Instruções

1. Observações gerais

Âmbito: Empresas de seguros e de resseguros com sede em Portugal e sociedades gestoras de fundos de pensões.

Periodicidade: Mensal

Para efeitos do presente modelo de reporte, define-se como incidente cibernético (cf. https://www.cncs.gov.pt/pt/glossario/#linhasobservacao):

- um evento com um efeito adverso real na segurança das redes e dos sistemas de informação;
- ações tomadas através da utilização de uma rede de computadores que resultam num efeito atual ou potencialmente adverso sobre um sistema de informação e/ou a informação aí armazenada.

O reporte de incidentes cibernéticos permite que estes sejam reportados de forma agrupada, por classe de incidentes. No entanto, devem ser utilizadas tantas linhas quantas sejam necessárias de modo a preencher adequadamente todas as variáveis exigidas no ficheiro de reporte.

O ficheiro de reporte "Incidentes cibernéticos" está estruturado em três secções distintas, nomeadamente:

- **Informação Geral:** Esta secção contém os campos referentes à identificação da entidade supervisionada e informação referente ao responsável pelo preenchimento do ficheiro de reporte;
- **Reporte de Incidentes Cibernéticos:** Esta secção contém informação sobre a caracterização dos incidentes, dados gerais dos incidentes, impacto operacional, medidas tomadas, impacto económico e outros dados relevantes sobre os incidentes;
- **Reporte de Incidentes Cibernéticos em Resolução:** Esta secção contém informação sobre o estado dos incidentes em resolução e só deve ser preenchido se a entidade supervisionada tiver reportado algum incidente com o estado "Em processo de resolução" no mês anterior.

2. Instruções de Preenchimento

ELEMENTO	INSTRUÇÕES
Cabeçalho	
Data de Reporte	Data de referência do reporte (por exemplo, 31-01-2024).
Nome da entidade	Nome da entidade supervisionada a que se refere a resposta.
Código Estatístico da entidade	Código estatístico utilizado para efeitos de reporte à ASF.
Nome da pessoa responsável	Nome da pessoa responsável pelo preenchimento do questionário (vd. informação a prestar aos titulares dos dados na folha "Informação Geral").
Contacto telefónico da pessoa responsável	Contacto telefónico da pessoa responsável pelo preenchimento do ficheiro de reporte (vd. informação a prestar aos titulares dos dados na folha "Informação Geral").
Endereço *e-mail* da pessoa responsável	Endereço de *e-mail* da pessoa responsável pelo preenchimento do ficheiro de reporte (vd. informação a prestar aos titulares dos dados na folha "Informação Geral").
LEI (*Legal Entity Identifier*)	Identificador de Entidade Jurídica. Código alfanumérico de 20 carateres baseado na norma ISO 17442 desenvolvida pela Organização Internacional de Normalização (ISO), que permite identificar de forma clara e única entidades que participam em transações financeiras e os dados de referência associados.
Incidentes cibernéticos	
Caracterização dos incidentes	
Incidente já reportado como Severo	Indicação se o incidente foi previamente reportado à ASF como severo, ao abrigo da Norma Regulamentar n.º 9/2024-R, de 26 de setembro[1], ou do Regulamento Delegado (UE) 2025/301 da Comissão, de 23 de outubro de 2024[2], e do Regulamento de Execução (UE) 2025/302 da Comissão, de 23 de outubro de 2024[3]. Em caso afirmativo, é necessário preencher apenas o campo "Código interno do incidente" com o ID da notificação inicial, dispensando-se o preenchimento dos demais campos de reporte.
Código interno do incidente	Código interno único atribuído a um grupo homogéneo de incidentes. O código deverá apresentar o seguinte formato: RI_CE_Ano-Mês-Numeração Contínua (ex. RI101120240401), sendo que: RI – Reporte de Incidentes; CE – Código Estatístico da entidade; Ano – Ano atual do reporte de incidentes; Mês – Mês atual do reporte de incidentes;

[1] A Norma Regulamentar n.º 9/2024-R, de 26 de setembro, pode ser consultada aqui.
[2] Complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam o conteúdo e os prazos para a notificação inicial e os relatórios intercalar e final sobre incidentes de carácter severo relacionados com as TIC, bem como o conteúdo da notificação voluntária de ciberameaças significativas, e que pode ser consultado aqui.
[3] Estabelece normas técnicas de execução para a aplicação do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita aos formulários, modelos e procedimentos normalizados que as entidades financeiras devem utilizar para comunicar incidentes de carácter severo relacionados com as TIC e notificar uma ciberameaça significativa, e que pode ser consultado aqui.

<table>
<tr><th>ELEMENTO</th><th>INSTRUÇÕES</th></tr>
<tr><td></td><td>Numeração contínua – Número de incidentes reportado pela entidade, começando na numeração “01” no reporte de janeiro.

Em caso de incidente de carácter severo reportado à ASF ao abrigo da Norma Regulamentar n.º 9/2024-R, de 26 de setembro, ou do Regulamento Delegado (UE) 2025/301 da Comissão, de 23 de outubro de 2024, e do Regulamento de Execução (UE) 2025/302 da Comissão, de 23 de outubro de 2024, o código deverá coincidir com o da Notificação Inicial, com o seguinte formato: RI-CE-Ano_Mês-Numeração do reporte-NI.</td></tr>
<tr><td>Classe de incidentes</td><td>Classificação dos incidentes, de acordo com a Taxonomia Comum da Rede Nacional de CSIRT (https://www.cncs.gov.pt/docs/taxonomia-cncs.pdf).</td></tr>
<tr><td>Indicação dos tipos mais frequentes</td><td>Indicação dos tipos de incidentes mais frequentes, de acordo com a Taxonomia Comum da Rede Nacional de CSIRT (https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf), para cada classe de incidentes indicada.
Os números das tipologias (pode ser selecionado mais do que um) devem ser separados por vírgula, em linha com a seguinte tabela (por exemplo, «6.1,6.3»):
<table>
<tr><th>Classe Incidente</th><th>Tipo Incidente</th></tr>
<tr><td rowspan="4">1 - Código Malicioso</td><td>1.1 - Sistema Infetado</td></tr>
<tr><td>1.2 - Servidor C2</td></tr>
<tr><td>1.3 - Distribuição de Malware</td></tr>
<tr><td>1.4 - Configuração de malware</td></tr>
<tr><td rowspan="5">2 - Disponibilidade</td><td>2.1 - Negação de Serviço</td></tr>
<tr><td>2.2 - Negação de Servido Distribuida</td></tr>
<tr><td>2.3 - Configuração incorreta</td></tr>
<tr><td>2.4 - Saboatagem</td></tr>
<tr><td>2.5 - Interrupção</td></tr>
<tr><td rowspan="3">3 - Recolha de Informação</td><td>3.1 - Scanning</td></tr>
<tr><td>3.2 - Sniffing</td></tr>
<tr><td>3.3 - Engenharia Social</td></tr>
<tr><td rowspan="4">4 - Intrusão</td><td>4.1 - Compromisso de Conta Privilegiada</td></tr>
<tr><td>4.2 - Compromisso de Conta Não Privilegiada</td></tr>
<tr><td>4.3 - Compromisso de Aplicação</td></tr>
<tr><td>4.4 - Arrombamento</td></tr>
<tr><td rowspan="3">5 - Tentativa de Intrusão</td><td>5.1 - Exploração de Vulnerabilidade</td></tr>
<tr><td>5.2 - Tentativa de Login</td></tr>
<tr><td>5.3 - Nova Assinatura de Ataque</td></tr>
<tr><td rowspan="4">6 - Segurança da Informação</td><td>6.1 - Acesso não autorizado</td></tr>
<tr><td>6.2 - Modificação não autorizada</td></tr>
<tr><td>6.3 - Perdade dados</td></tr>
<tr><td>6.4 - Exfiltração de Informação</td></tr>
<tr><td rowspan="4">7 - Fraude</td><td>7.1 - Utilização indevida ou não autorizada de recursos</td></tr>
<tr><td>7.2 - Direitos de autor</td></tr>
<tr><td>7.3 - Utilização ilegitima de nome de terceiros</td></tr>
<tr><td>7.4 - Phishing</td></tr>
<tr><td rowspan="3">8 - Conteudo Abusivo</td><td>8.1 - SPAM</td></tr>
<tr><td>8.2 - Discurso nocivo</td></tr>
<tr><td>8.3 - Exploração sexual de menores, racismo e apologia da violência</td></tr>
<tr><td rowspan="5">9 - Vulnerabilidade</td><td>9.1 - Criptografia fraca</td></tr>
<tr><td>9.2 - Amplificador DDoS</td></tr>
<tr><td>9.3 - Serviços acessíveis potencialmente indesejados</td></tr>
<tr><td>9.4 - Revelação de informação</td></tr>
<tr><td>9.5 - Sistema vulnerável</td></tr>
<tr><td rowspan="2">10 - Outros</td><td>10.1 - Sem tipo</td></tr>
<tr><td>10.2 - Indeterminado</td></tr>
<tr><td>11 - Teste</td><td>11.1 - Destinado a testes</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>ELEMENTO</th><th>INSTRUÇÕES</th></tr>
<tr><td>Sistema Alvo</td><td>Indicação do sistema/rede alvo do incidente, de acordo com a seguinte classificação[4]:
<table>
<tr><th>Sistema-Alvo</th><th>Tipo</th></tr>
<tr><td rowspan="2">1- Redes</td><td>1.1 - LAN</td></tr>
<tr><td>1.2 - WAN</td></tr>
<tr><td rowspan="5">2- Servidores</td><td>2.1 - Web</td></tr>
<tr><td>2.2 - E-mail</td></tr>
<tr><td>2.3 - Servidores de Base de Dados</td></tr>
<tr><td>2.4 - Servidores de ficheiros</td></tr>
<tr><td>2.5 - Outros</td></tr>
<tr><td rowspan="6">3- Equipamentos de Utilizadores</td><td>3.1 - Desktops (Torres)</td></tr>
<tr><td>3.2 - Laptops (Portáteis)</td></tr>
<tr><td>3.3 - Smartphones</td></tr>
<tr><td>3.4 - Tablets</td></tr>
<tr><td>3.5 - Discos Amovíveis</td></tr>
<tr><td>3.6 - Outros</td></tr>
<tr><td rowspan="6">4- Base de Dados</td><td>4.1 - Dados de Apólices</td></tr>
<tr><td>4.2 - Dados de Sinistros</td></tr>
<tr><td>4.3 - Dados de Clientes/Segurados</td></tr>
<tr><td>4.4 - Dados de Corretores/Parceiros</td></tr>
<tr><td>4.5 - Dados Financeiros</td></tr>
<tr><td>4.6 - Outros dados sensíveis</td></tr>
<tr><td rowspan="5">5- Aplicações Web</td><td>5.1 - Portal do Segurado</td></tr>
<tr><td>5.2 - Portal do Corretor</td></tr>
<tr><td>5.3 - Website Institucional</td></tr>
<tr><td>5.4 - Redes Sociais</td></tr>
<tr><td>5.5 - Outros Serviços Digitais</td></tr>
<tr><td rowspan="6">6- Sistemas Point-of-Sale</td><td>6.1 - Sistema de Cotação</td></tr>
<tr><td>6.2 - Sistema de Emissão</td></tr>
<tr><td>6.3 - Sistema de Sinistros</td></tr>
<tr><td>6.4 - Sistema de Pagamentos</td></tr>
<tr><td>6.5 - Sistema de Comissionamento</td></tr>
<tr><td>6.6 - Outros</td></tr>
<tr><td>7- Outros</td><td>7.1 - Outros</td></tr>
</table></td></tr>
<tr><td>Detalhe</td><td>Detalhar, no caso de a opção selecionada na coluna anterior ser “Outros” e/ou caso considere relevante incluir outras informações sobre ativos ou dados com maior criticidade que tenham sido comprometidos.</td></tr>
<tr><td><u>Dados gerais</u></td><td></td></tr>
<tr><td>N.º de incidentes (aproximadamente)</td><td>N.º (aproximado) de incidentes cibernéticos que ocorreram durante o período de referência, para a mesma classe de incidentes.

Note-se que o número total de incidentes corresponde ao total de incidentes ocorridos no mês do reporte (por exemplo, 100 e-mails de phishing).</td></tr>
<tr><td>Frequência dos incidentes (aproximadamente)</td><td>Frequência (aproximada) com que ocorreram os incidentes cibernéticos durante o período de referência, para a mesma classe de incidentes. Expresse essa regularidade com uma das seguintes opções por período:
Vários por dia (em que se verificam vários incidentes por dia);
Diário (em que os incidentes se concentraram, maioritariamente, num único dia do mês);
Semanal (em que os incidentes se concentraram, maioritariamente, numa semana, em particular, do mês);
Mensal (em que os incidentes se distribuíram ao longo mês);</td></tr>
</table>

[4] Quando houver múltiplos sistemas ou redes como alvos do incidente, cada um deve ser registado em linhas separadas.

ELEMENTO	INSTRUÇÕES
	• Ato isolado (em que existe um incidente num único dia). A título ilustrativo, considerem-se os seguintes exemplos: • num cenário de ocorrência de 100 *e-mails* de *phishing,* havendo registo de várias ocorrências por dia ao longo do todo o mês, o campo "N.º de incidentes cibernéticos" deve ser preenchido com o valor numérico de "100" e o campo "Regularidade dos incidentes" deverá ser preenchido com a opção "Vários por dia"; • num cenário em que ocorrem 10 incidentes de negação de serviço, em que as ocorrências se distribuem equitativamente em três semanas do mesmo mês, o campo "N.º de incidentes cibernéticos" deve ser preenchido com o valor numérico de "10" e o campo "Regularidade dos incidentes" deverá ser preenchido com a opção "Mensal".
Impacto Operacional	
Grau de impacto operacional	1 – Sem impacto operacional. (Por exemplo, um *e-mail* de *spam* é automaticamente bloqueado pelo servidor ou um ataque de código malicioso é bloqueado pelo antivírus.) 2 – Impacto operacional reduzido e limitado à área responsável pela gestão dos sistemas informáticos. (Por exemplo, é identificada uma vulnerabilidade e a área de sistemas informáticos tem de proceder manualmente a algumas atualizações.) 3 – Com impacto operacional nas áreas de negócio. (Por exemplo, ocorreu um ataque de negação de serviço e o *site* institucional esteve indisponível durante 30 minutos.) 4 – Ativação do Plano de Continuidade de Negócio (PCN). Note-se que as situações apresentadas são meramente ilustrativas, visando somente enquadrar a resposta pretendida em cada um dos campos.
Estado dos incidentes	Resolvidos – caso todos os incidentes indicados já tenham sido totalmente resolvidos. Em processo de resolução – caso exista pelo menos um incidente em processo de investigação ou cuja resolução ainda esteja em curso.
Detalhes sobre o estado dos incidentes	Caso haja incidentes em processo de resolução, prestação de informação sobre os mesmos.
Tempo de inatividade do sistema	Intervalo de tempo em que o sistema alvo esteve inoperacional (métrica em minutos).
Medidas tomadas	
Tempo de deteção do incidente	Intervalo de tempo entre a ocorrência do incidente e a sua deteção (métrica em minutos).
Tempo de mitigação do incidente	Intervalo de tempo entre a ocorrência do incidente e a contenção das partes afetadas (métrica em minutos).
Tempo de resolução do incidente	Intervalo de tempo entre a ocorrência e a recuperação/resolução do incidente (métrica em minutos).

ELEMENTO	INSTRUÇÕES
Exemplo prático: Um Ataque de Negação de Serviço (DoS) sobrecarrega os servidores da uma entidade supervisionada. A deteção é rápida, mas a mitigação do ataque pode levar até 1 hora para redirecionar o tráfego e aumentar a capacidade. A investigação completa e a implementação de medidas de segurança adicionais podem levar até 2 horas. Portanto, a entidade supervisionada deverá reportar: • Tempo de Deteção: 5 minutos; • Tempo de Mitigação: 60 minutos; • Tempo de Resolução: 120 minutos.	
Comunicação do evento a outras entidades/ autoridades	"Sim" – se foram notificadas outras entidades/autoridades (e.g. CNPD, CNCS, PJ, clientes, prestadores de serviços); neste caso, deverão ser indicadas quais. "Não" – caso não tenham sido notificadas outras entidades/autoridades.
Entidades/ autoridades contactadas	Indicar o nome das entidades/autoridades, caso a resposta à questão anterior seja afirmativa.
Impacto económico	
Despesas de gestão corrente	Estimativa dos gastos correntes, diretos e indiretos, resultantes da alocação de recursos internos à resolução do incidente em causa: *a)* Análise e resposta ao incidente por equipas internas; *b)* Comunicação e gestão interna; *c)* Investimento em *hardware* e/ou *software* adicionais para mitigação/resolução do incidente; *d)* Formação e ações de sensibilização a colaboradores; *e)* Perda de produtividade.
Despesas extraordinárias	Os custos e perdas incorridos pela entidade (pode basear-se em estimativas quando os valores reais não puderem ser determinados). Tipos de custos diretos e indiretos a considerar: *a)* Análise e resposta ao incidente; *b)* Comunicação e gestão; *c)* Investimento em *hardware* e/ou *software* adicionais; *d)* Formação e ações de sensibilização; *e)* Perda de produtividade.
Outros dados	
Outras informações consideradas relevantes	Neste campo podem ser incluídas outras informações consideradas relevantes. Em especial, sugere-se a inclusão de um descritivo das medidas tomadas no caso de ocorrência de incidentes cibernéticos que tenham conduzido à ativação do plano de continuidade de negócio e/ou à comunicação a outras autoridades/entidades.
Incidentes Cibernéticos em Resolução	
Caracterização dos incidentes	
Código interno do incidente	Código interno único atribuído a um grupo homogéneo de incidentes. O código deverá apresentar o seguinte formato: RI_CE_Ano-Mês-Numeração Contínua (ex. RI101120240401), sendo que: RI – Reporte de Incidentes;

ELEMENTO	INSTRUÇÕES
	CE – Código Estatístico da entidade; Ano – Ano atual do reporte de incidentes; Mês – Mês atual do reporte de incidentes; Numeração contínua – Número de incidentes reportado pela entidade, começando na numeração "01" no reporte de janeiro.
Detalhe	Detalhar, no caso de se considerar relevante incluir outras informações sobre ativos ou dados com maior criticidade que tenham sido comprometidos.
Impacto Operacional	
Grau de impacto operacional	1 – Sem impacto operacional. (Por exemplo, um *e-mail* de *spam* é automaticamente bloqueado pelo servidor ou um ataque de código malicioso é bloqueado pelo antivírus.) 2 – Impacto operacional reduzido e limitado à área responsável pela gestão dos sistemas informáticos. (Por exemplo, é identificada uma vulnerabilidade e a área de sistemas informáticos tem de proceder manualmente a algumas atualizações.) 3 – Com impacto operacional nas áreas de negócio. (Por exemplo, ocorreu um ataque de negação de serviço e o *site* institucional esteve indisponível durante 30 minutos.) 4 – Ativação do PCN. Note-se que as situações apresentadas são meramente ilustrativas, visando somente enquadrar a resposta pretendida em cada um dos campos.
Estado dos incidentes	Resolvidos – caso todos os incidentes indicados já tenham sido totalmente resolvidos. Em processo de resolução – caso exista pelo menos um incidente em processo de investigação ou cuja resolução ainda esteja em curso.
Detalhes sobre o estado dos incidentes	Caso haja incidentes em processo de resolução, prestação de informação sobre os mesmos.
Tempo de inatividade do sistema	Intervalo de tempo em que o sistema esteve inoperacional (métrica em minutos).
Medidas tomadas	
Tempo de mitigação do incidente	Intervalo de tempo entre a ocorrência do incidente e a contenção das partes afetadas (métrica em minutos).
Tempo de resolução do incidente	Intervalo de tempo entre a ocorrência e a recuperação/resolução do incidente (métrica em minutos).
Exemplo prático: Um Ataque de Negação de Serviço (DoS) sobrecarrega os servidores da uma entidade supervisionada. A deteção é rápida, mas a mitigação do ataque pode levar até 1 hora para redirecionar o tráfego e aumentar a capacidade. A investigação completa e a implementação de medidas de segurança adicionais podem levar até 2 horas. Portanto, a entidade supervisionada deverá reportar: • Tempo de Deteção: 5 minutos;	

ELEMENTO	INSTRUÇÕES
• Tempo de Mitigação: 60 minutos; • Tempo de Resolução: 120 minutos.	
Comunicação do evento a outras entidades/ autoridades	"Sim" – se foram notificadas outras entidades/autoridades (e.g. CNPD, CNCS, PJ, clientes, prestadores de serviços); neste caso, deverão ser indicadas quais. "Não" – caso não tenham sido notificadas outras entidades/autoridades.
Entidades/ autoridades contactadas	Indicar o nome das entidades/autoridades, caso a resposta à questão anterior seja afirmativa.
Impacto económico	
Despesas de gestão correntes	Estimativa dos gastos correntes, diretos e indiretos, resultantes da alocação de recursos internos à resolução do incidente em causa: *a)* Análise e resposta ao incidente por equipas internas; *b)* Comunicação e gestão interna; *c)* Investimento em *hardware* e/ou *software* adicionais para mitigação/resolução do incidente; *d)* Formação e ações de sensibilização a colaboradores; *e)* Perda de produtividade.
Despesas extraordinárias	Os custos e perdas incorridos pela entidade (pode basear-se em estimativas quando os valores reais não puderem ser determinados). Tipos de custos diretos e indiretos: *a)* Análise e resposta ao incidente; *b)* Comunicação e gestão; *c)* Investimento em *hardware* e/ou *software* adicionais; *d)* Formação e ações de sensibilização; *e)* Perda de produtividade.
Outros dados	
Outras informações consideradas relevantes	Neste campo podem ser incluídas outras informações consideradas relevantes. Em especial, sugere-se a inclusão de um descritivo das medidas tomadas no caso de ocorrência de incidentes cibernéticos que tenham conduzido à ativação do plano de continuidade de negócio e/ou à comunicação a outras autoridades/entidades.

3. Procedimento de submissão

O processo de submissão de reporte de incidentes cibernéticos é efetuado através do Portal ASF[5], especificamente na secção designada para esse fim. Na eventualidade de ocorrer um erro durante a submissão, o procedimento a seguir inclui o acesso ao Portal ASF e o envio de mensagem solicitando a correção da submissão. Após esta ação, deve aguardar uma comunicação formal indicando a possibilidade de nova submissão do reporte em questão.

[5] https://portalasf.asf.com.pt/