Nota: A Versão de Consulta Rápida serve apenas para auxiliar numa breve verificação dos passos a realizar numa situação de crise de cibersegurança e não dispensa a leitura da versão completa do Referencial de Comunicação de Risco e de Crise em Cibersegurança do CNCS.

FASE 1

PREPARAR A COMUNICAÇÃO DE UMA CRISE DE CIBERSEGURANÇA

A ORGANIZAÇÃO **DEVE TER DEFINIDO:**	A ORGANIZAÇÃO **DEVE TER PREPARADO:**
• O que constitui um incidente de cibersegurança;	• Lista de contactos (24/7) a contactar numa crise;
• O que constitui uma crise de cibersegurança;	• *Templates* de comunicação para os diferentes grupos de interesse;
• Quais são os riscos presentes na Organização;	• *War rooms*;
• Plano de comunicação;	• Meios de comunicação alternativos
• Equipa de comunicação e respetivas funções de cada membro da equipa;	• Cópias impressas dos procedimentos de resposta a incidentes;
• Quais são os grupos de interesse;	• Infraestruturas e sistemas de armazenamento seguro.
• Os meios através dos quais a comunicação será feita.	

FASE 2

RESPONDER EFICAZMENTE

AÇÕES DE COMUNICAÇÃO DURANTE A FASE DE RESPOSTA AO INCIDENTE:
• Ativar a equipa de comunicação;
• Reportar o incidente;
• Documentar o incidente;
• Comunicar o encerramento formal da crise;
• Recuperar a reputação.

INFORMAÇÕES ÚTEIS PARA O REPORTE DE INCIDENTES AO CNCS		
Há três tipos de notificação a ter em conta.*		
A	**B**	**C**
Notificação inicial	Notificação de fim de impacto relevante ou substancial	Notificação final

*Estes tipos de notificação diferem da notificação voluntária de incidentes, não incluída no RJSC.
As notificações voluntárias devem ser realizadas por via do *website* ou do correio eletrónico indicados.

COMO PROCEDER À NOTIFICAÇÃO AO CNCS?		
Via *website*:	**Via correio electrónico:**	**Via contacto telefónico:**
https://www.cncs.gov.pt/pt/notificacao-incidentes/	cert@cert.pt	(+351) 210 497 399 **24/7**: (+351) 910 599 284

FASE 3

APRENDER LIÇÕES E MELHORAR

ATIVIDADES A REALIZAR PÓS-INCIDENTE PARA RETIRAR LIÇÕES E MELHORAR

- Recolher *feedback* acerca das ações realizadas durante a crise;
- Rever o incidente e avaliar o plano de comunicação;
- Reavaliar e rever riscos;
- Comunicar os resultados da nova análise de riscos.

EXEMPLOS DE *TEMPLATES* DE COMUNICAÇÃO

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

Destinatários da comunicação: Grupos de interesse internos e externos

Meios de comunicação recomendados: *E-mail* e *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 clientes (uso externo)

Destinatários da comunicação: Clientes (individuais e coletivos)

Meios de comunicação recomendados: *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, pelo que 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 da comunicação: Órgãos de comunicação social

Meios de comunicação recomendados: *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)"