CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de **Cibersegurança**

RELATÓRIO SOBRE OS **SETORES DOS OPERADORES DE SERVIÇOS ESSENCIAIS**

Metodologia de Identificação de Ameaças

Caracterização, Regulamentação e Recomendações no Âmbito do Observatório de Cibersegurança

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

Índice

Índice de Figuras

Índice de Tabelas

Introdução

No âmbito da elaboração do Relatório sobre Operadores de Serviços Essenciais (ROSE), o Centro Nacional de Cibersegurança (CNCS) reconheceu a crescente necessidade de fornecer aos Operadores de Serviços Essenciais (OSE) uma metodologia robusta para a identificação de ciberameaças. Com o aumento da interdependência entre setores críticos e a intensificação das ameaças latentes no ciberespaço, torna-se essencial que os OSE disponham de ferramentas eficazes para antecipar e mitigar riscos que possam comprometer a continuidade e a segurança dos seus serviços.

A metodologia proposta visa mapear as principais ciberameaças que, com maior ou menor frequência, impactam cada setor, permitindo uma análise personalizada e detalhada de riscos. Para garantir a abrangência e a relevância dos dados, parte desta metodologia deverá basear-se em informações provenientes de fontes internacionais de referência, complementadas por dados nacionais obtidos pelo Observatório de Cibersegurança do CNCS. Este cruzamento de dados permitirá não apenas uma visão global das ameaças, mas também uma contextualização no ciberespaço nacional, abordando particularidades regionais e setoriais que podem influenciar o perfil de risco dos OSE.

Com esta metodologia, o CNCS procura apoiar os OSE na criação de estratégias mais sólidas e proativas de cibersegurança, essenciais para proteger a suas infraestruturas e garantir a resiliência digital do país face ao crescente cenário de ameaças no ciberespaço.

Tal como o Relatório, esta metodologia foi criada com a colaboração da PwC, entidade parceira do CNCS.

1. Metodologia de recolha de dados e análise de ameaças

Tendo em conta o atual cenário de ameaças, torna-se crucial que os OSE tenham à sua disposição uma metodologia para a deteção, identificação, análise e mitigação dessas mesmas ameaças. O CNCS pretende disponibilizar aos OSE essa metodologia.

Assim, é apresentada uma metodologia de caráter geral, aplicável e repetível por todos os setores dos OSE. Esta metodologia deverá depois ser adaptada à realidade setorial e organizativa de cada organização, conforme as suas especificidades e necessidades.

1. Identificar os ativos e processos críticos da organização

1.1. Inventário e classificação de ativos

A recolha de dados e análise de ameaças deve começar com a identificação dos ativos da organização. Esses ativos podem ser tecnológicos (*hardware*, *software*, dispositivos de rede e sistemas), pessoas, informação, ambiente físico e localizações e terceiros prestadores (que consistem nas dependências contratuais internas ou externas ao serviço), entre outros[1].

De acordo com o **Quadro Nacional de Referência para a Cibersegurança (QNRCS)**[2], a inventariação e classificação de ativos deve incluir as seguintes atividades:

- Inventariação dos dispositivos físicos, redes e sistemas de informação existentes na organização (ID.GA-1)[3];
- Inventariação das aplicações e plataformas de *software* que suportam os processos dos serviços críticos (ID.GA-2)[4];
- Classificação dos ativos necessários (dispositivos, sistemas, *software*, entre outros) para a prestação de bens e serviços (ativos críticos, não críticos) (ID.GA-5)[5].

[1] CNCS, "Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança", Versão 1.1, dezembro de 2022, 20, https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.
[2] CNCS, "Quadro Nacional de Referência para a Cibersegurança", 2019, https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf.
[3] CNCS, "Quadro Nacional de Referência para a Cibersegurança", 54.
[4] CNCS, "Quadro Nacional de Referência para a Cibersegurança", 55.
[5] CNCS, "Quadro Nacional de Referência para a Cibersegurança", 57.

Criar diagramas de rede com todos os ativos das redes poderá também ser útil para visualizar as interligações e os caminhos de comunicação entre ativos, processos e pontos de entrada na rede (ID.GA-3)[6]. Quanto mais detalhe houver sobre os ativos identificados e sobre a sua relação com os restantes, maior será a qualidade da informação a trabalhar no processo de análise e avaliação dos riscos, bem como de todo o processo de gestão dos riscos.

De seguida, apresenta-se um breve exemplo de como um inventário de ativos pode ser estruturado:

Tabela 1 – Exemplo de estrutura de um inventário de ativos

ID	Fabricante	N.º de série	Modelo	Proprietário / *Owner*	Responsável	Localização	Versão do *software* / *firmware*	Classificação
A001	XYZ	12345	T14	José Silva	Hugo Dias	Ao cuidado do proprietário	V.05.01.02	Não-crítico
A002	ABC	67890	S21	Hugo Dias	Hugo Dias	*Data centre*	V3.11	Crítico

Um inventário de ativos pode ser implementado de forma manual, em que as informações sobre os ativos são recolhidas por uma ou mais pessoas, e o preenchimento dos campos é feito sem auxílio de um *software* complementar. Outra opção é a implementação automática, que utiliza ferramentas especializadas para capturar informações específicas de cada ativo. Por fim, há a implementação mista, que combina as técnicas manuais e as ferramentas automáticas para obter um inventário completo e detalhado.

1.2. Recolha de dados e informações sobre vulnerabilidades e ameaças

A recolha de dados e informações sobre ameaças deve seguir duas abordagens estratégicas complementares. Primeiramente, as organizações devem realizar análises internas contínuas dos ativos da organização. Tais análises incluem a monitorização do tráfego da rede e de outros dados operacionais, com o objetivo de identificar sinais de atividades suspeitas ou anómalas. Como uma parte significativa do *malware* depende de comunicações com servidores externos para operar, a análise da rede torna-se crucial para a deteção proativa de ameaças. Esta análise deve procurar identificar artefactos maliciosos, como tentativas de ligação a endereços *IP* desconhecidos, padrões anómalos de tráfego e comportamentos que indicam a presença de agentes maliciosos. Combinadas, estas abordagens fortalecem a capacidade de resposta da organização frente ao cenário dinâmico de ameaças de cibersegurança.

A segunda abordagem consiste no facto de as organizações precisarem de se manter atualizadas sobre as tendências globais de ciberameaças. Para tal, é recomendável que as organizações façam um acompanhamento regular de relatórios, publicações especializadas e notícias de fontes confiáveis e reconhecidas, incluindo centros de investigação, e outras autoridades em matéria de cibersegurança. Esta recolha de informação sobre ameaças deve ser adaptada às características

[6] CNCS, "Quadro Nacional de Referência para a Cibersegurança", 55.

e necessidades de cada organização, considerando aspetos como os sistemas operativos, *software* e aplicações utilizadas, assim como a configuração da infraestrutura tecnológica[7].

Uma vulnerabilidade é uma fraqueza num ativo ou controlo que pode ser explorada por uma ameaça, a qual pode resultar em dados nos sistemas, indivíduos ou organizações. O ambiente organizacional está exposto a diversas vulnerabilidades, que podem ser identificadas através de ferramentas específicas, como análises de vulnerabilidades, *scans* automáticos e testes de intrusão nas redes e sistemas. A existência de vulnerabilidades só causa de danos quando uma ameaça as explora, seja intencionalmente ou acidentalmente[8].

1.3. Mapeamento das ameaças específicas ao OSE

O mapeamento de ameaças específicas ao Operador de Serviços Essenciais (OSE) é uma etapa crítica que visa identificar ameaças diretamente relevantes para os ativos e processos críticos identificados anteriormente. Este processo envolve:

1. **Identificação das ameaças internas e externas:** consiste em listar as potenciais fontes de ameaça que podem comprometer a segurança dos ativos. As ameaças internas incluem erros humanos, falhas de sistemas e ameaças de pessoal interno, enquanto as ameaças externas podem abranger *hackers*, grupos de cibercriminosos, ataques de negação de serviço (*DDoS*), *ransomware* e outras ameaças de cibersegurança[9];
2. **Classificação das ameaças por relevância e probabilidade:** Avaliar e priorizar as ameaças de acordo com a probabilidade de ocorrência e o impacto potencial sobre os ativos críticos. Esta classificação deve ter como base os serviços que o OSE presta e em dados históricos de incidentes ou eventos similares no setor[10].
3. **Identificação de vetores de ataque:** Analisar de que forma as ameaças podem materializar-se, identificando os vetores de ataque mais prováveis, como *phishing*, exploração de vulnerabilidades de *software*, ataques físicos a centros de dados ou infraestruturas críticas e tentativas de exploração de acesso remoto[11].
4. **Desenvolvimento de cenários de ameaça:** Elaborar cenários que descrevam possíveis ataques, considerando fatores como técnicas e táticas conhecidas (por exemplo a *framework* MITRE ATT&CK) e as especificidades dos ativos e processos do OSE. Os cenários ajudam a visualizar as possíveis consequências de ataques concretos e a ajustar as medidas de proteção[12].
5. **Avaliação contínua e atualização dos cenários de ameaça:** Devido ao caráter dinâmico do cenário de ameaças, é essencial que estes sejam revistos regularmente, integrando novas informações sobre ciberameaças emergentes, alterações tecnológicas e mudanças operacionais no OSE[13].

[7] International Organization for Standardization e International Electrotechnical Commission, "ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls", Controlo 5.7 *Threat Intelligence*, 15-17, https://www.iso.org/standard/75652.html.

[8] CNCS, "Guia para Gestão dos Riscos", 24-25.

[9] NIST, "NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments", setembro de 2012,1, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[10] NIST, "Guide for Conducting Risk Assessments", setembro de 2012, *Appendix E-1*.

[11] NIST, "Guide for Conducting Risk Assessments", setembro de 2012, *Appendix B-1*.

[12] NIST, "Guide for Conducting Risk Assessments", setembro de 2012, 8-9.

[13] NIST, "Guide for Conducting Risk Assessments", setembro de 2012, 6.

2. Análise das ameaças e atribuição do nível de risco

2.1. Análise de risco das vulnerabilidades e ameaças de cibersegurança

Uma vez recolhidos os dados e as informações sobre as ameaças que têm uma real hipótese de afetar a organização, deve-se-lhes atribuir o nível de risco correspondente

A consulta do **Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança** elaborado pelo CNCS poderá ser útil neste ponto.

O nível de risco associado a uma ameaça é definido com base em dois fatores: a probabilidade de a ameaça se concretizar e o impacto dessa concretização, na organização e nas pessoas a quem a organização presta serviços[14]. O impacto pode ser avaliado em diversas perspetivas, podendo estas ser do foro técnico, financeiro, humano, ou outro considerado relevante pela organização[15].

Risco = Probabilidade x Impacto

Para uma melhor visualização do nível de risco associado a uma determinada ameaça, é recomendada a elaboração de uma matriz de risco.

Para elaborar uma matriz de risco deverão ser definidos os níveis de risco, os respetivos critérios de aceitação do risco e o nível de priorização do tratamento de cada risco.

[14] CNCS, "Guia para Gestão dos Riscos", 27.

[15] CNCS, "Quadro Nacional de Referência para a Cibersegurança", 33.

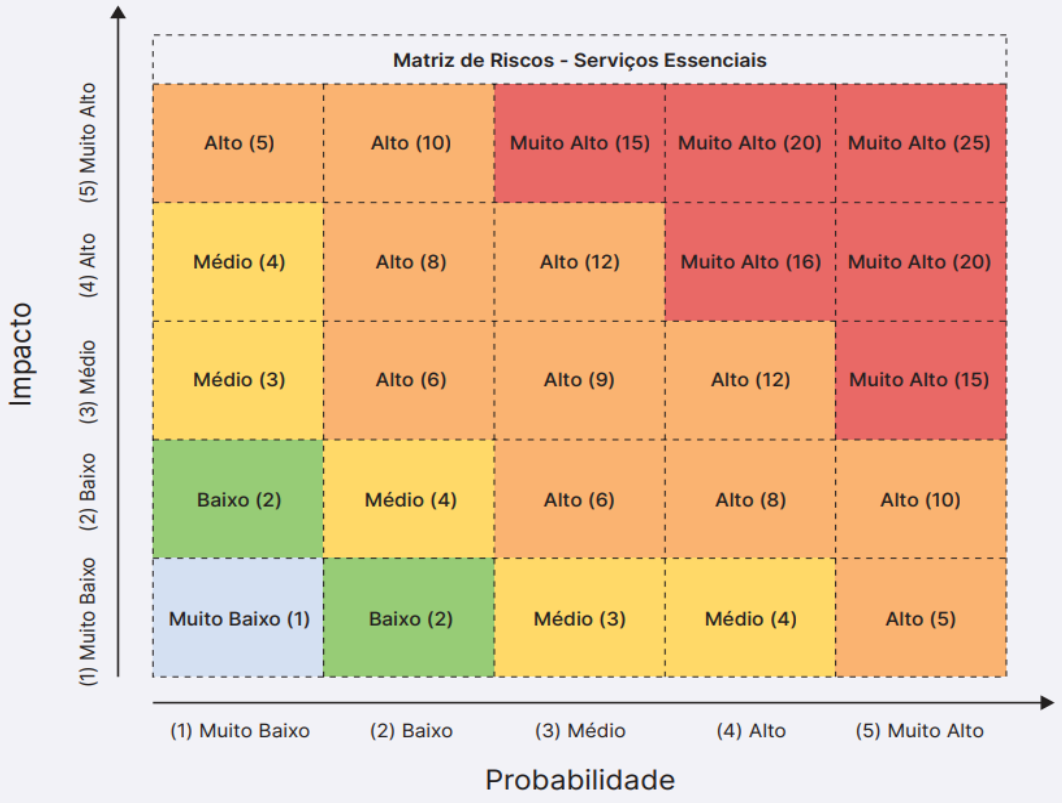
Figura 1 - Critérios de Aceitação dos Riscos - Exemplo

CRITÉRIOS DE ACEITAÇÃO DOS RISCOS - EXEMPLO		
Nível de Risco	**Critério de Aceitação dos Riscos**	**Priorização**
Muito alto	Não aceitável, requer tratamento imediato	1
Alto	Não aceitável, requer tratamento no prazo máximo de 15 dias	2
Médio	Não aceitável, requer tratamento no prazo máximo de 6 meses	3
Baixo	Risco cuja aceitação depende da avaliação do dono do risco, por norma será aceite, no entanto, pode decidir tratar.	4
Muito baixo	Risco aceitável, deve ser monitorizado e revisto a cada 12 meses.	5

Fonte: CNCS, "Guia para Gestão dos Riscos", 46.

Estando estes parâmetros definidos, poder-se-á agora elaborar a matriz de risco, como no exemplo abaixo:

Figura 2 - Matriz de Riscos - Exemplo



Fonte: CNCS, "Guia para Gestão dos Riscos", 33.

2.2. Análise dos vetores de ataque

Os vetores de ataque referem-se aos caminhos ou métodos que um agente de ameaça utiliza para obter o acesso não autorizado às redes, sistemas, dispositivos ou dados e informações de uma organização. É também importante não confundir os vetores de ataque com as superfícies de ataque. Enquanto os vetores de ataque se prendem com o meio através do qual o acesso é ganho, a superfície de ataque prende-se com o que é efetivamente atacado.

Os vetores de ataque podem ser variados, desde tentativas de *phishing*, ou de injeção de *malware* numa organização, ou passar pela exploração de vulnerabilidades não tratadas, configurações indevidas, ataques de força bruta, entre outros. É importante que uma organização seja capaz de identificar os vetores de ataque mais passíveis de serem explorados de modo a tentar impedir que os mesmos sejam utilizados contra si. Caso a organização já tenha sofrido ataques, revisitar os ataques concretizados para determinar os vetores utilizados e procurar adotar medidas que impeçam, que estes vetores sejam usados novamente.

2.3. (Re)avaliação dos controlos de cibersegurança existentes

Uma vez identificados os vetores de ataque das ameaças latentes, bem como os de ataques já concretizados, é importante avaliar ou reavaliar a eficácia dos controlos de segurança implementados. Esses controlos podem assumir diferentes aspetos: podem ser processos, políticas, dispositivos, práticas ou outras ações que modifiquem o risco[16].

São exemplos de controlos de segurança as medidas de segurança documentadas no **QNRCS**, organizadas através dos objetivos de Identificar, Proteger, Detetar, Responder e Recuperar[17].

Para avaliar ou reavaliar os controlos existentes, devem ser consideradas atividades como:

- Revisão de documentos que contenham informações sobre a implementação dos controlos (por exemplo: planos anteriores de implementação de processos de gestão do risco);
- Verificação junto dos responsáveis pela segurança da informação e cibersegurança (CISO, COO) sobre quais são os controlos que se encontram efetivamente implementados;
- Realização de uma avaliação presencial, no local, para aferir a implementação dos controlos físicos, comparando os que estão devidamente implementados com a lista dos controlos que deveriam estar e, verificando entre os implementados, se estes se encontram correta e eficazmente operacionalizados.

É também importante manter presente a noção de que "um controlo ou conjunto de controlos que estejam incorretamente implementados, podem traduzir-se em potenciais vulnerabilidades para a organização, logo devem ser identificados controlos complementares e/ou ações de forma que esse controlo mesmo seja substituído ou removido para endereçar esses riscos de forma eficaz"[18].

[16] CNCS, "Guia para Gestão dos Riscos", 23.
[17] CNCS, "Guia para Gestão dos Riscos", 23.
[18] CNCS, "Guia para Gestão dos Riscos", 23.

2.4. Tratamento dos riscos

Estando identificadas e analisadas as ameaças que poderão afetar a organização, e estando atribuídos os níveis de risco correspondentes a cada ameaça, a organização deverá depois decidir como tratar os riscos relativos às ameaças identificadas.

As ações possíveis são:

- **Mitigar ou Modificar:** "Diminuir a exposição dos riscos, elaborando planos de ação e aplicando controlos específicos, podendo haver lugar à implementação de controlos adicionais de forma a mitigar o risco ou reduzi-lo de modo a enquadrar-se nos critérios de aceitação dos riscos definidos pela organização"[19].

- **Evitar:** "Eliminar a causa do risco, eliminando o processo que o gera. Visa a descontinuidade das atividades de negócio ou ativos de informação ou de suporte que atuam como fonte do risco para a organização, eliminando de forma permanente o risco. Tipicamente, esta opção é considerada quando o plano de tratamento apresenta custos demasiado elevados e que a atividade de negócio ou ativo visadas já não possua uma importância tão visível para os objetivos de negócio da organização"[20].

- **Transferir ou Partilhar:** "Direcionar a responsabilidade das consequências a terceiros. A responsabilidade pelo risco é transferida para outra entidade que não a organização como, por exemplo, assegurar os ativos ou atividades de negócio através da atribuição da responsabilidade destes a fornecedores ou outros parceiros"[21].

- **Aceitar ou Reter:** "Tomar conhecimento do risco sem adotar controlos. Neste caso, é suportada a decisão de não aplicar qualquer tipo de ação corretiva ao risco e assumir as consequências que o mesmo pode trazer à organização em caso de materialização. Somente riscos de nível baixo e muito baixo devem ser retidos. Esta opção deve ser utilizada em situações em que:
    - O risco se encontra dentro dos critérios de aceitação definidos pela organização;
    - Quando a implementação dos controlos para a redução do nível apresenta custos superiores àqueles que o risco provoca em caso de materialização"[22].

[19] CNCS, "Guia para Gestão dos Riscos", 37.
[20] CNCS, "Guia para Gestão dos Riscos", 37.
[21] CNCS, "Guia para Gestão dos Riscos", 37.
[22] CNCS, "Guia para Gestão dos Riscos", 37.

3. Monitorização, deteção e comunicação de ameaças

3.1. Monitorização contínua *de ameaças*

A monitorização contínua de ameaças é uma abordagem proativa que permite às organizações identificar e responder rapidamente a incidentes de segurança. Para implementar um sistema eficaz de monitorização, devem ser considerados os seguintes elementos:

1. **Ferramentas de Monitorização**: Utilizar ferramentas de segurança, como sistemas de deteção de intrusões (IDS), soluções de prevenção de perda de dados (DLP), e plataformas de gestão de eventos e informações de segurança (SIEM). Estas ferramentas devem ser configuradas para monitorizar o tráfego de rede, sistemas e aplicações em tempo real, permitindo a identificação de comportamentos anómalos. Além disso, é importante que as ferramentas sejam atualizadas regularmente para que possam detetar as ameaças mais recentes[23].

2. **Análise de *Logs***: Estabelecer procedimentos para a análise regular de *logs* de sistema e de rede. Isso inclui *logs* de *firewall*, servidores, aplicações e dispositivos de rede, permitindo a deteção de atividades suspeitas e a identificação de potenciais vulnerabilidades[24].

3. **Alertas e Resposta a Incidentes**: Definir um sistema de alertas que notifique a equipa de segurança em caso de deteção de atividades anómalas ou potencialmente maliciosas. A implementação de uma equipa de resposta a incidentes (*IRT*) é essencial para garantir uma reação rápida e eficaz a ameaças identificadas[25].

4. **Avaliações Regulares**: Realizar avaliações regulares dos sistemas de monitorização e deteção. Isso inclui testes de penetração e simulações de ataques, que ajudam a validar a eficácia das ferramentas e processos em vigor. Essas avaliações ajudam a identificar pontos fracos na defesa e a garantir que as tecnologias e processos estejam atualizados para enfrentar novas ameaças. Além disso, as avaliações fornecem insights para ajustes no ambiente de monitorização, melhorando continuamente a eficácia da postura de segurança da organização[26].

[23] NIST, "NIST Special Publication 800-137: Information Security", setembro de 2011, 10, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf.
[24] NIST, "NIST Special Publication 800-92: Guide to Computer Security Log Management", setembro de 2006, 9, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.
[25] NIST, "NIST Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide", agosto de 2012, 21, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
[26] NIST, "NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment", setembro de 2008, 25, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

5. **Integração de Inteligência de Ameaças**: Integrar informações de inteligência de ameaças externas, que podem fornecer contexto sobre novas vulnerabilidades e ameaças emergentes. Isso pode incluir *feeds* de inteligência de ameaças, relatórios de segurança e atualizações de fornecedores de software[27].

6. **Formação e Conscientização**: Promover a formação contínua da equipa sobre as técnicas de monitorização e deteção de ameaças. Isso assegura que os colaboradores estejam atualizados sobre as melhores práticas e as tendências atuais em cibersegurança[28].

3.2. Estabelecimento de protocolos de comunicação de *ameaças*

A comunicação eficaz sobre ameaças é vital para garantir que todos os envolvidos na segurança da organização estejam informados e preparados para agir. Para tal, devem ser seguidos os seguintes passos:

1. **Definição de Canais de Comunicação**: Estabelecer canais claros para a comunicação de ameaças, que podem incluir e-mail, plataformas de mensagens seguras, e sistemas de alerta. Todos os colaboradores devem saber como e quando utilizar esses canais. Para incidentes críticos, deve-se priorizar canais de comunicação rápida, como plataformas de mensagens instantâneas seguras[29].

2. **Protocolos de Notificação**: Desenvolver protocolos que descrevam como e quando as ameaças devem ser comunicadas. Isso inclui[30]:

    - **Notificação Imediata**: Para incidentes críticos que requerem ação imediata, como violações de segurança ou comprometimento de dados, a notificação deve ser enviada a todos os membros da equipa de resposta e *stakeholders* relevantes assim que o incidente for identificado.

    - **Relatórios Regulares**: Estabelecer uma rotina de relatórios sobre o estado das ameaças e incidentes, que pode ser semanal ou mensal, dependendo da gravidade do ambiente de ameaça. Para monitorizar o estado das ameaças e incidentes, a organização deve estabelecer uma rotina de relatórios, que pode ser semanal ou mensal, dependendo da gravidade do ambiente de ameaça. Esses relatórios proporcionam uma visão geral do cenário de ameaças e informam sobre a eficácia das medidas de mitigação implementadas

3. **Identificação de *Stakeholders***: Identificar os principais *stakeholders* que devem ser notificados em caso de incidentes de segurança, incluindo a direção, a equipa de TI, e qualquer pessoal relevante da área jurídica ou de conformidade. Essa identificação também deve considerar os *stakeholders* externos, como parceiros e fornecedores críticos, que podem precisar de ser informados em incidentes que afetem operações conjuntas[31].

---

[27] NIST, "NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing", outubro de 2016, 6, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

[28] International Organization for Standardization, "ISO 27001-1:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements", 10-11, https://www.iso.org/standard/27001.html.

[29] NIST, "NIST Special Publication 800-61 Rev. 2", 36.

[30] NIST, "NIST Special Publication 800-61 Rev. 2", 33-34.

[31] NIST, "NIST Special Publication 800-61 Rev. 2", 37.

4. **Planos de Comunicação de Crise**: Elaborar planos de comunicação para situações de crise, que incluam mensagens pré-definidas e diretrizes sobre como abordar a comunicação com o público, os media, e as autoridades, se necessário. O plano deve ser testado regularmente para garantir que os responsáveis estejam prontos para implementá-lo, caso ocorra uma crise. É essencial que todas as comunicações sigam uma abordagem consistente e transparente[32].

5. **Revisão e Atualização dos Protocolos**: Rever regularmente os protocolos de comunicação para garantir que permaneçam eficazes e relevantes, incorporando lições aprendidas de incidentes passados e mudanças no cenário de ameaças. Alterações nos protocolos podem incluir ajustes nos canais de comunicação, atualizações nos procedimentos de notificação, e a inclusão de novos *stakeholders*. A revisão periódica também ajuda a manter a equipe familiarizada com os protocolos e prontos para agir em qualquer situação, minimizando atrasos e incertezas[33].

6. **Formação em Comunicação**: Proporcionar formação aos colaboradores sobre a importância da comunicação em cibersegurança, incluindo como comunicar incidentes e a necessidade de manter a confidencialidade e a integridade das informações[34].

[32] International Organization for Standardization, "ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements", 15-17, https://www.iso.org/standard/75106.html.
[33] International Organization for Standardization, "ISO 27035-1:2016: Information technology — Information security incident management", 18-22, https://www.iso.org/standard/78973.html.
[34] NIST, "NIST Special Publication 800-50 Rev.1: Building an Information Technology Security Awareness and Training Program", setembro de 2024, 7-10, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.

4. Revisão e melhoria contínua

É importante deixar um registo documental do processo seguido para a recolha de dados e informações sobre ameaças, para que o mesmo possa ser repetido e para que as consequências da realização do processo possam ser conhecidas. O relatório deve oferecer informação clara sobre as fontes consultadas, sobre as ameaças encontradas que podem afetar a organização, sobre o nível de risco atribuído a estas e sobre o tratamento dado a esse risco. A utilidade do relatório poderá estender-se além da estritamente associada à da recolha de dados e informações sobre ameaças, servindo como uma ferramenta que pode ajudar a justificar necessidades junto da administração, auxiliar na formação de colaboradores e servir como um guia para um dos processos seguidos dentro da organização.

4.1. Avaliação pós-incidente e lições aprendidas

A avaliação pós-incidente permite que a organização compreenda o impacto dos incidentes e ajuste processos para minimizar ocorrências futuras. Este processo inclui:

1. **Reunião de rescaldo pós-Incidente (lições aprendidas):** As organizações devem usar o processo de lições aprendidas para obter valor dos incidentes. Após um incidente importante ter sido tratado, a organização deve realizar uma reunião de lições aprendidas para rever a eficácia do processo de tratamento de incidentes e identificar as melhorias necessárias nos controlos e práticas de segurança existentes. As reuniões de lições aprendidas também podem ser realizadas periodicamente para incidentes menores, conforme o tempo e os recursos permitirem. As informações acumuladas de todas as reuniões de lições aprendidas devem ser utilizadas para identificar e corrigir fraquezas sistémicas e deficiências em políticas e procedimentos. Os relatórios de acompanhamento gerados para cada incidente podem ser importantes não apenas para fins probatórios, mas também para referência no tratamento de incidentes futuros e na formação de novos membros da equipa[35].

2. **Identificação de padrões de ataque e comportamento**: Avaliação de padrões de ataque[36] (por exemplo, *ransomware* ou *spear-phishing*). A análise de incidentes anteriores pode ajudar a identificar tendências e técnicas de ataque que podem estar a evoluir[37].

3. **Avaliação da eficácia dos controlos existentes**: Rever a eficácia de controlos como bloqueios de *firewall*, regras de acesso e configurações de *IDS*/*IPS*. Verifique se existiram

[35] NIST, “NIST Special Publication 800-61 Rev. 2”, 3.
[36] NIST, “NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations”, setembro de 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
[37] NIST, “NIST Special Publication 800-61 Rev. 2”, 3.

falhas nos controlos que permitiram o incidente, ajudando a ajustar configurações e endurecer proteções específicas[38].

4. **Elaboração de relatórios pós-incidente**: Documente todas as lições aprendidas em um relatório, incluindo a descrição do incidente, os fatores contribuintes e as melhorias necessárias. Este relatório é uma ferramenta para a continuidade e pode servir como uma base de referência para incidentes futuros[39].

5. **Integração de *feedback* em programas de formação**: Aplique as lições aprendidas para atualizar programas de formação. Por exemplo, se o incidente envolveu *phishing*, considerar sessões de formação específicas sobre identificação de *phishing* para toda a equipa[40].

4.2. Realização de auditorias e simulações periódicas

Para assegurar que os controlos e defesas permanecem atualizados, a realização de auditorias e simulações periódicas é essencial. O objetivo é ajustar e reforçar continuamente a postura de segurança. Os elementos incluem:

1. **Auditorias de Conformidade**: Realizar auditorias anuais para verificar a conformidade com políticas de segurança interna e regulamentações externas. Auditorias mais formais e focadas em determinar o alinhamento com leis e regulamentos específicos. Durante essas auditorias, a organização revê documentos, configurações de sistemas, políticas e práticas para avaliar o alinhamento com requisitos de segurança e privacidade. Auditorias regulares não só ajudam a mitigar riscos de não conformidade, como também oferecem uma visão clara do estado atual de segurança, orientando planos de melhoria contínua[41].

2. **Exercícios de Simulação de Ataques de Engenharia Social**: Realizar testes de engenharia social, como simulações de *phishing*, para avaliar a resposta dos colaboradores de identificar e reagir a tentativas de ataques que exploram o fator humano. Estes exercícios permitem medir o nível de consciência e a eficácia das políticas *anti-phishing* da organização. Os resultados dos testes fornecem *insights* para aprimorar os programas de consciencialização e reforçar a cultura de segurança entre os colaboradores, além de permitir ajustes nas políticas de segurança e nos controlos técnicos, como filtros de e-mail e alertas de segurança[42].

3. **Testes de Resiliência e Tolerância a Carga:** Avaliar a capacidade dos sistemas de manter operações críticas mesmo em cenários de alta carga ou falhas parciais. Esses testes ajudam a garantir que os sistemas críticos possuem resiliência suficiente para resistir a perturbações e continuar operando em um estado degradado, se necessário. Aplicando os princípios de design resiliente, tais como redundância, recuperação e adaptação, a organização pode identificar possíveis pontos de vulnerabilidade e desenvolver planos para assegurar que a infraestrutura essencial permaneça operacional durante eventos de stress. Essa abordagem pró-ativa permite que as equipes de engenharia ajustem continuamente os sistemas para

[38] NIST, “NIST Special Publication 800-53A Rev. 5: Assessing Security and Privacy Controls in Information Systems and Organizations”, 15-16, janeiro de 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf.
[39] NIST, “NIST Special Publication 800-61 Rev. 2”, 21.
[40] NIST, “NIST Special Publication 800-50 Rev.1”, 12.
[41] International Organization for Standardization, “ISO 27001-1:2022”, 8-9.
[42] NIST, “NIST Special Publication 800-53 Rev. 5”, 61.

melhorar a robustez e a continuidade, preparando-os para lidar com uma ampla gama de desafios operacionais e ameaças emergentes[43].

4. **Documentação e Implementação de Melhorias**: Registar cada auditoria e simulação, incluindo achados e correções aplicadas. Esse registo. fornece um histórico de vulnerabilidades e melhorias, que serve como base para futuras análises de segurança e auditorias. A documentação detalhada permite que a organização siga padrões de falhas, promovendo uma postura de segurança mais robusta. Além disso, esses registos podem ser utilizados para avaliar a eficácia das melhorias ao longo do tempo[44].

5. **Revisão de Planos de Recuperação e Continuidade**: Testar regularmente os planos de recuperação para garantir que a organização pode restaurar rapidamente operações críticas após um incidente. A revisão de planos de continuidade deve incluir testes de *backup*, *failover* de sistemas e simulação de cenários de interrupção[45].

[43] NIST, "NIST Special Publication 800-160 Vol. 1: Systems Security Engineering", março de 2018, 33-48, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.
[44] NIST, "NIST Special Publication 800-61 Rev. 2", 31.
[45] NIST, "NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems", maio de 2010, ES-1, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

Bibliografia

- CNCS. “Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança”, dezembro de 2022. https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.
- CNCS. “Quadro Nacional de Referência para a Cibersegurança”, 2019. https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf.
- International Organization for Standardization e International Electrotechnical Commission, “ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls”, 2022. https://www.iso.org/standard/75652.html.
- International Organization for Standardization. “ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements”. https://www.iso.org/standard/75106.html.
- International Organization for Standardization. “ISO 27001-1:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements”, 2022. https://www.iso.org/standard/27001.html.
- International Organization for Standardization. “ISO 27035-1:2016: Information technology — Information security incident management”, 2016. https://www.iso.org/standard/78973.html.
- NIST, “NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing”, outubro de 2016. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.
- NIST. “NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment”, setembro de 2008. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
- NIST. “NIST Special Publication 800-137: Information Security”, setembro de 2011. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf.
- NIST. “NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments”, setembro de 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
- NIST. “NIST Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide”, agosto de 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

- NIST. “NIST Special Publication 800-92: Guide to Computer Security Log Management”, setembro de 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.
- NIST. “NIST Special Publication 800-50 Rev.1: Building an Information Technology Security Awareness and Training Program”, setembro de 2024. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.
- NIST. “NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations”, setembro de 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.
- NIST. “NIST Special Publication 800-53A Rev. 5: Assessing Security and Privacy Controls in Information Systems and Organizations”, janeiro de 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf.
- NIST. “NIST Special Publication 800-160 Vol. 1: Systems Security Engineering”, março de 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.
- NIST. “NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems”, maio de 2010. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

www.cncs.gov.pt/

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Observatório
de **Cibersegurança**

PRR
Plano de Recuperação
e Resiliência

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU