CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

# Referencial de Comunicação de Risco e de Crise em Cibersegurança

v1.0
Abril de 2024
Centro Nacional
de Cibersegurança

PRR
Plano de Recuperação
e Resiliência

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU

Observatório
de Cibersegurança

# ÍNDICE

# LISTA DE ABREVIATURAS

**ANACOM** – Autoridade Nacional de Comunicações

**ANEPC** – Autoridade Nacional de Emergência e Proteção Civil

**ANSSI** – Agence Nationale de la Sécurité des Systèmes d'Information

**APPA** – American Public Power Association

**CCN** – Centro Criptológico Nacional

**CNPD** – Comissão Nacional de Proteção de Dados

**CSC** – Cyber Security Coalition

**ENSC** – Estratégia Nacional de Segurança do Ciberespaço 2019-2023

**GCS** – Government Communication Service

**ISAC** – Centros de Análise e Partilha de Informação

**ISO** – International Organization for Standardization

**PSC** – Public Safety Canada

**QNRCS** – Quadro Nacional de Referência para a Cibersegurança

**RJSC** – Regime Jurídico da Segurança do Ciberespaço

# 1. SUMÁRIO EXECUTIVO

O Referencial de Comunicação de Risco e de Crise em Cibersegurança (Referencial) apresenta-se como um conjunto de indicações e recomendações para as Organizações nacionais no âmbito da comunicação relativa aos riscos e às crises de cibersegurança.

O Referencial pretende servir como um documento de suporte ao desenvolvimento do setor da cibersegurança, auxiliando as demais Organizações na comunicação relativa à gestão do risco dentro das mesmas, bem como na elaboração de planos de comunicação a seguir em situações de crise de cibersegurança, elencando passos, identificando elementos e funções essenciais na equipa de comunicação formada para estas situações, e convidando ao contínuo aperfeiçoamento dos planos de comunicação em questão.

Alinhado com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, o Referencial pretende auxiliar na capacitação das Organizações na resposta a situações de crise de cibersegurança, durante as quais a comunicação assume um papel preponderante.

Tendo em vista estes objetivos, o Referencial não deve ser entendido como normativo ou receita prescritiva, mas sim como referência de partida para a elaboração de estratégias, políticas e planos, que devem ser adaptados ao contexto e necessidade de cada organização.

# 2. INTRODUÇÃO

Ano após ano, têm sido publicados diversos inquéritos de segurança que destacam perdas significativas para as Organizações em consequência da evolução das ciberameaças e dos ciberataques. Esta evolução exige que as abordagens e as capacidades de resposta se adaptem, dando espaço ao crescimento por parte da Organização no contexto da cibersegurança. Destaca-se um maior cuidado e atenção para com os colaboradores das organizações no que diz respeito à sensibilização e formação para as tecnologias de segurança da informação.

É necessário, por isso, que as Organizações se preparem para situações de comunicação de riscos e crises, em contexto de segurança de informação e dos sistemas, dada a sua crescente relevância nos últimos anos.

Os conteúdos apresentados no presente Referencial pretendem orientar as Organizações da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais, bem como todas as Organizações pequenas, médias e grandes a cumprir os requisitos propostos na legislação em vigor, e adotar as melhores práticas na comunicação de riscos e crises em cibersegurança.

O presente documento teve por base vários referenciais nacionais e práticas aplicadas em diferentes países, como é o caso da Bélgica, do Canadá, da Espanha, dos Estados Unidos da América, da França e do Reino Unido em matéria de planeamento e gestão da comunicação de riscos e crises em relação à cibersegurança, bem como a norma internacional ISO 22361:2022, dedicada à gestão de crises. Deste modo, pretendeu-se elencar os processos de identificação e comunicação de riscos e crises, reportados às entidades competentes, já existentes noutros países, encarados como uma boa prática, e passíveis de serem aplicados em contexto nacional.

O objetivo do presente documento é, assim, constituir uma referência em matéria de planeamento e gestão no que diz respeito à comunicação de risco e de crise em cibersegurança para todas as Organizações que necessitam dessa referência.

## 2.1. ENQUADRAMENTO

Considerando a Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, o Centro Nacional de Cibersegurança (CNCS) procura contribuir para o uso do ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes.

Considerando ainda os termos da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, aprovada em Conselho de Ministros, no dia 23 de maio de 2019, e publicada através da resolução n.º 92/2019, de 5 de junho de 2019, decorreu a necessidade de elaborar um referencial de comunicação de risco e de crise em cibersegurança.

Neste sentido, com o Referencial disponibiliza-se um corpo de conhecimento capaz de identificar aspetos-chave no âmbito da comunicação relativa aos riscos e às situações de crise em cibersegurança, servindo como documento de suporte ao desenvolvimento do setor da cibersegurança, contribuindo também para a definição e formulação de políticas e planos de comunicação nesta área.

## 2.2. OBJECTIVOS

Atendendo ao enquadramento estratégico e jurídico do Referencial e tendo em vista a sua utilidade prática, a conceptualização e construção do Referencial teve como objetivos:

- Identificar e explorar os pontos fortes dos vários referenciais nacionais e internacionais relativamente à comunicação em matéria de risco e de crise em cibersegurança, uniformizando as diferentes fases da comunicação, bem como os respetivos passos de cada fase;
- Explorar as sinergias entre os referenciais, minimizando as discrepâncias conceptuais e maximizando a interoperabilidade;
- Facilitar a atualização e a melhoria contínua do Referencial.

## 2.3. CONTEXTO DO REFERENCIAL

Para o desenvolvimento deste referencial foram utilizados, como principais referências externas, os seguintes documentos:

- "*Crisis of Cyber Origin: The Keys to Operational and Strategic Management*" - Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), **França**;[1]
- "*Cyber Security Incident Management Guide*" - Cyber Security Coalition (CSC), **Bélgica**;[2]
- "*Gestión de Cibercrisis. Buenas Prácticas en la Gestión de Crisis de Ciberseguridad*" - Centro Criptológico Nacional (CCN), **Espanha**;[3]
- "*Developing an Operational Technology and Information Technology Incident Response Plan*", Public Safety Canada (PSC), **Canadá**;[4]
- "*Public Power Cyber Incident Response Playbook*" - American Public Power Association (APPA)/Nexight Group, **Estados Unidos**;[5]
- "*Emergency Planning Framework*" - Government Communication Service (GCS), **Reino Unido**.[6]
- "*ISO 22361:2022 - Security and resilience — Crisis management — Guidelines*", **International Organization for Standardization**[7].

[1] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), "*Crisis of Cyber Origin: The Keys to Operational and Strategic Management*", março de 2022, https://cyber.gouv.fr/sites/default/files/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en1.pdf.
[2] Cyber Security Coalition (CSC), "*Cyber Security Incident Management Guide*", janeiro de 2016, revisto em setembro de 2021, https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf.
[3] Centro Criptológico Nacional (CCN-CERT), "*Gestión de Cibercrisis. Buenas Prácticas en la Gestión de Crisis de Ciberseguridad*", 2020, https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5428-ccn-cert-bp-20-buenas-pra-cticas-en-la-gestio-n-de-cibercrisis-1/file.html.
[4] Public Safety Canada (PSC), "*Developing an Operational Technology and Information Technology Incident Response Plan*", 2020, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dvlpng-ndnt-rspns-pln/index-en.aspx.
[5] American Public Power Association (APPA) e Nexight Group, "*Public Power Cyber Incident Response Playbook*", agosto de 2019, https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf.
[6] Government Communication Service (GCS), "*Emergency Planning Framework*", 2018, https://gcs.civilservice.gov.uk/wp-content/uploads/2020/04/Emergency-planning-framework-1.pdf.
[7] International Organization for Standardization, "*ISO 22361:2022 - Security and resilience — Crisis management — Guidelines*", https://www.iso.org/standard/50267.html.

## 2.4. ESTRUTURA DO DOCUMENTO

O essencial deste Referencial encontra-se no ponto 3 - “Referencial de Comunicação de Risco e de Crise em Cibersegurança” - do presente documento.

Neste ponto, são elencadas 3 fases que auxiliarão as Organizações que recorram a este Referencial no âmbito da comunicação referente ao risco e a crises de cibersegurança.

**Figura 1:** Estrutura do documento


A “**FASE 1:** PREPARAR A COMUNICAÇÃO DE UMA CRISE DE CIBERSEGURANÇA” debruça-se sobre a preparação e elaboração de um plano de comunicação, incluindo os passos necessários para esse fim, abordando também a necessidade de se fazer um levantamento dos riscos e de os comunicar às partes interessadas relevantes.

A “**FASE 2:** RESPONDER EFICAZMENTE” incide sobre os aspetos práticos e de execução da comunicação em contexto de crise, abordando a ativação da equipa de comunicação, as necessidades de reporte da crise e de notificação ao CNCS, bem como as necessidades de comunicar o impacto da crise, o seu encerramento formal e as indicações que poderão auxiliar a restabelecer a reputação da Organização caso esta tenha ficado afetada.

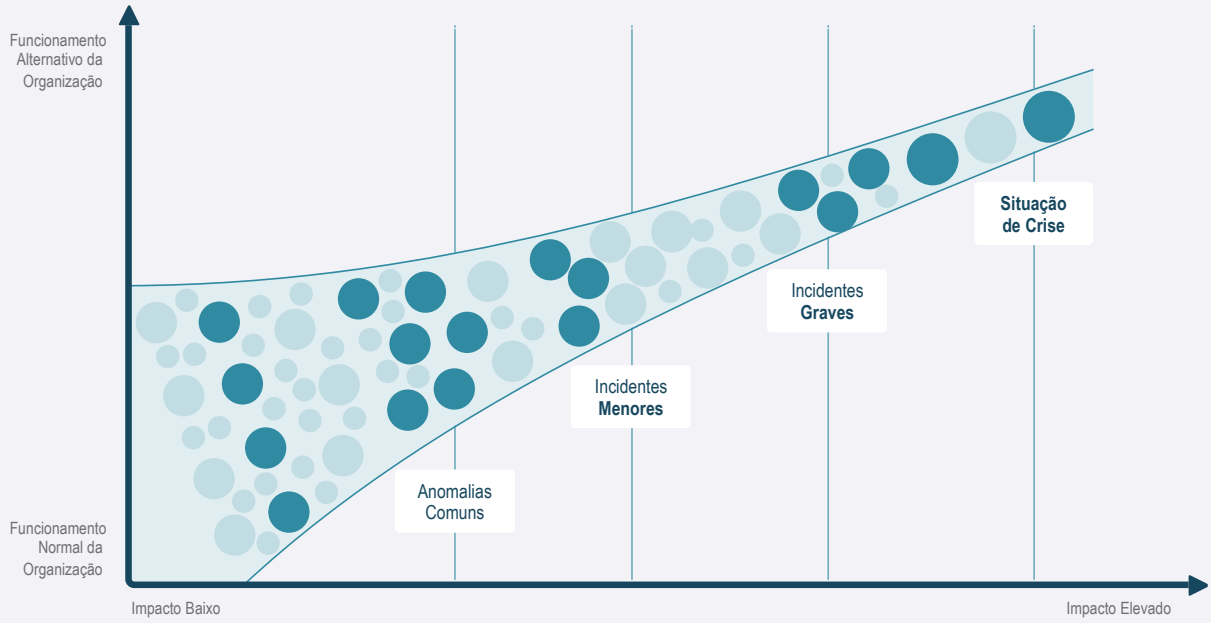
Por fim, a “**FASE 3:** LIÇÕES APRENDIDAS E MELHORIA” pretende conduzir a que se revisite o processo de análise da situação ocorrida para viabilizar a elaboração das respetivas conclusões sobre o que de positivo aconteceu, incluindo as oportunidades de melhoria no âmbito da execução do plano de comunicação. Desta forma, será facilitada a melhoria desse plano, incluindo a avaliação dos riscos a que a Organização está exposta.

**Dentro dos pontos de cada uma das fases** incluídas neste Referencial, **poderá ser encontrada uma tabela com as expectativas** relativamente ao ponto discutido **de acordo com três níveis de capacidades** - **Inicial, Intermédio e Avançado**. Estes são os mesmos níveis já encontrados no Quadro Nacional de Referência para a Cibersegurança (QNRCS) e no Quadro de Avaliação de Capacidades de Cibersegurança.

# 3. REFERENCIAL DE COMUNICAÇÃO DE RISCO E DE CRISE DE CIBERSEGURANÇA

De seguida, apresenta-se o Referencial, com base num conjunto estruturado e faseado de passos a adotar para que a comunicação relativa a riscos e crises em cibersegurança se processe de forma eficaz, agilizando procedimentos e melhorando a capacidade de resposta das Organizações em situações de crise.

**Figura 2:** Evolução do impacto de um incidente até a uma situação de crise




## O que é a Comunicação de Crise?

A comunicação de crise refere-se a todos os meios de comunicação que uma Organização pode usar para tratar um problema que afeta a sua Organização interna e respetiva reputação. Uma crise é uma situação em que o normal funcionamento de uma Organização é desestabilizado, disrompendo os processos e o ambiente operacional da mesma.

A comunicação de crise pretende, sobretudo, limitar os impactos negativos de uma crise numa Organização, seja nos seus serviços, nos seus produtos ou na sua reputação. Na eventualidade de uma crise, a prevenção, a rápida capacidade de resposta e a tomada de decisões no imediato são cruciais. Ter um plano de comunicação poderá ser a chave para gerir eficazmente a comunicação e evitar potenciais controvérsias.

A comunicação de crises deve, também, ser parte fundamental da estratégia de comunicação de uma Organização, uma vez que esta impacta todos os canais de comunicação, desde os internos aos externos, bem como as relações públicas, incluindo as relações com a imprensa e com as redes sociais.

Adicionalmente, a comunicação de crise é uma parte integral da gestão de crises, o que implica a consulta contínua junto dos membros da direção de uma Organização e junto dos membros da unidade de crise ou de resposta a incidentes.

Há duas componentes comummente reconhecidas na comunicação de crise:

- Comunicação durante a gestão da crise, que consiste em alertar os grupos de interesse e coordenar operações (QNRCS: RS.CO-2);
- Comunicação sobre como se lidou com a crise e sobre o que foi feito para ultrapassar a mesma, de modo a manter ou recuperar a reputação da Organização[8] (QNRCS: RC.CO-2).

## Porquê comunicar durante uma situação de crise?

A comunicação eficaz e eficiente durante uma situação de crise é essencial, quer para a respetiva condução, quer mesmo para a sua solução. Sem uma resposta apropriada à crise, a interpretação da situação fica aberta a cada um dos trabalhadores e demais grupos de interesse, o que pode gerar ainda mais confusão e desorganização no processo de resolução. Uma Organização que atravesse uma crise devido a um ciberataque deve, por isso, ponderar a comunicação, aos respetivos públicos de interesse, dos aspetos relevantes da mesma, reduzindo a margem para interpretações díspares e mensagens desalinhadas.

Os principais objetivos da comunicação de crise deverão ser a mitigação de eventuais preocupações dos públicos de interesse decorrentes da mesma e a proteção da imagem e da reputação da Organização. Neste processo, deverá existir a preocupação de veicular informação genuína, verosímil e consequente, em face da situação em questão[9].

## Organizações diferentes devem atuar de forma diferente

As Organizações não são todas iguais. Diferem em diversos aspetos, como na sua dimensão, no setor de atividade, nos recursos disponíveis, no tipo de dados e informações a que atribuem mais valor e até mesmo no nível de maturidade em cibersegurança. Atendendo a estas diferenças, apresentar uma única abordagem à comunicação de crise seria desajustado para a realidade de muitas Organizações. Assim sendo, **optou-se por, dentro dos pontos das fases incluídas neste Referencial, estabelecer o que é esperado de Organizações com diferentes níveis de capacidades, de acordo com os três níveis definidos no Quadro de Avaliação de Capacidades de Cibersegurança do CNCS - Inicial, Intermédio e Avançado.**

[8] C-Risk, *"Crisis Communication: How to manage crisis communication after a cyberattack?*", August 2, 2021, updated May 2, 2023, https://www.c-risk.com/en/blog/crisis-communication/.

[9] C-Risk, "*Crisis Communication*".

Tabela 1

| EXPECTATIVAS POR NÍVEL DE CAPACIDADES – VISÃO GERAL | |
|---|---|
| **Nível Inicial** | • Os processos/medidas/atividades, apesar de se verificarem, não estão estruturados ou definidos em plano, e são sobretudo executados de forma pontual / *ad hoc* em iniciativas isoladas e pouco formais. |
| **Nível Intermédio** | • Os processos/medidas/atividades estão planeados, documentados e formalizados, sendo executados e revistos com relativa regularidade. |
| **Nível Avançado** | • Os processos/medidas/atividades estão planeados, documentados e formalizados, envolvem monitorização contínua, avaliação e revisão recorrentes, em intervalos definidos, levando em consideração alterações, incidentes, testes e exercícios, para melhoria proativa dos mesmos. |

Importa sublinhar que, apesar de haver expectativas diferentes consoante o nível de capacidades das Organizações, existem elementos básicos que devem ser observados de forma transversal, em todos os níveis, mesmo no nível Inicial.

Estando estabelecidas as bases, as Organizações devem procurar atingir níveis de capacidades superiores, num exercício de melhoria contínua, de modo a aumentarem cada vez mais a sua resiliência e capacidade de resposta a situações de crise.

FASE 1

# PREPARAR A COMUNICAÇÃO DE UMA CRISE DE CIBERSEGURANÇA

# **FASE 1:** PREPARAR A COMUNICAÇÃO DE UMA CRISE DE CIBERSEGURANÇA

## 1. DEFINIR INCIDENTES E CRISE DE CIBERSEGURANÇA

Em qualquer um dos níveis de capacidades é essencial, para tornar a comunicação de uma crise de cibersegurança mais eficiente, definir o que é um incidente de cibersegurança e em que consiste uma crise de cibersegurança.

### O que é um incidente de cibersegurança?

Um incidente de cibersegurança é um evento com um efeito adverso real na segurança das redes e dos sistemas de informação[10].

### O que é uma crise de cibersegurança?

Uma crise é definida na ISO 22361:2022 como "uma situação ou um evento anormal ou extraordinário que ameaça a organização ou a comunidade e requer uma resposta estratégica, adaptativa e atempada de modo a preservar a sua viabilidade e integridade"[11].

Uma crise de cibersegurança pode ser definida do mesmo modo, com a adição de que a situação ou o evento anormal ou extraordinário resultam de um ou mais incidentes originados no ciberespaço de interesse da organização, com o potencial de afetar a confidencialidade, a integridade e a disponibilidade dos seus sistemas de informação e estrutura tecnológica.

Para responder adequadamente a uma crise de cibersegurança, torna-se fundamental a preparação dos procedimentos de comunicação para a gestão dessas situações. Uma vez que é difícil pré-determinar a duração de uma crise, bem como de calcular o impacto que esta poderá ter numa Organização, é imprescindível que a comunicação durante a mesma se processe de forma ágil e eficaz. A comunicação durante a gestão da crise requer, por isso, adequada preparação, de modo a garantir que o processo de ação é bem-sucedido, que se realiza de forma simples e frequente e que permite inteirar as entidades envolvidas e afetadas pela crise quanto à evolução da recuperação dos sistemas impactados.

[10] Lei n.º 46/2018, de 13 de agosto.

[11] International Organization for Standardization, "*ISO 22361:2022*", 2.

## 1.1. EFETUAR LEVANTAMENTO DE RISCO

Antes de se definir propriamente um plano de comunicação de crise, deve ser efetuado um levantamento dos riscos aos quais a organização está exposta.

De acordo com o **Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança**, um processo de Levantamento dos Riscos procura identificar, quantificar e descrever os riscos e capacitar as Organizações a priorizá-los de acordo com a sua gravidade percecionada, ou com outros critérios estabelecidos[12].

Este processo divide-se em três etapas principais:

- Identificação dos riscos;
- Análise dos riscos;
- Avaliação dos riscos.

Os objetivos deste levantamento passam por determinar o valor dos ativos de informação, identificar as ameaças e vulnerabilidades que lhes estão associadas, identificar os controlos existentes e os seus efeitos no risco identificado, determinar as consequências ou impactos possíveis e, por último, priorizar os riscos derivados.

Esta análise revelar-se-á uma etapa crucial para perceber quais os cenários e riscos que podem ocorrer e sobre os quais se deve trabalhar de maneira a comunicar de forma eficiente quando ocorrerem.

## 1.2. COMUNICAÇÃO DOS RISCOS

Uma vez identificados, analisados e compreendidos os riscos é altura de utilizar essa informação para construir o plano de comunicação adaptado a cada um dos cenários de risco identificados.

Segundo o **Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança**, a comunicação dos riscos é uma atividade que tem como objetivo alcançar não só o consenso sobre como gerir os riscos de segurança da informação e cibersegurança, através da troca e/ou partilha das informações sobre os riscos entre os responsáveis e as outras partes interessadas, como promover a consciencialização sobre a importância do processo de gestão dos riscos em toda a organização.

[12] Centro Nacional de Cibersegurança (CNCS), "*Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança*", versão 1.1., dezembro de 2022, 10, https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.

Tabela 2

| EXPECTATIVAS QUANTO AO LEVANTAMENTO E COMUNICAÇÃO DOS RISCOS POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • Os riscos são identificados, mas não existe processo formal de tratamento; |
| **Nível Intermédio** | • Os riscos são identificados e tipificados nos ativos de informação;<br>• Existe um processo de gestão de riscos que monitoriza os ativos, de acordo com riscos atuais e novos;<br>• Existe um mapa de ameaças conhecidas, associado a cada tipo de ativo;<br>• Existe uma indicação de tratamento de cada ameaça mapeada;<br>• Os riscos são priorizados conforme os critérios de tratamento estabelecidos, de acordo com o nível de exposição percebida e a importância do ativo para a organização;<br>• Os riscos são comunicados de forma sistematizada, estando documentados e disponibilizados de forma consultável. |
| **Nível Avançado** | • Existe um processo formal de revisão e análise recorrente dos riscos identificados;<br>• Os riscos e vulnerabilidades são identificados automaticamente por sistemas de pesquisa de vulnerabilidades dedicados;<br>• O processo de gestão de riscos encontra-se estabelecido com critérios definidos e os seus resultados e estratégias de tratamento são revistos em intervalos regulares;<br>• O processo de gestão de riscos é avaliado e testado quanto à sua efetividade;<br>• Os riscos são categorizados numa escala de importância para a priorização dos tratamentos;<br>• O tratamento dos riscos tem em conta o custo financeiro e operacional entre o dano previsto e o custo financeiro e operacional de implementação dos controlos definidos.<br>• Os riscos são comunicados de forma sistematizada, estando documentados, disponibilizados de forma consultável e tendo sido definidos e aprovados pela gestão de topo. |

## 2. DEFINIR UM PLANO DE COMUNICAÇÃO PARA VÁRIOS CENÁRIOS DE RISCO E CRISE

Tendo em conta os múltiplos aspetos de uma crise, desde a sua imprevisibilidade à velocidade com que tudo se pode alterar, é importante que a Organização estabeleça, para diferentes cenários de crise, os níveis de criticidade e categorização adequados para uma aplicação correta e flexível do plano de comunicação de crise, como indicado no QNRCS (RS.CO-4).

Face a essa imprevisibilidade, apresentam-se de seguida alguns pressupostos a ter em consideração aquando da elaboração de um plano de comunicação de crise, para que o mesmo se adeque a situações variadas.

### Pressupostos a ter em conta na elaboração do plano de comunicação

Apesar de não existirem duas crises iguais, existem alguns pressupostos que devem ser tidos em consideração aquando da elaboração de um plano de comunicação perante um cenário de crise de cibersegurança.

- **Rapidez**
  Durante uma ocorrência de cibersegurança é importante que a comunicação seja feita rapidamente e que alcance de imediato o pessoal referenciado com responsabilidades de ação. Para que tal aconteça, é fundamental que, com a devida antecedência, se identifique o tipo de crise e os colaboradores-chave.

- **Transparência**
  É um pressuposto que deve estar implícito aquando da preparação de um plano de comunicação de crise de cibersegurança e que deve ser observado ao longo de toda a situação de crise. As organizações, tanto as do setor privado como as do setor público, devem ser tão transparentes e informativas quanto possível.

- **Flexibilidade**
  Embora o planeamento da resposta a uma crise seja muito útil, é natural que situações imprevistas ocorram, tornando-se importante, previamente, garantir a flexibilidade do plano de forma que seja possível a sua adaptação perante essas situações imprevistas[13].

- **Unicidade da mensagem**
  Em situações de crise, é essencial que as Organizações comuniquem a uma só voz.
  Por comunicar a uma só voz entenda-se comunicar a mesma mensagem, mantendo a coesão
  e a coerência da organização, sem versões alternativas ou acrescentos. A mensagem deve ser a mesma, independentemente de com quem se contacte dentro da Organização. A Organização deve comunicar o que é mais relevante, e deve ser a Organização a controlar o fluxo de comunicação, de modo a proteger a sua reputação e diminuir os potenciais impactos da crise (QNRCS: RC.CO-1).

## 2.1. EXEMPLOS DE CENÁRIOS DE CRISE DE CIBERSEGURANÇA

No quadro seguinte apresentam-se alguns exemplos de tipos de cenários que podem levar a uma crise de cibersegurança, os possíveis alvos e o que deve ser tido em consideração sobre a comunicação a realizar e indicações sobre os grupos de interesse que devem receber comunicações sobre a crise em questão.

[13] GCS, "*Emergency Planning Framework*", 7.

Tabela 3

| TIPO DE CENÁRIO | ALVOS MAIS FREQUENTES | CONSIDERAÇÕES SOBRE O QUE COMUNICAR | A QUEM COMUNICAR |
|---|---|---|---|
| **Comprometimento de sistemas próprios do trabalho remoto** | Banca, Saúde, serviços de *streaming*, serviços postais e de transporte, operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | O que é preciso dizer, a quem e porquê?<br>Como é que o conteúdo da mensagem pode variar de acordo com o público e como será feita essa distinção?<br>Fará sentido definir tipos de comunicação distintos para contatos internos e externos?<br>Quem precisa de estar envolvido na elaboração da mensagem?<br>Se já ocorreu uma situação de crise, os canais de comunicação utilizados funcionaram para a organização ou foram afetados pela crise?<br>Que canais de comunicação tem neste momento à sua disposição?<br>Qual é a melhor forma de alcançar o seu público numa situação de crise?<br>Qual a gravidade da crise?<br>Quem poderá ser afetado?<br>Quais as possíveis consequências desta crise para cada um dos grupos de interesse?<br>Qual a probabilidade dos impactos da crise sobre os clientes serem amplamente divulgados nos meios de comunicação social?<br>Qual é o número atual de pedidos de informação por parte dos clientes? Está além do "normal"?<br>Somos obrigados a partilhar informações com a população impactada?<br>Quais são os impactos reputacionais atuais e potenciais?<br>É preciso emitir comunicações de forma proativa para as principais partes interessadas? Sabemos priorizar as comunicações / notificações?<br>Sabemos quais os cronogramas que precisamos de cumprir para comunicações / notificações? | Direção<br>Colaboradores |
| **Ciberespionagem** | Operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | | Vítimas da crise<br>Autoridades<br>CNCS<br>Direção |
| **Comprometimento de cadeias de fornecimento** | Operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | | Fornecedores<br>Colaboradores<br>Direção |
| **Comprometimento de contas** | Operadores de serviços essenciais, Administração Pública, Órgãos de Soberania e cidadão em geral | | Clientes<br>Fornecedores<br>Colaboradores<br>Direção |
| **DDoS (*Distributed Denial of Service*)** | Operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | | Direção<br>Clientes<br>Fornecedores<br>Colaboradores<br>CNCS |
| ***Defacements*** | Operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | | Direção<br>Clientes<br>Fornecedores<br>Colaboradores<br>CNCS |
| **Exploração de vulnerabilidades** | Operadores de serviços essenciais, Administração Pública, Órgãos de Soberania e cidadão em geral | | Direção<br>Vítimas da crise<br>CNCS |
| **Intrusões** | Operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | | Direção<br>Vítimas da crise<br>CNCS |
| ***Phishing*, *phishing* massificado e *spear phishing*** | Banca, Saúde, serviços de *streaming*, serviços postais e de transporte, operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | | Direção<br>Vítimas da crise<br>CNCS<br>Fornecedores |
| ***Ransomware* e/ou cibersabotagem** | Operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | | Direção<br>Colaboradores |
| **Abuso de IA (Inteligência Artificial)** | Operadores de serviços essenciais, Administração Pública e Órgãos de Soberania | | Vítimas da crise<br>Autoridades<br>CNCS<br>Direção |
| ***Deep fakes* e desinformação variada** | Operadores de serviços essenciais, Administração Pública, Órgãos de Soberania e cidadão em geral | | Fornecedores<br>Colaboradores<br>Direção |

**Fonte:** Centro Nacional de Cibersegurança e Observatório de Cibersegurança, "*Relatório Cibersegurança em Portugal: Riscos e Conflitos*", 4.ª edição, junho de 2023.

## 2.2. CRIAR UMA EQUIPA DE COMUNICAÇÃO DE CRISE DE CIBERSEGURANÇA

Para que um plano de comunicação realmente funcione e seja útil num momento de instabilidade provocada por uma crise de cibersegurança, é necessário que sejam atribuídas funções e responsabilidades e que estas estejam devidamente documentadas no plano. Recomenda-se que estejam atribuídas as funções de seguida elencadas, sendo possível atribuir mais do que uma função à mesma pessoa. Deve-se definir:

- O **ponto de contacto para incidentes/crises** de cibersegurança e o modo de o contactar[14];
- As **tarefas de resposta a incidentes/crises** a serem executadas e **quem executa cada tarefa**;
- O/a **responsável por gerir a resposta global ao incidente/crise** (deverá pertencer à organização e ter autoridade para a tomada de decisões);
- O/a **responsável pelo contacto e transmissão de informação com a gestão de topo**;
- O/a r**esponsável pelo contacto com parceiros externos de resposta a incidentes**;
- O/a **responsável pelo reporte da situação junto das autoridades** (ex: polícia, CNCS, Autoridade Nacional de Segurança);
- O/a **responsável pela comunicação com a comunicação social e com os parceiros externos**;
- Quem **exercerá as funções de porta-voz** (poderá haver mais do que uma pessoa nesta função, de acordo com as necessidades da Organização);

**Tabela 4**

| EXPECTATIVAS QUANTO À EQUIPA DE COMUNICAÇÃO DE INCIDENTES POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • Não existe uma equipa definida, no entanto há conhecimento informal e não estruturado das funções de cada interveniente da organização. |
| **Nível Intermédio** | • A equipa está definida.<br>• Os colaboradores têm conhecimento dos procedimentos a seguir e das responsabilidades a cumprir. |
| **Nível Avançado** | • A equipa está definida e são realizados exercícios de treino de execução do plano regularmente.<br>• Os colaboradores têm conhecimento dos procedimentos a seguir e das responsabilidades a cumprir.<br>• As partes externas relevantes são envolvidas nas atividades de comunicação. |

[14] Recorde-se que, de acordo com o Decreto-lei n.º 65/2021, de 30 de julho, a Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais devem nomear um ponto de contacto permanente para a segurança da sua rede e dos seus sistemas de informação de modo a permitir a comunicação contínua com as autoridades competentes no caso de ocorrência de um incidente de cibersegurança.

## 2.3. IDENTIFICAR GRUPOS DE INTERESSE

Uma crise raramente envolve uma única Organização, por isso é fundamental que se identifique quem mais terá interesse na resolução da crise e se encontrem maneiras de tornar essa resolução um esforço integrado.

As relações e os protocolos estabelecidos com outras organizações poderão ser uma ajuda valiosa numa situação de crise. Saber quem contactar junto de cada entidade externa é essencial numa situação de crise, uma vez que permitirá às Organizações poupar tempo na realização dos contactos necessários e dedicar-se à resolução da crise.

À medida que novas relações e protocolos são iniciados e outros são terminados, é importante que a identificação das partes interessadas relevantes seja regularmente atualizada, de modo a evitar tanto o contacto com organizações que já não são relevantes no contexto atual, como a evitar a falta de ligação com as organizações que devem realmente ser contactadas, informadas e incluídas na comunicação e resolução da crise.

Igualmente importante é ter em mente o público a quem a Organização se dirige, uma vez que este poderá responder de maneira imprevisível perante uma situação de crise.

**Tabela 5**

| EEXPECTATIVAS QUANTO À IDENTIFICAÇÃO DE GRUPOS DE INTERESSE POR NÍVEL DE CAPACIDADE | |
|---|---|
| **Nível Inicial** | • A Organização consegue identificar os grupos de interesse internos e externos e fá-lo de forma pontual, não existindo um intervalo definido para a atualização desse registo.<br>• A identificação não está amplamente divulgada e não é conhecida por todos os trabalhadores essenciais. |
| **Nível Intermédio** | • A Organização consegue identificar os grupos de interesse internos e externos e fá-lo com alguma regularidade.<br>• A identificação está divulgada e é do conhecimento de todos os trabalhadores essenciais. |
| **Nível Avançado** | • A Organização consegue identificar os grupos de interesse internos e externos, sendo estes revistos em intervalos regulares definidos.<br>• A identificação está divulgada e é do conhecimento de todos os trabalhadores.<br>• Os relacionamentos e os protocolos com os grupos de interesse internos e externos são revistos em intervalos regulares definidos, mantendo o registo atualizado. |

## 2.4. DESENVOLVER UMA LISTA DE CONTACTOS 24/7 PARA OS COLABORADORES E PARCEIROS DE RESPOSTA

Para ter um plano de comunicação eficaz é fundamental ter uma lista de pessoas-chave que estejam envolvidas na gestão de crises de cibersegurança e que estejam informadas sobre a crise em questão.

Essas pessoas-chave podem ser divididas em contactos internos e externos para facilitar a organização da lista. Deve-se garantir que se dispõe dos contactos corretos de cada uma dessas pessoas e que se identificou a melhor forma de as contactar.

A **lista de contactos interna** deve incluir:

- Líderes dos departamentos na equipa de resposta a incidentes/crises (gestão de topo, segurança de IT, colaboradores das operações, relações públicas, representantes legais, etc.);
- CISO (*Chief Information Security Officer*) e o departamento de segurança de TI;
- Responsável pela comunicação;
- Colaboradores com responsabilidades operacionais[15].

A Organização deve certificar-se de que tem a lista de contatos atualizada e hierarquizada pelos principais responsáveis da Organização e um responsável pela comunicação. Esta lista deverá incluir os horários em que os funcionários estão ausentes e respetiva informação de contacto como, por exemplo, os nomes, funções, contactos e informações de *backup* dos mesmos e as possíveis alternativas para cada função. Recomenda-se que esta lista seja mantida *online* e também num local *offline* e deve ser divulgada junto dos elementos da equipa de resposta a incidentes/crises de cibersegurança.

A **lista de contactos externa** deve incluir:

- Fornecedores de sistemas críticos, que podem fornecer informações sobre a importância das entradas de *logs* ou ajudar a identificar falsos positivos para certas assinaturas de deteção de intrusão;
- Fornecedor de serviços de Internet, que pode fornecer informações solicitadas sobre os principais ataques na rede, identificar as potenciais origens ou potencialmente bloquear os caminhos de comunicação conforme necessário;
- Fornecedores de serviços de segurança contratados para monitorização, investigação e análise forense e resposta a incidentes/crises, se aplicável;
- Corretores de seguros e outros recursos legais ou comerciais para apoiar a continuidade do negócio;
- Comunicação Social[16].

[15] APPA e Nexight Group, "*Public Power Cyber Incident Response Playbook*", 10.
[16] APPA e Nexight Group, "*Public Power Cyber Incident Response Playbook*",10-11.

Depois de identificados todos os grupos de interesse relevantes para uma resposta a incidentes/crises é importante identificar os contactos de parceiros de resposta a incidentes pertencentes ao mesmo setor da Organização e do governo como:

- Contactos com as autoridades (ex: agências locais);
- Contactos de organizações para reporte de incidentes/crises e partilha de informação através dos Centros de Análise e Partilha de Informação (ISAC);
- Contactos de assistência de cibersegurança (ex: CERT.PT);
- Contactos com clientes/utentes.

Garantir um bom relacionamento com os principais grupos de interesse é essencial. Mesmo que não seja possível assegurar esse bom relacionamento previamente, é importante que, durante uma situação de crise, a comunicação reflita esse objetivo.

**A comunicação junto dos grupos de interesse não se trata de um mero formalismo, mas sim de uma prioridade**. A comunicação de informações aos grupos de interesse evita a disseminação de informações falsas e garante que estes se sentem informados e tranquilos. A organização deve assegurar-se de que identifica a maneira mais eficaz de comunicar com os grupos de interesse. Quando dentro de uma Organização existem departamentos de grandes dimensões, poderá ser útil dividi-los por áreas para que se torne mais acessível o contacto numa situação de crise[17].

Recomenda-se que se identifique uma ou mais pessoas, caso a dimensão da estrutura da Organização o justifique, como **porta-voz/es**, responsável/eis por **comunicar os aspetos importantes com a comunicação social**. Os responsáveis pelo tratamento da comunicação têm como principais responsabilidades a gestão da informação e o apoio aos porta-vozes de modo a proteger a reputação da Organização e garantir que todas as mensagens que passam são consistentes. Não se recomenda que se aguarde por uma situação de crise para treinar os porta-vozes da Organização, que devem ser treinados antecipadamente para este propósito. As Organizações devem certificar-se de que reservam tempo para treinar a abordagem a ser feita para quando for necessário.

[17] GCS, "*Emergency Planning Framework*", 9.

Tabela 6

| EXPECTATIVAS QUANTO À LISTA DE CONTACTOS 24/7 POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | Existe uma lista de contactos internos e uma lista de contactos externos e são atualizadas pontualmente.<br>A lista interna está hierarquizada. |
| **Nível Intermédio** | Existe uma lista de contactos internos e uma lista de contactos externos que são atualizadas com alguma regularidade.<br>As listas estão hierarquizadas e incluem os horários de ausência e formas alternativas de contacto para esses horários. |
| **Nível Avançado** | Existe uma lista de contactos internos e uma lista de contactos externos que são atualizadas em intervalos regulares definidos.<br>As listas estão hierarquizadas e incluem os horários de ausência e formas alternativas de contacto para esses horários.<br>As listas incluem contactos (pessoas) alternativos para situações de indisponibilidade dos contactos primários.<br>Os porta-vozes foram treinados para potenciais situações de crise. |

## 2.5. DEFINIR TEMPLATES DE COMUNICAÇÃO PARA OS DIFERENTES GRUPOS DE INTERESSE

A equipa de resposta a incidentes/crises deve pré-estabelecer *templates* de comunicação e diretrizes apropriadas sobre o tipo e o nível de informação que deve ser fornecida tanto às equipas técnicas, como aos *middle managers*, gestão de topo, parceiros industriais, CERT.PT, público, e demais entidades relevantes. Protocolos apropriados de revisão e aprovação devem também ser estabelecidos para permitir que as informações sejam divulgadas a outros participantes, parceiros e grupos de interesse, conforme a sua relação com a crise e o respetivo impacto resultante.

### Os *templates* de comunicação pré-estabelecidos deverão definir:

- O que comunicar: que conteúdo, o que é necessário dizer imediatamente (por exemplo: a forma adequada como foi tratada uma crise de cibersegurança) a contactos internos e externos, como é que o conteúdo pode/deve variar em função do público e como deve ser feita essa distinção;
- Que mensagem: forma e formato, que tipo de meio será usado, desde pequenos textos a imagens, metáforas, vídeos, entre outros;
- Quem deve comunicar: deve ser nomeado um responsável/porta-voz com a autoridade e autonomia para comunicar, particularmente com organizações externas;
- A quem comunicar: destinatários da comunicação;
- Como comunicar: que canais devem ser usados para obter a melhor eficácia na difusão da mensagem (por exemplo: mensagens de correio eletrónico e protetores de ecrã)[18].

[18] GCS, "*Emergency Planning Framework*", 17.

Exemplos de *templates* de comunicação estão contidos no Anexo 1.

**Tabela 7**

| EXPECTATIVAS QUANTO AOS *TEMPLATES* DE COMUNICAÇÃO POR NÍVEL DE CAPACIDADE | |
|---|---|
| **Nível Inicial** | • A organização tem definido um *template* de comunicação genérico para utilizar em situações de crise;<br>• O *template* de âmbito geral é utilizado tanto internamente como externamente. |
| **Nível Intermédio** | • A organização tem definidos *templates* de comunicação diferentes para a utilização interna e externa;<br>• A organização tem definidos *templates* de comunicação diferentes para a utilização interna e externa e para diferentes graus de severidade da crise. |
| **Nível Avançado** | • A organização tem definidos *templates* de comunicação diferentes para a utilização interna e externa;<br>• A organização tem definidos *templates* de comunicação diferentes para a utilização interna e externa e para diferentes graus de severidade da crise;<br>• A organização tem definidos *templates* de comunicação diferentes para utilização interna e externa e ajustados aos públicos-alvo a que pretende dirigir-se (ex: internos - diferentes departamentos, como recursos humanos, dept. jurídico, dept. financeiro, entre outros; externos - clientes, comunicação social, parceiros de negócio, entre outros). |

## 2.6. DETERMINAR OS MEIOS ATRAVÉS DOS QUAIS A COMUNICAÇÃO SERÁ FEITA

Quando surge uma crise, é imprescindível dispor de meios de comunicação rápidos e eficazes para dar a conhecer os aspetos do acontecimento aos grupos de interesse rapidamente. Devem ser consideradas quais as melhores e mais rápidas maneiras de divulgar informação na organização e certificar-se de que se dispõe dos dados de contacto necessários corretos e que estão disponíveis.

Neste ponto é importante considerar as seguintes questões:

- Se a Organização já passou por uma situação de crise, os canais utilizados funcionaram? Ou ficaram afetados pela crise?
- Que canais de comunicação tem neste momento a Organização à sua disposição?
- Qual é a melhor forma de alcançar os públicos relevantes para a Organização numa situação de crise?

As necessidades de comunicação são distintas para diferentes organizações e diferentes tipos de crises. Recomenda-se que se identifiquem espaços, como salas de reunião e canais de comunicação, para situações de crise. A organização deve estar ciente de que os sistemas digitais dos quais normalmente dependem as comunicações podem ser afetados durante a ocorrência de incidentes e crises de cibersegurança.

Recomenda-se que o plano de comunicação providencie várias alternativas de comunicação viáveis para os membros da equipa de resposta a incidentes/crises. Sugere-se que contenha também instruções específicas para cada alternativa para o caso de o sistema primário de comunicação ficar indisponível durante um incidente ou crise.

Para ações internas diretas e para a disseminação de informação necessária, devem ser utilizados canais de comunicação internos seguros como o *e-mail* e mensagens de *chat* cifradas, sendo que apenas alguns detalhes serão compartilhados com os grupos de interesse.

### Alguns exemplos de comunicações alternativas que incluem:

- Portais *web* seguros e acessíveis pela rede pública com sistemas de autenticação separados;
- Ligações à Internet secundárias e terciárias, como dados móveis ou satélite;
- *E-mail* com as listas de distribuição de resposta a incidentes/crises previamente definidas;
- Sistemas de colaboração baseados na Internet e/ou canais de comunicação de áudio;
- Telemóveis;
- Telefones fixos;
- Telefones satélite;
- Sistemas de rádio VHF/UHF (*Very High Frequency/ Ultra High Frequency*)[19].

[19] PSC, "*Developing an Operational Technology and Information Technology Incident Response Plan*", 28- 29.

Tabela 8

| EXPECTATIVAS QUANTO AOS MEIOS ALTERNATIVOS DE COMUNICAÇÃO POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • A Organização dispõe de meios de comunicação alternativos para comunicações por e-mail e comunicações telefónicas. |
| **Nível Intermédio** | • A Organização dispõe de meios de comunicação alternativos para comunicações por e-mail e comunicações telefónicas seguras e cifradas/encriptadas.<br>• A Organização dispõe de um sítio web alternativo próprio ou de perfil nas redes sociais que serve como ponto único de comunicação para o público em geral. |
| **Nível Avançado** | • A Organização dispõe de todos os meios anteriores, suportados por sistemas de redundância, como sistemas de comunicação via satélite que asseguram a viabilidade das comunicações em situação de crise. |

## 2.7. DEFINIR ESTRATÉGIA DE COMUNICAÇÃO DURANTE A MITIGAÇÃO

Durante a ocorrência de uma situação de crise, o principal objetivo de uma Organização será mitigar e ultrapassar essa situação. Para tal, a Organização deve definir e aplicar processos e procedimentos sistematizados, para a resolução e tratamento de incidentes e crises (QNRCS: RS.MI-2).

Estando estabelecido com quem comunicar e o que comunicar, deve-se decidir **quando** comunicar. Os momentos de comunicação de um incidente ou crise às partes interessadas relevantes são importantíssimos, e é igualmente relevante saber definir os momentos em que o silêncio é uma opção mais sensata.

Dito de outro modo, **deve-se considerar que, de modo a não alertar o(s) atacante(s) de que se sabe das suas ações, pode ser necessário definir uma fase de não comunicação** desde o momento em que o incidente foi detetado até ao momento em que se tenha uma imagem completa do incidente/ crise e esteja traçado um plano para a mitigação do mesmo. Se o(s) atacante(s) for(em) alertado(s), poderá/ão abandonar o ataque e tentar eliminar qualquer rasto, ou então tentar provocar um dano final, como furtar a informação mais importante à organização ou instalar *backdoors*[20].

De forma a evitar fugas de informação durante este período de não-comunicação, deve-se manter uma lista das pessoas que estão cientes da ocorrência do incidente ou crise de cibersegurança. Através desta lista será mais fácil detetar a pessoa responsável pela fuga, quando a mesma acontecer, podendo assim tomar ações legais.

[20] CSC, "*Cyber Security Incident Management Guide*", 31.

Assim sendo, os momentos da comunicação devem ser baseados nos objetivos definidos anteriormente, nas necessidades da Organização para a mitigação e nas necessidades dos diversos grupos de interesse.

**Tabela 9**

| EXPECTATIVAS QUANTO À COMUNICAÇÃO DURANTE A MITIGAÇÃO POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • A comunicação durante a fase de mitigação dos incidentes/crises é efetuada de forma reativa e não estruturada. |
| **Nível Intermédio** | • A comunicação durante a mitigação segue procedimentos pré-definidos.<br>• Os procedimentos de mitigação e as ações de comunicação durante a mitigação são documentados. |
| **Nível Avançado** | • A comunicação é realizada de forma eficiente até à mitigação do incidente/crise.<br>• É realizada uma análise das ações de comunicação durante o tratamento dos incidentes/crises para efeitos de melhoria contínua. |

## 2.8. TESTAR O PLANO DE COMUNICAÇÃO ATRAVÉS DE EXERCÍCIOS

Responder com eficácia a uma crise requer que a resposta seja testada anteriormente. Neste processo de treino é fundamental envolver os grupos de interesse relevantes de forma a garantir e reforçar a relação entre ambas as partes.

Até ao momento em que um plano de crise de cibersegurança é efetivamente testado, dificilmente se garante que o mesmo realmente funciona numa situação de crise.

A preparação e o teste dos aspetos que devem constituir um plano de emergência são pontos cruciais na preparação de uma crise de forma a identificar os pontos fracos existentes e apoiar a Organização e os colaboradores a tomarem consciência dos mesmos, e assim identificarem medidas para os endereçar.

Por que são os exercícios de testagem do plano tão importantes? Porque permitem:

- Treinar;
- Testar;
- Validar o plano.

Que tipo de exercício é o correto para a Organização? O tipo de exercício a escolher dependerá de vários fatores onde se incluem a duração, o valor, as instalações e a disponibilidade dos participantes.

De seguida apresentam-se três opções para exercícios de treino e os prós e contras de cada tipo de exercício:

**Tabela 10**

| EXERCÍCIOS BASEADOS EM DISCUSSÃO | EXERCÍCIOS DE MESA | EXERCÍCIOS REAIS |
|---|---|---|
| Cria oportunidade para se discutirem os planos em contexto de grupo, permite que a abordagem seja verificada e corrigida e garante que todos tenham uma noção clara da estratégia. | São exercícios de simulação de cenários específicos. São bons para validar planos e explorar possíveis pontos fracos. | Envolvem um treino completo e ao vivo da implementação de uma estratégia. Funcionam bem para testar a logística, as comunicações e as capacidades físicas. |
| **PRÓS** | | |
| • Baixo custo, rápidos e relativamente fáceis de configurar.<br>• Úteis na fase de desenvolvimento para redefinir os planos.<br>• Garantem que todos têm uma visão clara dos planos. | • Úteis para testar planos de *stress* e ajudar os envolvidos a entender o seu papel.<br>• Podem identificar potenciais pontos fracos na abordagem.<br>• Ajudam a fortalecer as relações de trabalho de forma prática. | • Equipas ganham experiência direta e prática de cenários, aprendendo fazendo.<br>• Testam como o *staff* e os sistemas podem responder numa situação de crise real.<br>• Testam desafios lógicos e operacionais bem como a estratégia. |
| **CONTRAS** | | |
| • Maior dificuldade para testar desafios logísticos e operacionais que podem ocorrer durante uma crise.<br>• Não permitem testar como é que o staff e os sistemas irão reagir na “vida real”. | • Requerem cuidado no planeamento e desenvolvimento de cenários apropriados.<br>• Identificar o formato e o local pode ser um desafio.<br>• Não permitem testar como é que o *staff* e os sistemas irão reagir na “vida real”. | • Podem ter custos muito elevados e levar muito para planear e pôr em prática.<br>• Podem ter consequências não intencionais, como minar a confiança da equipa. |

**Fonte:** GCS, “*Emergency Planning Framework*”.

### Recomendações para os exercícios de teste do plano de comunicação de crises:

A Organização deve estabelecer objetivos claros para os exercícios a realizar. Tentar testar todos os aspetos de um plano num único exercício poderá ser excessivamente ambicioso ou até mesmo contraproducente. Recomenda-se, por isso, que os exercícios sejam orientados no sentido de testar a capacidade de execução das funções definidas e atribuídas no plano, distribuindo essas funções por vários exercícios a serem realizados em diferentes momentos[21].

Ter vários exercícios que testem diferentes capacidades em vez de um único exercício que procure testar todos os aspetos do plano não significa simplificar excessivamente os exercícios. Para cada exercício, o cenário de crise definido deve ser adequadamente desafiante, complexo e realista, refletindo as características gerais de uma situação de crise passível de ocorrer dentro da Organização[22].

## 2.8.1. AVALIAÇÃO DOS EXERCÍCIOS

Após a realização de cada exercício, a Organização deve avaliar se o desempenho verificado durante estes se adequa ao desempenho pretendido. Caso se tenha ficado aquém do pretendido, as falhas verificadas devem ser identificadas e registadas de modo que se possa trabalhar nelas e colmatá-las posteriormente[23].

No processo de avaliação, é importante que as Organizações façam uma análise rigorosa do desempenho obtido num exercício e que não desconsiderem quaisquer falhas verificadas. Uma falsa sensação de segurança na capacidade de resposta a crises pode ter consequências gravosas para uma Organização. Aconselha-se, também, que não se atente apenas às falhas humanas, mas que se verifique também se o próprio plano de comunicação de crises responde às necessidades da Organização durante uma crise, ou se este também deve ser alvo de melhorias.

Uma vez analisado o desempenho durante o exercício e identificadas as falhas ocorridas, deve ser elaborado e implementado um plano de ação para corrigir essas falhas. Uma vez corrigidas essas falhas (e tendo a correção dessas falhas sido testada em exercícios posteriores), poder-se-á identificar essa correção como “lições aprendidas”[24].

[21] International Organization for Standardization, “*ISO 22361:2022*”, 33.
[22] International Organization for Standardization, “*ISO 22361:2022*”, 33.
[23] International Organization for Standardization, “*ISO 22361:2022*”, 34.
[24] International Organization for Standardization, “*ISO 22361:2022*”, 34.

As atividades pós-exercício devem incluir:

- Questionários estruturados para os intervenientes no exercício;
- Escrutínio e avaliação das decisões e da sua implementação;
- Identificação dos pontos fortes observados e das oportunidades de melhoria;
- Análise do cumprimento dos objetivos definidos para o exercício em causa;
- Lições identificadas e relevância das mesmas para a capacitação da Organização;
- Planos de ação para a implementação das lições e mecanismo de confirmação da mesma.

### 2.8.2. VALIDAÇÃO DOS EXERCICIOS E DO PLANO

Por fim, a realização de exercícios deve servir para validar o plano de comunicação de crises.

Esta validação deve ocorrer apenas após a realização dos exercícios e a implementação das melhorias identificadas, incluindo a subsequente testagem dessas melhorias em exercícios posteriores.

Tendo sido comprovada a capacidade de execução do plano ao nível pretendido, bem como a adequação do mesmo às necessidades da Organização em contexto de crise, mesmo, este deve ser validado pela gestão de topo da mesma.

Uma vez validado o plano, este deve continuar a ser testado regularmente, de modo a assegurar que a capacidade de execução do mesmo é mantida e que este continua atual.

Reforça-se que os exercícios devem contribuir para a evolução das capacidades tanto a nível coletivo como a nível individual, numa perspetiva de melhoria contínua dentro da Organização. Os exercícios realizados devem permitir explorar os pontos fortes previamente identificados e proporcionar oportunidades de melhoria ao longo do tempo[25].

[25] International Organization for Standardization, "*ISO 22361:2022*", 34-35.

Tabela 11

| EXPECTATIVAS QUANTO À TESTAGEM DO PLANO DE COMUNICAÇÃO POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • São realizados exercícios simples (sobretudo exercícios de discussão) para testar o plano de comunicação de forma pontual, sem regularidade definida. |
| **Nível Intermédio** | • São realizados exercícios que simulam cenários específicos de situações de crise com alguma regularidade.<br>• São identificados pontos fortes e oportunidades de melhoria durante a realização dos exercícios.<br>• É elaborado um plano de ação para a implementação das melhorias, sendo essas melhorias testadas em novos exercícios. |
| **Nível Avançado** | • São realizados exercícios reais que permitem testar a estratégia adotada, a reação real do *staff* e os sistemas que podem ser afetados em intervalos regulares definidos.<br>• São identificados pontos fortes e oportunidades de melhoria durante a realização dos exercícios.<br>• São escrutinadas e avaliadas todas as decisões tomadas no decorrer do exercício.<br>• São realizados questionários a todos os intervenientes nos exercícios.<br>• É elaborado um plano de ação para a implementação das melhorias, sendo essas melhorias testadas em novos exercícios. |

FASE 2

# RESPONDER EFICAZMENTE

# **FASE 2:** RESPONDER EFICAZMENTE

Para responder eficazmente a uma crise, os colaboradores devem conhecer as suas funções, bem como executar corretamente as suas atividades, nomeadamente aqueles que se encontram envolvidos na resolução de uma crise, tal como referido no QNRCS (RS.CO-1).

## 1. ATIVAR A EQUIPA DE COMUNICAÇÃO

A partir do momento em que é detetado um incidente de cibersegurança, este deverá ser analisado e confirmado. Estando confirmado que o incidente detetado constitui efetivamente uma crise, deverá ser ativada a equipa de resposta a incidentes/crises, incluindo a equipa responsável pela comunicação de crise.

**Figura 3:** Processo de ativação do plano de resposta


Consoante a gravidade da situação, poderão existir cenários nos quais não é necessário mobilizar todos os meios e colaboradores para dar resposta à crise. Ou seja, uma crise de baixa gravidade pode exigir apenas uma equipa de suporte técnico IT, equipa de relações públicas e representantes legais para a contenção e investigação da mesma, enquanto incidentes ou crises de alta gravidade podem exigir a convocação imediata de todos os elementos com responsabilidades na resposta a incidentes/crises para iniciar uma operação de resposta com toda a capacidade disponível.

O plano de resposta a crises de cibersegurança da Organização deve delinear o processo de ativação da equipa de resposta e toda a logística para a suportar. A equipa de resposta a incidentes/crises deve determinar com que frequência a equipa se reúne e é informada, como as atualizações acerca da crise são dadas (exemplo: *e-mail*, reuniões pessoais) e métodos de comunicação a adotar se os sistemas principais tiverem sido afetados pela crise de cibersegurança.

Neste sentido, para a coordenação da equipa de resposta a incidentes/crises, deve estar preparado o já mencionado na Fase 1, tal como:

- Uma ou mais salas de reunião dedicadas (*war rooms*), centralizando as comunicações e coordenação e um canal de comunicação dedicado para os membros da equipa trocarem informações;
- Sistemas de mensagens cifradas ou outros sistemas seguros para comunicação de crises;
- Telemóveis dedicados para membros da equipa de resposta a incidentes/crises para suporte "fora de horas" e comunicações no local de trabalho;
- Cópias impressas dos procedimentos de resposta a incidentes/crises, lista de contactos e formulários de tratamento de incidentes/crises;
- Infraestruturas de armazenamento seguro para proteger evidências e outros materiais confidenciais;
- Sistema de ficheiros seguros, aplicações ou base de dados com acessos restritos para armazenar formulários e informações confidenciais de tratamento de incidentes/crises[26].

## 2. REPORTAR OS INCIDENTES CONFORME EXIGIDO NOS REGULAMENTOS E CONTRATOS

As Organizações devem reportar os incidentes de cibersegurança por dois grandes motivos.

O primeiro motivo é a conformidade - legal, regulatória e contratual - de modo a não incorrerem em incumprimento da lei, de regulamentos ou dos contratos celebrados em vigor.

O segundo motivo prende-se com a reputação da Organização. As Organizações que tardam em reportar às partes interessadas relevantes um incidente ou crise ou que deixam mesmo que essas partes venham a saber do incidente ou crise por terceiros em vez de por si próprias tendem a ter as maiores perdas reputacionais. Por outro lado, as Organizações que notificam as partes interessadas dos incidentes/crises tendem a ter melhores resultados na manutenção da sua reputação e da confiança dos clientes.

Por estes motivos, o intuito de informar as partes interessadas e de reportar um incidente deve estar contemplado no plano de comunicação das Organizações, suportado pelas respetivas estratégias de comunicação, conforme referido no QNRCS (DE.PD-4, RS.CO-2, RS.CO-3).

[26] APPA e Nexight Group, "*Public Power Cyber Incident Response Playbook*", 16.

Contudo, há cuidados a ter antes de reportar um incidente ou crise a grupos de interesse. É importante considerar:

- Consultar o departamento jurídico (ou advogados da Organização) antes de realizar qualquer reporte fora da Organização;
- Determinar e autorizar antecipadamente quais as circunstâncias aceitáveis para proceder à notificação;
- Rever a proteção de informações e acordos de confidencialidade em vigor antes de voluntariamente compartilhar informação;
- Trabalhar com a equipa jurídica para rever e assinar os acordos de confidencialidade com antecedência;
- Identificar claramente que tipo de informação pode ser partilhada relativa ao incidente/crise com outras entidades;
- Identificar contactos e construir relacionamentos com as autoridades antecipadamente. Compreender as expectativas de informação e acessos, por parte das autoridades, se a Organização reportar um cibercrime e como coordenar com a aplicação da lei durante a resposta e recuperação[27].

## 2.1. NOTIFICAÇÃO DE INCIDENTES DE CIBERSEGURANÇA AO CNCS

Tal como refere o disposto no n.º1 do artigo 11.º do Decreto-Lei n.º 65/2021, de 30 de julho, a Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais notificam o CNCS da ocorrência de incidentes com impacto relevante ou substancial nos termos, respetivamente, dos artigos 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço (Lei n.º 46/2018, de 13 de agosto).

### Há três tipos de notificação a ter em conta:

**a)** Notificação inicial (artigo 13.º do DL 65/2021);

**b)** Notificação de fim de impacto relevante ou substancial (artigo 14.º do DL 65/2021);

**c)** Notificação final (artigo 15.º do DL 65/2021).

[27] APPA e Nexight Group, "*Public Power Cyber Incident Response Playbook*", 17.

### a) Notificação inicial

A notificação inicial deve ser enviada logo que a entidade possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até duas horas após essa verificação, devendo a entidade, sem prejuízo do cumprimento deste prazo, dar prioridade à mitigação e à resolução do incidente.

A notificação inicial deve incluir a seguinte informação:

1. Nome, número de telefone e endereço de correio eletrónico de um representante da entidade, quando diferente do ponto de contacto permanente a que se refere o artigo 4.º, para efeito de um eventual contacto por parte do CNCS;
2. Data e hora do início ou, em caso de impossibilidade de o determinar, da deteção do incidente;
3. Breve descrição do incidente, incluindo a indicação da categoria da causa raiz e dos efeitos produzidos, de acordo com a taxonomia definida no artigo 16.º e, sempre que possível, o respetivo detalhe;
4. Estimativa possível do impacto, considerando:
   i) Número de utilizadores afetados pela perturbação do serviço;
   ii) Duração do incidente;
   iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
5. Outra informação que a entidade considere relevante.

### b) Notificação de fim de impacto relevante ou substancial

A notificação de fim de impacto relevante ou substancial do incidente deve ser submetida ao CNCS logo que possível, dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial.

A notificação de fim de impacto relevante ou substancial deve incluir a seguinte informação:

1. Atualização da informação transmitida na notificação inicial, caso exista;
2. Breve descrição das medidas adotadas para a resolução do incidente;
3. Descrição da situação do impacto existente no momento de fim de impacto relevante ou substancial, nomeadamente:
   i) Número de utilizadores afetados pela perturbação do serviço;
   ii) Duração do incidente;
   iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
   iv) Tempo estimado para a recuperação total dos serviços.

### c) Notificação final

A notificação final deve ser enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar.

A notificação final deve incluir a seguinte informação:

1. Data e hora em que o incidente assumiu o impacto relevante ou substancial;
2. Data e hora em que o incidente perdeu o impacto relevante ou substancial;
3. Impacto do incidente, considerando:
   - i) Número de utilizadores afetados pela perturbação do serviço;
   - ii) Duração do incidente;
   - iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
   - iv) Descrição do incidente, com indicação da categoria da causa raiz e dos efeitos produzidos, de acordo com a taxonomia definida no artigo seguinte, e o respetivo detalhe;
4. Indicação das medidas adotadas para mitigar o incidente;
5. Descrição da situação residual do impacto existente à data da notificação final, nomeadamente:
   - i) Número de utilizadores afetados pela perturbação do serviço;
   - ii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
   - iii) Tempo estimado para a recuperação total dos serviços ainda afetados;
6. Indicação, sempre que aplicável, da apresentação de notificação do incidente em causa às autoridades competentes, nomeadamente ao Ministério Público, à ANEPC, à ANACOM, à CNPD, à Polícia Judiciária e a outras autoridades setoriais, nos termos previstos nas disposições legais e regulamentares aplicáveis;
7. Outra informação que a entidade considere relevante.
   - i) Nos casos em que exista uma situação residual do impacto à data da notificação final, descrita ao abrigo do disposto na alínea 5, as entidades devem comunicar ao CNCS, logo que possível, a recuperação total dessa situação residual.

## Como proceder à notificação ao CNCS?

O envio das notificações de incidentes e de informação adicional ao CNCS deve ser realizado através do sítio na *Internet* do CNCS - **https://www.cncs.gov.pt** - na funcionalidade «Notificação de Incidentes», mediante o preenchimento do modelo de reporte estabelecido para o efeito, ou via API (*Application Programming Interface*) disponibilizada pelo CNCS. Nos casos em que a entidade em resultado do incidente ou por outro motivo de natureza eminentemente técnica devidamente justificado, não tiver, temporariamente, capacidade operacional para assegurar a notificação no sítio na Internet do CNCS, ou nos casos em que o mesmo esteja indisponível, a notificação poderá ser efetuada, a título excecional, através:

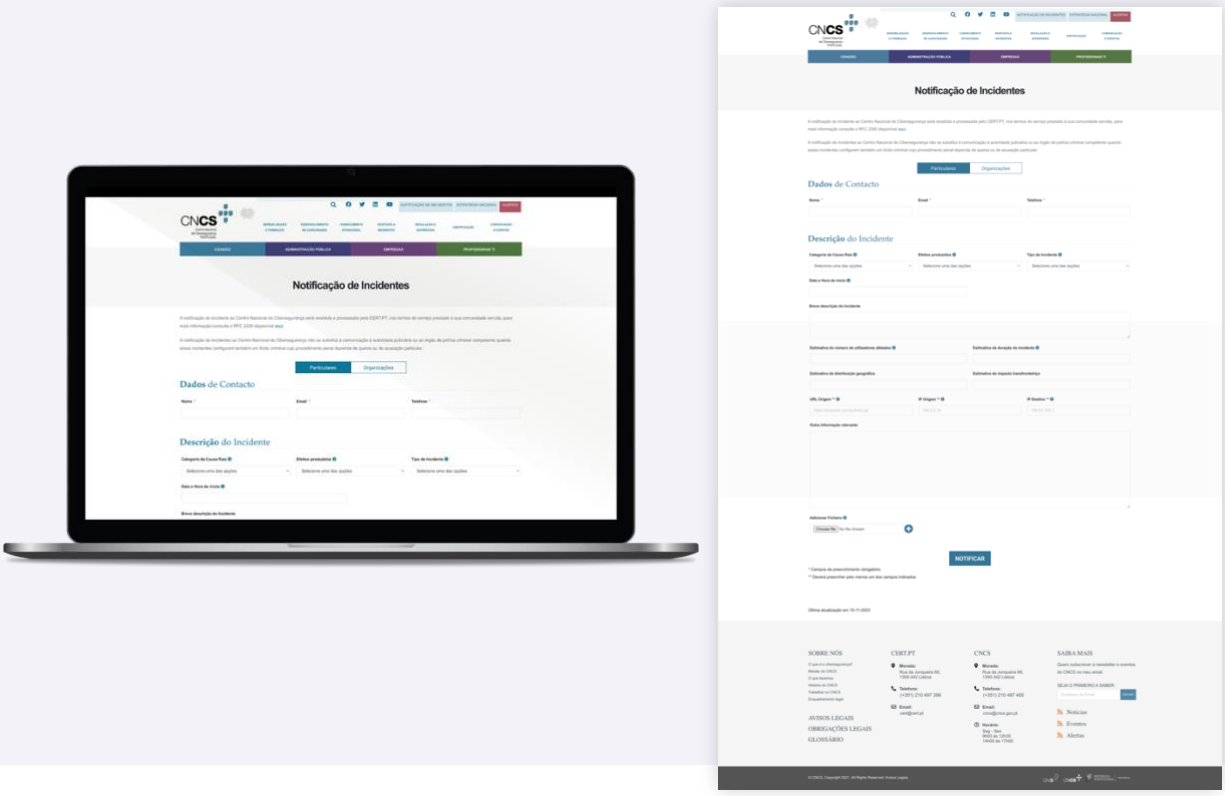
– De correio eletrónico remetido para o seguinte endereço: **cert@cert.pt**;

– Do número de telefone **(+351) 210 497 399**;

– Do número de telefone **(+351) 910 599 284**, em disponibilidade contínua (24 horas por dia e sete dias por semana).

Caso as entidades pretendam enviar a notificação protegida por método criptográfico, podem proteger a informação utilizando a chave pública de PGP, associada ao endereço de correio eletrónico já referido – **cert@cert.pt** –, publicada no sítio na Internet do CNCS. A chave pública está disponível em **https://www.cncs.gov.pt/pt/certpt/chave-pgp/**.

**Figura 4:** Formulário de Notificação de Incidentes do CNCS.



**É ainda de referir que qualquer entidade, para além das previamente mencionadas, pode notificar, a título voluntário, os incidentes com impacto importante na continuidade dos serviços por si prestados.** Essa notificação voluntária não pode dar origem a quaisquer obrigações às quais a entidade notificante não teria sido sujeita se não tivesse procedido a essa notificação.

Importa também sublinhar que a notificação de incidentes ao CNCS não isenta as entidades de outras obrigações de notificação, tais como obrigações de notificação decorrentes do Regulamento Geral sobre a Proteção de Dados (RGPD), à autoridade de controlo e/ou aos titulares de dados, no caso de o incidente ter resultado numa violação de dados pessoais e as circunstâncias dessa violação obrigarem a essas notificações, nem se substitui à comunicação à autoridade judiciária ou ao órgão de polícia criminal competente quando esses incidentes configurem também um ilícito criminal cujo procedimento penal dependa de queixa ou de acusação particular.

### Benefícios da notificação antecipada de incidentes

i. Correlacionar incidentes em toda a indústria para identificar ataques coordenados ou tendências de ataque. Reportar incidentes suspeitos ou confirmados às entidades governamentais permite que estes parceiros analisem o relatório em relação a outros relatórios e informações sobre ameaças, permitindo a deteção precoce de um ataque mais coordenado e generalizado;

ii. Medidas de mitigação. As Organizações podem recomendar etapas de mitigação para incidentes de cibersegurança ou realizar análise de *malware* ou análise de ameaças para identificar e mitigar o incidente;

iii. Apoio à investigação de incidentes. Vários grupos externos de resposta podem oferecer suporte à análise forense e à investigação de um incidente, seja remota ou localmente;

iv. Preparar recursos de resposta e coordenação. Notificar os grupos externos de resposta com antecedência pode ajudar a iniciar a coordenação entre setores, preparar as equipas de resposta para incidentes potencialmente graves e dar suporte à coordenação de mensagens entre os parceiros de resposta[28].

**Tabela 12**

| EXPECTATIVAS QUANTO AO REPORTE DE INCIDENTES POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • Existe o conhecimento informal e não estruturado dos canais de reporte dos incidentes. |
| **Nível Intermédio** | • A capacidade de reporte de incidentes está garantida;<br>• Estão estabelecidos critérios de reporte de incidentes. |
| **Nível Avançado** | • Estão estabelecidos critérios para envolver as partes interessadas externas no tratamento dos incidentes;<br>• O reporte de incidentes é realizado de maneira integrada. |

[28] APPA e Nexight Group, "*Public Power Cyber Incident Response Playbook*", 17.

## 3. DOCUMENTAR O INCIDENTE

Deve iniciar-se, assim que possível, o registo detalhado e preciso da informação relativo à suspeita desse incidente e, posteriormente, a atualização contínua da documentação do incidente durante a ação de resposta ao mesmo.

O responsável pela coordenação da resposta de incidentes de cibersegurança deve coordenar a equipa na função de recolha de informações que permitirá documentar a resposta no decorrer do incidente; informar a equipa de resposta a incidentes e/ou outros grupos de interesse e conduzir os relatórios necessários ou outras notificações, tais como:

- O tipo de incidente;
- A data e hora do incidente;
- Se o incidente ainda está ativo;
- Como é que o incidente foi identificado e os colaboradores que o identificaram;
- Dispositivos, aplicações ou sistemas afetados;
- Impactos atuais ou futuros do incidente, em contexto interno e externo da Organização;
- O tipo e a sensibilidade dos dados armazenados nos sistemas afetados;
- Quaisquer medidas de mitigação planeadas ou já tomadas;
- *Logs* ou outros registos do incidente;
- Lista dos grupos de interesse já contactados ou outros recursos envolvidos;
- Detalhes dos pontos de contacto entre a equipa de resposta a incidentes e a organização[29].

Para manter os registos de informação de incidentes é necessária a utilização de uma aplicação ou base de dados segura, devendo o seu acesso ser restrito de acordo com o grau de sensibilidade dos dados neles contidos.

[29] APPA e Nexight Group, "*Public Power Cyber Incident Response Playbook*", 29.

Tabela 13

| EXPECTATIVAS QUANTO À DOCUMENTAÇÃO DOS INCIDENTES POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • O incidente é documentado de forma pouco estruturada e sem uniformidade da informação. |
| **Nível Intermédio** | • Estão estabelecidas práticas de documentação dos incidentes;<br>• A informação sobre o incidente é recolhida de forma estruturada e uniforme. |
| **Nível Avançado** | • Estão definidos *templates* para a documentação do incidente;<br>• Os *templates* registam todos os pontos supramencionados;<br>• A estrutura da informação recolhida permite a fácil leitura da documentação do incidente pelas partes interessadas relevantes. |

## 4. COMUNICAR O ENCERRAMENTO FORMAL DA CRISE

Na maioria das vezes, a pressão vivida durante uma situação de crise faz com que as Organizações queiram ultrapassar a crise o mais rapidamente possível, o que pode levar a que não se executem todos os passos essenciais na resolução da crise. Um passo frequentemente esquecido é o da comunicação do encerramento formal da crise.

Comunicar o encerramento formal da crise significa comunicar o fim da mesma, tanto a nível interno como externo. A comunicação nesta fase inclui, para além de anunciar o fim da crise, a comunicação das atividades que foram levadas a cabo para a ultrapassar, bem como transmitir aos grupos de interesse e à opinião pública em geral a mensagem de que a Organização aprendeu com o sucedido e está agora mais bem preparada para o futuro e mais capaz de resistir a eventos semelhantes. Este é também um momento oportuno para agradecer a todos aqueles que tenham estado envolvidos na resolução da crise, aos níveis individual e institucional.

Reforça-se que esta comunicação é pertinente a nível interno e externo. Deste modo, devem ser enviadas mensagens de agradecimento pelo trabalho realizado e a evidenciar a importância de todos estarem preparados para situações deste tipo, enfatizando assim a necessidade de todos os membros da Organização estarem em estado de alerta[30].

[30] CCN-CERT, "*Gestión de Cibercrisis*", 25.

Tabela 14

| EXPECTATIVAS QUANTO ÀS ATIVIDADES DE ENCERRAMENTO FORMAL DA CRISE POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • Não está definido um processo para a comunicação do encerramento formal da crise.<br>• O encerramento da crise é comunicado, a nível interno e externo, através de mensagem geral e simples, por exemplo, por e-mail, a nível interno, e por publicação em website ou página de rede social da Organização, a nível externo. |
| **Nível Intermédio** | • Estão definidos processos para a comunicação do encerramento formal da crise.<br>• O encerramento da crise é formalmente comunicado a nível interno e externo, seguindo os processos definidos, mencionando, dentro do possível, os motivos da crise e medidas tomadas para a resolução da mesma. |
| **Nível Avançado** | • Estão definidos processos para o encerramento formal da crise.<br>• O encerramento da crise é formalmente comunicado a nível interno e externo, seguindo os processos definidos, mencionando, dentro do possível, os motivos da crise e medidas tomadas para a resolução da mesma, fazendo agradecimentos e demonstrando o compromisso da Organização a tornar-se mais resiliente a situações semelhantes que possam ocorrer no futuro.<br>• Estão instalados processos de revisão dos incidentes/crises e da comunicação realizada durante a resolução dos mesmos. |

## 5. RECUPERAR A REPUTAÇÃO

Tal como o encerramento formal da crise, as atividades de recuperação são frequentemente negligenciadas enquanto etapa final na comunicação de crise, uma vez que as Organizações e as equipas procuram retomar imediatamente as rotinas normais.

A Organização deve garantir que os grupos de interesse (internos e externos) são informados das atividades de recuperação (QNRCS: RC.CO-2).

Após uma crise, a comunicação desempenha um papel importante para ajudar a organização a redefinir as relações com as pessoas afetadas e a reconstruir a reputação que possa ter sido perdida[31].

Apresentam-se de seguida seis atividades que poderão auxiliar a equipa e a Organização a reconstruir e reparar a sua reputação e/ou relacionamentos[32].

[31] ANSSI, "*Crisis of Cyber Origin: The Keys to Operational and Strategic Management*", 20.
[32] GCS, "*Emergency Planning Framework*", 33.

## Considerar a recuperação desde o início

A recuperação deve estar na agenda desde o início de uma crise. Se uma crise chegar ao fim e não se tiver contemplado a recuperação, poder-se-á perder a oportunidade imediata de recuperar de qualquer impacto na reputação da Organização.

RECOMENDAÇÕES:

- Designar uma ou duas pessoas da equipa para trabalhar em estreita colaboração com colegas da área jurídica para trabalhar na recuperação enquanto a crise ainda está a decorrer;
- Estabelecer objetivos claros sobre a reconstrução da reputação que podem ajudar a informar sobre ações enquanto a crise ainda está a ser gerida.

## Criar confiança através de ações e não de palavras

Uma crise pode alterar fundamentalmente a opinião de um ou mais grupos de interesse acerca da Organização. Por isso, uma boa forma de reconstruir essa confiança poderá ser demonstrar que o desempenho da Organização está novamente de acordo com aquelas que são as expectativas dos grupos de interesse relativamente às atividades e aos serviços da Organização.

RECOMENDAÇÕES:

- A reputação é demonstrada através de ações. A melhor forma de recuperar a reputação será demonstrar como os compromissos assumidos estão a ser e vão continuar a ser cumpridos;
- Para os comunicadores, esta demonstração significa demonstrar o que está a ser feito. Por outras palavras, a comunicação feita deve ser acompanhada de provas que possam ser apresentadas aos grupos de interesse.

## Envolver os colaboradores da Organização

Manter a coesão interna durante uma situação de crise é um aspeto essencial para a resolução da mesma. Deve-se, por isso, tanto quanto possível, manter os colaboradores informados sobre a crise, desde a sua origem ao que está a ser feito para a solucionar.

RECOMENDAÇÕES:

- Certificar-se de que a comunicação interna é parte integrante de qualquer plano de recuperação - os próprios funcionários são os maiores defensores da Organização;
- Comunicar com a gestão de topo relativamente aos desafios de envolver e reconectar com o *staff* após uma crise - a sua visibilidade é vital.

## Redefinir a agenda através de uma comunicação ativa

É importante não permitir que a Organização seja condicionada por uma crise. Deve-se, por isso, ter uma comunicação proativa, coerente e alicerçada nas decisões tomadas para tornar a Organização mais resiliente a crises semelhantes que possam ocorrer no futuro.

RECOMENDAÇÕES:

- Desenvolver um plano de comunicação coerente e proativo que suporte as decisões da Organização;
- Refletir sobre como é que a Organização pode demonstrar a sua capacidade de liderança e ultrapassar a crise redefinindo as suas prioridades.

## Cumprir as promessas feitas e ter em atenção os prazos estabelecidos

No decorrer de uma crise, muitas vezes as Organizações optam por fazer promessas ou dar garantias com o intuito de reduzir as críticas dirigidas aos responsáveis pela crise.

RECOMENDAÇÕES:

- Acompanhar todos os compromissos assumidos publicamente no decorrer da crise e certificar-se de que os prazos desses mesmos compromissos são cumpridos;
- Certificar-se de que as equipas mantêm contacto com os responsáveis pelo cumprimento dos compromissos assumidos, de forma a realizarem uma gestão proativa e reduzirem o risco de perda de reputação.

## Usar janelas de oportunidade para realizar alterações de longo prazo

"As janelas de oportunidade" no decorrer de uma crise devem ser utilizadas por parte das Organizações para alterações na direção, valores ou estratégia a adotar.

RECOMENDAÇÕES:

- Refletir sobre quais as consequências não intencionais que podem ser exploradas (por exemplo: uma seca pode ser uma oportunidade para mudar as atitudes do público-alvo em relação ao consumo de água);
- Refletir como a crise pode ter alterado o cenário de comunicação.

É de salientar que estas indicações e recomendações, por si só, não podem garantir a recuperação da reputação de uma Organização, mas poderão constituir um bom ponto de partida para essa recuperação[33].

[33] GCS, "*Emergency Planning Framework*", 33-34.

Tabela 15

| EXPECTATIVAS QUANTO ÀS ATIVIDADES DE MANUTENÇÃO/RECUPERAÇÃO DA REPUTAÇÃO POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • São adotadas medidas *ad hoc* para mitigar impactos ou perdas na reputação. |
| **Nível Intermédio** | • Estão definidas atividades/medidas para manter/recuperar a reputação da Organização;<br>• A Organização é proativa na comunicação, estabelecendo compromissos (ex: atualizações sobre a situação em intervalos temporais iguais) e cumprindo-os com relativo rigor. |
| **Nível Avançado** | • Está estabelecida uma estratégia de recuperação/manutenção da reputação da Organização;<br>• A Organização é proativa na comunicação, estabelecendo compromissos e cumprindo-os dentro dos prazos estabelecidos;<br>• A Organização tem capacidade para, se necessário, redefinir prioridades e estratégias, comunicando essas redefinições às partes interessadas relevantes. |

FASE 3

# APRENDER LIÇÕES E MELHORAR

# **FASE 3:** APRENDER LIÇÕES E MELHORAR

Os momentos posteriores a uma situação de crise constituem uma oportunidade para aprender e melhorar processos. Por isso, estabelecer um processo de *feedback* a respeito das ações e atividades realizadas na resolução da crise é fundamental para retirar lições e melhorar globalmente a resposta a situações futuras da mesma natureza.

O processo de *feedback* deve ser faseado em duas etapas baseadas na componente estratégica da Organização.

A primeira etapa do processo, focada na estruturação do *feedback*, deve iniciar-se com a identificação, por parte da unidade estratégica da Organização, da equipa responsável por recolher o *feedback* acerca da gestão de crise.

Uma vez criada esta equipa, devem ser identificadas, na segunda etapa do processo, as pessoas a serem entrevistadas sobre a crise e a gestão da mesma, a sua ordem de entrevista e é recomendável que se estruturem os aspetos práticos da ronda de entrevistas (horário, forma, resumo, documentação, coordenação)[34].

Após a obtenção do *feedback*, que deve ser estruturado e organizado para ser apresentado à componente estratégica e operacional da Organização, deve-se, no prazo máximo definido pela Organização, compreendido entre o fim da crise e o fim do processo de *feedback*, concluir esse processo de *feedback*, pedindo um relatório da investigação e o seu sumário (para as equipas de gestão) aos fornecedores dos serviços mobilizados.

**Figura 5:** Processo de recolha de *feedback* lições aprendidas e melhorias


[34] ANSSI, "*Crisis of Cyber Origin: The Keys to Operational and Strategic Management*", 64.

A informação obtida na revisão da crise pode ajudar a resposta operacional de várias maneiras:

- Deve manter a equipa de resposta a crises no caminho certo, lembrando-a dos seus objetivos de comunicação;
- Deve permitir que se adapte rapidamente o conteúdo e os canais de divulgação em resposta a qualquer *feedback*;
- Deve demonstrar se as mensagens importantes estão a chegar ao público-alvo e onde é necessário investir mais para informar ou persuadir o público pretendido.

## 1. REVISÃO DA CRISE E AVALIAÇÃO GLOBAL DO PLANO DE COMUNICAÇÃO

A revisão após a crise e as possíveis lições aprendidas devem fazer parte do plano de gestão de crises de cibersegurança (QNRCS: RC.ME-1).

Uma revisão à crise é uma retrospetiva detalhada que permite uma Organização compreender com pormenor cada parte dessa crise, do início ao fim. É um passo do processo de resposta a incidentes/crises que permite realmente compreender a causa do incidente/crise e toda a sua dimensão.

Avaliar o plano de comunicação - ou avaliar a execução do plano de comunicação e o impacto das mensagens selecionadas - é essencial para a Organização verificar a adequação do plano existente e para compreender as expectativas da comunicação social e dos grupos de interesse, permitindo melhorar os seus processos, mecanismos e estratégias de comunicação para circunstâncias futuras.

Para tal, é necessário avaliar se as informações dos principais contactos estavam acessíveis desde o início da crise, bem como se os canais de comunicação definidos para as situações de crise operaram sem problemas. Esta avaliação permite à Organização renovar e reforçar as informações que possui relativamente aos contactos de crise, bem como atualizar quais os melhores canais de comunicação a serem utilizados nestas ocorrências.

É necessário, igualmente, avaliar se a mensagem desenvolvida produziu os efeitos desejados para os públicos-alvo pretendidos. Esta ponderação permite à Organização ter conhecimento se a mensagem deve ser ou não adaptada, para futuras ocasiões.

Verificar se ocorreu um encerramento formal da crise para com os grupos de interesse é fundamental para tranquilizar e reassegurar que a crise foi concluída. Realizar esta atividade poderá fazer a diferença na manutenção da confiança entre a Organização e os seus parceiros.

É também necessário verificar se a reputação da Organização foi afetada, se ficou intacta ou se teve de ser recuperada. Esta verificação é essencial para aplicar os recursos corretos a cada situação.

Tendo feito estas avaliações e verificações, e outras que se considerem pertinentes, será importante rever e/ou reformular o plano de comunicação de modo a colmatar quaisquer falhas que possam ter sido identificadas, para que as mesmas não se repitam posteriormente.

Uma boa revisão da crise deve resultar numa lista de ações práticas que abordam cada um dos aspetos que permitiram ao atacante ter sucesso. As ações práticas listadas devem ir no sentido de melhorar a resiliência da Organização a tentativas de ataque, melhorar a sua capacidade de resposta e a sua comunicação.

A lista de ações práticas resultante da revisão da crise deverá depois ficar refletida no plano de comunicação atualizado. As atualizações feitas devem ser comunicadas a todos os envolvidos nas atividades de resposta a incidentes/crises[35].

**Tabela 16**

| EEXPECTATIVAS QUANTO AO PROCESSO DE LIÇÕES APRENDIDAS E MELHORIA POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • A Organização realiza uma revisão informal da crise. Não existe método formal de revisão e avaliação das falhas que possam ser identificadas;<br>• O plano de comunicação é atualizado em conformidade com as falhas detetadas. |
| **Nível Intermédio** | • Existem e são avaliadas métricas relativas aos planos de recuperação;<br>• As equipas (internas e externas) afetas à recuperação de incidentes/crises são formadas e geridas, estando estabelecidos fluxos de comunicação entre as mesmas;<br>• O plano de comunicação é formalmente atualizado, de acordo com as lições aprendidas e melhorias aplicáveis identificadas. |
| **Nível Avançado** | • Estão estabelecidos procedimentos de revisão periódica das estratégias de recuperação, por parte da gestão de topo;<br>• A análise de lições aprendidas para melhoria dos procedimentos de resposta a incidentes/crises inclui:<br>o Documentos de suporte ao plano de resposta a incidentes/crises;<br>o Registos de reuniões e demais interações, no contexto da melhoria contínua;<br>o Registo do tratamento de vulnerabilidades resultantes de incidentes/crises ocorridos.<br>• Os planos de recuperação são atualizados de acordo com as melhorias identificadas e com o envolvimento da gestão de topo. |

[35] Cybereason, "*Post-Incident Review: Examining the Importance of Post-Incident Review for Security Teams*", https://www.cybereason.com/resources/post-incident-review.

## 2. MONITORIZAÇÃO E REVISÃO DOS RISCOS

Mesmo sem a ocorrência de uma crise de cibersegurança, a monitorização e a revisão dos riscos são atividades que as Organizações devem realizar regularmente.

Contudo, existe sempre a possibilidade de ocorrer uma situação de crise e, por isso, é necessário que as Organizações, após uma situação de crise, procedam a uma revisão e reavaliação, não só do da crise e dos planos de resposta existentes, mas também dos riscos. Esta revisão e reavaliação permite que as Organizações alterem as classificações e os níveis atribuídos aos riscos identificados até ao momento de crise, bem como identificar novos riscos que até então não tinham sido identificados na Organização (QNRCS: RS.MI-3).

Esta revisão, devidamente documentada, é necessária, tendo em conta a constante alteração de probabilidade e de impacto dos riscos conhecidos por parte das Organizações, assim como o surgimento de novos riscos que impactam a continuidade do negócio das mesmas.

Tendo sido realizada e documentada a revisão e reavaliação dos riscos pós-crise, é importante voltar ao processo de comunicação e consulta dos riscos, de modo a alcançar novo consenso sobre como gerir os novos riscos de segurança da informação e cibersegurança.

A comunicação da revisão e reavaliação dos riscos deverá incluir a partilha das informações sobre os riscos entre os responsáveis da Organização e os grupos de interesse relevantes (QNRCS: RC.CO-2) de modo a alertar para os novos riscos, se encontrados, e promover a consciencialização sobre os mesmos em toda a Organização.

**Tabela 17**

| EXPECTATIVAS QUANTO À MONITORIZAÇÃO E REVISÃO DOS RISCOS POR NÍVEL DE CAPACIDADES | |
|---|---|
| **Nível Inicial** | • A monitorização e revisão é realizada de forma pontual e não estruturada. |
| **Nível Intermédio** | • Existe um processo estabelecido de gestão de vulnerabilidades/riscos;<br>• Existem critérios definidos para mitigação das vulnerabilidades/riscos. |
| **Nível Avançado** | • Processo de análise de vulnerabilidades/risco é definido e constante;<br>• Existe um processo de formalização e aceitação das vulnerabilidades/risco;<br>• Os novos riscos/vulnerabilidades são comunicados aos responsáveis da Organização e aos seus grupos de interesse. |

# 4. NOTAS METODOLÓGICAS

O presente documento tem como propósito principal a preparação das Organizações para conjunturas de crise, além de como devem proceder na comunicação das mesmas às entidades competentes, incluindo o CNCS.

Com este propósito, a metodologia aplicada na construção deste documento iniciou-se com a recolha de dados e informação de diversos documentos de referência, na preparação e comunicação de crises de cibersegurança, utilizados por vários países cuja maturidade de cibersegurança se encontra equiparada ou superior à realidade portuguesa. Seguiu-se uma fase de análise dos dados e informações recolhidas, terminando com uma revisão do texto produzido.

Os dados recolhidos foram fornecidos pelo CNCS, sendo que a sua análise e consequente produção e elaboração do referencial, foram realizados pela PwC, entidade parceira do CNCS na realização do presente documento.

# 5. BIBLIOGRAFIA

## 5.1. PRINCIPAIS REFERÊNCIAS

1. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). "*Crisis of Cyber Origin: The Keys to Operational and Strategic Management*". Março de 2022. https://www.ssi.gouv.fr/uploads/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en.pdf

2. American Public Power Association (APPA) e Nexight Group. "*Public Power Cyber Incident Response Playbook*". Agosto de 2019. https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf

3. Centro Criptológico Nacional (CCN-CERT). "*Gestión de Cibercrisis. Buenas Prácticas en la Gestión de Crisis de Ciberseguridad*". 2020. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5428-ccn-cert-bp-20-buenas-pra-cticas-en-la-gestio-n-de-cibercrisis-1/file.html

4. Cyber Security Coalition (CSC). "*Cyber Security Incident Management Guide*". Janeiro de 2016, revisto em setembro de 2021. https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

5. Government Communication Service (GCS). "*Emergency Planning Framework*". 2018. https://gcs.civilservice.gov.uk/wp-content/uploads/2020/04/Emergency-planning-framework-1.pdf

6. International Organization for Standardization, "*ISO 22361:2022 - Security and resilience — Crisis management — Guidelines*". https://www.iso.org/standard/50267.html

7. Public Safety Canada (PSC). "*Developing an Operational Technology and Information Technology Incident Response Plan*". 2020. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dvlpng-ndnt-rspns-pln/index-en.aspx

## 5.2. OUTRAS REFERÊNCIAS


1. Centro Nacional de Cibersegurança (CNCS). "*Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança*". Versão 1.1., dezembro de 2022. https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf

2. Centro Nacional de Cibersegurança (CNCS) e Observatório de Cibersegurança. "*Relatório Cibersegurança em Portugal: Riscos e Conflitos*" 4.ª edição: junho de 2023. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

3. C-Risk."*Crisis Communication: How to manage crisis communication after a cyberattack?*". 2 de agosto de 2021, atualizado a 2 maio de 2023. https://www.c-risk.com/en/blog/crisis-communication/

4. Cybereason. "*Post-Incident Review: Examining the Importance of Post-Incident Review for Security Teams*". https://www.cybereason.com/resources/post-incident-review

5. Government Communication Service Behavioural Science Team. "*Crisis communication: A behavioural approach*". Cabinet Office, agosto de 2022. https://gcs.civilservice.gov.uk/publications/crisis-communication-a-behavioural-approach/.


## 5.3. LEGISLAÇÃO


1. Lei n.º 46/2018, de 13 de agosto.

2. Decreto-Lei n.º 65/2021, de 30 de julho.

# 6. ANEXOS

## A1: EXEMPLOS DE *TEMPLATES* DE COMUNICAÇÃO

Como referido no Referencial, os *templates* de comunicação devem definir o que comunicar (conteúdo), que mensagem utilizar (texto sucinto, metáforas, imagens, vídeos), quem deve comunicar, a quem comunicar (que grupos de interesse serão os recipientes da informação) e como comunicar (canais a ser utilizados para a difusão da mensagem, como *e-mail* ou SMS).

Os exemplos de *templates* apresentados neste Referencial são apenas isso - exemplos - pelo que as Organizações deverão procurar adequar os mesmos do melhor modo possível às suas necessidades de comunicação em situação de crise. As Organizações deverão também considerar a necessidade de novos momentos comunicacionais com os mesmos grupos de interesse.

Para fazer a adequação dos exemplos providenciados, as Organizações devem, tanto quanto possível, tentar antecipar os potenciais cenários de crise e definir os seus *templates* de comunicação de acordo com os cenários antecipados e com os objetivos de comunicação da Organização.

**Exemplo 1:** *Template* genérico (para uso interno e externo)

**Destinatários da comunicação:** Grupos de interesse internos e externos

**Meios de comunicação recomendados:** SMS, *e-mail*, publicação em *website*/redes sociais

"Olá a todos,

O/A (nome da Organização) deseja informar-vos acerca de um incidente de cibersegurança recente que afetou a organização.

As nossas equipas detetaram o incidente pelas (inserir hora) do dia (inserir dia e mês) e têm, desde então, estado a trabalhar empenhadamente na resolução do mesmo.

A vossa segurança, bem como a segurança dos nossos e dos vossos dados, é da maior importância para nós.

O nosso plano de resposta a incidentes foi imediatamente ativado e medidas de contenção foram prontamente aplicadas.

(Caso já tenha sido determinado o tipo de incidente/ataque e seja seguro revelá-lo:)

Cremos tratar-se de um ataque de (inserir o tipo - *malware, ransomware, Denial of Service,* etc.).
A extensão e o impacto do ataque abrangeram (referir o que foi afetado) / são ainda desconhecidos (selecionar consoante a realidade do incidente).

Compreendemos a gravidade desta situação e estamos dedicados à sua rápida resolução.

Manter-vos-emos atualizados à medida que a resolução do incidente progride.

Quaisquer questões ou preocupações acerca deste assunto poderão ser colocadas ao/à (inserir pessoa/departamento/divisão/direção e contactos)

Obrigado pela vossa compreensão e cooperação durante este momento difícil.

Atenciosamente,

(Autor do comunicado/A Organização)."

**Exemplo 2:** *Template* para uso com cliente (uso externo)

**Destinatários da comunicação:** Clientes (individuais e coletivos)

**Meios de comunicação recomendados:** SMS, *e-mail*.

"Estimado/a Cliente,

Lamentamos informar que o/a (nome da Organização) foi recentemente afetado/a por um incidente de cibersegurança e que, face ao sucedido, desejamos que esteja informado/a acerca desta situação.

As nossas equipas detetaram o incidente pelas (inserir hora) do dia (inserir dia e mês) e têm, desde então, estado a trabalhar empenhadamente na resolução do mesmo.

O nosso plano de resposta a incidentes foi imediatamente ativado e medidas de contenção foram prontamente aplicadas.

(Caso já tenha sido determinado o tipo de incidente/ataque e seja seguro revelá-lo:)

Cremos tratar-se de um ataque de (inserir o tipo - *malware, ransomware, Denial of Service,* etc.). A extensão e o impacto do ataque abrangeram (referir o que foi afetado) / são ainda desconhecidos (selecionar consoante a realidade do incidente).

A segurança dos seus dados é da maior importância para nós, e estamos a fazer todos os possíveis para lidar com esta situação de modo a garantir a segurança dos mesmos. Compreendemos as preocupações que esta situação possa gerar, pelo que estamos empenhados em mantê-lo/a a par dos progressos da resolução do incidente. Quaisquer preocupações ou questões que tenha poderão ser dirigidas ao/à (inserir pessoa/departamento/divisão/direção e contactos).

Pedimos desculpa por qualquer incómodo que esta situação possa causar e agradecemos a sua confiança no/na (nome da Organização).

Atenciosamente,

(Autor do comunicado/Organização)"

**Exemplo 3:** *Template* para uso com a comunicação social (uso externo)

**Destinatários:** Órgãos de comunicação social

**Meios de comunicação recomendados:** SMS, *e-mail*.

"O/A (nome da Organização), emitiu um comunicado sobre um recente incidente de cibersegurança para garantir a transparência com os seus interlocutores.

O/A (nome da Organização) lamenta informar que foi recentemente afetado/a por um incidente de cibersegurança.

As suas equipas detetaram o incidente pelas (inserir hora) do dia (inserir dia e mês) e têm, desde então, estado a trabalhar empenhadamente na resolução do mesmo.

O seu plano de resposta a incidentes foi imediatamente ativado e medidas de contenção foram prontamente aplicadas.

(Caso já tenha sido determinado o tipo de incidente/ataque e seja seguro revelá-lo:)

O/A (nome da Organização) crê tratar-se de um ataque de (inserir o tipo - *malware, ransomware, Denial of Service,* etc.). A extensão e o impacto do ataque abrangeram (referir o que foi afetado) / são ainda desconhecidos (selecionar consoante a realidade do incidente).

O/A (nome da Organização) reitera a sua dedicação à resolução deste incidente, sublinhando a importância de manter o público informado e assumindo o compromisso de adotar todas as medidas necessárias para prevenir incidentes futuros.

(Para complementar a comunicação feita à imprensa, poderá inserir uma citação de um alto dirigente ou de um porta-voz da Organização, tal como: (Nome da pessoa), (cargo da pessoa), declarou que no/na (nome da Organização) "estamos totalmente dedicados à resolução deste incidente e a trabalhar ativamente para garantir a segurança dos nossos sistemas e dados. A nossa prioridade continua a ser a segurança dos nossos ativos, dos nossos parceiros e trabalhadores e do público.

Para questões de imprensa ou entrevistas, por favor contacte:

(Nome do responsável)

(endereço de e-mail)

(número de telefone/telemóvel)

Agradecemos a vossa atenção a este assunto. Continuaremos a atualizar-vos à medida que formos progredindo na resolução deste incidente.

Atenciosamente,

(Autor do comunicado/Organização)"

## VISITE O NOSSO SITE

CNCS

Centro Nacional
de Cibersegurança
PORTUGAL

PRR
Plano de Recuperação
e Resiliência

REPÚBLICA
PORTUGUESA

Financiado pela
União Europeia
NextGenerationEU

Observatório
de **Cibersegurança**