenação de projetos de investigação e desenvolvimento. • Assegurar a integração de novas tecnologias nos projetos de investigação. • Gestão da colaboração entre diferentes equipas de investigação.
Gestores de Equipa Drª Rodrigues Martins	• Gestão direta de equipas específicas dentro do CIDT. • Assegurar o cumprimento dos objetivos de projeto de cada equipa. • Facilitar a comunicação entre a equipa e a gestão superior.
Engenheiros	• Desenvolvimento e implementação de soluções técnicas. • Contribuição para o avanço técnico dos projetos de investigação. • Apoio técnico contínuo às operações do CIDT.
Chefe de Segurança Jesus Sousa	• Responsável pela segurança física do CIDT. • Implementação de políticas e procedimentos de segurança. • Monitorização e resposta a ameaças de segurança.

Administrador de Redes Dr. Fernandes Gonçalves	• Gestão e manutenção da infraestrutura de rede do CIDT. • Assegurar a segurança e eficiência da rede. • Implementação de upgrades e resolução de problemas de rede.
Administrador de Sistemas de Informação Eng. Gomes Lopes	• Gestão dos sistemas de informação do CIDT. • Garantir a integridade e segurança dos dados. • Suporte técnico e upgrades dos sistemas.
Gestor de TI Eng. Marques Alves	• Supervisão geral da tecnologia da informação no CIDT. • Planeamento estratégico de TI e gestão de recursos tecnológicos. • Coordenação das atividades de TI com outras funções organizacionais.

3.2 Mapa de Recursos e Funções

Table 3.2: Mapa de Recursos e Funções

Recurso	**Tipo**	**Função**
Laboratórios de Investigação	Físico	Facilitar a condução de investigações científicas e desenvolvimento de novas tecnologias.
Espaços de Escritório	Físico	Providenciar áreas para gestão, planeamento e suporte administrativo.

Instalações de Teste	Físico	Permitir o teste e validação de protótipos e tecnologias desenvolvidas.
Sistemas de HVAC	Físico	Manter condições ambientais ótimas para experimentação e conforto no trabalho.
Auditórios	Físico	Receber conferências, seminários e workshops para disseminar conhecimento e promover colaboração.
Biblioteca Técnica	Físico	Disponibilizar acesso a livros, revistas científicas e outros recursos informativos para suporte às investigações.
Servidores de Alta Performance	Tecnológico	Executar cálculos complexos e suportar simulações avançadas em investigações.
Redes Seguras	SI	Garantir a proteção de dados sensíveis e facilitar a comunicação segura.
Sistemas de Backup	SI	Proteger dados de investigação importantes contra perda e corrupção.
Sistemas de Gestão de Dados de Investigação	SI	Organizar, armazenar e aceder a dados de investigação de forma eficiente.
Plataforma de Colaboração Online	SI	Facilitar a colaboração entre equipas de investigação e parceiros externos.
Sistemas de Videoconferência	Tecnológico	Permitir reuniões virtuais e colaborações à distância com qualidade e segurança.
Software CAD	Software	Assistir no design e modelação de protótipos e componentes técnicos.
MATLAB/Simulink	Software	Realizar simulações matemáticas e análises complexas para suportar a investigação e desenvolvimento.
Ferramentas de Análise de Big Data	Software	Analisar grandes volumes de dados para extrair informações relevantes para a investigação.
Serviço de Cloud Computing	Tecnológico	Prover escalabilidade e flexibilidade no armazenamento e processamento de dados.
Equipamentos de Laboratório Especializado	Físico	Suportar experimentos específicos com equipamentos de alta precisão.

Impressoras 3D	Tecnológico	Facilitar a criação rápida de protótipos e peças personalizadas para testes.
Sistemas de Realidade Virtual/Aumentada	Tecnológico	Proporcionar ambientes simulados para testes e desenvolvimento de soluções inovadoras.
Equipamentos de Segurança	Físico	Garantir a segurança física dos colaboradores e proteção das instalações.
Veículos de Serviço	Logístico	Facilitar o transporte de materiais, equipamentos e pessoal entre diferentes locais.
Centro de Dados	Tecnológico	Alojamento seguro e eficiente de servidores, sistemas e dados críticos.
Ferramentas de Gestão de Projetos	Software	Apoiar o planeamento, execução e monitorização de projetos de investigação e desenvolvimento.
Plataforma de Gestão de Documentos	Software	Organizar e gerir documentos de forma eficiente, garantindo acesso controlado e seguro.

3.3 Infraestrutura de Rede

A infraestrutura de rede é o sistema que sustenta toda a operação informática do CIDT, possibilitando a comunicação entre os seus diversos sistemas internos e externos.

A arquitetura da rede do CIDT é projetada para garantir eficiência operacional e escalabilidade. Baseada numa abordagem hierárquica, ela inclui componentes de rede distribuídos em diferentes camadas para otimizar o desempenho e a segurança. Switches de Camada 3 são utilizados para fornecer roteamento de pacotes entre diferentes redes locais e sub-redes, garantindo conectividade eficaz em todo o centro.

Um servidor proxy é implementado para intermediar as conexões entre os dispositivos internos do CIDT e os recursos da internet. Isto não só melhora o desempenho ao armazenar em cache conteúdo frequentemente acedido, mas também aumenta a segurança ao filtrar o tráfego da web e proteger a rede contra ameaças externas.

Uma firewall robusta é implantada para garantir a segurança da rede, monitorizando e controlando o tráfego de entrada e saída com base em políticas de segurança predefinidas.

O CIDT mantém uma conexão com provedores de serviços de internet (ISPs) para garantir conectividade fiável com a internet. Uma medida de mitigação de risco crucial é a diversificação dos provedores de serviços de internet. Ao utilizar múltiplos ISPs, o CIDT reduz a dependência de um único provedor e mitiga os impactos de falhas de conectividade, garantindo que a investigação e as operações continuem sem interrupções, mesmo em caso de problemas com um provedor específico.

4. Gestão dos Sistemas de Informação

4.1 Sistemas de Informação

Table 4.1: Gestão dos Sistemas de Informação

Área	**Descrição**
Políticas e Procedimentos de Segurança de TI	O CIDT desenvolveu políticas e procedimentos de segurança de TI para proteger os sistemas de informação contra ameaças, focando-se na privacidade, integridade e disponibilidade dos dados. Isto inclui uma política de uso aceitável que define o uso apropriado dos recursos de TI e um protocolo para a gestão de incidentes de segurança. Os funcionários devem ler e assinar estas políticas durante a integração e participar em formações anuais para garantir a conformidade contínua.
Gestão de Acesso e Controlo de Privacidade	Para garantir a privacidade dos dados, o CIDT utiliza um sistema de controlo de identidade e acesso (IAM) que restringe o acesso aos recursos de informação a utilizadores autorizados. Cada colaborador recebe permissões de acesso baseadas nas suas funções. A autenticação multifator é obrigatória para acesso a dados sensíveis, incluindo uma combinação de senha e verificação via dispositivo móvel. Revisões trimestrais das permissões de acesso asseguram que os direitos de acesso estão atualizados e apropriados.
Segurança de Software e Hardware	Para manter a integridade e disponibilidade dos dados, o CIDT implementa firewalls robustos, software antivírus e sistemas de deteção de intrusões (IDS). Todos os dispositivos de hardware recebem atualizações regulares com patches de segurança. A criptografia é utilizada para proteger dados em trânsito e em repouso. Além disso, a política de gestão de configuração proíbe a instalação de software não autorizado em dispositivos da organização.

Table 4.1: Gestão dos Sistemas de Informação

Área	**Descrição**
Gestão de Vulnerabilidades e Patching	A gestão de vulnerabilidades no CIDT inclui auditorias de segurança regulares e o uso de ferramentas automatizadas de avaliação de vulnerabilidades para assegurar a integridade dos sistemas. Quando uma vulnerabilidade é identificada, a equipa de TI aplica patches e atualizações de segurança de forma imediata. O CIDT segue um cronograma rigoroso de atualizações de software e hardware para garantir a disponibilidade contínua dos sistemas.
Monitorização de Segurança de TI	O CIDT utiliza um sistema de gestão de eventos e informações de segurança (SIEM) para monitorizar continuamente o tráfego de rede e as atividades dos utilizadores, garantindo a integridade e a disponibilidade dos dados. Este sistema permite a deteção em tempo real de atividades suspeitas, como tentativas de login falhadas repetidas. Quando um incidente é detetado, alertas automáticos são gerados e a equipa de resposta a incidentes é acionada para investigar e resolver o problema de imediato.
Backup e Recuperação de Dados	Para garantir a disponibilidade e integridade dos dados, o CIDT desenvolveu um plano abrangente de backup e recuperação de dados. Backups diários são realizados e armazenados em locais seguros, incluindo servidores externos e soluções de armazenamento na nuvem. Em caso de falha do sistema ou perda de dados, os backups permitem a recuperação rápida e eficiente dos dados. Testes periódicos dos processos de recuperação são realizados para garantir a eficácia dos planos de backup.
Consciencialização em Segurança de TI	O CIDT promove a consciencialização em segurança de TI através de programas de formação regulares para todos os funcionários. Workshops trimestrais cobrem tópicos como reconhecimento de ameaças cibernéticas, criação de senhas fortes e precauções ao lidar com e-mails e websites suspeitos. Estes programas ajudam a criar uma cultura de segurança dentro da organização e a reduzir o risco de ataques baseados em engenharia social, protegendo a privacidade dos dados.

Table 4.1: Gestão dos Sistemas de Informação

Área	**Descrição**
Gestão de Incidentes de Segurança de TI	O CIDT estabeleceu procedimentos claros para a gestão de incidentes de segurança de TI para manter a integridade e disponibilidade dos sistemas. Em caso de violação de segurança, o incidente é imediatamente comunicado ao departamento de TI, que inicia uma investigação forense para identificar a origem e o impacto do incidente. A equipa de TI trabalha em estreita colaboração com outras unidades organizacionais para recuperar rapidamente os sistemas comprometidos e implementar medidas preventivas, minimizando o impacto sobre as operações do CIDT.

4.2 Suporte do Ciclo de Vida

O suporte do ciclo de vida dos sistemas de informação no CIDT inclui todas as fases desde a aquisição, implementação, manutenção, até à desativação. O objetivo é garantir que os sistemas permaneçam eficientes, seguros e alinhados com os objetivos organizacionais durante toda a sua vida útil.

Table 4.2: Suporte do Ciclo de Vida

Fase	**Descrição**
Aquisição	Identificação e seleção de sistemas que atendam às necessidades do CIDT, seguindo o processo descrito anteriormente.
Implementação	Planeamento e execução da instalação e configuração dos sistemas adquiridos, incluindo a integração com sistemas existentes e formação de utilizadores.
Manutenção	Monitorização contínua, atualização e resolução de problemas dos sistemas para garantir a operação eficiente e segura.
Suporte Técnico	Fornecimento de suporte técnico contínuo aos utilizadores para resolver problemas e maximizar a utilização dos sistemas.
Desativação	Planeamento e execução da desativação de sistemas obsoletos, garantindo a migração segura de dados e a minimização de interrupções nas operações.

4.3 Restrições de Uso de Software

No CIDT, o uso de software é regido por políticas rigorosas para garantir a conformidade legal e a segurança dos sistemas de informação. Estas políticas incluem restrições específicas sobre o uso de software não autorizado e a necessidade de seguir procedimentos de aquisição e instalação.

Table 4.3: Restrições de Uso de Software

Restrição	**Descrição**
Uso de Software Não Autorizado	Proibição do uso de software não autorizado ou não licenciado nos sistemas do CIDT. Todos os softwares devem ser adquiridos através dos canais oficiais do CIDT.
Instalação de Software	A instalação de qualquer software deve ser realizada pela equipa de TI ou com a sua supervisão direta para garantir a compatibilidade e segurança.
Atualizações de Software	Todas as atualizações de software devem ser aprovadas pela equipa de TI e realizadas de acordo com um cronograma estabelecido para minimizar interrupções nas operações.
Conformidade com Licenciamento	Todos os softwares utilizados devem estar devidamente licenciados e a conformidade deve ser verificada regularmente pela equipa de TI.
Política de Utilização de Software Livre	Incentivar o uso de software livre e de código aberto, quando apropriado, para reduzir custos e aumentar a flexibilidade.

4.4 Software Instalado pelo Utilizador

A instalação de software pelos utilizadores é estritamente controlada para garantir a segurança e a integridade dos sistemas de informação do CIDT. Procedimentos específicos foram estabelecidos para gerir este processo.

Table 4.4: Software Instalado pelo Utilizador

Política	**Descrição**
Procedimentos de Solicitação	Os utilizadores devem submeter um pedido formal à equipa de TI para a instalação de qualquer software, justificando a necessidade do mesmo.

Avaliação de Segurança	Antes da instalação, a equipa de TI deve avaliar o software solicitado para garantir que não representa um risco de segurança.
Aprovação e Instalação	Apenas softwares aprovados pela equipa de TI podem ser instalados. A instalação deve ser realizada pela equipa de TI ou sob sua supervisão.
Monitorização de Uso	O uso de software instalado pelos utilizadores deve ser monitorizado para garantir conformidade com as políticas do CIDT e evitar atividades não autorizadas.
Atualização e Manutenção	A equipa de TI é responsável por manter o software instalado atualizado e realizar manutenções regulares para garantir o seu funcionamento correto.

4.5 Serviços Externos do Sistema de Informação

O CIDT utiliza serviços externos de sistemas de informação para complementar as suas capacidades internas e garantir a continuidade das operações. Estes serviços incluem hospedagem na nuvem, serviços de backup e recuperação de desastres, e suporte técnico especializado.

Table 4.5: Serviços Externos do Sistema de Informação

Serviço	**Descrição**
Hospedagem na Nuvem	Utilização de serviços de nuvem para hospedar sistemas críticos e dados, garantindo escalabilidade e redundância.
Backup e Recuperação de Desastres	Contratação de serviços externos de backup e recuperação de desastres para garantir a disponibilidade e integridade dos dados em caso de falha.
Suporte Técnico Especializado	Utilização de serviços externos para suporte técnico especializado, como segurança cibernética, otimização de rede e manutenção de hardware.
Monitorização e Gestão de Redes	Contratação de serviços de monitorização e gestão de redes para garantir a segurança e eficiência da infraestrutura de TI do CIDT.
Consultoria de TI	Contratação de consultores externos para ajudar na implementação de novas tecnologias e melhorar as práticas de gestão de TI.

A implementação eficaz destas políticas e procedimentos garante que o CIDT está bem preparado para gerir a aquisição e utilização de sistemas e serviços de informação, prote-

gendo os seus recursos e assegurando a continuidade das suas operações de investigação e desenvolvimento tecnológico.

4.6 Políticas de Confidencialidade

As Políticas de Confidencialidade no CIDT são estabelecidas para assegurar que os dados são geridos e protegidos de acordo com a sua sensibilidade e importância. A classificação de dados é essencial para garantir que a informação é manipulada de forma adequada e está protegida contra acessos não autorizados.

Table 4.6: Requisitos de Classificação

Classificação	**Descrição e Medidas de Proteção**
Confidencial	Inclui dados altamente sensíveis, como informações de investigação proprietária, dados pessoais de funcionários e parceiros, e detalhes financeiros críticos. Esses dados são acessíveis apenas a pessoal autorizado com necessidade específica de acesso. Medidas de proteção incluem criptografia forte, acesso restrito, autenticação multifator, e auditorias de acesso regulares.
Restrito	Abrange dados que, se divulgados, podem causar danos moderados à organização, como planos de projetos em desenvolvimento e documentação interna estratégica. Acesso concedido a grupos específicos de funcionários com permissões baseadas em funções. Protegido por criptografia, controlo de acesso rigoroso, e monitorização contínua.
Interno	Contém informações que são utilizadas dentro do CIDT, mas que não devem ser divulgadas publicamente, como políticas internas e procedimentos operacionais. Acesso permitido a todos os funcionários, mas com medidas de controlo de versão e auditorias periódicas para evitar modificações não autorizadas.
Público	Inclui dados destinados à divulgação pública, como relatórios anuais, comunicados de imprensa e materiais de marketing. Embora não exijam proteção rigorosa, é necessário garantir a precisão e integridade das informações divulgadas.

5. Análise e Mitigação de Riscos

5.1 Identificação e Categorização dos Riscos

A identificação de riscos no CIDT é um processo contínuo que envolve todos os departamentos e níveis hierárquicos. Os riscos são identificados através de auditorias regulares, revisões de projetos e feedback dos funcionários. Utilizando a metodologia CRAMM (CCTA Risk Analysis and Management Method), os riscos são categorizados de forma estruturada em várias classes, tais como riscos tecnológicos, operacionais, de segurança, financeiros e de conformidade [2].

Table 5.1: Categorização dos Riscos no CIDT

Categoria de Risco	**Descrição e Exemplos**
Riscos Tecnológicos	Incluem falhas de hardware, vulnerabilidades de software e tecnologias obsoletas. Exemplo: Falha crítica de servidores que pode levar à perda de dados importantes.
Riscos Operacionais	Relacionam-se com a interrupção das operações diárias, incluindo falhas de infraestrutura e problemas de logística. Exemplo: Interrupção na cadeia de fornecimento que pode atrasar o desenvolvimento de protótipos.
Riscos de Segurança	Envolvem ameaças à segurança física e cibernética, como intrusões, ataques de Malware e violações de dados. Exemplo: Ataque de Ransomware que pode comprometer dados sensíveis de investigação.
Riscos Financeiros	Referem-se a problemas relacionados com a gestão financeira, incluindo falta de fundos, desvio de verbas e custos imprevistos. Exemplo: Cortes no orçamento que podem afetar a continuidade de projetos importantes.
Riscos de Conformidade	Relacionam-se com a não conformidade com regulamentações e normas, que podem resultar em penalizações legais e de reputação. Exemplo: Não conformidade com as normas de proteção de dados que pode levar a multas pesadas.

5.2 Avaliação e Classificação dos Riscos

A avaliação de riscos no CIDT é realizada utilizando a abordagem CRAMM, que combina técnicas qualitativas e quantitativas. Cada risco identificado é avaliado com base na sua probabilidade de ocorrência e impacto potencial nas operações do CIDT. Estes fatores são utilizados para classificar os riscos em níveis de prioridade (alto, médio e baixo).

Table 5.2: Matriz de Avaliação e Classificação dos Riscos no CIDT

Critério	**Descrição**
Probabilidade	Avaliação da frequência com que um risco pode ocorrer. Classificações: Baixa (1), Média (2), Alta (3).
Impacto	Avaliação do efeito potencial de um risco nas operações e objetivos do CIDT. Classificações: Baixo (1), Médio (2), Alto (3).
Nível de Risco	Calculado pela multiplicação da probabilidade pelo impacto. Classificações: Baixo (1-2), Médio (3-4), Alto (6-9).

5.3 Gestão e Mitigação do Risco

A gestão e mitigação dos riscos no CIDT envolve a implementação de estratégias baseadas na metodologia CRAMM para reduzir a probabilidade de ocorrência dos riscos e/ou o seu impacto. Estas estratégias podem incluir a aceitação, mitigação, transferência ou eliminação do risco.

Table 5.3: Estratégias de Mitigação de Riscos no CIDT

Estratégia	**Descrição e Exemplos**
Reduzir o Risco	Implementação de medidas para diminuir a probabilidade e/ou impacto do risco. Estas ações são proativas e visam minimizar a chance de que um risco se materialize ou, caso aconteça, reduzir o seu impacto. Exemplo: Realizar manutenções preventivas em equipamentos para reduzir o risco de avarias. Também pode incluir formação regular dos colaboradores para garantir que todos estejam cientes das melhores práticas de segurança.

Prevenção de Perdas	Adoção de medidas para evitar a ocorrência de perdas antes que estas possam ocorrer. Este enfoque preventivo visa eliminar ou neutralizar os riscos potenciais antes que eles se manifestem. Exemplo: Implementação de políticas de segurança da informação, como o uso de firewalls e encriptação de dados, para prevenir fugas de informação. Além disso, pode incluir a criação de uma equipa de resposta a incidentes para lidar rapidamente com potenciais ameaças de segurança.
Limitação de Perdas	Ações para limitar a extensão das perdas caso um risco se materialize. Estas medidas são reativas e visam minimizar os danos quando um evento adverso ocorre. Exemplo: Instalação de sistemas de deteção de incêndio para limitar danos em caso de incêndio. Outras medidas podem incluir planos de contingência detalhados e exercícios regulares para garantir que todos saibam como responder em emergências.
Transferência de Perdas	Transferência do risco para uma terceira parte, geralmente através de contratos ou seguros. Esta estratégia envolve a delegação da responsabilidade financeira ou operacional para outra entidade. Exemplo: Contratar um seguro contra falhas de equipamentos críticos para cobrir os custos de reparação ou substituição em caso de avarias. Alternativamente, pode envolver a externalização de certos processos para empresas especializadas que podem gerir melhor os riscos associados.
Aceitação do Risco	Decisão de aceitar o risco quando os custos de mitigação superam os benefícios. Esta estratégia é escolhida quando o impacto potencial do risco é baixo ou o custo para mitigá-lo é proibitivo. Exemplo: Aceitar pequenos atrasos nos projetos devido à falta temporária de recursos, considerando que tais atrasos não afetarão significativamente os resultados finais. Também pode incluir a manutenção de um fundo de reserva para cobrir pequenas perdas não previstas.

5.4 Processo Contínuo de Gestão de Riscos

A gestão de riscos no CIDT é um processo contínuo que envolve a revisão e atualização regular das estratégias de mitigação. Auditorias internas e externas são conduzidas para avaliar a eficácia das medidas de gestão de riscos implementadas e para identificar novas ameaças. O feedback dos funcionários e a análise de incidentes passados também são utilizados para melhorar continuamente o processo de gestão de riscos.

Table 5.4: Processo Contínuo de Gestão de Riscos no CIDT

Etapa	**Descrição**

Identificação Contínua	Realização de auditorias regulares e recolha de feedback dos funcionários para identificar novos riscos.
Avaliação Regular	Revisão periódica da probabilidade e impacto dos riscos existentes para ajustar as classificações de risco conforme necessário.
Atualização de Estratégias	Adaptação e melhoria contínua das estratégias de mitigação de riscos com base em novas informações e análises de incidentes passados.
Monitorização e Relatório	Monitorização constante dos riscos e comunicação regular sobre o estado da gestão de riscos para a administração do CIDT.

A implementação eficaz destes processos e estratégias garante que o CIDT esteja bem preparado para identificar, avaliar, gerir e mitigar riscos, protegendo assim os seus recursos e assegurando a continuidade das suas operações de investigação e desenvolvimento tecnológico.

5.5 Identificação dos Riscos

Table 5.5: Análise de Riscos no CIDT

ID	**Risco**	**Tipo**	**Probabilidade**	**Impacto**	**PxI**
1	Falha de servidor crítico	Tecnológico	Alta (3)	Alta (3)	9
2	Ataque de ransomware	Segurança	Alta (3)	Alta (3)	9
3	Roubo de equipamentos	Segurança	Média (2)	Média (2)	4
4	Não conformidade com RGPD	Conformidade	Média (2)	Alta (3)	6
5	Hardware obsoleto	Tecnológico	Alta (3)	Média (2)	6
6	Falha de software de missão crítica	Tecnológico	Média (2)	Alta (3)	6
7	Fuga de dados confidenciais	Segurança	Média (2)	Alta (3)	6
8	Falha de backups	Tecnológico	Média (2)	Alta (3)	6

Table 5.5: Análise de Riscos no CIDT

ID	Risco	Tipo	Probabilidade	Impacto	PxI
9	Comprometimento de contas de e-mail	Segurança	Média (2)	Média (2)	4
10	Erro de configuração de rede	Tecnológico	Média (2)	Alta (3)	6
11	Ataques DDoS	Segurança	Média (2)	Alta (3)	6
12	Ausência de política de segurança atualizada	Conformidade	Média (2)	Alta (3)	6
13	Perda de dados devido a erro humano	Segurança	Alta (3)	Média (2)	6
14	Falta de redundância em sistemas críticos	Tecnológico	Média (2)	Alta (3)	6
15	Incompatibilidade de hardware	Tecnológico	Média (2)	Média (2)	4
16	Intrusão física no centro	Segurança	Baixa (1)	Alta (3)	3
17	Uso indevido de dados sensíveis	Conformidade	Média (2)	Alta (3)	6
18	Ataque interno de um funcionário desonesto	Segurança	Baixa (1)	Alta (3)	3
19	Violação de propriedade intelectual	Conformidade	Média (2)	Alta (3)	6
20	Ataques de Phishing	Segurança	Alta (3)	Média (2)	6
21	Furto de dispositivos móveis	Segurança	Média (2)	Média (2)	4
22	Interrupção na atualização de sistemas	Tecnológico	Média (2)	Alta (3)	6
23	Falha na integração de novos sistemas	Tecnológico	Média (2)	Alta (3)	6

Table 5.5: Análise de Riscos no CIDT

ID	Risco	Tipo	Probabilidade	Impacto	PxI
24	Exposição a Malware através de dispositivos USB	Segurança	Alta (3)	Média (2)	6
25	Ataques de engenharia social	Segurança	Alta (3)	Média (2)	6
26	Roubo de dados por espionagem industrial	Segurança	Baixa (1)	Alta (3)	3
27	Falta de sistemas de monitorização adequados	Tecnológico	Média (2)	Alta (3)	6
28	Exposição a vulnerabilidades de dia zero	Segurança	Alta (3)	Alta (3)	9
29	Falta de auditorias de segurança regulares	Conformidade	Média (2)	Alta (3)	6
30	Ataques via redes sociais corporativas	Segurança	Alta (3)	Média (2)	6
31	Software obsoleto	Tecnológico	Alta (3)	Média (2)	6
32	Falha na comunicação com *stakeholders* externos	Operacional	Média (2)	Média (2)	4
33	Falta de uma política de recuperação de desastres	Tecnológico	Média (2)	Alta (3)	6
34	Problemas com a gestão de licenças de software	Conformidade	Média (2)	Alta (3)	6
35	Problemas na gestão de propriedade intelectual	Conformidade	Média (2)	Alta (3)	6
36	Problemas na gestão de contratos de pesquisa	Conformidade	Média (2)	Média (2)	4

Table 5.5: Análise de Riscos no CIDT

ID	Risco	Tipo	Probabilidade	Impacto	PxI
37	Falta de sistemas de backup externos	Tecnológico	Média (2)	Alta (3)	6
38	Perda de dados devido a falha de disco rígido	Tecnológico	Média (2)	Alta (3)	6
39	Falhas nos sistemas de videoconferência	Tecnológico	Média (2)	Média (2)	4
40	Falta de um plano de continuidade de negócios	Operacional	Média (2)	Alta (3)	6
41	Fraude interna	Segurança	Baixa (1)	Alta (3)	3
42	Falha na calibração de equipamentos de laboratório	Tecnológico	Média (2)	Média (2)	4
43	Não conformidade com normas ISO	Conformidade	Média (2)	Alta (3)	6
44	Dificuldade na implementação de novas tecnologias	Tecnológico	Alta (3)	Média (2)	6
45	Exposição a ataques de Spear phishing	Segurança	Alta (3)	Média (2)	6
46	Dificuldade em cumprir regulamentos ambientais	Conformidade	Média (2)	Alta (3)	6
47	Problemas com a integração de sistemas legados	Tecnológico	Média (2)	Alta (3)	6
48	Injeção de SQL	Segurança	Alta (3)	Alta (3)	9
49	Exfiltração de Dados	Segurança	Alta (3)	Alta (3)	9
50	Acesso não autorizado	Segurança	Média (2)	Alta (3)	6
51	Ataques Man-in-the-Middle	Segurança	Média (2)	Alta (3)	6

Table 5.5: Análise de Riscos no CIDT

ID	Risco	Tipo	Probabilidade	Impacto	PxI
52	Subida de Privilégios	Segurança	Média (2)	Alta (3)	6
53	Configurações de segurança inadequadas	Segurança	Média (2)	Alta (3)	6

5.6 Mitigação de Riscos

Table 5.6: Mitigação dos Riscos no CIDT

ID	Mitigação
1	Implementar redundância e backups regulares, monitorização contínua.
2	Implementar sistemas avançados de antivírus e formação em segurança, backups regulares.
3	Melhorar a segurança física, implementar controlo de inventário.
4	Realizar auditorias de conformidade, formação em proteção de dados.
5	Atualizar hardware regularmente, planear ciclos de substituição.
6	Implementar testes rigorosos e manutenção regular.
7	Implementar criptografia de dados, monitorização de acesso.
8	Verificar regularmente os sistemas de backup, realizar testes de recuperação.
9	Implementar autenticação multifator, monitorização de contas.
10	Realizar auditorias de configuração, implementar padrões de configuração.
11	Implementar serviços de mitigação DDoS, fortalecer firewalls.
12	Atualizar políticas de segurança regularmente, comunicar mudanças.
13	Fornecer formação em melhores práticas de TI, implementar verificações automáticas.
14	Implementar sistemas de redundância, monitorização contínua.
15	Planear a compra de hardware compatível, realizar testes de integração.

Table 5.6: Mitigação dos Riscos no CIDT

ID	Mitigação
16	Melhorar a segurança física com câmaras e controlo de acesso.
17	Implementar políticas de uso de dados, realizar auditorias regulares.
18	Implementar monitorização de atividades, política de acesso restrito.
19	Implementar monitorização de IP, políticas de proteção de dados.
20	Fornecer formação de consciencialização, implementar filtros de e-mail.
21	Implementar políticas de segurança para dispositivos móveis, controlo de inventário.
22	Planear atualizações fora do horário de expediente, realizar backups antes das atualizações.
23	Realizar testes de integração rigorosos, fornecer formação aos utilizadores.
24	Implementar políticas de segurança para dispositivos USB, conferir dispositivos antes de uso.
25	Fornecer formação de consciencialização, implementar políticas de verificação.
26	Implementar monitorização de atividades, criptografia de dados sensíveis.
27	Implementar sistemas avançados de monitorização, alertas automáticos.
28	Implementar monitorização contínua de ameaças, aplicar patches imediatamente.
29	Realizar auditorias de segurança trimestrais, corrigir vulnerabilidades identificadas.
30	Monitorizar atividades nas redes sociais, fornecer formação de segurança.
31	Planear atualizações regulares de software, monitorizar tendências de tecnologia.
32	Implementar canais de comunicação eficientes e regulares.
33	Desenvolver e testar regularmente uma política de recuperação de desastres.
34	Monitorizar licenças de software regularmente, garantir conformidade.
35	Implementar monitorização de IP, formar funcionários em gestão de IP.
36	Revisar contratos regularmente, envolver consultores jurídicos.

Table 5.6: Mitigação dos Riscos no CIDT

ID	Mitigação
37	Implementar soluções de backup na nuvem, testar regularmente.
38	Implementar redundância, monitorização de saúde de discos rígidos.
39	Implementar soluções de videoconferência redundantes, realizar testes regulares.
40	Desenvolver e testar regularmente um plano de continuidade de negócios.
41	Implementar políticas rigorosas de auditoria, monitorização de atividades financeiras.
42	Implementar um cronograma de calibração regular, auditorias de qualidade.
43	Realizar auditorias regulares, garantir conformidade com as normas ISO.
44	Fornecer formação contínua, suporte técnico.
45	Fornecer formação de consciencialização, implementar filtros de e-mail.
46	Monitorizar mudanças regulatórias, adaptar políticas conforme necessário.
47	Fornecer suporte técnico, realizar testes de integração rigorosos.
48	Implementar validação de entrada, usar prepared statements e stored procedures.
49	Monitorizar e analisar tráfego de rede, implementar DLP (Data Loss Prevention).
50	Implementar controles de acesso baseados em funções, usar logs e auditorias.
51	Usar criptografia de ponta a ponta, autenticação de dois fatores.
52	Atualizar regularmente software, implementar controles de acesso mínimos.
53	Rever e testar configurações de segurança regularmente, usar guias de configuração segura.

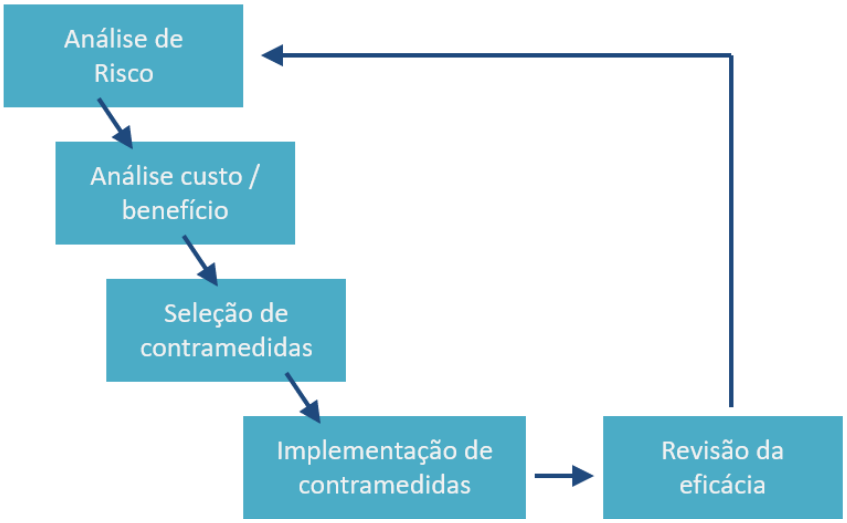

Figure 5.1: Esquema do Processo Contínuo de Gestão de Riscos

6. Plano de Contingência

6.1 Introdução

O plano de contingência do CIDT é essencial para assegurar a continuidade das operações em caso de interrupções significativas, especialmente relacionadas a riscos de cibersegurança. Este plano detalha as estratégias e procedimentos a serem seguidos para mitigar os impactos de ataques cibernéticos, falhas de sistemas e outras ameaças digitais que possam comprometer a integridade, disponibilidade e privacidade dos dados do CIDT. Dada a natureza sensível e crucial das atividades de investigação e desenvolvimento realizadas pelo CIDT, a implementação de um plano robusto de contingência é vital para proteger os seus recursos e assegurar a continuidade dos projetos.

6.2 Objetivos do Plano de Contingência

Os principais objetivos do plano de contingência do CIDT são:

- Garantir a segurança, integridade e disponibilidade dos dados de investigação e desenvolvimento.
- Minimizar a interrupção das operações científicas e administrativas.
- Assegurar a continuidade dos projetos de investigação e desenvolvimento sem comprometer prazos críticos.
- Recuperar rapidamente as operações após um incidente, minimizando impactos negativos.

6.3 Plano de Resposta a Incidentes

O plano de resposta a incidentes detalha as ações a serem tomadas imediatamente após a ocorrência de um incidente de cibersegurança. Este plano é crucial para minimizar os danos e garantir uma recuperação rápida e eficaz.

Table 6.1: Plano de Resposta a Incidentes

Incidente	**Ações Imediatas**
Ataques Cibernéticos	Isolar os sistemas afetados para conter o ataque, contactar a equipa de segurança cibernética, iniciar uma investigação forense para determinar a origem e extensão do ataque, comunicar o incidente às partes relevantes, incluindo parceiros e autoridades competentes.
Falhas de Sistemas Críticos	Contactar a equipa de TI imediatamente, iniciar procedimentos de recuperação de sistemas e dados, informar os utilizadores sobre o status e as expectativas de recuperação.
Exposição a Vulnerabilidades de Dia Zero	Aplicar patches de segurança imediatamente, isolar sistemas vulneráveis, monitorizar atividades suspeitas, informar todos os utilizadores sobre a vulnerabilidade e as medidas tomadas.
Ataques de Ransomware	Isolar sistemas afetados, não pagar resgates, restaurar dados a partir de backups, contactar as autoridades competentes e a equipa de resposta a incidentes cibernéticos.
Phishing e Spear phishing	Identificar e isolar contas comprometidas, redefinir senhas, informar os utilizadores afetados, realizar uma revisão de segurança completa.
Exposição a Malware através de Dispositivos USB	Desconectar dispositivos infectados, realizar uma varredura completa do sistema, aplicar ferramentas de remoção de malware, revisar políticas de uso de dispositivos USB.
Ataques de Engenharia Social	Informar todos os funcionários sobre o incidente, reforçar a importância da verificação de identidade, realizar auditorias de segurança para identificar qualquer acesso não autorizado.
Falhas de Energia	Ativar geradores de backup, contactar o fornecedor de energia, informar os funcionários sobre a situação e as medidas de contingência.
Desastres Naturais	Evacuar o edifício, contactar as autoridades competentes, ativar planos de recuperação de desastres e avaliar os danos quando possível.
Falhas de Hardware	Substituir ou reparar o hardware danificado, restaurar dados de backups, informar os utilizadores sobre o status e as medidas tomadas.
Erro Humano	Reverter as alterações feitas, restaurar os dados de backups, fornecer formação adicional aos funcionários envolvidos.

Table 6.1: Plano de Resposta a Incidentes

Incidente	**Ações Imediatas**
Vazamento de Dados	Isolar os sistemas afetados, iniciar uma investigação para identificar a fonte do vazamento, notificar as partes afetadas e tomar medidas para mitigar o impacto.
Falhas de Software	Aplicar correções e patches necessários, reiniciar os sistemas, testar funcionalidades restauradas e comunicar o status aos utilizadores.
Interrupção de Rede	Identificar a causa da interrupção, restaurar a conectividade, testar a rede e informar os utilizadores sobre o status.
Roubo de Equipamentos	Notificar as autoridades competentes, iniciar uma investigação interna, substituir os equipamentos roubados e reforçar a segurança física.
Violação de Propriedade Intelectual	Iniciar uma investigação, notificar os advogados e parceiros relevantes, tomar medidas legais apropriadas.
Falha de Fornecedores	Contactar fornecedores alternativos, ativar contratos de backup, informar os utilizadores sobre possíveis impactos nas operações.
Comprometimento de Dispositivos Móveis	Bloquear dispositivos comprometidos, redefinir credenciais de acesso, realizar uma revisão de segurança completa dos dispositivos afetados.
Ataques DDoS	Implementar medidas de mitigação de DDoS, contactar o provedor de serviços de internet, informar os utilizadores sobre possíveis interrupções temporárias.
Não Conformidade com Regulamentos	Realizar uma auditoria interna, corrigir as falhas de conformidade identificadas, notificar as autoridades reguladoras conforme necessário.
Fraude Interna	Realizar uma investigação interna, tomar medidas disciplinares contra os envolvidos, reforçar as políticas de auditoria e controlo interno.
Vulnerabilidades em Aplicações Web	Isolar as aplicações afetadas, aplicar patches de segurança, realizar testes de penetração para garantir a resolução das vulnerabilidades.
Ataques de Botnet	Identificar e isolar os dispositivos comprometidos, realizar uma limpeza completa dos sistemas afetados, reforçar as medidas de segurança de rede.

Table 6.1: Plano de Resposta a Incidentes

Incidente	**Ações Imediatas**
Infiltração por Ameaças Internas	Revogar o acesso dos indivíduos comprometidos, realizar uma investigação interna, reforçar as políticas de segurança e monitorização.

6.4 Plano de Recuperação de Desastres

O plano de recuperação de desastres assegura que o CIDT possa retomar as operações normais o mais rapidamente possível após um incidente significativo de cibersegurança. Este plano inclui etapas específicas para avaliar danos, recuperar dados, reparar sistemas e comunicar-se eficazmente com todas as partes interessadas.

Table 6.2: Plano de Recuperação de Desastres

Atividade	**Descrição**
Avaliação de Danos	Avaliar o alcance dos danos aos sistemas, instalações e dados de investigação.
Recuperação de Dados	Utilizar backups para restaurar dados críticos e garantir a integridade dos dados recuperados.
Reparo de Sistemas	Reparar ou substituir hardware danificado, reinstalar e configurar software necessário para retomar as operações de investigação.
Comunicação	Informar todas as partes interessadas, incluindo funcionários, parceiros de investigação e financiadores, sobre o status da recuperação e prazos esperados para a retomada das operações normais.
Teste de Sistemas	Testar todos os sistemas restaurados para garantir que estão operacionais e seguros, realizando verificações de integridade e desempenho.
Revisão Pós-Incidente	Realizar uma revisão detalhada do incidente e da resposta, identificar lições aprendidas e ajustar o plano de contingência conforme necessário para melhorar a resposta a futuros incidentes.

6.5 Plano de Continuidade de Negócios

O plano de continuidade de negócios descreve as medidas para manter as operações essenciais durante e após um incidente de cibersegurança, assegurando que as atividades críticas de investigação e desenvolvimento do CIDT não sejam comprometidas.

Table 6.3: Plano de Continuidade de Negócios

Medida	**Descrição**
Priorização de Atividades	Identificar e priorizar atividades e serviços essenciais que devem ser mantidos durante um incidente de cibersegurança.
Recursos Alternativos	Identificar recursos alternativos, incluindo locais de trabalho, fornecedores e tecnologias que possam ser utilizados em caso de interrupção das operações normais.
Plano de Comunicação	Estabelecer um plano de comunicação claro para manter todas as partes interessadas informadas durante o incidente, garantindo a transparência e a confiança na gestão do CIDT.
Equipa de Continuidade	Designar uma equipa de continuidade responsável pela implementação do plano e pela tomada de decisões durante o incidente, assegurando uma resposta coordenada e eficaz.
Testes e Formações	Realizar testes regulares do plano de continuidade e fornecer formação contínua aos funcionários para garantir a prontidão e eficácia do plano, promovendo uma cultura de resiliência dentro do CIDT.

6.6 Monitorização e Revisão do Plano de Contingência

O plano de contingência do CIDT é monitorizado e revisto regularmente para assegurar a sua eficácia e atualidade. A adaptação contínua do plano é crucial para responder a novas ameaças e garantir que o CIDT está sempre preparado para enfrentar desafios de cibersegurança.

Table 6.4: Monitorização e Revisão do Plano de Contingência

Atividade	**Descrição**
Auditorias Internas	Realizar auditorias internas para avaliar a eficácia das medidas de contingência e identificar áreas de melhoria, assegurando que todas as práticas de cibersegurança estão atualizadas.

Table 6.4: Monitorização e Revisão do Plano de Contingência

Atividade	**Descrição**
Auditorias Externas	Conduzir auditorias externas para garantir conformidade com padrões de segurança e regulamentações internacionais, beneficiando de perspetivas independentes sobre a robustez do plano.
Feedback dos Funcionários	Recolher e analisar feedback dos funcionários regularmente para identificar problemas e áreas de melhoria, promovendo um ambiente de melhoria contínua e envolvimento da equipa.
Análise de Incidentes	Analisar incidentes passados para identificar falhas no plano de contingência e implementar melhorias, utilizando cada incidente como uma oportunidade para fortalecer as defesas do CIDT.
Atualização Contínua	Rever e atualizar o plano de contingência continuamente com base em novas informações e mudanças no ambiente de negócios, assegurando que o plano permanece relevante e eficaz face às evoluções tecnológicas e de ameaças.

A implementação eficaz deste plano de contingência, alinhada com a análise e mitigação de riscos descrita no capítulo anterior, garante que o CIDT está bem preparado para responder a incidentes de cibersegurança, proteger os seus recursos e assegurar a continuidade das suas operações de investigação e desenvolvimento tecnológico.

7. Formações de Cibersegurança

O plano de formações de cibersegurança tem como objetivo capacitar os colaboradores do CIDT com conhecimentos e habilidades necessárias para proteger os sistemas de informação contra ameaças cibernéticas. Este plano abrange diferentes níveis de formação, desde a consciencialização básica até a especialização em áreas específicas de cibersegurança.

7.1 Objetivos do Plano de Formações

Os principais objetivos do plano de formações de cibersegurança são:

- Aumentar a consciencialização sobre ameaças cibernéticas.
- Desenvolver habilidades práticas para identificar e responder a ameaças.
- Assegurar a conformidade com políticas de segurança.
- Promover uma cultura de segurança cibernética na organização.

7.2 Estrutura do Plano de Formações

O plano de formações de cibersegurança é estruturado em três níveis: Consciencialização Básica, Formação Intermediária e Formação Avançada.

Table 7.1: Estrutura do Plano de Formações de Cibersegurança

Nível	**Descrição**
Consciencialização Básica	Formação destinada a todos os colaboradores, focada em conceitos básicos de cibersegurança, identificação de ameaças comuns e boas práticas de segurança.
Formação Intermediária	Formação para colaboradores que utilizam sistemas de informação de forma intensiva, incluindo práticas avançadas de segurança e gestão de incidentes.

Formação Avançada	Formação especializada para a equipa de TI e gestores de segurança, cobrindo tópicos como análise forense, resposta a incidentes e gestão de riscos cibernéticos.

7.3 Plano de Formação

O plano detalhado inclui os módulos de formação, objetivos, público-alvo, frequência e métodos de avaliação.

7.3.1 Consciencialização Básica

Table 7.2: Consciencialização Básica

Módulo	**Objetivo**	**Público-Alvo**	**Frequência**
Introdução à Cibersegurança	Familiarizar os colaboradores com conceitos básicos de cibersegurança e a importância da segurança cibernética.	Todos	Anual
Reconhecimento de	Ensinar como identificar e evitar ataques de phishing.	Todos	Anual
Boas Práticas de Senhas	Demonstrar a importância de senhas fortes e como criar e gerir senhas seguras.	Todos	Anual
Segurança de E-mail	Instruir sobre o uso seguro do e-mail e a identificação de e-mails suspeitos.	Todos	Anual
Políticas de Segurança do CIDT	Informar sobre as políticas de segurança internas e a conformidade com estas políticas.	Todos	Anual

7.3.2 Formação Intermediária

Table 7.3: Formação Intermediária

Módulo	**Objetivo**	**Público-Alvo**	**Frequência**
Gestão de Incidentes	Capacitar os colaboradores para responder a incidentes de segurança de forma eficaz.	Utilizadores Intensivos de TI	Semestral

Segurança em Dispositivos Móveis	Ensinar práticas seguras para o uso de dispositivos móveis no ambiente de trabalho.	Utilizadores Intensivos de TI	Semestral
Proteção de Dados Sensíveis	Demonstrar como proteger dados sensíveis e cumprir com as regulamentações de proteção de dados.	Utilizadores Intensivos de TI	Semestral
Uso Seguro da Internet	Informar sobre práticas seguras ao navegar na internet e utilizar recursos online.	Utilizadores Intensivos de TI	Semestral
Backup e Recuperação de Dados	Ensinar a importância dos backups regulares e os procedimentos de recuperação de dados.	Utilizadores Intensivos de TI	Semestral

7.3.3 Formação Avançada

Table 7.4: Formação Avançada

Módulo	**Objetivo**	**Público-Alvo**	**Frequência**
Análise Forense Digital	Capacitar a equipa de TI a realizar análises forenses de incidentes cibernéticos.	Equipa de TI	Trimestral
Resposta a Incidentes	Ensinar técnicas avançadas de resposta a incidentes cibernéticos e recuperação.	Equipa de TI	Trimestral
Gestão de Riscos Cibernéticos	Desenvolver habilidades para identificar, avaliar e mitigar riscos cibernéticos.	Equipa de TI	Trimestral
Segurança de Redes	Capacitar a equipa de TI para proteger a infraestrutura de rede contra ameaças cibernéticas.	Equipa de TI	Trimestral
Auditoria de Segurança	Ensinar como conduzir auditorias de segurança e avaliar a conformidade com as políticas de segurança.	Equipa de TI	Trimestral

7.4 Métodos de Avaliação

Para garantir a eficácia das formações, são utilizados diversos métodos de avaliação:

Table 7.5: Métodos de Avaliação

Método	**Descrição**
Questionários	Aplicação de questionários pós-formação para avaliar o conhecimento adquirido.
Simulações de Incidentes	Realização de exercícios de simulação de incidentes para avaliar a capacidade de resposta dos colaboradores.
Avaliações Práticas	Execução de avaliações práticas para testar habilidades específicas aprendidas durante a formação.
Feedback dos Participantes	Recolha de feedback dos participantes para identificar áreas de melhoria na formação.
Relatórios de Desempenho	Análise de relatórios de desempenho para medir a eficácia das formações na melhoria das práticas de segurança.

7.5 Cronograma de Implementação

O cronograma de implementação detalha as etapas necessárias para a execução do plano de formações de cibersegurança.

Table 7.6: Cronograma de Implementação

Etapa	**Descrição**
Planeamento	Definir o conteúdo dos módulos de formação, identificar os instrutores e elaborar materiais de formação.
Comunicação	Informar os colaboradores sobre o plano de formações e os seus benefícios, bem como os cronogramas de formação.
Execução Inicial	Iniciar a formação com módulos de consciencialização básica para todos os colaboradores.
Formação Contínua	Implementar formações intermediárias e avançadas conforme o cronograma estabelecido.
Avaliação e Ajuste	Realizar avaliações contínuas das formações e ajustar os conteúdos e métodos conforme necessário para melhorar a eficácia.

7.6 Cronograma das Formações

Aqui podemos ver as formações marcadas para o ano de 2024.

Table 7.7: Cronograma de Formações

Formação	**Responsável**	**Mai**	**Jun**	**Jul**	**Ago**	**Set**	**Out**	**Nov**	**Dez**
Segurança de TI	*a definir*								
Privacidade de Dados	*a definir*								
Gestão de Incidentes	*a definir*								
Proteção contra Phishing	*a definir*								
Cibersegurança Avançada	*a definir*								
Formação Contínua	*a definir*								
Proteção de Dados Sensíveis	*a definir*								
Uso Seguro da Internet	*a definir*								
Análise Forense Digital	*a definir*								
Resposta a Incidentes	*a definir*								
Segurança de Redes	*a definir*								
Auditoria de Segurança	*a definir*								

8. Auditorias

O plano de auditorias de segurança do CIDT tem como objetivo assegurar a conformidade com as políticas de segurança, identificar vulnerabilidades e implementar melhorias contínuas nos sistemas de informação. Este plano descreve as auditorias regulares, responsabilidades, metodologias e cronograma de execução, baseando-se na metodologia COBIT (Control Objectives for Information and Related Technologies).

8.1 Objetivos das Auditorias

Os principais objetivos das auditorias de segurança são:

- Assegurar a conformidade com as políticas de segurança.
- Identificar vulnerabilidades e riscos nos sistemas de informação.
- Avaliar a eficácia das medidas de segurança implementadas.
- Fornecer recomendações para melhorar a segurança cibernética.

8.2 Estrutura das Auditorias

O plano de auditorias é estruturado em auditorias internas e externas, cobrindo diferentes áreas críticas de segurança.

Table 8.1: Estrutura do Plano de Auditorias

Tipo de Auditoria	**Descrição**
Auditorias Internas	Realizadas pela equipa de operações, focando na avaliação contínua das políticas e procedimentos de segurança.
Auditorias Externas	Realizadas por entidades externas independentes, proporcionando uma avaliação imparcial da segurança cibernética e conformidade do CIDT.
Auditorias de Conformidade	Focadas na verificação do cumprimento das normas e regulamentações aplicáveis, como o RGPD (Regulamento Geral de Proteção de Dados), realizadas pelo departamento jurídico.
Auditorias de Vulnerabilidade	Avaliação específica para identificar e mitigar vulnerabilidades nos sistemas e infraestruturas de TI, realizadas pelo departamento de TI.
Auditorias de Segurança Física	Avaliação das medidas de segurança física das instalações para proteger contra intrusões e outros riscos físicos, realizadas pela equipa de segurança.

8.3 Plano de Auditorias

O plano detalhado de auditorias inclui os objetivos, responsáveis, frequência e metodologia para cada tipo de auditoria.

8.3.1 Auditorias Internas

Table 8.2: Auditorias Internas

Objetivo	**Descrição**	**Responsável**	**Frequência**
Avaliar a Conformidade	Verificar a adesão às políticas de segurança internas.	Dept. Operações	Trimestral
Identificar Vulnerabilidades	Realizar testes de penetração e avaliações de vulnerabilidade.	Dept. Operações	Trimestral
Recomendar Melhorias	Propor melhorias baseadas nas descobertas da auditoria.	Dept. Operações	Trimestral

8.3.2 Auditorias Externas

Table 8.3: Auditorias Externas

Objetivo	Descrição	Responsável	Frequência
Avaliar a Segurança	Avaliar de forma independente a eficácia das medidas de segurança.	Entidade Externa	Anual
Revisar a Conformidade	Verificar a conformidade com normas e regulamentações.	Entidade Externa	Anual
Identificar Ameaças	Identificar ameaças emergentes e áreas de risco.	Entidade Externa	Anual

8.3.3 Auditorias de Conformidade

Table 8.4: Auditorias de Conformidade

Objetivo	Descrição	Responsável	Frequência
Verificar Conformidade RGPD	Avaliar o cumprimento das obrigações do RGPD.	Dept. Jurídico	Semestral
Revisar Políticas de Dados	Verificar a adequação das políticas de proteção de dados.	Dept. Jurídico	Semestral
Avaliar Processos de Gestão de Dados	Verificar os processos de gestão de dados sensíveis.	Dept. Jurídico	Semestral

8.3.4 Auditorias de Vulnerabilidade

Table 8.5: Auditorias de Vulnerabilidade

Objetivo	Descrição	Responsável	Frequência
Identificar Vulnerabilidades	Realizar avaliações de vulnerabilidade nos sistemas de TI.	Dept. de TI	Trimestral
Testar Resiliência	Conduzir testes de penetração para avaliar a resiliência dos sistemas.	Dept. de TI	Trimestral
Mitigar Riscos	Implementar medidas corretivas para mitigar vulnerabilidades identificadas.	Dept. de TI	Trimestral

8.3.5 Auditorias de Segurança Física

Table 8.6: Auditorias de Segurança Física

Objetivo	Descrição	Responsável	Frequência
Avaliar Segurança Física	Verificar a eficácia das medidas de segurança física.	Equipa de Segurança	Semestral
Identificar Riscos Físicos	Identificar riscos de segurança física nas instalações.	Equipa de Segurança	Semestral
Implementar Melhorias	Propor e implementar melhorias nas medidas de segurança física.	Equipa de Segurança	Semestral

8.4 Metodologias de Auditoria

As auditorias de segurança no CIDT utilizam metodologias comprovadas para garantir uma avaliação abrangente e precisa, baseando-se na metodologia COBIT.

8.4.1 Metodologia de Auditoria Interna

- **Planeamento**: Definição do âmbito e objetivos da auditoria.
- **Recolha de Dados**: Recolha de informações através de entrevistas, questionários e análise de documentação.
- **Análise**: Avaliação dos dados recolhidos para identificar conformidade e vulnerabilidades.
- **Relatório**: Elaboração de um relatório detalhado com as recomendações.
- **Acompanhamento**: Verificação da implementação das recomendações.

8.4.2 Metodologia de Auditoria Externa

- **Planeamento**: Coordenação com a entidade externa para definir o âmbito e cronograma.
- **Execução**: Realização da auditoria conforme o plano acordado.
- **Relatório**: Receção e análise do relatório de auditoria externa.
- **Implementação**: Ação sobre as recomendações feitas pela auditoria externa.

8.4.3 Metodologia de Auditoria de Conformidade

- **Verificação de Políticas**: Revisão das políticas e procedimentos internos.
- **Análise de Processos**: Avaliação dos processos de gestão de dados e conformidade.
- **Entrevistas**: Entrevistas com os responsáveis pelas áreas auditadas.
- **Relatório**: Documentação das recomendações para garantir a conformidade contínua.

8.4.4 Metodologia de Auditoria de Vulnerabilidade

- **Testes Automatizados**: Utilização de ferramentas de análise de vulnerabilidade.
- **Testes de Penetração**: Simulação de ataques para identificar vulnerabilidades.
- **Avaliação Manual**: Revisão manual de sistemas e configurações.
- **Relatório**: Detalhamento das vulnerabilidades encontradas e sugestões de mitigação.

8.4.5 Metodologia de Auditoria de Segurança Física

- **Inspeções no Local**: Verificação física das medidas de segurança.
- **Entrevistas**: Conversas com o pessoal de segurança e outros funcionários.
- **Análise de Risco**: Identificação e avaliação de riscos físicos.
- **Relatório**: Relatório com recomendações para melhorar a segurança física.

8.5 Cronograma de Auditorias

O cronograma de auditorias define as datas específicas para a realização das auditorias, assegurando uma cobertura abrangente e contínua.

Table 8.7: Cronograma de Auditorias

Tipo	**Responsável**	**Mai**	**Jun**	**Jul**	**Ago**	**Set**	**Out**	**Nov**	**Dez**
Internas	Dept. Operações	■		■		■		■	
Externas	Entidade Externa						■		
Conformidade	Dept. Jurídico			■					■
Vulnerabilidade	Dept. de TI		■		■		■		■
Segurança Física	Equipa de Segurança				■				■

Este cronograma assegura que todas as áreas críticas são auditadas regularmente, garantindo a identificação precoce de possíveis problemas e a implementação de medidas corretivas eficazes.

Referências

[1] 2018. A study on malware and malware detection techniques. *International Journal of Education and Management Engineering* (8). 20.

[2] 2002. A qualitative risk analysis and management tool–cramm. *SANS InfoSec Reading Room White Paper* (11). 12–32.

[3] 2015. Identificação de práticas e recursos de gestão do valor das ti no cobit 5/identification of it value management practices and resources in cobit 5. *Revista Ibérica de Sistemas e Tecnologias de Informação* . 17.

[4] 2012. *Cobit 5*. ISA.

[5] 2012. *Ransomware: A growing menace*. Symantec Corporation Arizona, AZ, USA.

[6] 2007. Introducing octave allegro: Improving the information security risk assessment process. *Hansom AFB, MA* .

[7] 2011. Recommendations of the national institute of standards and technology. *NIST special publication* (800). 155.

[8] 2023. Management of enterprise cyber security: A review of iso/iec 27001: 2022. Em *2023 International conference on cyber management and engineering (CyMaEn)*, 117–122. IEEE.