Projeto

Documento Confidencial

Mestrado em Cibersegurança e Informática Forense

Tratamento de Incidentes de Segurança Informática

Estudantes:

Emanuel Lopes Nº 2220557

Filipe Bagagem Nº 2220558

Pedro Marques Nº 2220562

Roberto Leal Nº 2220561

Docente: Adaíl Oliveira

30 de junho de 2023

Resumo

Este documento tem como objetivo o estudo pormenorizado de um ambiente empresarial real, da HRV - Equipamentos De Processo, S.A. Ao longo deste trabalho são apresentados os diversos objetivos do Quadro Nacional de Referência para a Cibersegurança (QNRCS), que é: Identificar, Proteger, Detetar, Responder e Recuperar. Estes objetivos estão organizados por categorias e subcategorias temáticas onde se explanam medidas técnicas e processuais, bem como evidências de implementação que permitem a organização melhorar a sua capacidade de proteção e de resposta aos desafios do ciberespaço e da segurança da informação.

O documento é composto por dez capítulos, assim sendo, no capítulo I é feita a caraterização do ambiente empresarial. Seguindo para o capítulo II em que se descreve a arquitetura presenta do sistema de informação. No capítulo III é descrita a análise de risco da organização. Em seguida no capítulo IV é descrito o Plano de Resposta a Incidentes que desenhamos para a organização. Seguindo-se do capítulo V apresentamos as nossas conclusões e o trabalho futuro a realizar. Seguindo do capítulo VI com as referências e terminando com o capítulo VII com os respetivos anexos.

30 de junho de 2023

Índice

I. Lista de Acrónimos I
II. Lista de Figuras II
III. Lista de Tabelas II
1 Caracterização do ambiente empresarial 1
1.1 Estrutura empresarial 1
1.2 Localização física 1
1.3 Principais ramos de atividade 2
1.4 Os principais parceiros de negócio e seus setores da atividade empresarial 2
1.5 A estrutura de administração empresarial, a relação com clientes/fornecedores, recurso a *outsourcing / insourcing* 2
1.6 O enquadramento da empresa com o mundo digital 3
2 Arquitetura do Sistema de Informação 4
2.1 Negócio, identificando as principais unidades de negócio e respetivos processos e atividades do ponto de vista de negócio 4
2.2 Dados que devem ser recolhidos, organizados, protegidos e distribuídos 4
2.3 Identificação das principais aplicações utilizadas, tais como softwares desenvolvidos à medida e softwares generalistas, e dos principais fluxos de informação existentes 5
2.4 Tecnologias utilizadas, tais como sistemas operativos de rede e de clientes, plataformas móveis e fixas, sistemas de comunicação, sistemas de armazenamento 5
2.5 Localização dos ativos tecnológicos e de informação, *on premises* ou *cloud* 5
3 Análise de Risco 7
3.1 Identificação dos riscos 7
3.2 Análise do risco 8
3.2.1 Identificar os Ativos de Informação 9
3.2.2 Identificação dos ativos 10
3.2.3 Determinar o Valor da Informação 10
3.2.4 Determinar a Probabilidade de Ocorrência 11
3.2.5 Determinar o Risco 13
3.2.6 Identificar os Controlos a Aplicar 14
3.2.7 Implementar o Plano de Ação de Mitigação 14
3.2.8 Revisão da Avaliação de Riscos 14
4 Plano de resposta a incidentes 19
4.1 Definição do que é um incidente de acordo com a organização 19
4.2 Definição e identificação da equipa e modelo de resposta a incidente 20
4.3 Responsável pela Resposta a Incidentes 20

4.4 Membros da equipa de resposta a incidentes 21
4.5 Ferramentas a usar pela equipa de resposta a incidentes 22
4.6 Domínio do plano de resposta a incidentes 24
4.6.1 Aplicabilidade 24
4.6.2 Incidentes 24
4.7 Identificação das partes interessadas 24
4.7.1 Equipas de resposta a incidentes 25
4.7.2 Contactos 27
4.7.3 Exemplo de cenários de incidentes 27
a. Deteção de *Phishing* 27
b. Exploração de vulnerabilidade 28
c. Ataque de negação de Serviço 29
4.8 Processo de resposta a incidentes 30
4.8.1 Ciclo de vida 30
4.9 Definição dos níveis de severidade dos incidentes e sua triagem 32
4.10 Plano e matriz de comunicação e de escalonamento 34
4.11 Tipos de incidentes e determinar os playbooks 35
4.12 Playbooks 36
4.13 Definição dos processos de comunicação de incidentes por parte da comunidade 45
Comunicação interna 45
Comunicação externa 48
4.14 Definição dos critérios de ativação no PRI: 49
4.14.1 Plano de Continuidade de Negócio 49
4.14.2 Plano de recuperação de desastres 50
4.15 Definição do plano de testes 50
4.16 Definição do plano de comunicação interna e de formação 51
4.16.1 Enquadramento 51
4.16.2 Definição de Plano de Comunicação Interna 51
4.16.3 Vantagens de um Plano Comunicação Interna 52
4.16.4 Implementação de um Plano de Comunicação Interna 52
4.16.5 Tecnologia utilizada pela HRV 53
5 Conclusões e recomendações futuras 55
6 Referências 56
7 Anexos 57
Anexo 1 - anexo_Playbook_Malware.pdf 57
Anexo 2 - anexo_Playbook_Phishing.pdf 57

Anexo 3 - anexo_Playbook_DDoS.pdf 57
Anexo 4 - anexo_Playbook_ExfiltraçãoDados.pdf 57
Anexo 5 - anexo_Playbook_InjecaoCodigo.pdf 57

I. Lista de Acrónimos

ABREVIATURA	DEFINIÇÃO
CISO	Chief Information Security Officer – Responsável de Segurança de Informação.
CIO	Chief Information Office
CSIRT	Computer Security Incident Response Team – Equipa de Resposta a Incidentes de Segurança Informática.
CVE	Lista de registos que contêm um número de identificação, uma descrição e, pelo menos, uma referência pública para vulnerabilidades de segurança.
DMZ	Demilitarized Zone – Zona desmilitarizada.
DMZ	Demilitarized Zone – Zona Desmilitarizada
DNS	Domain Name System – Sistema de resolução de nomes de domínio.
DDoS	Distributed Denial-of-Service – Ataque de negação de serviço
ENISA	Agência da União Europeia para a Cibersegurança
ENSC	Estratégia Nacional de Segurança do Ciberespaço 2019-2023
IDS	Intrusion Detection System – Sistema de deteção de intrusões.
IDS	Intrusion Detection System – Sistema de Deteção de intrusões
IP	Internet Protocol – Protocolo de comunicações.
IPS	Intrusion Prevention System – Sistema de prevenção de intrusões.
ISO	International Organization for Standardization – Organização internacional de normalização.
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission – Organização internacional de normalização/ Comissão eletrotécnica internacional.
MAC Address	Media Access Control Address – Endereço Físico da placa de rede
QNRCS	Quadro Nacional de Referência para a Cibersegurança.
RASIC	Responsible – Responsável, Accountable – Aprovador, Supports – Suporte, Consulted – Consultado e Informed – Informado. Matriz de atribuição de Responsabilidades.
SLA	Service Level Agreement
SGSI	Sistema de Gestão de Segurança da Informação.
SOC	Security Operations Center – Centro de Operações de Segurança
SRI	Segurança das Redes e da Informação.
SWOT	Strengths – Forças, Weaknesses – Fraquezas, Opportunities – Oportunidades e Threats – Ameaças
TI	Tecnologias de Informação
UPS	Uninterruptible Power Source – Unidade de alimentação ininterrupta
VLAN	Virtual Local Area Network – Sub-redes
VPN	Virtual Private Network – Rede privada virtual.
WAF	Web Application Firewall – Firewall de aplicações web
WWW	World Wide Web – Rede mundial de computadores.
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan

Tabela 1 - Abreviaturas

II. Lista de Figuras

Figura 1 - Estrutura Empresarial HRV 1
Figura 2 – Localização da HRV 1
Figura 3 - Análise de Risco 7
Figura 4 - Identificação do Risco 7
Figura 5 - Gestão e tratamento de Incidentes adaptado [3] 20
Figura 6 - Organização da CSIRT 22
Figura 7 - Relação das diferentes ferramentas e plataformas disponíveis para CSIRT 23
Figura 8 - Ciclo de vida de resposta de incidentes 25
Figura 9 - Cenário de comunicação de phishing 28
Figura 10 - Exploração de vulnerabilidade 28
Figura 11 - Ataque DDOS 29
Figura 12 - Ciclo de vida resposta a incidentes da HRV 30
Figura 13 - Plataforma GLPI (Plataforma para reportar incidentes) 46
Figura 14 - Processo de comunicação interna de incidentes de segurança 47
Figura 15 - Processo de comunicação externa de incidentes de segurança 49
Figura 16 - Plano de Comunicação 52

III. Lista de Tabelas

Tabela 1 - Abreviaturas I
Tabela 2 - Identificação dos Riscos 8
Tabela 3 - Matriz valor da informação 10
Tabela 4 - Classificação de vulnerabilidades nos ativos 13
Tabela 5 – Matriz de risco 13
Tabela 6 - Avaliação dos riscos dos ativos 15
Tabela 7 – Principais Tipos de Incidentes 19
Tabela 8 - Contactos 27
Tabela 9 - Critérios para a definição da severidade de um incidente de segurança 33
Tabela 10 - Escala de classificação 33
Tabela 11 - Tipos de Incidentes (Comunicação Interna) 47
Tabela 12 - Tipos de Incidentes (Comunicação Externa 48

1 Caracterização do ambiente empresarial

1.1 Estrutura empresarial

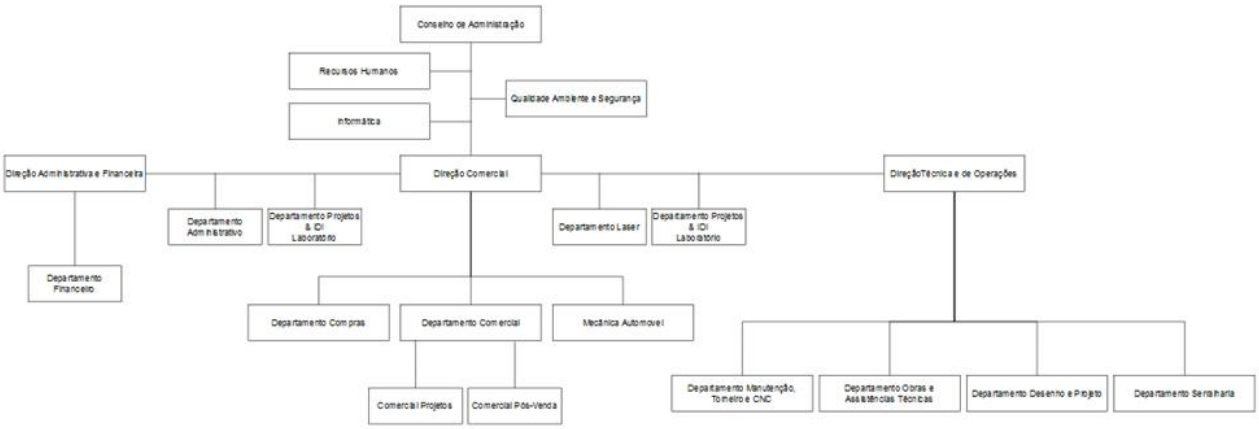


Figura 1 - Estrutura Empresarial HRV

1.2 Localização física

Figura 2 – Localização da HRV

Morada

Rua da Finlândia, Lt 46

Zona Industrial da Marinha Grande

2430-028 Marinha Grande

1.3 Principais ramos de atividade

A HRV é especialista na conceção, instalação e manutenção de processos industriais automatizados para os segmentos dos alimentos compostos para animais (convencionais, peixe e pet), biomassa (energia, carvão vegetal e composto orgânico) e química (sólidos e polvorosos).

Com reconhecida experiência, a HRV oferece hoje aos seus clientes um serviço de soluções integradas, inovadoras e que se pretendem sempre mais sustentáveis.

1.4 Os principais parceiros de negócio e seus setores da atividade empresarial

A parceria específica e estratégica que mantém com a Andritz Feed & Biofuel permite garantir aos seus clientes equipamentos de elevada qualidade, fiabilidade e tecnologicamente avançados. A experiência acumulada e os investimentos sustentados feitos ao longo do tempo em I&D, formação, equipamentos e instalações, resultam num acompanhamento especializado em cada um dos segmentos onde atua, sempre adaptado às necessidades de cada cliente.

Outros parceiros:

Parceiro	**Setor de Atividade**
Technipes	Produção de Máquinas/Componentes
Hosokawa	Produção de Máquinas/Componentes
Jesma	Produção de Máquinas/Componentes
Simeza	Produção de Silos Metálicos
Borghi	Produção de Máquinas/Componentes
Rollier	Produção de Máquinas Vibratórias

Tabela 1 – Parceiros HRV

1.5 A estrutura de administração empresarial, a relação com clientes/fornecedores, recurso a *outsourcing / insourcing*

Uma estrutura organizacional bem definida é fundamental para que os processos de negócio fluam sem constrangimentos, garantindo assim fronteiras de responsabilidade. A definição de tarefas, a sua alocação, calendarização e avaliação, permite que cada departamento de forma autónoma possa gerir a sua eficácia no processo e em conjunto atinjam os objetivos propostos. A HRV tem como elemento principal o conselho de administração, que é constituído pelo conjunto de acionistas da empresa. Os acionistas da empresa são os responsáveis pelos principais departamentos da empresa que se subdividem em subdepartamentos com responsáveis específicos para as diferentes áreas.

A organização HRV sendo uma empresa de produção industrial tem necessidade de envolver uma quantidade significativa de clientes e fornecedores e de comunicar com eles. A relação digital com os clientes/fornecedores resume-se na sua totalidade à plataforma de email. Os contactos tanto com clientes como fornecedores envolvem a troca de informação confidencial, qualquer fuga de informação poderá pôr em causa a credibilidade e confiança da organização, colocando em causa a sua continuidade.

A HRV recorre a *outsourcing* no domínio das TI, nomeadamente ao nível do ERP, para garantir a sua atualização ao nível de requisitos legais e ao nível da presença web (página institucional). Nos casos de outsourcing é necessário garantir:

- Controlos de Acesso ao Sistema;
- Definição de Áreas de Intervenção;
- Identificação dos utilizadores de outsourcing com credenciais especificas e únicas.

Nos restantes projetos desenvolvidos na organização e uma vez que a empresa dispõe de meios técnicos, são desenvolvidos em regime de *insourcing*.

1.6 O enquadramento da empresa com o mundo digital.

A HRV, como grande parte das empresas, encontra-se neste momento a atravessar um processo de digitalização. Os principais processos de negócio encontram-se digitalizados ou em fase final de integração com os sistemas digitais já implementados. A recolha de dados de chão-de-fabrica é executada já de forma digital e é uma ferramenta fundamental para o processo de negócio. A HRV desenvolveu software de gestão de produção/armazém/pessoal internamente integrado com o ERP PHC, permitindo desta forma desburocratizar e tornar mais ágil o processo.

A presença da HRV no mundo digital passa ainda pela sua página web e presença nas redes sociais.

2 Arquitetura do Sistema de Informação

2.1 Negócio, identificando as principais unidades de negócio e respetivos processos e atividades do ponto de vista de negócio

A HRV produz e instala linhas de produção automatizadas a partir da fábrica sedeada na Marinha Grande cobrindo toda a área nacional continental e ilhas.

Na estrutura da empresa identificam-se sete processos de negócio:

- Comercial;
- Compras / Importação;
- Financeiro;
- Projeto;
- Produção;
- Qualidade e Ambiente;
- Investigação e Desenvolvimento.

2.2 Dados que devem ser recolhidos, organizados, protegidos e distribuídos

No seu processo de negócios a HRV tem a necessidade de recolher e manter dados de índole confidencial de clientes, fornecedores e colaboradores.

Os dados recolhidos são os estritamente necessários para a finalidade a que se destinam. No caso de fornecedores e clientes os dados recolhidos são os legalmente necessários para o processo venda/compra e faturação, nomeadamente:

- Nome empresa;
- NIF;
- Morada;
- Contactos;
- Sector de Atividade;
- Dados Financeiros;
- Dados Bancários.

Os dados recolhidos dos colaboradores são os dados necessários ao processamento de salários e/ou subscrição de serviços aplicáveis ao funcionário ou ao agregado familiar (p. ex. seguro de saúde), nomeadamente:

- Nome;
- Morada;
- NIF;
- Data Nascimento;
- Cartão Cidadão;
- Habilitações Escolares;
- Contacto Pessoal;
- Formações;

- Carta Condução;
- Dados Bancários.

2.3 Identificação das principais aplicações utilizadas, tais como softwares desenvolvidos à medida e softwares generalistas, e dos principais fluxos de informação existentes

Os principais softwares utilizados no processo de negócio da HRV são:

1. ERP PHC;
2. Siemens Solid Edge;
3. Microsoft Office 365;
4. GestPro (Desenvolvido).

Os programas enumerados destinam-se a dar suporte aos processos operacionais da organização e também ao processo de tomada de decisão.

O processo de negócio na HRV desenvolve-se numa primeira fase entre o cliente, o Departamento Comercial e o Departamento de Projeto, fase de proposta, projeto e negociação. Caso seja adjudicado a proposta/projeto é enviada como adjudicada ao responsável de operações que inicia o processo de fabrico, criando pedidos de produção que são os trabalhos a desenvolver pelas várias secções da produção e calendarizando-as de acordo com o acordado com o cliente. As secções produtivas efetuam os pedidos de materiais ao armazém, que os fornece ou caso exista rotura de stock envia pedido ao Departamento de Compras que efetua as consultas aos fornecedores e estabelece os acordos de fornecimentos. Os materiais comprados são geridos pelo armazém que os receciona e distribui pelas secções produtivas.

Nas várias fases são utilizados o GestPro na gestão da atividade operacional (materiais pedidos, materiais gastos no projeto, receção de materiais no armazém, gestão de stocks, horas de trabalho de cada funcionário por secção no projeto, máquinas utilizadas e tempos de utilização), PHC (compras a fornecedores, encomendas de clientes, faturação) e na fase de Projeto o Siemens Solid Edge.

2.4 Tecnologias utilizadas, tais como sistemas operativos de rede e de clientes, plataformas móveis e fixas, sistemas de comunicação, sistemas de armazenamento

A infraestrutura dos sistemas de informação da HRV assenta em servidores baseados em Windows Server virtualizados numa solução VMWare (ESXI), os postos de trabalho que compreendem máquinas desktop ou portáteis com sistemas operativos Windows 10/11, o sistema de armazenamento de dados está implementado numa solução de NAS da Synology. Os dispositivos de comunicação móveis utilizados na organização são suportados por Android e IOS.

2.5 Localização dos ativos tecnológicos e de informação, *on premises* ou *cloud*

A HRV tem investido numa infraestrutura de TI "*on premises*" assegurando dessa forma que a informação está guardada em servidores e/ou repositórios de dados totalmente controlados pela organização e que depende apenas da sua infraestrutura em questões de disponibilidade,

redundância e segurança. A solução *"on premises"* permite uma redução significativa de custos relativamente a uma solução *"cloud"* pública face ao volume de dados que é necessário manter.

3 Análise de Risco

Como enquadramento, a análise de risco (Figura 3) tem como objetivo verificar qual ou quais as origens dos riscos identificados, as suas consequências, os seus impactos e qual a probabilidade de ocorrência. Para a execução desta fase, foi necessário identificar primeiramente os riscos, as ameaças e as vulnerabilidades, referentes aos ativos da organização e quais os controlos implementados, bem como a sua eficácia [1].

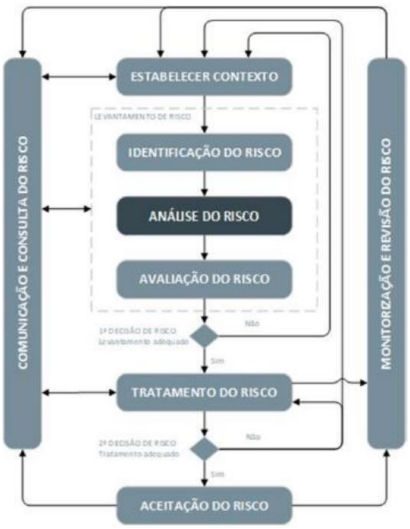


Figura 3 - Análise de Risco

3.1 Identificação dos riscos

A identificação do risco (ponto 2) é a primeira etapa do levantamento de risco (ponto 1), como é possível observar na Figura 4. Permite determinar as ocorrências que poderão causar uma potencial perda à organização e permite apurar como, onde e porquê esta perda pode acontecer [1].

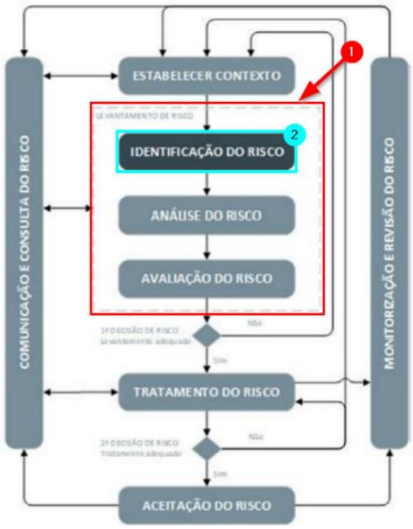


Figura 4 - Identificação do Risco

Nesta fase, foram identificados, reconhecidos e descritos todos os riscos que possam trazer constrangimentos à organização ou até mesmo, impedir que esta consiga atingir os objetivos a que se propôs. O principal objetivo foi identificar e determinar as ocorrências que poderão causar uma potencial perda à organização [1].

Para a identificação do risco foram realizadas várias atividades, tais como:

- Análise de vulnerabilidades internas e externas;
- *Brainstorming* com os recursos humanos envolvidos nos processos críticos;
- Questionários com gestores ou responsáveis pelos processos críticos;
- Análise de cenários de ameaça internas e externas;
- Auditorias de segurança.

Assim sendo, na Identificação dos Riscos (Tabela 2), encontra-se a identificação dos riscos, com as respetivas entradas.

Identificação dos Riscos		
Entradas (Inputs)	**Atividades**	**Saídas (Outputs)**
Atividades descritas acima	- Identificação de ativos; - Identificação de ameaças; - Identificação dos controlos existentes; - Identificação de vulnerabilidades;	- Lista de ativos identificados; - Lista de ameaças; - Lista de controlos existentes; - Lista de vulnerabilidades; - Riscos devidamente identificados e documentados;

Tabela 2 - Identificação dos Riscos

3.2 Análise do risco

A análise do risco que tem sido adotada pela HRV baseia-se na mitigação. Parte das organizações já possuem um sistema de gestão de riscos da informação, que permite fazer um mapeamento através dos seguintes procedimentos simplificados [2]:

- Definição do âmbito;
- Identificação dos riscos;
- Análise dos riscos;
- Avaliação dos riscos;
- Gestão e Monitorização dos riscos.

De uma forma geral, o Risco é o resultado da função Probabilidade x Impacto ou Valor.

Risco = Probabilidade x Impacto ou Valor

Para esta análise de risco, consideramos os cinco tipos de risco, nomeadamente:

- **Risco estratégico**
  Refere-se ao posicionamento da organização em relação ao produto ou serviço, estratégias de mercado, concorrentes e afins, e quais os fatores que podem afetar cada um destes aspetos, principalmente a médio e longo prazo.

- **Risco financeiro**
  Trata-se de riscos que afetam diretamente o fluxo de caixa e a receita gerada pelo negócio, podendo prejudicar até a saúde financeira da organização.

- **Risco operacional**
  São aqueles que podem render altas perdas para a organização, como por exemplo, falhas operacionais, perda de documentos importantes, falhas de segurança, fraudes, entre outros.

- **Riscos de conformidade**
  Refere-se ao cumprimento de todas as normas e leis que a organização está obrigada a cumprir. Em caso de incumprimento, a organização poderá ter coimas avultadas que podem criar graves problemas financeiros como reputacionais.

- **Riscos cibernéticos**
  Este é o risco que mais preocupa os responsáveis das organizações, porque este pode afetar a estratégia da organização, a área financeira, a área operacional e pode colocar em causa a sobrevivência da organização.

Para uma análise mais cuidada e completa possível, é necessário recorrer a pelo menos sete processos, nomeadamente:

- 1. Identificar os Ativos de Informação;
- 2. Determinar o Valor da Informação;
- 3. Determinar a Probabilidade de Ocorrência;
- 4. Determinar o Risco;
- 5. Identificar os Controlos a Aplicar;
- 6. Implementar um Plano de Ação de Mitigação;
- 7. Revisão da Avaliação de Riscos;

De seguida, iremos analisar cada um dos processos para permitir identificar e quantificar os riscos que podem afetar a organização.

3.2.1 Identificar os Ativos de Informação

São designados ativos da informação, **sistemas**, **portais**, **servidores**, **base de dados**, **equipamentos de comunicação, serviços de eletricidade, refrigeração, iluminação e contratos** que devem ser identificados no âmbito da segurança da informação com o respetivo dono associado.

3.2.2 Identificação dos ativos

Os ativos que apresentam maior importância financeira e estratégica para a empresa, são:

- *Firewall*;
- Servidor administrativo (Não está exposto para a internet);
- Servidor operacional (Está exposto para a internet);
- UPS (Estabilizador de corrente elétrica);
- Impressoras / Fotocopiadoras;
- Router ISP (Internet);
- *Switchs*;
- Computadores – *Desktop*;
- Computadores – Portáteis;
- Computadores do Executivo.

3.2.3 Determinar o Valor da Informação

Para cada ativo de informação identificado, é efetuada a classificação no que se refere à confidencialidade, integridade e disponibilidade atendendo à seguinte tabela:

	Baixa [1]	**Média [2]**	**Alta [3]**
Disponibilidade Assegurar que os utilizadores autorizados têm acesso à informação quando necessário	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito adverso **limitado** nas operações, bens ou colaboradores da HRV.	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito adverso **significativo** nas operações, bens ou colaboradores da HRV.	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito adverso **catastrófico** nas operações, bens ou colaboradores da HRV.
Confidencialidade Assegurar que a informação apenas está acessível a quem está autorizado	O acesso não autorizado à informação tem um efeito **limitado** nas operações, bens ou colaboradores da HRV.	O acesso não autorizado à informação tem um efeito **significativo** nas operações, bens ou colaboradores da HRV.	O acesso não autorizado à informação tem um efeito **catastrófico** nas operações, bens ou colaboradores da HRV.
Integridade Salvaguardar que a informação (e o método de processamento) é exata e completa	Uma alteração não autorizada à informação ou destruição da mesma tem um efeito adverso **limitado** nas operações, bens ou colaboradores da HRV.	Uma alteração não autorizada à informação ou destruição da mesma tem um efeito adverso **significativo** nas operações, bens ou colaboradores da HRV.	Uma alteração não autorizada à informação ou destruição da mesma tem um efeito adverso **catastrófico** nas operações, bens ou colaboradores da HRV.

Tabela 3 - Matriz valor da informação

$$\text{Valor da informação} = (\text{Confidencialidade} + \text{Integridade} + \text{Disponibilidade}) / 3$$

É determinado o **Valor do Ativo da Informação** que caracterize o impacto da perda para cada propriedade (confidencialidade, integridade e disponibilidade):

- **Alto**: Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo: **Alta|Alta|Alta ou Alta|Alta**

- **Médio**: Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo: **Média ou Média|Média ou Média|Média|Média**

- **Baixo**: Se a combinação Confidencialidade, Integridade e Disponibilidade for do tipo: **Baixa|Baixa ou Baixa|Baixa|Baixa**

3.2.4 Determinar a Probabilidade de Ocorrência

Para cada ativo de informação identificado devem ser identificadas as **vulnerabilidades** e possíveis **ameaças,** de acordo com as seguintes definições:

- **Vulnerabilidade**: É uma condição ou um conjunto de condições que permitem que ameaças afetem os ativos;
- **Ameaça**: Causa incidentes indesejados que podem resultar em dano/perda de um ativo;
- **Probabilidade de Ocorrência**: Probabilidade que uma ameaça tem de explorar inerentes ao ativo;

Critérios para a Probabilidade de ocorrência das ameaças:

i. **Alta [3]** – Ocorrência frequente (Diária/ Semanal)
ii. **Média [2]** – Ocorrência repetitiva (Mensal/ Anual)
iii. **Baixo [1]** – Ocorrência muito pouco frequente (últimos três a cinco anos)

3.2.4.1 Identificação dos tipos de ameaças

Atualmente, as ameaças identificadas são:

- **Ataque malicioso**
  - Intrusão em sistemas, infiltrações e entradas não autorizadas;
  - Utilização de Código malicioso (por exemplo: vírus, *ransomware*, Cavalo de Troia e etc.);
  - Ataque a sistemas (por exemplo, ataque distribuído de negação de serviço);
  - Engenharia social.
- **Fenómeno natural**
  - Inundação;
  - Fenómeno meteorológico.
- **Falha no fornecimento de bens ou serviços por terceiro**
  - Interrupção do fornecimento de energia;
  - Interrupção do fornecimento do serviço de telecomunicações

3.2.4.2 Identificação dos tipos de vulnerabilidades

Listadas as ameaças, o próximo passo foi identificar as vulnerabilidades que podem ser exploradas. Para avaliar riscos é importante considerar quais são as fontes, ou seja, as vulnerabilidades dos ativos que podem expor a organização a falhas de segurança. Apresentamos alguns exemplos na tabela abaixo, onde relacionamos o ativo com as ameaças e a probabilidade de ocorrência, bem como a vulnerabilidade que expõe o ativo.

Ativo	Ameaças	Probabilidade Ocorrência	Vulnerabilidades
Firewall	Ataque malicioso	**Média**	Atualizações por realizar
	Fenómeno natural	**Baixa**	Inundação, por se encontrar num piso subterrâneo.
	Falha de terceiros	**Média**	Correção de uma falha no firmware
Servidor administrativo (Não está exposto para a internet)	Ataque malicioso	**Média**	Software sem atualização
	Fenómeno natural	**Baixa**	Inundação, por se encontrar num piso subterrâneo.
	Falha de terceiros	**Alta**	Servidor com hardware descontinuado.
Servidor operacional (Está exposto para a internet)	Ataque malicioso	**Alta**	Software sem atualização
	Fenómeno natural	**Baixa**	Inundação, por se encontrar num piso subterrâneo.
	Falha de terceiros	**Alta**	Servidor com hardware descontinuado.
UPS	Ataque malicioso	**Baixa**	Por dispor de ligação à rede, Atualizações por realizar
	Fenómeno natural	**Média**	Descarga elétrica. Inundação, por se encontrar num piso subterrâneo.
	Falha de terceiros	**Alta**	Fornecimento de energia instável e sem redundaria de fornecedor
Impressoras (*Renting*)	Ataque malicioso	**Média**	Atualizações por realizar
	Fenómeno natural	**Baixa**	Descarga elétrica, equipamento não ligado à UPS.
	Falha de terceiros	**Alta**	Falta de consumíveis e manutenção.
Router ISP (Internet)	Ataque malicioso	**Média**	Router do ISP, atualização por realizar
	Fenómeno natural	**Baixa**	Vento. E Inundação, por se encontrar num piso subterrâneo.
	Falha de terceiros	**Alta**	Falta de redundância de fornecedor
Switchs	Ataque malicioso	**Média**	Atualizações por realizar
	Fenómeno natural	**Baixa**	Inundação, por se encontrar num piso subterrâneo

	Falha de terceiros	**Média**	Correção de uma falha no firmware
Computadores *Desktop*	Ataque malicioso	**Média**	Atualizações por realizar (sistema operativo Windows, antivírus ESET, Office 365)
	Fenómeno natural	**Média**	Descarga elétrica, equipamento não ligado à UPS.
	Falha de terceiros	**Baixa**	Disponibilização de uma atualização para corrigir uma falha
Computadores Portáteis	Ataque malicioso	**Média**	Atualizações por realizar (sistema operativo Windows, antivírus ESET, Office 365)
	Fenómeno natural	**Baixa**	Descarga elétrica, equipamento não ligado à UPS.
	Falha de terceiros	**Baixa**	Disponibilização de uma atualização para corrigir uma falha
Computadores do Executivo	Ataque malicioso	**Alta**	Software sem atualização
	Fenómeno natural	**Baixa**	Descarga elétrica
	Falha de terceiros	**Alta**	Servidor com hardware descontinuado.

Tabela 4 - Classificação de vulnerabilidades nos ativos

3.2.5 Determinar o Risco

O risco é determinado pela combinação do Valor com a Probabilidade de Ocorrência de acordo com a seguinte matriz:

		Valor		
	RISCO	**Alta [3]**	**Média [2]**	**Baixa [1]**
Probabilidade	**Alta [3]**	Elevado (9)	Alto (6)	Médio (3)
	Média [2]	Alto (6)	Médio Alto (4)	Baixo (2)
	Baixa [1]	Médio (3)	Baixo (2)	Desprezável (1)

Tabela 5 – Matriz de risco

$$\text{Risco} = \text{Probabilidade x Valor}$$

Esta matriz permite priorizar os riscos em termos de grau de urgência de atenção.

3.2.6 Identificar os Controlos a Aplicar

O risco associado às ameaças identificadas pode ser **eliminado** ou **reduzido**.

Atualmente, os controlos existentes são:

- **Controlos Organizacional**
  - Políticas de segurança da informação;
  - Segregação de funções;
  - Controlo de acesso;
  - Conformidade com políticas, regras e normas para segurança da informação.

- **Controlos de pessoas**
  - Trabalho remoto.

- **Controlos físicos**
  - Perímetros de segurança física;
  - Manutenção de equipamentos.

- **Controlos Tecnológicos**
  - Restrições de acesso privilegiado;
  - Segurança de Redes;
  - Autenticação Segura.
  -

3.2.7 Implementar o Plano de Ação de Mitigação

Para cada **controlo** com necessidade de implementação de plano de ação, devem ser estabelecidas um conjunto de ações, responsabilidades e prazos que permitam assegurar a execução dos controlos definidos.

3.2.8 Revisão da Avaliação de Riscos

É aconselhável semestralmente a reavaliação dos riscos de forma a:

- Incluir alterações nos ativos de informação;
- Incorporar mudanças nas prioridades e necessidades;
- Considerar novas ameaças e vulnerabilidades;
- Verificar se os controlos permanecem eficazes e apropriados.

O resultado desta avaliação, permite identificar e quantificar os riscos que podem afetar a segurança da informação de acordo com a seguinte tabela:

1		2				3	4	5	6
Ativo de Informação		**Valor da Informação (D + C + I) / 3**				**Probabilidade de Ocorrência Ameaça** (Máx. 3)	**Risco** (Máx. 9) (Probabilidade x Valor)	**Controlos**	**Plano para Mitigação**
Identificação	Proprietário	Disponibilidade	Confidencialidade	Integridade	**Valor** (Máx. 3)				
Firewall	HRV	Média	Média	Alta	2,3	5/3=1,6	3,68	Físicos e Tecnológicos	#01
Servidor administrativo (Não está exposto para a internet)	HRV	Alta	Alta	Alta	3	6/3 =2	6	Organizacional, Pessoas, Físicos e Tecnológicos	#02
Servidor operacional (Está exposto para a internet)	HRV	Alta	Média	Alta	2,6	7/3 =2,3	5.98	Organizacional, físicos e Tecnológicos	#03
UPS (energia)	HRV	Alta	Baixa	Média	2	6/3 =2	4	Físicos	#04
Impressoras (*Renting*)	Ext.	Média	Média	Média	2	6/3 =2	4	Físicos	#05
Router ISP	Ext.	Alta	Alta	Alta	3	6/3 =2	6	Tecnológicos e Físicos	#06
Switchs	HRV	Alta	Alta	Alta	3	6/3 =2	6	Tecnológicos e Físicos	#07
Computadores (Desktop)	HRV	Média	Média	Média	2	5/3=1,6	3,2	Tecnológicos e Físicos	#08
Computadores (Portáteis)	HRV	Média	Média	Média	2	4/3=1,3	2,6	Tecnológicos e Físicos	#09
Computadores (Executivo)	HRV	Média	Alta	Alta	2,6	7/3 =2,3	5.98	Tecnológicos e Físicos	#10

Tabela 6 - Avaliação dos riscos dos ativos

Observação: Nos casos em que o ativo não pertence à HRV, o proprietário do ativo é EXTERNO (Ext.) o risco é transferido para a Entidade terceira. A HRV dispõe de um contrato que salvaguarda os interesses da organização, que é garantir que os *downtimes* dos sistemas/serviços não ultrapassam o que está definido ao nível do contrato.

Plano para a mitigação das ameaças

#01 - Firewall
• Atualizar regularmente o *firmware* da Firewall com as últimas atualizações de segurança e correções de vulnerabilidades. • Definir políticas de segurança claras e rigorosas para a configuração e gestão da Firewall. • Utilizar senhas complexas e com a autenticação de dois fatores ativa. • Configurar a Firewall para bloquear o tráfego não autorizado e permitir somente o tráfego necessário de acordo com as políticas de segurança da organização. • Configurar *logs* e alertas para monitorizar as atividades suspeitas na Firewall. • Limitar o acesso à Firewall somente aos administradores dos sistemas. • Realizar testes regulares de segurança para identificar vulnerabilidades na Firewall. • Estabelecer planos de contingência para lidar com incidentes de segurança na Firewall. • Criar cópias de segurança dos registos e configurações da Firewall para ajudar na recuperação, caso esta seja comprometida.

#02 – Servidor Administrativo
• Complexidade nas palavras-passes dos utilizadores do domínio. • A informação confidencial, quando em repouso, deve estar cifrada, para evitar que seja acedida por pessoas não autorizadas. • Políticas de acesso restrito ou controlado, para permitir que apenas as pessoas autorizadas tenham acesso aos dados, reduzindo o risco de fraude ou exposição de dados sensíveis. • Atualização e manutenção de software, para garantir que o software (aplicações e serviços) encontra-se atualizado de acordo com o suporte prestado pelo fabricante. Isto ajudará a garantir que todos os *patch's* de segurança sejam aplicados, restringindo as vulnerabilidades presentes no servidor. • Realização periodicamente testes de penetração, para identificar pontos fracos e ajustar as medidas de segurança para mitigar os riscos e reforçar uma posição mais defensiva. • Realização periodicamente backups, garantindo a integridade e confidencialidade dos dados, para locais externos (*Cloud*);

#03 – Servidor Operacional
• Complexidade nas palavras-passes dos utilizadores do domínio. • A informação confidencial, quando em repouso, deve estar cifrada, para evitar que seja acedida por pessoas não autorizadas. • Políticas de acesso restrito ou controlado, para permitir que apenas as pessoas autorizadas tenham acesso aos dados, reduzindo o risco de fraude ou exposição de dados sensíveis. • Atualização e manutenção de software, para garantir que o software (aplicações e serviços) encontra-se atualizado de acordo com o suporte prestado pelo fabricante. Isto ajudará a garantir que todos os *patch's* de segurança sejam aplicados, restringindo as vulnerabilidades presentes no servidor. • Realização periodicamente testes de penetração, para identificar pontos fracos e ajustar as medidas de segurança para mitigar os riscos e reforçar uma posição mais defensiva. • Realização periodicamente backups, garantindo a integridade e confidencialidade dos dados, para locais externos (*Cloud*).

#04 - UPS

- Atualizar regularmente o *firmware* e o software da UPS, garantindo que as vulnerabilidades sejam corrigidas.
- Implementar controlos de acesso físico à UPS para restringir o acesso não autorizado por pessoas não autorizadas.
- Proteger o acesso à configuração da UPS com senhas fortes, autenticação multifator e criptografia para evitar acesso não autorizado.
- Monitorizar periodicamente o desempenho da UPS.
- Realizar manutenções periódicas ao equipamento, como testes e substituição das baterias.

#05 - Impressoras

- Atualizar regularmente o *firmware* e o software da UPS, garantindo que as vulnerabilidades sejam corrigidas.
- Políticas de acesso restrito ou controlado,
- Controle de acesso, para permitir que apenas as pessoas autorizadas tenham acesso ao equipamento, como imprimir, fotocopiar e digitalizar documentos.
- Garantir que a comunicação entre o computador e a impressora é cifrada para proteger os dados em trânsito.
- Autenticação do utilizador, as impressoras têm de solicitar a autenticação ao utilizador para garantir que apenas os utilizadores autorizados têm acesso às funções da impressora.

#06 – Router ISP

- Atualizar regularmente o *firmware* do Router com as últimas atualizações de segurança e correções de vulnerabilidades.
- Definir políticas de segurança claras e rigorosas para a configuração e gestão do Router.
- Utilizar senhas complexas e com a autenticação de dois fatores ativa.
- Configurar *logs* e alertas para monitorizar as atividades suspeitas no Router.
- Limitar o acesso ao Router somente aos administradores dos sistemas.
- Realizar testes regulares de segurança para identificar vulnerabilidades no Router.
- Estabelecer planos de contingência para lidar com incidentes de segurança no Router.
- Criar cópias de segurança dos registos e configurações do Router para ajudar na recuperação, caso este seja comprometido.

#07 - Switchs

- Atualizar regularmente o *firmware* dos *Switchs* com as últimas atualizações de segurança e correções de vulnerabilidades.
- Definir políticas de segurança claras e rigorosas para a configuração e gestão dos *Switchs*.
- Utilizar senhas complexas.
- Limitar o acesso ao *Switchs* somente aos administradores dos sistemas.
- Realizar testes regulares de segurança para identificar vulnerabilidades nos *Switchs*.
- Estabelecer planos de contingência para lidar com incidentes de segurança nos *Switchs*.
- Criar cópias de segurança dos registos e configurações dos *Switchs* para ajudar na recuperação, caso estes sejam comprometidos.

#08 – Computadores Desktop

- Atualização e manutenção de software, para garantir que o software (aplicações e serviços) encontra-se atualizado de acordo com o suporte prestado pelo fabricante. Isto ajudará a garantir que todos os *patch's* de segurança sejam aplicados, restringindo as vulnerabilidades presentes no posto de trabalho.
- Manter a firewall do Sistema Operativo ativa e não abrir novos portos, esta tarefa terá de ser realizada pelos Administradores de Sistemas.
- Manter o antivírus sempre atualizado.
- Cifrar os dados sensíveis, para proteger a informação confidencial, como senhas e dados financeiros, tornando a informação inacessível por pessoas não autorizadas.
- Treinar regularmente os colaboradores da organização para aumentar os níveis de consciencialização sobre os riscos de segurança e como podem ser evitados.
- Realizar backups dos computadores desktop periodicamente, para evitar que alguns dados sejam perdidos em caso de um ciberataque ou falha do sistema.

#09 – Computadores Portáteis

- Atualização e manutenção de software, para garantir que o software (aplicações e serviços) encontra-se atualizado de acordo com o suporte prestado pelo fabricante. Isto ajudará a garantir que todos os *patch's* de segurança sejam aplicados, restringindo as vulnerabilidades presentes no posto de trabalho.
- Utilizar senhas complexas e com a autenticação de dois fatores ativa (SMS ou envio do *Token* para o *Smartphone*).
- Os discos rígidos devem ser cifrados, porque são equipamentos que andam no exterior.
- Proteção remota em todos os computadores portáteis, que permita que os Administradores de Sistemas consigam bloquear o dispositivo e eliminar os dados, em caso de perda ou roubo do equipamento.
- Manter a firewall do Sistema Operativo ativa e não abrir novos portos, esta tarefa terá de ser realizada pelos Administradores de Sistemas.
- Manter o antivírus sempre atualizado.
- Treinar regularmente os colaboradores da organização para aumentar os níveis de consciencialização sobre os riscos de segurança e como podem ser evitados.
- Realizar backups dos computadores portáteis periodicamente, para evitar que alguns dados sejam perdidos em caso de um ciberataque ou falha do sistema.

#10 – Computadores do Executivo

- Atualização e manutenção de software, para garantir que o software (aplicações e serviços) encontra-se atualizado de acordo com o suporte prestado pelo fabricante. Isto ajudará a garantir que todos os *patch's* de segurança sejam aplicados, restringindo as vulnerabilidades presentes no posto de trabalho.
- Utilizar senhas complexas e com a autenticação de dois fatores ativa (SMS ou envio do *Token* para o Smartphone).
- Manter a firewall do Sistema Operativo ativa e não abrir novos portos, esta tarefa terá de ser realizada pelos Administradores de Sistemas.
- Manter o antivírus sempre atualizado.
- Cifrar os dados sensíveis, para proteger a informação confidencial, como senhas e dados financeiros, tornando a informação inacessível por pessoas não autorizadas.
- Treinar regularmente os colaboradores da organização para aumentar os níveis de consciencialização sobre os riscos de segurança e como podem ser evitados.
- Realizar backups dos computadores desktop periodicamente, para evitar que alguns dados sejam perdidos em caso de um ciberataque ou falha do sistema.

4 Plano de resposta a incidentes

4.1 Definição do que é um incidente de acordo com a organização

A cibersegurança é uma preocupação crescente num mundo cada vez mais dependente da tecnologia e interligado digitalmente. As organizações devem adotar medidas proativas de cibersegurança, como políticas, formação, atualizações de *software*, *firewalls*, sistemas de deteção de intrusões e monitorização contínua para evitar e mitigar incidentes de cibersegurança.

De acordo com o QNRCS um incidente é definido como "*Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação*".

No âmbito deste documento podemos definir que um incidente de cibersegurança é um evento que compromete a segurança dos sistemas de computador, redes ou dados de uma organização. Pode ser uma ação maliciosa, como um ataque cibernético, ou uma falha de segurança acidental que resulta na exposição, roubo, corrupção ou dano dos ativos digitais. Os incidentes de cibersegurança podem assumir várias formas, como intrusões, exfiltração de dados, malware, *phishing*, negação de serviço (DDoS), *ransomware*, ou outros, podem também ser resultado de erros humanos, falhas técnicas ou desastres naturais, entre outros.

Quando ocorre um incidente de cibersegurança, é importante que a organização tome medidas rápidas e eficazes para minimizar os danos, proteger os dados e restaurar a normalidade dos sistemas. Isso normalmente envolve a identificação e resposta ao incidente, a investigação das causas e a revisão da estratégia de segurança para evitar futuros incidentes. Dependendo da gravidade e do impacto do incidente, pode ser necessário notificar as autoridades competentes e os indivíduos afetados.

No âmbito da definição de incidente de segurança, são identificados no quadro abaixo os principais tipos de incidentes:

Tipo de Incidente	**Descrição**
DDoS	Ataque que visa colocar os serviços indisponíveis
Malware	Infeção dos Sistemas através da Cifragem dos Dados
Exfiltração de Dados/ Violação de Dados	Recolha Ilícita de Dados por Parte do Atacante
Intrusão/Acesso Não Autorizado	Intrusão do sistema através da exploração de vulnerabilidades
Phishing	Obtenção de Informações Confidenciais
Engenharia Social	Manipulação Psicológica para obtenção de informações confidenciais
Injeção de Código	Injeção de código maliciosos em aplicações cujo objetivo é a exploração de uma vulnerabilidade
Outros	Tipo de Incidente Não Especificado

Tabela 7 – Principais Tipos de Incidentes

4.2 Definição e identificação da equipa e modelo de resposta a incidente

Deverá ser definida uma equipa, com o nome *Computer Security Incident Response Team* (CSIRT), com as funções de recolher e analisar incidentes de segurança. A equipa deve ser constituída por elementos com conhecimentos, principalmente, em análise, investigação e em recuperações de potenciais incidentes de segurança. A equipa também deve ter a responsabilidade de comunicar com serviços e parceiros externos, caso exista essa necessidade.

A equipa CSIRT contém elementos que tem cargos com maior relevância, que tem competência para gerir da melhor forma os incidentes de segurança. Sendo descrito de seguida cada um destes cargos.

Seguindo a *farmework* ENISA, define quais as diferentes etapas na gestão e tratamento de incidentes de segurança, tanto nas capacidades de procedimento de incidentes, a sua análise, atenuação de vulnerabilidades e envio de alertas de segurança, como se pode verificar na Figura 5.

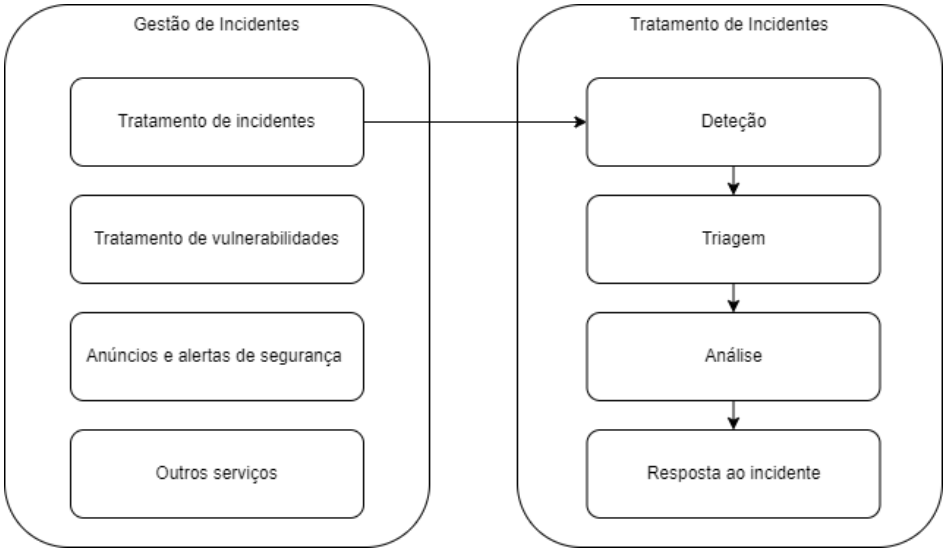


Figura 5 - Gestão e tratamento de Incidentes adaptado [3]

4.3 Responsável pela Resposta a Incidentes

Dentro da equipa CSIRT será nomeado um elemento que tem a responsabilidade de supervisionar e fazer a gestão dos incidentes de segurança detetados. Este elemento tem de ser detentor de experiência em analise, resolução e gestão de incidentes de segurança.

Tem a responsabilidade de entender e colocar em prática os *Service Level Agreement* (SLA) que estão definidos e acordados, de acordo com a criticidade de um incidente, dentro da HRV, tal como os SLA definidos e acordados com serviços e parceiros externos, caso seja necessário intervenção ou suporte dos mesmos.

Também necessário ter competências de comunicação de forma clara, já que será este elemento a fazer a comunicação com o *Chief Information Office* (CIO) sobre os possíveis impactos de um incidente de segurança.

Este elemento além das funções anteriormente descritas, também contém as funções e responsabilidade descrita de seguida:

- Único ponto de contacto entre a equipa CSIRT e o CIO;
- Construir e gerir uma equipa CSIRT;
- A calcular que cada elemento da equipa CSIRT tem as competências, formações e as certificações adequadas para o tratamento de incidentes de segurança;
- Manter atualizado o plano e os procedimentos tendo como base os resultados dos testes periódicos que serão realizados na HRV;
- Retificação do plano e dos procedimentos, não menos que uma vez por ano civil;
- Realização de testes ao plano de resposta a incidentes e aos seus respetivos procedimentos;
- Conhecimentos das políticas de cibersegurança e os procedimentos mais atuais;
- Entrega de relatórios mensais dos incidentes de segurança para o CIO.

4.4 Membros da equipa de resposta a incidentes

Como referido anteriormente o responsável pela equipa de resposta a incidentes, tem a função de criar uma equipa de CSIRT. Os elementos pertencentes à equipa têm de ter a capacidade de analisar os detalhes de incidente de segurança. Os elementos pertencentes podem ser oriundos de várias áreas, tais como:

- Analistas de segurança:
  - Elementos que iram primariamente fazer o tratamento dos incidentes de segurança.
- Analistas forenses:
  - Elementos primariamente vão fazer uma análise mais criminal em caso de falhas ou fugas de informação;
  - De forma secundaria, fazem tratamentos dos incidentes de segurança.
- Elementos de *Threat Intel* e *Threat Hunting*;
  - Elementos que primariamente fazem a busca e auditoria de possíveis falhas de segurança;
  - De forma secundaria, fazem tratamentos dos incidentes de segurança.
- Elementos de engenharia:
  - Elementos que são orientados para ferramentas de segurança.
  - Fazer a manutenção das ferramentas que serão usadas na equipa CSIRT;
  - Instalação de novas ferramentas quando necessário.

À semelhança do responsável da pela equipa de CSIRT, os elementos da equipa de resposta a incidentes também têm as suas responsabilidades, sendo que tem de haver uma partilha de informação entre todos e os detalhes dos factos encontrados durante a análise de um incidente de segurança. De seguida as funções dos elementos da equipa CSIRT:

- Fazer o tratamento e análise dos incidentes de segurança;
- Cada elemento tem de ter o conhecimento do plano de resposta a incidentes, tal como procedimentos para a resposta de forma apropriada a um incidente de segurança;
- Conhecimento dos SLA tanto os internos como os externos;
- Desenvolvimento contínuo das competências de gestão e de resposta a incidentes de segurança;
- Garantir que todas as ferramentas utilizadas, estão configuradas e a funcionar de forma correta;
- Análise constante de todos os serviços utilizados de forma a encontrar possíveis vulnerabilidades;
- Analisar o tráfego de rede, de forma a encontrar anomalias;

- Criação e gestão do inventário de elementos produtores de eventos de *log*;
- Recolher os eventos de *log* dos sistemas de forma a encontrar possíveis atividades suspeitas e guardar esses eventos de *logs* para futuras investigações forenses;
- Efetuar a correlação das várias informações recolhidas, como eventos de *logs*, análise da rede e análise de vulnerabilidade de forma a criar regras de deteção a pedido do responsável da equipa CSIRT;
- Garantir consultoria a pedido do CIO;
- Elaborar relatórios mensais do estado da segurança instalada na HRV;
- Participação nos testes do plano e nos procedimentos de resposta a incidentes.

Na Figura 6 encontra-se o que está no *scope* de cada parte da equipa CSIRT tem de ter em consideração durante o dia a dia, como se pode observar todos elementos devem partilhar todo o conhecimento adquirido da análise dos incidentes de segurança.

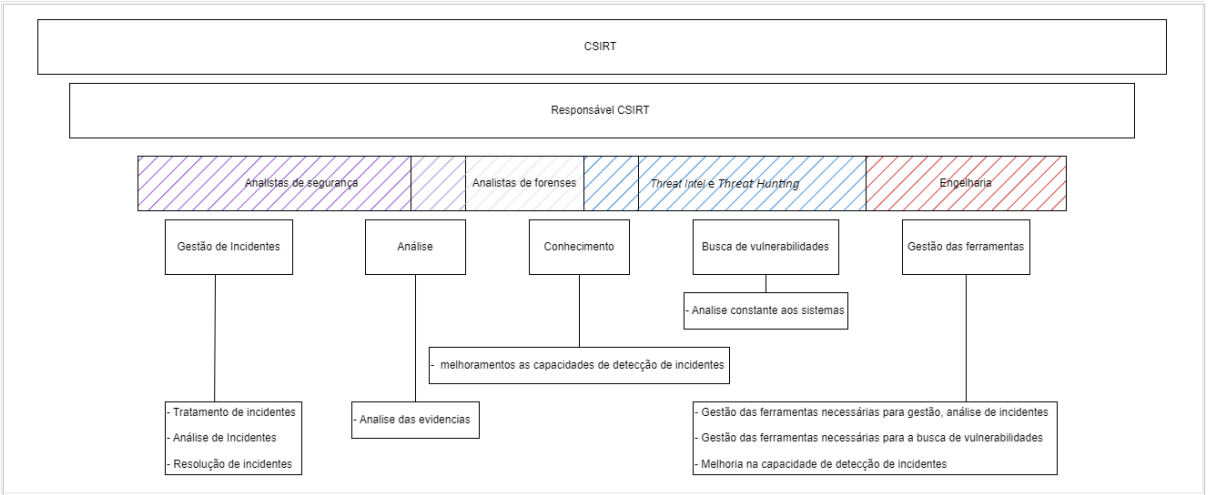


Figura 6 - Organização da CSIRT

4.5 Ferramentas a usar pela equipa de resposta a incidentes

São necessárias ferramentas para que a equipa CSIRT consiga fazer o seu trabalho de deteção e análise de incidentes de segurança da forma mais correta e eficiente. Todas as ferramentas utilizadas devem ter um propósito, de fácil interação e de utilização. Assim sendo, de seguida estão descritas as ferramentas que podem ser utilizadas pela equipa CSIRT:

- **Para gestão e armazenamento de eventos log**:
    - OpenSearch: Esta ferramenta *open-source* permite fazer o armazenamento de eventos *log* para deteção de incidentes de segurança e futura análise florenses.
- **Para análise de rede da HRV e gestão dos incidentes de segurança**:
    - SecurityOnion: Uma plataforma *open-source* que permite fazer a monitorização, deteção e análise de segurança em redes. É um agregador de várias ferramentas ou módulos, tais como *Intrusion Detections Systems* (IDS), *Hosts Detections Systems* (HDS) e *Network and Systems Management* (NSM). Os eventos encontrados devem ser enviados para o OpenSearch.
        - Esta ferramenta também atua como *Security information and event management* (SIEM) permitindo fazer uma gestão dos incidentes de

segurança e gestão de automações ou *playbooks*. Esta ferramenta está interligada com o openSearch.

- **Inventário:**
  - *Gestionnaire Libre de Parc Informatique* (*GLPI*): Um *software open-source* que permite fazer a gestão do inventário. Este *software* também tem capacidade de gestão de incidentes;
  - *Open Computers and Software Inventory Next Generation* (OCS Inventory NG): ferramenta open-*source*, que se interliga com o GLPI, sendo que recolhe toda a informação sobre um ativo e envia-a para o GLPI.
- **Gestão de *passwords*:**
  - KeepPass: é uma plataforma do tipo *open-source* que permite que seja feita uma gestão segura das *passwords*.
- **Gestão de *Indicator of Compromise* (IOC):**
  - *Malware Information Sharing Platform* (MISP): Uma ferramenta também do tipo *open-source* que permite que diferentes organizações partilhem entre si IOC, como *Internet Portocol* (IP), *Uniform Resource Locator* (URL), *hash* de arquivos entre outras informações. Estas informações permitem enriquecer os eventos recolhidos pelo openSearch.
- **Gestão de vulnerabilidades:**
  - *Open Vulnerability Assessment System* (*OpenVAS*), uma plataforma web, *open-source*, que permite fazer testes automáticos de forma a identificar vulnerabilidades nos sistemas.

Na Figura 7, encontra-se ilustrado as ferramentas e plataformas disponíveis para equipa CSIRT.

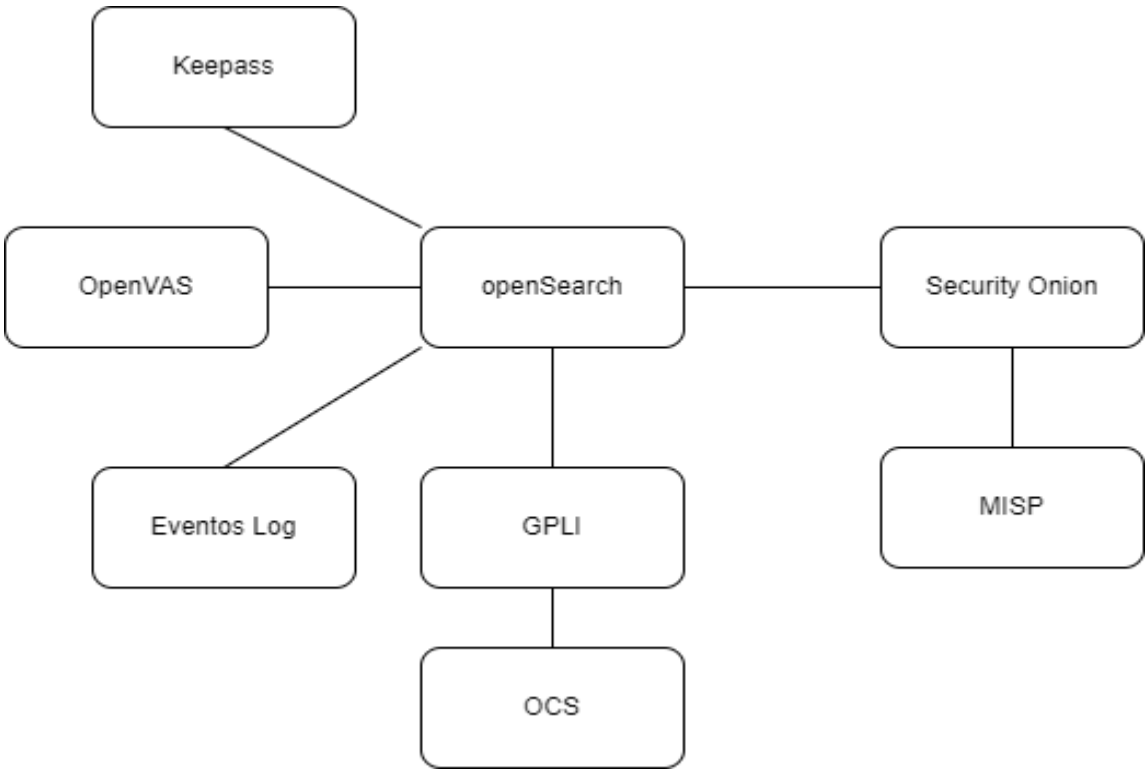


Figura 7 - Relação das diferentes ferramentas e plataformas disponíveis para CSIRT

As plataformas anteriormente descritas devem ser acedidas por todos elementos da equipa CSIRT, sendo que, os elementos que fazem engenharia têm o dever de manter toda infraestrutura de CSIRT, operacional e disponível, incluindo ferramentas, a plataformas descritas anteriormente e criação e gestão das regras de deteção.

4.6 Domínio do plano de resposta a incidentes

Para facilitar a criação de um plano de resposta a incidentes, é necessário a organização ter uma noção sobre os ativos que devem ser monitorizados e que devem entrar no domínio do PRI.

Portanto, para este caso em específico podemos utilizar a ferramenta *GLPI* e a ferramenta *OCS Inventory NG*, de forma a organizar os nossos ativos por criticidade e, obtermos assim uma visão geral da organização.

4.6.1 Aplicabilidade

Em termos de aplicabilidade, devemos seguir a informação que se encontra no software de gestão de ativos, o mesmo deverá ter a informação o mais atualizada possível, sendo que enumerando aqui, todos os ativos como (computadores, impressoras, equipamentos de rede, equipamentos elétricos, e funcionários), deverão estar abrangidos pelo plano de resposta a incidentes, tendo sempre em conta o nível de criticidade de cada ativo para a organização, de forma a não existir perda de negócio.

4.6.2 Incidentes

O plano de resposta a incidentes destina-se a incidentes de grau elevado, isto é, todos os ativos que tenham impacto no funcionamento do negócio. No entanto o nível de criticidade por ativo, deverá estar documentando no software de gestão de ativos, pois assim, em caso de incidente, torna-se mais fácil identificar quais os ativos com impacto ou não no negócio.

No caso de existir um incidente de criticidade considerada baixa e que não tenham impacto no negócio, não devem ser considerados ameaça ao ponto de ativar o plano de resposta a incidentes.

4.7 Identificação das partes interessadas

Tal como abordado em capítulos anteriores, a organização está vulnerável a todo o tipo de incidentes, pois com a quantidade de ataques / técnicas de ataque, não é possível evitar todos os incidentes na organização.

Neste documento descrevemos a lista de contactos agrupada por departamento, de forma que a mesma seja simples e de fácil acesso.

Desta forma a lista de contactos atualizada, permite dar uma resposta mais célere.

Na comunicação às partes interessadas deverá estar por exemplo a descrição de um incidente e os seus impactos, sendo que esta comunicação deverá ser separada por grupos, no quais abordamos os mesmos nos tópicos em baixo.

4.7.1 Equipas de resposta a incidentes

Portanto neste capítulo fazemos uma descrição/lista dos contactos técnicos, organizado claro por grupos e as suas responsabilidades.

A comunicação dos incidentes ou outro tipo de comunicações, de um modo geral deve ser feita através dos meios oficiais da organização, isto é, via ticket, email ou telefone.

4.7.1.1 Equipa CSIRT

A CSIRT é uma equipa com elementos especializados em segurança informática, com o objetivo de tratar de forma eficiente os incidentes que ocorrem na organização.

O responsável da equipa CSIRT responde diretamente ao CIO, tem a função de supervisionar todas as ações efetuadas durante o processo de incidente, sendo ele o membro principal, deverá ser o primeiro a ser contactado em caso de incidente.

As principais funções desta equipa é a de realizar processos e técnicas para detetar e mitigar incidentes.

Os processos por sua vez já deverão estar previamente documentados, no entanto se existir um incidente e esse processo não esteja documentado, é necessário criar essa mesma documentação para uma análise futura.

As principais funções estão relacionadas com a Figura 8, que é o ciclo da resposta a incidentes.

- Preparação;
- Detetar Incidentes;
- Investigar Incidentes;
- Mitigar incidentes;
- Realizar tarefas técnicas na resposta a incidentes.

Figura 8 - Ciclo de vida de resposta de incidentes

4.7.1.2 Departamento Tecnológico

Atualmente nenhum software ou serviço é completamente seguro, sendo que todos os dias vários bugs de software e más configurações de serviços são conhecidas, devido a estas situações, é necessário ter uma equipa que esteja devidamente ligada às tarefas de manutenção de serviços e software.

Sendo assim, o departamento tecnológico trata de executar tarefas relacionadas com a manutenção de serviços, bem como, o software que é desenvolvido pela própria organização de forma a mitigar riscos e resolver incidentes.

Quando existe um incidente e o problema em questão está relacionado com a manutenção de serviços / *software*, o responsável pelo departamento deverá ser informado, que por sua vez, o mesmo delegará a tarefa de correção ou o mesmo irá proceder à mitigação do incidente o mais rapidamente possível.

Funções do departamento:

- Manutenção de serviços / *software*;
- Auxiliar na identificação de vulnerabilidades a fim de mitigar o incidente;
- Auxiliar a equipa de CSIRT em tarefas técnicas de engenharia;
- Mitigação de vulnerabilidades.

4.7.1.3 Administração / Direção

A administração deverá ter conhecimento de um incidente independentemente dos conhecimentos técnicos dos mesmos. Sendo que a administração deverá ser informada sobre o mesmo e também dará a tomada de decisão em tarefas que têm impacto direto ao negócio e é necessária autorização superior.

Funções do departamento:

- Auxiliar tomadas de decisões críticas para o negócio.

4.7.1.4 Serviços Jurídicos

O departamento jurídico ao qual também pertence à administração, trata de todo o tipo de tarefas relacionadas com serviços jurídicos. No caso de ocorrer um incidente, é necessário que exista uma comunicação do mesmo às entidades competentes.

Este mesmo departamento, trata de todas as burocracias necessárias, para que exista uma comunicação clara e rápida entre as entidades competentes, e as mesmas fiquem com o conhecimento do incidente que está a acontecer.

No caso de existência de acesso a dados, é necessário validar e enviar essa mesma informação às entidades competentes.

Funções do departamento:

- Reportar de forma clara e rápida o Incidente às entidades competentes;
- Tratar da burocracia relacionada com o Incidente;

4.7.1.5 Relações públicas

O departamento das relações públicas tem como objetivo lidar com toda a comunicação que é feita aos clientes.

No caso de existir um incidente em que a informação dos clientes foi disponibilizada sem autorização a um desconhecido, a mesma deverá ser comunicada ao cliente obrigatoriamente, de forma que a perda de credibilidade da organização não seja tão significativa.

Além disso, sempre que existir ataques conhecidos aos clientes, os mesmos devem ser alertados para esses mesmos ataques, de forma que os clientes fiquem em modo alerta.

Funções do departamento:

- Comunicar aos clientes sempre que sua informação for acedida por terceiros não autorizada;
- Comunicar de forma oficial o incidente que afete dados dos clientes, de forma a não existir uma perda de credibilidade tão grande;
- Alertar os clientes em caso de ataques redirecionados diretamente aos clientes.

4.7.2 Contactos

Nesta Tabela 8 indica-se os contactos agrupados pelos vários departamentos, que têm um papel significativo na resposta a incidentes.

Como é mostrado na tabela em baixo, estes contactos não são pessoais, estes mesmos são contactos de grupo, isto é, se for enviado um email para o departamento jurídico, só os funcionários associados ao jurídico é que vão receber esse email, desta forma a comunicação por departamento fica mais organizada e claro, vai permitir também minimizar o tempo de resposta a incidentes.

Departamento	Contacto
CSIRT	csirt@hrv.pt
Departamento Tecnológico	dtech@hrv.pt
Administração	admin@hrv.pt
Serviços Jurídicos	juridico@hrv.pt
Relações Públicas	rp@hrv.pt

Tabela 8 - Contactos

4.7.3 Exemplo de cenários de incidentes

Neste documento descrevem-se alguns cenários de exemplo de forma a auxiliar a interpretação dos fluxos de comunicação entre os vários departamentos, de modo a compreender e a facilitar no futuro a comunicação eficiente em caso de incidente.

Os vários incidentes aqui descritos são apenas simulados, tanto que os incidentes reais podem ter algumas variações, mas de um modo geral não deve ser muito diferente do que vai ser elaborado aqui no documento.

Os cenários escolhidos são exemplos de incidentes que podem acontecer na organização, sendo que se torna impossível descrever todos os cenários de incidente que podem ocorrer.

a. Deteção de *Phishing*

Neste primeiro exemplo, deparamo-nos com o facto da organização estar a receber emails de *phishing*, sendo que esses emails foram recebidos pelos funcionários da organização, sendo um ataque de engenharia social dirigido à organização. No entanto, não se sabe se estes mesmos emails estão a ser enviados para clientes.

Nos emails de *phishing*, o atacante envia um link malicioso onde o mesmo tem um formulário a pedir a autenticação usando o email e a password, no entanto, nesse mesmo email contém um pdf malicioso.

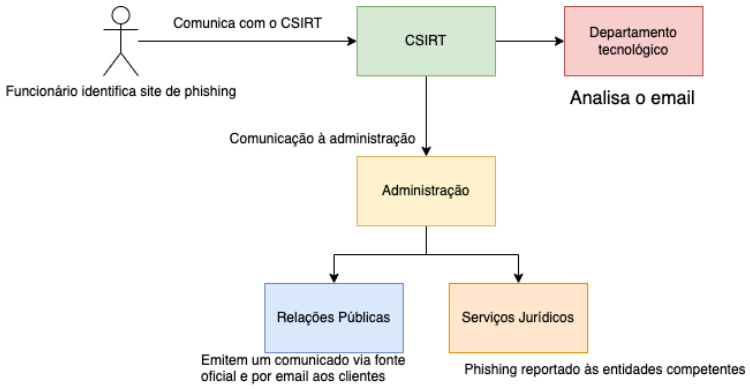


Figura 9 - Cenário de comunicação de phishing

Neste cenário o que se descreve aqui através da Figura 9, é o facto de um funcionário da organização ter detetado um email de *phishing*, pois o mesmo tem uma origem um pouco duvidosa e o sistema de filtragem de spam não foi capaz de o detetar como spam.

No seguimento, esse funcionário comunica com o CSIRT de forma a alertar sobre o email de phishing, sendo que o CSIRT envia essa mesma informação ao departamento técnico de forma a melhorar as regras para deteção de spam (phishing).

Ao mesmo tempo o CSIRT, comunica à administração, que por sua vez irá comunicar aos serviços jurídicos para reportar esse mesmo problema às autoridades competentes.

De forma a minimizar o impacto com os clientes, o departamento de relações-públicas irá criar um comunicado no website e enviar um email aos clientes alertando para um possível ataque de *phishing*.

b. Exploração de vulnerabilidade

Neste cenário descreve-se um ataque de uma vulnerabilidade conhecida pelo atacante e o *exploit* encontra-se na internet de forma a explorar e ganhar acesso aos dados da organização e dos clientes.

Este cenário, mostra um serviço que se encontra desatualizado e o mesmo não foi atualizado quando a correção da vulnerabilidade foi disponibilizada.

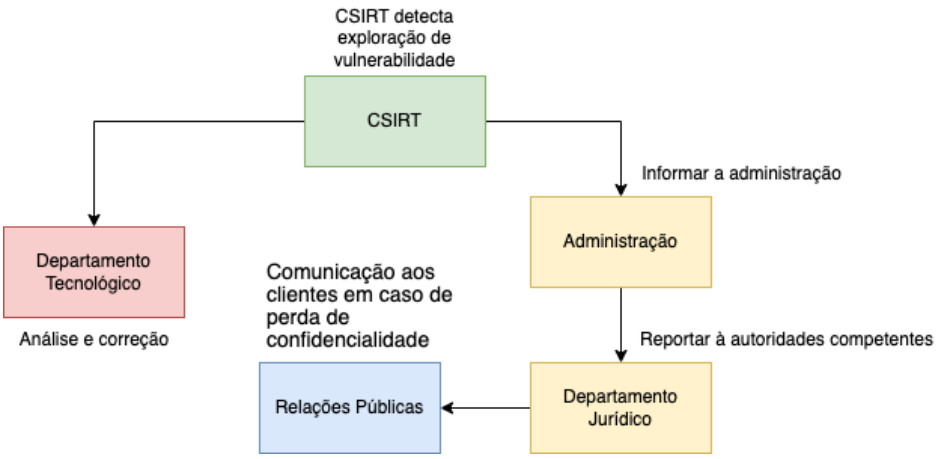


Figura 10 - Exploração de vulnerabilidade

O departamento CSIRT deteta uma exploração de vulnerabilidade, onde os mesmos vão analisar que tipo de serviço ou aplicação foi afetada. Após terem esta informação, a administração irá ser contactada de forma a ficarem informados e comunicarem por sua vez a intrusão na organização.

Ao mesmo tempo, o departamento técnico irá ser alertado sobre a intrusão e irá receber um relatório dos serviços que foram afetados. Após a análise desse relatório, irá ser verificado se o serviço é ou desenvolvido dentro da organização. Se for feito na organização é aplicado um *patch* de segurança de forma a resolver a falha. Se for um serviço externo, é necessário recorrer ao sistema de atualizações de forma a verificar se a falha já se encontra resolvida por parte do fabricante.

Durante este processo, em paralelo, o departamento jurídico irá reportar essa mesma intrusão às autoridades competentes. Em caso de existir acesso aos dados dos clientes, o departamento de relações públicas deverá ser alertado de forma que o mesmo alerte os clientes da organização.

c. Ataque de negação de Serviço

Um cenário de ataque de negação de serviço, é um ataque bastante popular e muitas das vezes o mesmo faz com que as organizações tenham perda de lucro, pois a dimensão do ataque pode ser de tal forma que os serviços não irão conseguir responder a todos os pedidos.

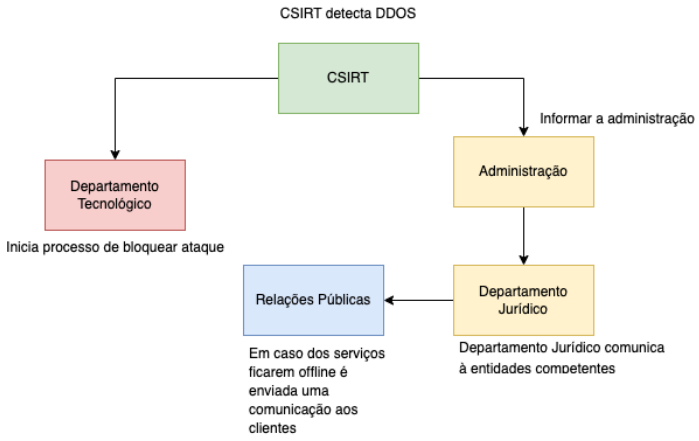


Figura 11 - Ataque DDOS

Nesta situação, um ataque de negação de serviço foi detetado pelo CSIRT, este mesmo, irá ser comunicado ao Departamento tecnológico, e em conjunto tentam bloquear o ataque de forma a prevenir que o sistema fique indisponível para os clientes.

Por sua vez o departamento administrativo irá ser notificado sobre o ataque DDOS, sendo que o mesmo irá ser reportado ao Departamento jurídico para ser devidamente comunicado às autoridades competentes.

No caso de o sistema ficar indisponível para os clientes, o departamento de relações publicas irá comunicar com os clientes através de email no caso dos seus serviços estarem indisponíveis há mais de 20 minutos.

4.8 Processo de resposta a incidentes

O processo de resposta a incidentes é um processo que descreve as ações que as várias equipas dentro da organização devem seguir para lidar com um incidente de segurança.

Como já mostrado na Figura 8, o ciclo de vida de um incidente já se encontra definido de uma forma muito generalizada, o mesmo é aplicado seguindo as seguintes fases, preparação, deteção e análise, contenção e atividade pós incidente, isto permite minimizar o tempo de resposta a um incidente e também os respetivos danos na organização.

Na continuação deste capítulo, abordaremos o ciclo de resposta a incidentes, descendo a um nível menos abstrato, de forma a se enquadrar com a própria organização.

4.8.1 Ciclo de vida

Tal como já abordado em cima, todos os planos de resposta a incidentes seguem várias metodologias, sendo que variam um pouco consoante as organizações, o mesmo plano é variável de forma que fique completamente ajustado aos requisitos da organização.

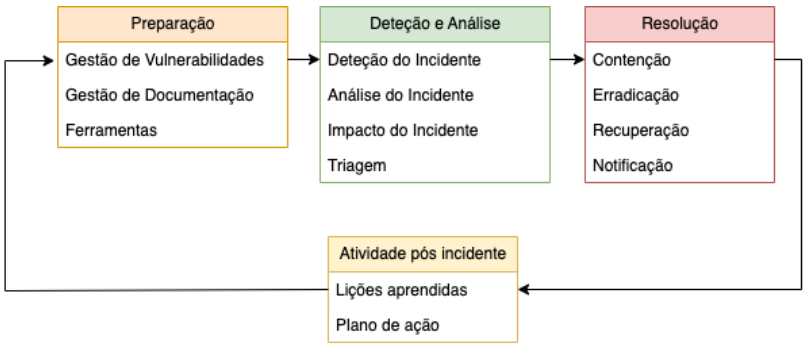


Figura 12 - Ciclo de vida resposta a incidentes da HRV

4.8.1.1 Preparação

A preparação é um dos passos do ciclo de resposta a incidentes, neste passo, a equipa de CSIRT em conjunto com a equipa técnica, desenvolvem mecanismos de gestão de vulnerabilidades bem com a própria documentação a usar em caso de existir um incidente.

O objetivo desta fase é manter o ambiente da organização seguro, sendo que a equipa de CSIRT tem uma visão geral do sistema/serviços que a organização utiliza e os mesmos estão suficientemente seguros.

Nesta fase normalmente também são adquiridas e utilizadas ferramentas de forma a testar o sistema como se tratasse de um ataque real, isto desta forma previne alguns incidentes que possam vir a acontecer.

4.8.1.2 Deteção e Análise

Esta é uma das fases mais importantes no ciclo de resposta a incidentes.

A equipa responsável nesta fase é a CSIRT, pois a mesma implementa os mecanismos de monitorização e de deteção, de forma que os incidentes sejam detetados o mais rapidamente possível.

No caso de se detetar um incidente, a equipa trata de fazer uma primeira análise ao mesmo, de forma a analisar o impacto que o incidente teve para a organização de uma forma mais superficial.

Após essa análise, é feito um levantamento do impacto que o mesmo está a causar, sendo que o impacto do incidente está dividido em dois grupos, funcional e de informações.

- **O impacto funcional**, são todos os incidentes que têm impacto com o funcionamento da organização, sendo que se comprometer o funcionamento normal da organização, este incidente deve ser tratado o mais rapidamente possível.
- **O impacto de informações**, são todos os incidentes onde é conhecido que existiu acesso a informações da organização por uma terceira pessoa não autorizada.

Após verificar o impacto, é feita a triagem do incidente, para conhecer se o mesmo têm prioridade ou não comparativamente a outros incidentes.

4.8.1.3 Resolução

A resolução é a fase mais importante do ciclo de resposta a incidentes, a mesma é gerida pela equipa técnica, sendo que já tem um relatório superficial do incidente por parte da equipa de CSIRT.

Nesta mesma fase, faz-se uma análise profunda sobre o incidente e faz-se também a contenção do incidente, isto é, evitar que o incidente se espalhe por outras áreas da organização. Por exemplo, se a organização for alvo de *malware*, é necessário bloquear as ligações a essa máquina de forma a isolá-la o mais rapidamente possível.

Além disso, começa a ser feito o processo de mitigação do incidente, pois, neste passo, são efetuadas ações para garantir a continuidade dos processos de negócio, eliminando de vez o problema causado no incidente.

Após a eliminação, inicia-se o processo de restauro das máquinas afetadas, e por sua vez, a recuperação dos dados, onde se analisa os dados perdidos e como é que podem ser recuperados.

No final, e paralelamente à tarefa de recuperação, verifica-se se é necessário realizar tarefas de comunicação aos clientes afetados, no caso de ser necessário, é feita uma comunicação ao departamento de Relações Públicas a fim de estes enviarem a comunicação aos clientes afetados.

Não obstante, o departamento jurídico, envia a comunicação do incidente para as autoridades competentes de forma a ir ao encontro da Lei.

4.8.1.4 Atividade Pós incidente

Nesta fase, o incidente deverá ter sido mitigado e todos os serviços restaurados devidamente.

A equipa de resposta a incidentes avalia os resultados obtidos de modo a garantir que o mesmo não volta a acontecer.

Durante esta fase, inicia-se o processo de documentação, isto é, todos os procedimentos efetuados têm de ser documentados para uma análise futura em caso de ocorrer o mesmo ataque ou um similar.

Com base nesta documentação, voltamos ao passo inicial “preparação”, onde se aplicam melhorias no plano de resposta a incidentes.

Este acaba por ser um processo cíclico, pois o mesmo está em melhoria contínua, pois, todos os dias surgem novos e diferentes tipos de incidentes, então a melhoria contínua do processo irá sempre acontecer.

4.9 Definição dos níveis de severidade dos incidentes e sua triagem

No decorrer da deteção de incidentes de segurança, esses incidentes deverão ser agrupados por tipo de incidente e classificados com um nível de impacto para assim ser possível fazer uma triagem e priorização mais rápida e eficiente.

Assim é necessário haver uma classificação com base de um cálculo e uma definição da severidade de um incidente de segurança, como objetivo no decorrer de uma deteção de um incidente de segurança com valor de classificação que não seja definido por um ponto de vista de um elemento da equipa CSIRT, mas sim a classificação seja definida por um processo. Contudo é necessário ter em conta que não deverá haver mais de quatro níveis de severidade de forma que não dificulte a classificação e periodização dos incidentes de segurança.

Assim sendo, na Tabela 9**Erro! A origem da referência não foi encontrada.** encontra-se os tipos de incidente, a sua respetiva classificação, um exemplo e o seu valor numérico, sendo necessário mais tarde para classificar a severidade de um incidente.

Foram definidos dez critérios que definem a severidade de um incidente de segurança, também atribuído um valor compreendido entre um e três, assim sendo o valor um represente o valor menos severo e o três o mais grave.

ID	Tipo de incidente	Classificação	Exemplo	Valor
1	Impacto na reputação	Alta	Divulgados documentos classificados	3
		Média	Divulgados parcialmente documentos sem relevo	2
		Baixa	Não foram Divulgados documentos	1
2	Impacto nos clientes	Alta	Paragem total da produção	3
		Média	Paragem parcial da produção	2
		Baixa	Sem paragem na produção	1
3	Impacto nos funcionários	Alta	Paragem total dos serviços administrativos	3
		Média	Paragem parcial dos serviços administrativos	2
		Baixa	Sem paragem dos serviços administrativos	1
4	Informações dos clientes	Alta	Divulgados documentos classificados dos clientes	3
		Média	Divulgados parcialmente documentos classificados dos clientes	2
		Baixa	Não foram divulgados documentos classificados dos clientes	1
5	Informações dos funcionários	Alta	Divulgados documentos classificados dos funcionários	3
		Média	Divulgados parcialmente documentos classificados dos funcionários	2

		Baixa	Não foram divulgados documentos classificados dos funcionários	1
6	Horas necessárias para a resolução de um incidente de segurança	Alta	Mais de 40 horas	3
		Média	Até 40 horas	2
		Baixa	Menos de 40 horas	1
7	Recursos necessários para a resolução de um incidente de segurança	Alta	A equipa CSIRT necessita de suporte de várias entidades externas	3
		Média	A equipa CSIRT necessita de suporte de uma entidade externa	2
		Baixa	A equipa CSIRT tem os recursos necessários para resolver internamente	1
8	Volume de clientes afetados por um incidente de segurança	Alta	Mais de 25% dos clientes afetados	3
		Média	Entre 5% a 25% dos clientes afetados	2
		Baixa	Menos 5% dos clientes afetados	1
9	Volume de funcionários afetados por um incidente de segurança	Alta	Mais de 25% dos clientes afetados	3
		Média	Entre 5% a 25% dos clientes afetados	2
		Baixa	Menos 5% dos clientes afetados	1
10	Impacto nas atividades e tarefas que são realizadas pelos funcionários durante um incidente de segurança	Alta	Serviços inoperacionais, não é possível utilizar processos ou realizar atividades relacionadas com atividade normal da empresa	3
		Média	Afetação parcial dos serviços, sendo possível utilizar processos ou realizar atividades relacionadas com atividade normais da empresa	2
		Baixa	Sem afetação dos serviços, sendo possível a realização das atividades da empresa com normalidade	1

Tabela 9 - Critérios para a definição da severidade de um incidente de segurança

Recorrendo à Tabela 9 para encontrar a escala de classificação de um incidente, fazendo o somatório de cada classificação por tipo de incidente encontra-se o critério de severidade, sendo que o valor é compreendido entre dez e trinta, onde o valor de dez é o menos impacto e o valor de trinta o mais impacto e que vai requer a atenção imediata pela equipa CSIRT, sendo que estas classificações deveram serem revistas periodicamente.

Foi elaborado a Tabela 10 em que representa a escala, classificação e o respetivo nível de classificação.

Escala	**Classificação**	**Nível**	**Descrição**
26-30	Critico	Severidade 4	Impacto critico, requer tratamento imediato
19-25	Alta	Severidade 3	Alto impacto, requer atenção elevada
16-18	Média	Severidade 2	Medio impacto
10-15	Baixa	Severidade 1	Baixo ou inexistente impacto

Tabela 10 - Escala de classificação

4.10 Plano e matriz de comunicação e de escalonamento

Um plano de comunicação é uma componente importante de uma estratégia abrangente de gestão de incidentes de cibersegurança. Ela ajuda a garantir uma resposta eficaz, coordenada e transparente durante e após um incidente.

Neste plano de comunicação de resposta a incidentes será descrita como a comunicação será gerida durante um incidente de cibersegurança. Serão definidas as diretrizes, responsabilidades e procedimentos relacionados com a comunicação interna e externa. O plano inclui informações sobre como relatar um incidente, quem deve ser notificado, qual é o fluxo de comunicação interna entre as equipas de resposta, como as atualizações serão partilhadas com partes interessadas externas, como clientes, acionistas, autoridades reguladoras, entre outros.

1. Lista detalhada de contatos de emergência

Lista de Contactos de Emergência		
Nome	**Cargo**	**Contacto**
Pedro Marques	Responsável IT	964 299 029
		pedro.marques@hrv.pt
Bruno Silva	Admin. Sistemas	964 998 017
		bruno.silva@hrv.pt
Vitalino Carvalho	Administração / Operações	966 597 291
		vitalino@hrv.pt
Hélia Verissimo	Administração / Dep.to Jurídico	966 781 561
		helia@hrv.pt
Joana Pedrosa	Responsável RH / Comunicação	924 128 970
		joana.pedrosa@hrv.pt

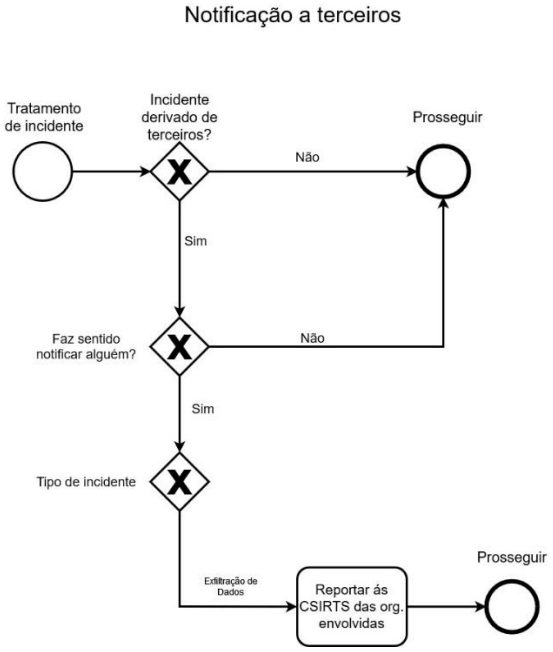
2. Partes Interessadas

Designação	**Canal Preferencial**
Funcionários	Email / Telefone
Clientes	Email / Telefone
Fornecedores	Email / Telefone
Prestadores de Serviços	Email / Telefone

3. Processo de Comunicação Interna

Classificação do Incidente	**Equipa a Notificar**	**Canal Preferencial**
Crítico	Responsável IT/CSIRT / Administração / Dep.to Jurídico	Telefone / Email
Alta	Responsável IT/CSIRT / Administração / Dep.to Jurídico	Telefone / Email
Média	Responsável IT / CSIRT	Telefone / Email
Baixa	Responsável IT / CSIRT	Telefone / Email

4. Processo de Comunicação Externa



O reporte às CSIRTS das organizações envolvidas será da responsabilidade das equipas de Responsável RH / Comunicação coordenada com a equipa de Administração / Dep.to Jurídico.

4.11 Tipos de incidentes e determinar os playbooks

Num plano de resposta a incidentes no qual são identificados e classificados os incidentes, surge a necessidade de definir os passos a seguir para a resolução/mitigação do problema. Num momento em que o tempo de resposta é imperativo, a definição de ações e das equipas responsáveis por essas ações é crucial para evitar a propagação e/ou comprometimento de sistemas contíguos. Na tabela abaixo são identificadas as principais ameaças e sua descrição. No capítulo 4.12 são apresentados os *playbooks* detalhados para cada uma das ameaças identificadas.

Tipo de Incidente / Playbook	Descrição
DDoS	Ataque que visa colocar os serviços indisponíveis
Malware	Infeção dos Sistemas Recorrendo a Código Malicioso
Exfiltração de Dados/ Violação de Dados	Recolha Ilícita de Dados por Parte do Atacante
Intrusão/Acesso Não Autorizado	Intrusão do sistema através da exploração de vulnerabilidades
Phishing	Obtenção de Informações Confidenciais
Engenharia Social	Manipulação Psicológica para obtenção de informações confidenciais
Injeção de Código	Injeção de código maliciosos em aplicações cujo objetivo é a exploração de uma vulnerabilidade
Outros	Tipo de Incidente Não Especificado

4.12 Playbooks

Playbooks das Ameaças Identificadas:

Palybook Malware[1]

Fase Preparação		
Objetivos	• Preparar resposta a incidente. • Sensibilizar colaboradores da organização.	
Atividade	Descrição	Equipa Envolvida
Preparação para a Resposta	• Implementar soluções anti-malware • Garantir backups para repositórios diferentes dos que alojam os dados • Não permitir instalação de software pelos colaboradores.	IT
	• Analisar incidentes recentes e sua resolução.	IT/CSIRT
	• Rever os procedimentos de responsabilidade, • escalonamento e gestão dos mesmos para que • quando existir um incidente, estarem preparados	IT/CSIRT
	• Manter diagrama da rede	IT/CSIRT
	• Definir e identificar o risco, a ameaça e o alerta com a solução SIEM – Security Onion	IT/CSIRT
Formação dos colaboradores	• Realizar ações de formação para sensibilizar os colaboradores sobre os riscos que podem ocorrer e cuidados a ter	IT/CSIRT

Identificação da Ameaça		
Objetivos	• Detetar e reportar falhas que comprometam a confidencialidade, integridade e disponibilidade dos dados • Reportar formalmente o *malware* para as equipas correspondentes de incidentes de cibersegurança.	
Atividade	Descrição	Equipa Envolvida
Detetar/Reportar Incidente	• Monitorização de eventos de rede • Utilização de SIEM – Security Onion • Gestão de Eventos e Alertas	IT/CSIRT
	• Criação de Ticket para Seguimento/Escalonamento	IT
	• Verificar se Existiu Perda ou fuga de Dados	IT/CSIRT/Dpto Juridico
	• Identificar Necessidade de Comunicação com Terceiros	IT/CSIRT/Comunicação
	• Classificar Incidente	CSIRT
Investigação do Incidente	• Documentar ações realizadas pelo malware	IT/CSIRT
	• Manter cópias dos indicios do incidente para posteriores análises forenses	IT/CSIRT

[1] Diagrama do Playbook em anexo - anexo_Playbook_Malware.pdf

Fase De Análise		
Objetivos	• Analisar Incidente • Identificar e Reportar Comportamentos • Definir Linhas da Investigação Forense	
Atividade	Descrição	Equipa Envolvida
Analisar Incidente	• Verificar Analise da Ferramenta que Detetou o Malware	IT/CSIRT
	• Análise de Código do Malware para perceber as suas interações e o seu comportamento	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT

Fase De Contenção / Erradicação da Ameaça		
Objetivos	• Conter a Ameaça • Isolar Aplicações / Sistemas Comprometidos • Remoção do Agente malicioso	
Atividade	Descrição	Equipa Envolvida
Contenção	• Verificar Analise da Ferramenta que Detetou o Malware	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT
Erradicação	• Remoção do Agente Malicioso de Todos os Sistemas	IT/CSIRT

Fase De Recuperação e Restauro		
Objetivos	• Restaurar Serviços e Sistemas Afetados	
Atividade	Descrição	Equipa Envolvida
Reposição De Sistemas	• Verificar Analise da Ferramenta que Detetou o Malware	IT/CSIRT
	• Reposição dos Sistemas Afetados	IT
	• Reposição de Backups	IT
	• Monitorização das Áreas Afetadas para Garantir que Não Existe Reincidência.	IT/CSIRT
Monitorização	• Garantir Monitorização de Todo o Sistema	IT/CSIRT

Fase Pós-Incidente		
Objetivos	• Criação de Relatórios Detalhados do Incidente • Discussão do Incidente Inter Equipas • Correções a Aplicar ao Sistema	
Atividade	Descrição	Equipa Envolvida
Avaliação	• Elavoração de Relatório Detalhado	IT/CSIRT
	• Avaliação de KPI do Processo	IT/CSIRT
	• Análise do Processo e Definição de Melhorias	IT/CSIRT

Playbook Phishing[2]

Fase Preparação		
Objetivos	• Preparar resposta a incidente. • Sensibilizar colaboradores da organização.	
Atividade	Descrição	Equipa Envolvida
Preparação para a Resposta	• Garantir backups para repositórios diferentes dos que alojam os dados • Não permitir instalação de software pelos colaboradores.	IT
	• Analisar incidentes recentes e sua resolução.	IT
	• Rever os procedimentos de responsabilidade, • escalonamento e gestão dos mesmos para que • quando existir um incidente, estarem preparados	IT/CSIRT
	• Manter diagrama da rede	IT/CSIRT
	• Definir e identificar o risco, a ameaça e o alerta com a solução SIEM – Security Onion	IT/CSIRT
Formação dos colaboradores	• Realizar ações de formação para sensibilizar os colaboradores sobre os riscos que podem ocorrer e cuidados a ter	IT/CSIRT

Identificação da Ameaça		
Objetivos	• Detetar e reportar falhas que comprometam a confidencialidade, integridade e disponibilidade dos dados • Reportar formalmente o *Phishing* para as equipas correspondentes de incidentes de cibersegurança.	
Atividade	Descrição	Equipa Envolvida
Detetar/Reportar Incidente	• Monitorização de eventos de rede • Utilização de SIEM – Security Onion • Gestão de Eventos e Alertas	IT/CSIRT
	• Criação de Ticket para Seguimento/Escalonamento	IT/CSIRT
	• Verificar se Existiu Perda ou fuga de Dados	IT/CSIRT/Dpto Juridico
	• Identificar Necessidade de Comunicação com Terceiros	IT/CSIRT/Comunicação
	• Classificar Incidente	IT/CSIRT
Investigação do Incidente	• Documentar ações realizadas pelo Phishing	IT/CSIRT
	• Manter cópias dos indícios do incidente para posteriores análises forenses	IT/CSIRT

Fase De Análise		
Objetivos	• Analisar Incidente • Identificar e Reportar Comportamentos • Definir Linhas da Investigação Forense	
Atividade	Descrição	Equipa Envolvida

[2] Diagrama do Playbook em anexo - anexo_Playbook_Phishing.pdf

Analisar Incidente	• Verificar Analise da Ferramenta que Detetou o Phishing	IT/CSIRT
	• Análise da Fonte do Phishing para perceber as suas interações e o seu comportamento	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT

Fase De Contenção / Erradicação da Ameaça		
Objetivos	• Conter a Ameaça • Isolar Aplicações / Sistemas Comprometidos • Remoção do Agente malicioso	
Atividade	Descrição	Equipa Envolvida
Contenção	• Verificar Analise da Ferramenta que Detetou o Phishing	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT
Erradicação	• Remoção do Agente Malicioso de Todos os Sistemas	IT

Fase De Recuperação e Restauro		
Objetivos	• Restaurar Serviços e Sistemas Afetados	
Atividade	Descrição	Equipa Envolvida
Reposição De Sistemas	• Verificar Analise da Ferramenta que Detetou o Phishing	IT/CSIRT
	• Reposição dos Sistemas Afetados	IT
	• Reposição de Backups	IT
	• Monitorização das Áreas Afetadas para Garantir que Não Existe Reincidência.	IT/CSIRT
Monitorização	• Garantir Monitorização de Todo o Sistema	IT/CSIRT

Fase Pós-Incidente		
Objetivos	• Criação de Relatórios Detalhados do Incidente • Discussão do Incidente Inter Equipas • Correções a Aplicar ao Sistema	
Atividade	Descrição	Equipa Envolvida
Avaliação	• Elavoração de Relatório Detalhado	IT/CSIRT
	• Avaliação de KPI do Processo	IT/CSIRT
	• Análise do Processo e Definição de Melhorias	IT/CSIRT

Playbook DDoS[3]

Fase Preparação		
Objetivos	• Preparar resposta a incidente.	
Atividade	Descrição	Equipa Envolvida
	• Garantir backups para repositórios diferentes dos que alojam os dados	IT
	• Analisar incidentes recentes e sua resolução.	IT/CSIRT

[3] Diagrama do Playbook em anexo - anexo_Playbook_DDoS.pdf

Preparação para a Resposta	• Rever os procedimentos de responsabilidade, escalonamento e gestão dos mesmos para que quando existir um incidente, estarem preparados	IT/CSIRT
	• Manter diagrama da rede	IT/CSIRT
	• Definir e identificar o risco, a ameaça e o alerta com a solução SIEM – Security Onion • Definir e identificar o risco, a ameaça com Firewall / IPS	IT/CSIRT

Identificação da Ameaça		
Objetivos	• Detetar e reportar falhas de Indisponibilidade de Serviço • Reportar formalmente o DDoS para as equipas correspondentes de incidentes de cibersegurança.	
Atividade	Descrição	Equipa Envolvida
Detetar/Reportar Incidente	• Monitorização de eventos de rede • Utilização de SIEM – Security Onion • Gestão de Eventos e Alertas	IT/CSIRT
	• Criação de Ticket para Seguimento/Escalonamento	IT/CSIRT
	• Verificar se Existe Indisponibilidade dos Serviços	IT/CSIRT
	• Identificar Necessidade de Comunicação com Terceiros	IT/CSIRT/Comunicação
	• Classificar Incidente	IT/CSIRT
Investigação do Incidente	• Documentar ações realizadas pelo DDoS	IT/CSIRT
	• Manter cópias dos indícios do incidente para posteriores análises forenses	IT/CSIRT

Fase De Análise		
Objetivos	• Analisar Incidente • Identificar e Reportar Comportamentos • Definir Linhas da Investigação Forense	
Atividade	Descrição	Equipa Envolvida
Analisar Incidente	• Verificar Analise da Ferramenta que Detetou o DDoS	IT/CSIRT
	• Análise da Fonte do DDoS para perceber eventuais Reincidências	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT

Fase De Contenção / Erradicação da Ameaça		
Objetivos	• Conter a Ameaça • Isolar Serviços Comprometidos	
Atividade	Descrição	Equipa Envolvida
Contenção	• Verificar Analise da Ferramenta que Detetou o DDoS	IT/CSIRT
	• Avaliar Eventual Desligamento de Serviços	IT/CSIRT
Erradicação	• Documentar os Resultados • Bloqueio da Fonte do DDoS	IT/CSIRT
Fase De Recuperação e Restauro		

Objetivos	• Restaurar Serviços e Sistemas Afetados	
Atividade	Descrição	Equipa Envolvida
Reposição De Sistemas	• Verificar Analise da Ferramenta que Detetou o DDoS	IT/CSIRT
	• Reposição dos Sistemas Afetados	IT/CSIRT
	• Reposição de Backups	IT
	• Monitorização das Áreas Afetadas para Garantir que Não Existe Reincidência.	IT/CSIRT
Monitorização	• Garantir Monitorização de Todo o Sistema	IT/CSIRT

Fase Pós-Incidente		
Objetivos	• Criação de Relatórios Detalhados do Incidente • Discussão do Incidente Inter Equipas • Correções a Aplicar ao Sistema	
Atividade	Descrição	Equipa Envolvida
Avaliação	• Elavoração de Relatório Detalhado	IT/CSIRT
	• Avaliação de KPI do Processo	IT/CSIRT
	• Análise do Processo e Definição de Melhorias	IT/CSIRT

Playbook Exfiltração de Dados/ Violação de Dados – Intrusão / Acesso Ilegítimo[4]

Fase Preparação		
Objetivos	• Preparar resposta a incidente. • Sensibilizar colaboradores da organização.	
Atividade	Descrição	Equipa Envolvida
Preparação para a Resposta	• Implementar soluções Intrusão • Garantir backups para repositórios diferentes dos que alojam os dados • Não permitir instalação de software pelos colaboradores.	IT
	• Analisar incidentes recentes e sua resolução.	IT/CSIRT
	• Rever os procedimentos de responsabilidade, • escalonamento e gestão dos mesmos para que • quando existir um incidente, estarem preparados	IT/CSIRT
	• Manter diagrama da rede	IT/CSIRT
	• Definir e identificar o risco, a ameaça e o alerta com a solução SIEM – Security Onion	IT/CSIRT
Formação dos colaboradores	• Realizar ações de formação para sensibilizar os colaboradores sobre os riscos que podem ocorrer e cuidados a ter	IT/CSIRT

Identificação da Ameaça	
Objetivos	• Detetar e reportar falhas que comprometam a confidencialidade, integridade e disponibilidade dos dados

[4] Diagrama do Playbook em anexo - anexo_Playbook_ExfiltraçãoDados.pdf

	• Reportar intrusões para as equipas correspondentes de incidentes de cibersegurança.	
Atividade	Descrição	Equipa Envolvida
Detetar/Reportar Incidente	• Monitorização de eventos de rede • Utilização de SIEM – Security Onion • Gestão de Eventos e Alertas	IT/CSIRT
	• Criação de Ticket para Seguimento/Escalonamento	IT/CSIRT
	• Verificar se Existiu Perda ou fuga de Dados	IT/CSIRT/Dto Juridico
	• Identificar Necessidade de Comunicação com Terceiros	IT/CSIRT/Comunicação
	• Classificar Incidente	IT/CSIRT
Investigação do Incidente	• Documentar ações realizadas no âmbito da exfiltração de Dados	IT/CSIRT
	• Manter cópias dos indícios do incidente para posteriores análises forenses	IT/CSIRT

Fase De Análise		
Objetivos	• Analisar Incidente • Identificar e Reportar Comportamentos • Definir Linhas da Investigação Forense	
Atividade	Descrição	Equipa Envolvida
Analisar Incidente	• Verificar Analise da Ferramenta que Detetou a Exfiltração de Dados	IT/CSIRT
	• Perceber as Causas da Exfiltração de Dados	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT

Fase De Contenção / Erradicação da Ameaça		
Objetivos	• Conter a Ameaça • Isolar Aplicações / Sistemas Comprometidos • Remoção do Agente malicioso	
Atividade	Descrição	Equipa Envolvida
Contenção	• Verificar Analise da Ferramenta que Detetou a Exfiltração de Dados	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT
Erradicação	• Remoção do Agente Malicioso de Todos os Sistemas	IT

Fase De Recuperação e Restauro		
Objetivos	• Restaurar Serviços e Sistemas Afetados	
Atividade	Descrição	Equipa Envolvida
Reposição De Sistemas	• Reposição dos Sistemas Afetados	IT
	• Reposição de Backups	IT
	• Monitorização das Áreas Afetadas para Garantir que Não Existe Reincidência.	IT/CSIRT
Monitorização	• Garantir Monitorização de Todo o Sistema	IT/CSIRT

Fase Pós-Incidente		
Objetivos	• Criação de Relatórios Detalhados do Incidente • Discussão do Incidente Inter Equipas • Correções a Aplicar ao Sistema	
Atividade	Descrição	Equipa Envolvida
Avaliação	• Elavoração de Relatório Detalhado	IT/CSIRT
	• Avaliação de KPI do Processo	IT/CSIRT
	• Análise do Processo e Definição de Melhorias	IT/CSIRT

Playbook Injeção de Código[5]

Fase Preparação		
Objetivos	• Preparar resposta a incidente.	
Atividade	Descrição	Equipa Envolvida
Preparação para a Resposta	• Implementar soluções Intrusão • Garantir backups para repositórios diferentes dos que alojam os dados • Adotar medidas preventivas no Desenvolvimento Aplicacional	IT
	• Analisar incidentes recentes e sua resolução.	IT/CSIRT
	• Rever os procedimentos de responsabilidade, • escalonamento e gestão dos mesmos para que • quando existir um incidente, estarem preparados	IT/CSIRT
	• Manter diagrama da rede	IT/CSIRT
	• Definir e identificar o risco, a ameaça e o alerta com a solução SIEM – Security Onion	IT/CSIRT

Identificação da Ameaça		
Objetivos	• Detetar e reportar falhas que comprometam a confidencialidade, integridade e disponibilidade dos dados • Reportar Ameaças.	
Atividade	Descrição	Equipa Envolvida
Detetar/Reportar Incidente	• Monitorização de eventos de rede • Utilização de SIEM – Security Onion • Gestão de Eventos e Alertas	IT/CSIRT
	• Criação de Ticket para Seguimento/Escalonamento	IT/CSIRT
	• Verificar se Existiu Perda ou fuga de Dados	IT
	• Identificar Necessidade de Comunicação com Terceiros	IT/CSIRT/Comunicação
	• Classificar Incidente	IT/CSIRT
Investigação do Incidente	• Documentar ações realizadas no âmbito da injeção de código	IT/CSIRT
	• Manter cópias dos indícios do incidente para posteriores análises forenses	IT/CSIRT

[5] Diagrama do Playbook em anexo - anexo_Playbook_InjecaoCodigo.pdf

Fase De Análise		
Objetivos	• Analisar Incidente • Identificar e Reportar Comportamentos • Definir Linhas da Investigação Forense	
Atividade	Descrição	Equipa Envolvida
Analisar Incidente	• Verificar Analise da Ferramenta que Detetou a injeção de código	IT/CSIRT
	• Perceber as Causas da injeção de código	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT

Fase De Contenção / Erradicação da Ameaça		
Objetivos	• Conter a Ameaça • Isolar Aplicações / Sistemas Comprometidos • Remoção do Agente malicioso	
Atividade	Descrição	Equipa Envolvida
Contenção	• Verificar Analise da Ferramenta que Detetou a injeção de código	IT/CSIRT
	• Documentar os Resultados	IT/CSIRT
Erradicação	• Correção dos Sistemas Afetados	IT/CSIRT

Fase De Recuperação e Restauro		
Objetivos	• Restaurar Serviços e Sistemas Afetados	
Atividade	Descrição	Equipa Envolvida
Reposição De Sistemas	• Reposição dos Sistemas Afetados	IT
	• Reposição de Backups	IT
	• Monitorização das Áreas Afetadas para Garantir que Não Existe Reincidência.	IT/CSIRT
Monitorização	• Garantir Monitorização de Todo o Sistema	IT/CSIRT

Fase Pós-Incidente		
Objetivos	• Criação de Relatórios Detalhados do Incidente • Discussão do Incidente Inter Equipas • Correções a Aplicar ao Sistema	
Atividade	Descrição	Equipa Envolvida
Avaliação	• Elaboração de Relatório Detalhado	IT/CSIRT
	• Avaliação de KPI do Processo	IT/CSIRT
	• Análise do Processo e Definição de Melhorias	IT/CSIRT

4.13 Definição dos processos de comunicação de incidentes por parte da comunidade

Os processos de comunicação de incidentes dentro de uma organização referem-se à forma como os incidentes (problemas, falhas, comprometimento dos dados confidenciais, etc.) são reportados, geridos e comunicados aos responsáveis dentro da organização.

Os principais processos de comunicação de incidentes são:

- **Identificação de incidentes**
  À medida que os incidentes ocorrem, eles têm de ser identificados e registados.

- **Avaliação e classificação de incidentes**
  Cada incidente tem de ser avaliado e classificado para determinar sua gravidade e impacto.

- **Resposta a incidentes**
  Após a avaliação do incidente, a equipa de resposta a incidentes deve ser notificada para analisar e encontrar uma resposta para resolver o problema.

- **Comunicação durante a resposta a incidentes**
  Durante a resolução do incidente, as restantes equipas que estão envolvidas ou as partes interessadas têm de ser notificadas.

- **Notificação de incidente**
  Quando o estado de um incidente for alterado para "reconhecido", as partes interessadas têm de ser notificadas sobre: a causa, gravidade e impacto.

- **Análise de incidentes**
  Após a análise do incidente, é necessário descrever detalhadamente a causa-raíz e planear as melhorias para evitar que o incidente ocorra de novo.

- **Melhoria contínua**
  A organização precisa avaliar regularmente os seus processos de comunicação de incidentes para identificar o que pode ser ainda melhorado.

Desta forma, os processos de comunicação de incidentes dentro de uma organização garantem que os incidentes sejam tratados de maneira eficiente e eficaz, minimizando os seus impactos e melhorando a resiliência da organização.

Comunicação interna

Sempre que um colaborador identificar um incidente de segurança, este terá de o reportar à equipa CSIRT (Equipa de Resposta a Incidentes de Cibersegurança) através da plataforma **glpi.hrv.pt** (portal disponível apenas na rede interna da organização). Cada colaborador tem um acesso dedicado à plataforma.

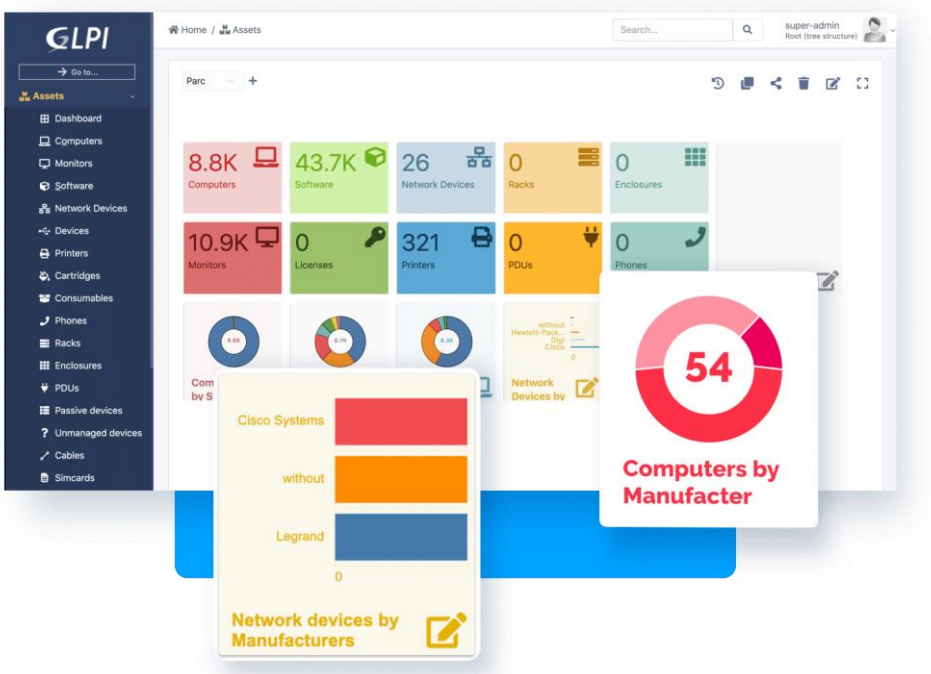


Figura 13 - Plataforma GLPI (Plataforma para reportar incidentes)

Dependendo do tipo de incidente, a informação a reportar difere consoante o tipo de incidente selecionado.

Na tabela abaixo identificamos a informação solicitada por cada tipo de incidente.

Tipo de Incidente	Campos do formulário	Descrição
Website suspeito (phishing)	Endereço	Endereço do website
	Data	Data de acesso ao website
	Informação confidencial	Identificar os dados potencialmente comprometidos
	Como teve conhecimento	Indicar como teve conhecimento da existência do website
	Descrever os passos	Descrever detalhadamente todos os passos realizados e que browser utilizou
	Anexar prova	Anexar uma imagem do conteúdo do website
Email suspeito (phishing)	Endereço	Endereço do email de origem
	Data	Data da receção do email
	Informação confidencial	Identificar os dados potencialmente comprometidos
	Descrever os passos	Descrever detalhadamente todos os passos realizados, após a leitura do email, quando aplicável

	Anexar prova	Anexar uma imagem do conteúdo do email
Malware	Data	Data da identificação do Malware
	Sistema afetado	Identificar o sistema afetado
	Informação confidencial	Identificar os dados potencialmente comprometidos
	Descrever os passos	Descrever detalhadamente todos os passos realizados, antes e após a identificação do malware, quando aplicável
	Ferramenta que identificou	Identificar as ferramentas utilizadas para identificar o incidente, quando aplicável
	Origem	Identificar a origem do incidente, quando conhecido
	Anexar prova	Anexar uma imagem do local do malware
Fuga de informação confidencial	Data	Data da identificação da fuga de informação
	Informação confidencial	Identificar os dados potencialmente comprometidos
	Descrever os passos	Descrição detalhada de como ocorreu o incidente
	Anexar prova	Anexar uma imagem da prova da fuga de informação confidencial
Outros tipos de incidentes	Data	Data da identificação do Incidente
	Sistema afetado	Identificar o sistema afetado.
	Descrição detalhada	Descrição detalhada do comportamento esperado e do comportamento observado
	Descrever os passos	Descrever os passos necessários para reproduzir o problema
	Anexar prova	Anexar imagens que provem o incidente, caso se aplique

Tabela 11 - Tipos de Incidentes (Comunicação Interna)

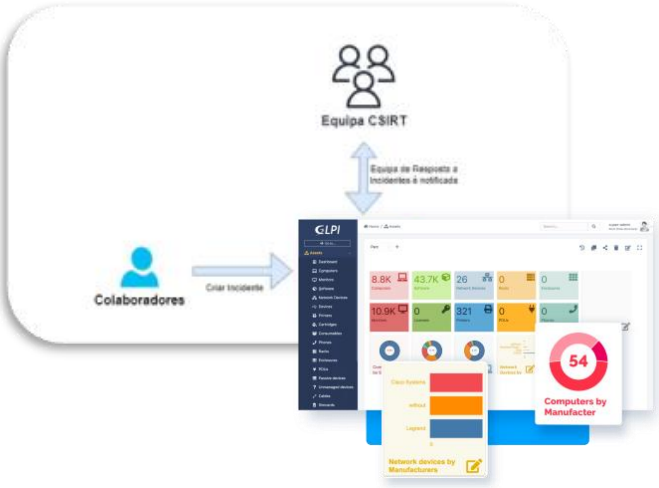


Figura 14 - Processo de comunicação interna de incidentes de segurança

Comunicação externa

Quando se trata de incidentes de segurança identificados por indivíduos ou entidades externas à organização, o meio de comunicação que deve ser utilizado é o email **csirt@hrv.pt**.

Na tabela seguinte é possível identificar que informação deve ser reportada em cada tipo de incidente e também que canal de comunicação deve ser utilizado:

Tabela 12 - Tipos de Incidentes (Comunicação Externa

Tipo de Incidente	O que reportar	Como fazer
Website suspeito (phishing)	Endereço do website	Enviar email para csirt@hrv.pt com o assunto "Notificar Incidente - Externo"
	Data de acesso ao website	
	Identificar os dados potencialmente comprometidos	
	Indicar como teve conhecimento da existência do website	
	Descrever detalhadamente todos os passos realizados e que browser utilizou	
	Anexar uma imagem do conteúdo do website	
Email suspeito (phishing)	Endereço do email de origem e destino	
	Data da receção do email	
	Identificar os dados potencialmente comprometidos	
	Descrever detalhadamente todos os passos realizados, após a leitura do email, quando aplicável	
	Anexar uma imagem do conteúdo do email	
Fuga de informação confidencial	Data da identificação da fuga de informação	
	Identificar os dados potencialmente comprometidos	
	Descrição detalhada de como ocorreu o incidente	
	Anexar uma imagem da prova da fuga de informação confidencial	
Outros tipos de incidentes	Data da identificação do Incidente	
	Identificar o sistema afetado.	
	Descrição detalhada do comportamento esperado e do comportamento observado	
	Descrever os passos necessários para reproduzir o problema	
	Anexar imagens que provem o incidente, caso se aplique	

Nos casos em que os indivíduos ou entidades externas identifiquem incidentes relacionados com a organização HRV, podem consultar o procedimento adotar na página institucional da organização, em www.hrv.pt/reportar-incidente.

A conta de email csirt@hrv.pt está configurada na plataforma GLPI para o próprio sistema criar o tickets automaticamente na plataforma, e alerta a equipa L1 (nível 1) para uma primeira análise e classificação do incidente.

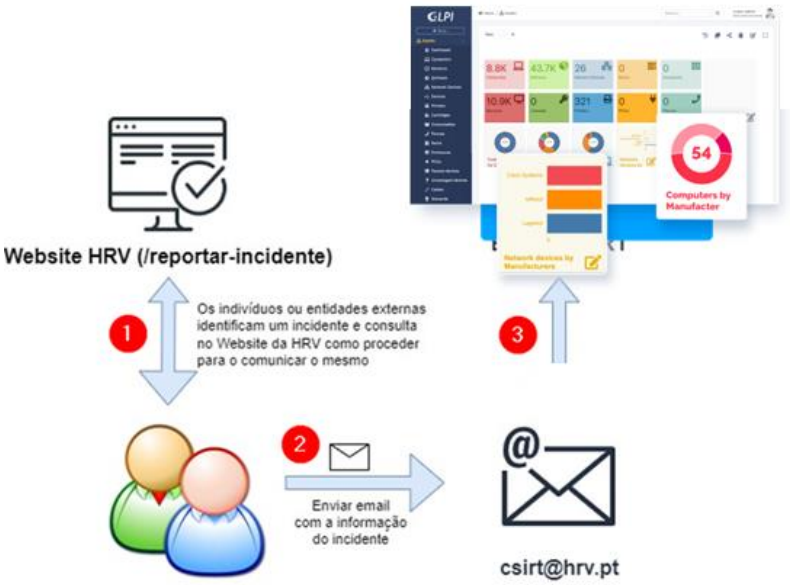


Figura 15 - Processo de comunicação externa de incidentes de segurança

4.14 Definição dos critérios de ativação no PRI:

Para um plano de resposta a incidentes ser plausível, e claro estar de acordo com as normas da organização, é necessário existir critérios para que em caso de incidente não exista perda de negócio para a organização.

Sendo assim, foram definidos dois critérios para a ativação do Plano de resposta a incidentes, sendo eles o Plano de continuidade de Negócio (BCP) e o Plano de Recuperação de Desastres (DRP).

4.14.1 Plano de Continuidade de Negócio

O Plano de Continuidade Negócio (BCP) pode ser descrito de forma sucinta que informa como a empresa vai continuar a operar em caso de uma interrupção das atividades, tanto como de chão de fábrica como a parte do escritório, os processos de negócio, de produção e de logística, os equipamentos, os recursos humanos e os clientes e os parceiros.

Este plano é somente ativado em caso de interrupção da atividade normal da empresa causadas pelas situações seguintes:

- Incidente de segurança que impede o acesso as instalações;
- Interrupção dos serviços afetos ao escritório;
- Interrupção dos serviços afetos ao chão de fábrica;
- Perde de funcionários não esperada;
- Fugas de informação;
- Falhas de segurança críticas;
- Quando existe uma interrupção dos serviços superior a 50%.

Ativação do plano é feita pelo responsável pela equipa CSIRT em articulação com CIO, sendo se possível limitar ao departamento ou departamentos afetados pelo incidente de segurança.

4.14.2 Plano de recuperação de desastres

O plano de Recuperação de Desastres (DRP) é ativa no caso de existir incidentes que comprometam a funcionalidade normal do negócio, isto é, se interromper o serviço nos ativos críticos.

Este mesmo plano é responsável por fornecer instruções detalhadas de forma a restabelecer os serviços/ sistema ao seu estado anterior (funcional), essas mesmas instruções são detalhadas de forma suscita pelo departamento tecnológico.

A ativação do plano é decidida pela equipa responsável por cada sistema /serviço que existe na organização.

No caso de existir múltiplos sistemas comprometidos, e esses mesmos sistemas estiverem dependentes uns dos outros, o *Chief Technology Officer* (CTO) será o responsável por ativar o plano.

Este plano pode ser executado ao mesmo tempo que o Plano de continuidade de negócio.

Quando existe a ativação do plano, e o serviço se encontra indisponível para os clientes, é necessário que a equipa das relações publicas faça um comunicado de forma transparente a comunicar a indisponibilidade do serviço e quando é que se espera os mesmos serviços voltarem ao normal.

Não esquecendo que após a ativação do DRP é necessário rever o Plano de resposta a incidentes e o mesmo deve incorporar as lições aprendidas com o incidente que ocorreu.

4.15 Definição do plano de testes

Para operacionalizar o plano de resposta a incidentes, detetar possíveis erros e analisar eventos com o objetivo de melhoria continua é necessário que se efetuem testes. A bateria de testes deve ter em consideração as ameaças mais significativas e cujo nível de impacto na organização seja elevado. A análise dos resultados dos testes, devidamente documentados para consulta, deve servir o propósito de aplicar correções e melhorias por forma a diminuir o nível de ameaça à qual o sistema está exposto e definir eventuais formações ou sensibilizações aos colaboradores da organização.

Os testes a implementar na HRV seguem o planeamento do quadro abaixo, tendo como premissa a sua revisão anual.

Mês/Incidente	Incidente 1	Incidente 2	Incidente 3	Incidente 4	Incidente 5	Incidente 6
Janeiro						
Fevereiro						
Março						
Abril						
Maio						
Junho						
Julho						
Agosto						
Setembro						
Outubro						
Novembro						
Dezembro						

Incidente 1 – Malware

Incidente 2 - Exfiltração de Dados/ Violação de Dados

Incidente 3 - Intrusão/Acesso Não Autorizado

Incidente 4 - Phising

Incidente 5 - Engenharia Social

Incidente 6 - Injeção de Código

Os testes do Plano de Testes serão realizados mensalmente e por incidente, terão a duração de 60 minutos. Será elaborado um relatório detalhado e discutido pelas equipas.

4.16 Definição do plano de comunicação interna e de formação

4.16.1 Enquadramento

O plano de comunicação interna e formação é um conjunto de estratégias, ações e ferramentas utilizadas pela organização para garantir que os seus colaboradores estão informados e capacitados para desempenhar suas funções de forma eficiente e responsável. A comunicação interna é fundamental para manter uma boa comunicação entre as equipas, para que todos possam trabalhar de forma coordenada, além de facilitar a divulgação de informações importantes dentro da organização. Por outro lado, a formação é essencial para promover o desenvolvimento profissional dos colaboradores e aumentar a produtividade da organização.

Nesse sentido, o plano de comunicação interna e formação deve incluir estratégias para aperfeiçoar a comunicação e a troca de informações entre os líderes (diretores dos vários departamentos) e os respetivos colaboradores, desenvolver programas de treino e capacitação, definir uma política de comunicação interna e criar canais de comunicação acessíveis e eficientes, sejam presenciais ou digitais, para garantir que todas as informações cheguem aos colaboradores de forma rápida e eficiente. O plano também deve considerar a avaliação do desempenho dos colaboradores e a recolha de opiniões regularmente, além de incentivar a comunicação aberta e o diálogo entre todos. Em resumo, o plano de comunicação interna e formação é essencial para garantir o sucesso de uma organização, através da motivação e do desenvolvimento dos seus colaboradores.

4.16.2 Definição de Plano de Comunicação Interna

Um plano de comunicação interna é um documento que estabelece as diretrizes e estratégias para a comunicação dentro de uma organização. Ele tem como objetivo garantir que todas as informações importantes sejam transmitidas de forma clara, eficaz e acessível a todos os colaboradores da organização.

Para elaborar um plano de comunicação interna, é preciso identificar as necessidades da organização em relação à comunicação, definir os canais de comunicação que serão utilizados, estabelecer metas e objetivos, definir as responsabilidades e prazos, elaborar um calendário de comunicação e avaliar constantemente os resultados.

Os canais de comunicação interna podem incluir reuniões presenciais, e-mails, comunicados internos, redes sociais corporativas, entre outros. É importante escolher os canais mais adequados para cada tipo de informação e para o perfil dos colaboradores.

Um plano de comunicação interna eficaz contribui para uma organização mais produtiva e coesa, além de ser fundamental para a construção de uma cultura organizacional forte e saudável.

No caso concreto da empresa HRV, esta atualmente não dispõe de nenhum Plano de Comunicação Interna e de Formação e, é nesse sentido que apresentamos neste tópico, as vantagens, a tecnologias, bem como algumas recomendações e como poderá ser realizada a implementação.

4.16.3 Vantagens de um Plano Comunicação Interna

Existem várias vantagens de um Plano de Comunicação Interna para uma organização, destacamos as seguintes:

- Melhora a comunicação entre as diferentes áreas e hierarquias dentro da organização;
- Orienta as equipas em torno dos objetivos e estratégias da organização, permitindo que todos compreendam qual o rumo a seguir;
- Motiva os colaboradores, aumentando o interesse e consequentemente a produtividade;
- Define uma cultura corporativa forte e coesa, garantindo que os valores e a missão da organização sejam compreendidos e que todos participem;
- Reduz a resistência à mudança, fornecendo informações claras e transparentes para a equipa sobre as mudanças a realizar;
- Melhora a imagem da organização, pois a comunicação clara e efetiva mostra que a organização se preocupa com seus colaboradores e que os mantém informados.
- Mitiga o risco de conflitos e má comunicação, fornecendo canais claros para a comunicação interna e garantindo que as informações sejam precisas e oportunas.

4.16.4 Implementação de um Plano de Comunicação Interna

Para implementar um Plano de Comunicação Interna eficiente para a HRV, é importante seguir algumas etapas, conforme ilustrado e descrito abaixo.

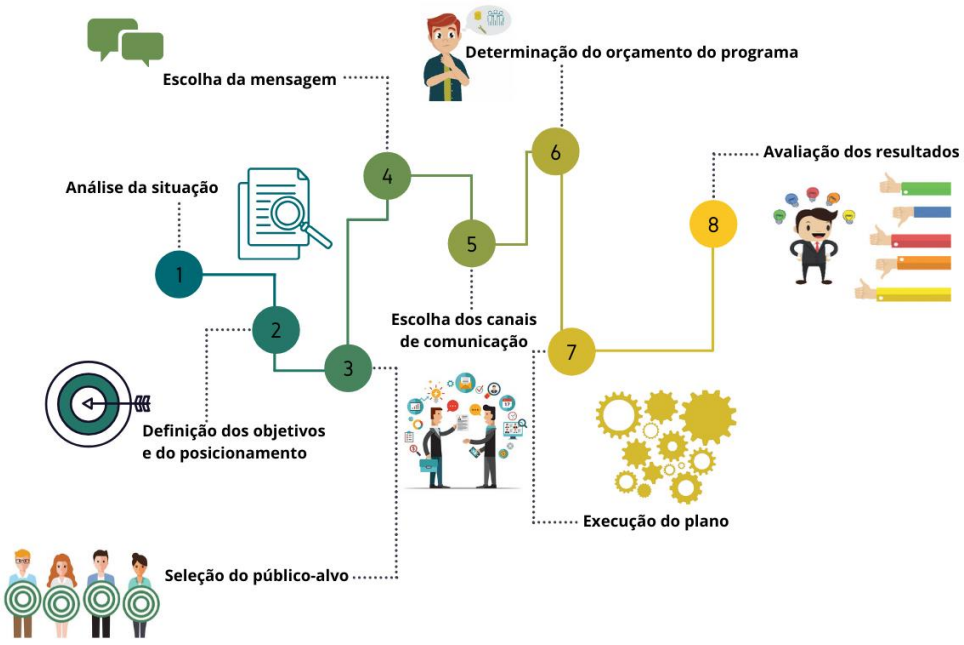


Figura 16 - Plano de Comunicação

- **[1] Análise da situação/âmbito**

Contextualizar a análise interna e externa da organização, recorrendo à análise SOT e PESTEL.

- **[2] Definir os objetivos da comunicação interna**

Qual o objetivo da organização e qual é o retorno esperado com a implementação do plano. Como por exemplo, aumentar o interesse dos colaboradores, melhorar a estratégia da organização, reforçar a cultura organizacional, etc.

- **[3] Identificar o público-alvo**

É importante definir qual é o destinatário da comunicação para ajustar a mesma consoante as necessidades específicas desse público.

- **[4] Escolher a mensagem**

Selecionar os pontos-chave para uma boa mensagem (ser clara, concisa e direta).

- **[5] Definir os canais de comunicação**

Para a informação chegar ao público-alvo da organização com sucesso, é necessário selecionar os canais mais adequados para o fazer. Como por exemplo, e-mails, intranet, reuniões, circulares, etc.

- **[6] Determinar o orçamento para o programa**

É necessário conhecer exatamente quais os recursos matérias e não matérias para serem alocados para se atingir os objetivos definidos.

- **[7] Executar o plano**

De acordo com todos os pontos anteriores, é definida cada ação e a linha temporal em que irá acontecer.

- **[8] Avaliar e monitorizar a eficácia do plano**

É importante acompanhar os resultados do plano de comunicação interna e avaliar se as metas estabelecidas foram alcançadas.

Recorrendo a estas etapas, é possível implementar um Plano de Comunicação Interna eficiente na HRV. A comunicação interna é essencial para manter os colaboradores informados, motivados e alinhados com os objetivos da organização, resultando em maior produtividade e interesse.

4.16.5 Tecnologia utilizada pela HRV

Existem diversas tecnologias que podem ser utilizadas num Plano de Comunicação Interna para uma organização. Apresentamos de seguida algumas que serão adotadas pela HRV, nomeadamente:

- **E-mail institucional**
  É um meio de comunicação rápido e eficiente que permite o envio de mensagens, anexos e permite convocar os intervenientes para reuniões e formações. É importante que a organização disponha de uma política de uso (PUA) do e-mail, para evitar problemas relacionados com a fuga de informação confidencial.

- **Chat (Skype)**
  Meio de comunicação instantânea entre os colaboradores, permitindo que as conversas ocorram de forma mais ágil e interativa.

- **Videoconferência (Teams)**
  Permite que colaboradores em teletrabalho ou que possam extar a exercer as suas funções no cliente, consigam participar em reuniões ou formações.

Existem muitas tecnologias que podem auxiliar no processo de comunicação interna de uma organização. Para a empresa HRV a seleção foi a que mencionados anteriormente, mas a qualquer momento podem ser adotadas outras tecnologias e mecanismo, nunca esquecendo as necessidades e objetivos da organização, bem como as preferências e hábitos dos colaboradores.

5 Conclusões e recomendações futuras

Atualmente, as organizações estão muito expostas com a crescente digitalização e dependência da tecnologia, e por essa razão devem adotar medidas de segurança robustas para garantir a confidencialidade, integridade e disponibilidade dos dados que possuem. Caso a organização não invista na cibersegurança, podem advir danos financeiros, reputacionais e legais.

Para isso é necessário implementar medidas de segurança adequadas, ter uma estrutura organizacional clara, um plano de resposta abrangente e melhorias contínuas com base nas lições aprendidas.

O Plano de Resposta a Incidentes (PRI) que criámos para a organização HRV - Equipamentos De Processo, S.A., está detalhado de forma a dar uma resposta à maioria das situações em caso de incidente, bem como todas as indicações para a sua correção e melhoria contínua dos processos. Seguindo todas as abordagens documentadas com rigor neste documento, a organização está preparada para enfrentar qualquer tipo de incidente.

Além disso e não esquecendo, todas as ferramentas e as formas de comunicar entre departamentos e autoridades competentes, estão explicitas neste documento, sendo que a organização nunca irá ter informações em falta no caso de incidente, melhorando também desta forma a sua presença digital, mantendo assim tanto as autoridades competentes bem como seus clientes informados.

Para recomendações futuras, sugerimos que a HRV mantenha o Plano de Resposta a Incidentes atualizado, pois o mesmo é um processo cíclico e com o decorrer do tempo o mesmo pode não se adequar à organização.

6 Referências

[1] CNCS, “cncs.gov.pt,” 12 2022. [Online]. Available: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf. [Acedido em 25 06 2023].

[2] P. d. E. d. P. d. Dados, “ANÁLISE DO RISCO DA SEGURANÇA DA INFORMAÇÃO,” Portal do Encarregado de Proteção de Dados, [Online]. Available: https://www.portaldodpo.pt/blog/service/risco/. [Acedido em 26 06 2023].

[3] ENISA, “Good Practice Guide for Incident Management,” 20 12 2010. [Online]. Available: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management. [Acedido em 22 06 2023].

[4] apcergroup, “apcergroup,” apcergroup, [Online]. Available: https://apcergroup.com/pt/certificacao/pesquisa-de-normas/146/np-iso-10002.

[5] apcergroup, “apcergroup,” [Online]. Available: https://www.apcergroup.com/pt/certificacao/pesquisa-de-normas/81/iso-9001.

[6] apcergroup, “apcergroup,” [Online]. Available: https://www.apcergroup.com/pt/certificacao/pesquisa-de-normas/177/iso-45001.

[7] isq, “isq,” [Online]. Available: https://www.isq.pt/servicos/servicos-regulamentares/instalacoes-industriais-e-equipamentos/avaliacao-de-conformidade-com-a-directiva-maquinas/.

[8] CNCS, “Boas Práticas de passwords - CNCS,” [Online]. Available: https://www.cncs.gov.pt/pt/boas-praticas-passwords/.

[9] CNCS, “Quadro Naciona de Referência para a Cibersegurança,” [Online]. Available: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf.

7 Anexos

Anexo 1 - anexo_Playbook_Malware.pdf

Anexo 2 - anexo_Playbook_Phishing.pdf

Anexo 3 - anexo_Playbook_DDoS.pdf

Anexo 4 - anexo_Playbook_ExfiltraçãoDados.pdf

Anexo 5 - anexo_Playbook_InjecaoCodigo.pdf