Notificação inicial

Dados Gerais da Entidade			
Campo	**Descrição**	**Observações**	**Etiqueta**
ID do Reporte	Identificador único atribuído a cada reporte. O Identificador único deverá apresentar deverá apresentar o seguinte formato: RI_CE_Ano-Mês-Numeração do reporte (ex. RI-1234-202404-01-NI), sendo que: RI – Reporte de Incidentes; CE – Código Estatístico da entidade (a preencher pela entidade); Ano – Ano atual do reporte de incidentes; Mês – Mês atual do reporte de incidentes (a preencher pela entidade); Numeração do reporte – Número de identificação do reporte incidentes indicado pela entidade, a iniciar na numeração "01" (a preencher pela entidade); NI – Notificação Inicial.	RI-XXXX-YYYYMMNN-NI	Pré-preenchido
Data da notificação	Data e hora da submissão da notificação inicial.	dd/mm/aaaa hh:mm	Obrigatório
Nome da entidade	Identificação da entidade que presta a informação.	Campo alfanumérico	Obrigatório
Código LEI	Identificador de entidade jurídica.	Campo alfanumérico	Obrigatório (se aplicável)
Código Estatístico	Código Estatístico da entidade que presta a informação.	Campo alfanumérico	Obrigatório
Tipo de entidade	Indicação da entidade afetada pelo incidente de acordo com o artigo 2.º da Norma Regulamentar n.º 9/2024-R, de 26 de setembro.	Escolha múltipla: *a)* Empresas de seguros e resseguros; *b)* Sociedades gestoras de fundos de pensões autorizadas em Portugal;	Obrigatório

		c) Mediadores de seguros, de resseguros e de seguros a título acessório residentes ou com sede em Portugal, que empreguem, no mínimo, 250 pessoas ou cujo volume de negócios anual é superior a 50 milhões de euros e o balanço total anual é superior a 43 milhões de euros, com exceção dos mediadores de seguros que também sejam instituições de crédito.	
Contacto			
Nome	Nome da pessoa responsável pelo reporte.	Campo alfanumérico	Obrigatório
Cargo/Função	Cargo/Função da pessoa responsável pelo reporte.	Campo alfanumérico	Obrigatório
E-mail	E-mail da pessoa responsável pelo reporte.	Campo alfanumérico	Obrigatório
Contacto telefónico	Contacto telefónico da pessoa responsável pelo reporte.	Campo numérico	Obrigatório
Dados do Incidente			
Data e hora da deteção do incidente	Data e hora da deteção do incidente.	dd/mm/aaaa hh:mm	Obrigatório
Data e hora da classificação do incidente como severo	Data e hora de classificação do incidente como severo de acordo com os critérios previstos no artigo 4.º da Norma Regulamentar n.º 9/2024-R, de 26 de setembro.	dd/mm/aaaa hh:mm	Obrigatório
Critérios de classificação do incidente como severo	Indicação dos critérios de classificação do incidente como severo de acordo com o previsto no artigo 4.º da Norma Regulamentar n.º 9/2024-R, de 26 de setembro.	Escolha múltipla: *a)* Qualquer acesso bem-sucedido, mal-intencionado e não autorizado às redes e sistemas de informação de apoio a funções críticas ou importantes; ou *b)* Afeta serviços críticos, e cumulativamente,	Obrigatório

		verificam-se duas ou mais das seguintes situações: *i)* Número de clientes afetados superior a 10% do total de clientes que utilizam o serviço afetado ou superior a cem mil clientes; *ii)* Impacto em termos de reputação; *iii)* Duração do incidente superior a 24 horas ou tempo de indisponibilidade do serviço crítico superior a 2 horas; *iv)* Afetação da disponibilidade, autenticidade, integridade ou confidencialidade dos dados, com impacto ou potencial impacto negativo na implementação dos objetivos de negócio ou no cumprimento de exigências regulatórias; *v)* Impacto económico, nomeadamente quando os custos e as perdas diretos e indiretos incorridos pela entidade devido ao incidente excedam ou provavelmente irão exceder os cem mil euros, sem considerar eventuais montantes recuperáveis.	
Descrição do Incidente			
Breve descrição do incidente	Descrição dos aspetos mais relevantes do incidente.	As entidades financeiras devem fornecer uma visão geral dos aspetos mais relevantes do incidente, tais como, possíveis causas, impactos imediatos, sistemas	Obrigatório

		e serviços afetados, modo de identificação do incidente, ou outros aspetos. Nos relatórios subsequentes, este campo pode ser atualizado de modo a permitir a compreensão contínua do incidente.	
Ativação do Plano de Continuidade do Negócio	Indicação se o Plano de Continuidade do Negócio foi acionado.	Expressão Booleana (Sim/Não)	Obrigatório (se aplicável)
Breve descrição das ações de mitigação tomadas	Descrição geral das medidas de mitigação tomadas (por exemplo, daquelas que figuram do plano de continuidade do negócio).	Campo alfanumérico	Obrigatório (se aplicável)
Origem do incidente	Indicação se o incidente tem origem num terceiro prestador de serviço ou noutra entidade financeira (incluindo entidades financeiras pertencentes ao mesmo grupo que a entidade que reporta).	Escolha múltipla: *a)* Terceiro prestador de serviços; *b)* Outra entidade financeira; *c)* Não aplicável.	Obrigatório

Relatório intercalar

Os campos seguintes são campos adicionais a juntar à informação constante da notificação inicial.

Dados Gerais da Entidade			
Campo	**Descrição**	**Observações**	**Etiqueta**
ID do Reporte	Identificador único atribuído a cada reporte. O Identificador único deverá apresentar deverá apresentar o seguinte formato: RI_CE_Ano-Mês-Numeração do reporte (ex. RI-1234-202404-01-NI), sendo que: RI – Reporte de Incidentes; CE – Código Estatístico da entidade (a preencher pela entidade); Ano – Ano atual do reporte de incidentes; Mês – Mês atual do reporte de incidentes (a preencher pela entidade); Numeração do reporte – Número de identificação do reporte incidentes indicado pela entidade, a iniciar na numeração "01" (a preencher pela entidade); RIn – Relatório Intercalar.	RI-XXXX-YYYYMMNN-RIn	Pré-preenchido
Data e hora da notificação	Data e hora da submissão do relatório intercalar.	dd/mm/aaaa hh:mm	Obrigatório
Data e hora da ocorrência do incidente	(se diferente da data e hora da deteção).	dd/mm/aaaa hh:mm	Obrigatório
Data e hora de recuperação das atividades	Data e hora de recuperação das atividades.	dd/mm/aaaa hh:mm	Obrigatório (se aplicável)
Descrição do Incidente			
Tipo de Incidente	Classificação da tipologia do incidente.	Escolha múltipla: *a)* Cibersegurança; *b)* Falha do processo; *c)* Falha do sistema; *d)* Evento externo;	Obrigatório

		e) Outro (especifique, por favor).	
Ameaças e técnicas utilizadas pelo agente de ameaça	Indicação das ameaças e técnicas utilizadas pelo agente de ameaça, caso tenha escolhido acima a hipótese "cibersegurança".	Escolha múltipla: *a)* Engenharia social (incluindo *phishing*); *b)* DoS/DDoS; *c)* Encriptação de dados (incluindo *ransomware*); *d)* Sequestro de recursos; *e)* Exfiltração e manipulação de dados, incluindo roubo de identidade; *f)* Destruição de dados; *g)* *Defacement*; *h)* Ataque à cadeia de valor (ataque simultâneo); *i)* Outro (especifique, por favor).	Obrigatório (se aplicável)
Número de clientes afetados	Número de clientes afetados pelo incidente [Artigo 3.º, alínea *a)* da Norma Regulamentar n.º 9/2024-R, de 26 de setembro.	Campo numérico	Obrigatório
Percentagem de clientes afetados	Percentagem de clientes afetados pelo incidente em relação ao número total de clientes que utilizam o serviço afetado. Caso haja mais do que um serviço afetado, a percentagem refere-se ao número total de clientes afetados face ao número total dos clientes dos serviços afetados. Quando o número efetivo de clientes afetados não puder ser determinado, a entidade deve utilizar estimativas baseadas em dados disponíveis de períodos de referência comparáveis.	Campo numérico (percentagem)	Obrigatório
Áreas e processos de negócio afetados pelo incidente	As **áreas** de negócio podem incluir, mas não estão limitadas a: – Marketing e desenvolvimento do negócio;	Campo alfanumérico	Obrigatório

	– Gestão de produto; – Compliance; – Gestão de risco; – Contabilidade, financeiro e tesouraria; – Recursos humanos e serviços gerais; – Tecnologia de informação; – Processos operacionais. Os **processos** podem incluir, mas não estão limitados a: – Informação contabilística; – Serviços atuariais; – Autenticação/autorização; – Inscrição digital (*on-boarding*) de prestadores de serviços/clientes; – Gestão de pensões; – Gestão de pagamentos de pensões – Gestão de apólices de seguros; – Gestão de pagamentos; – Gestão de sinistros; – Gestão e processamento de dados; – Débitos diretos; – Gestão de investimentos; – Cálculo do ativo líquido; – Emissão de subscrição de apólices; – Cobrança de prémios; – Resseguro; – Liquidação.		
Componentes da infraestutura que apoiam processos de negócio	Indicação sobre se houve componentes da infraestrutura (servidores, sistemas operativos, *software*, servidores de aplicações, *middleware*, componentes de rede, outros) que apoiam os processos de negócio, a ser afetados pelo incidente.	Escolha múltipla: *a)* Sim; *b)* Não; *c)* Sem informação disponível.	Obrigatório

Sistemas afetados pelo incidente na infraestrutura	Listagem dos sistemas afetados, incluindo as versões dos sistemas operativos.	Escolha múltipla: *a)* Servidores; *b)* Sistemas Operativos; *c)* *Middleware* *d)* Componentes de rede; *e)* Sem informação disponível; *f)* Outros.	Obrigatório
Impacto em termos de reputação	Informação sobre o impacto em termos de reputação resultante do incidente.	Escolha múltipla: *a)* O incidente atraiu a atenção dos meios de comunicação social; *b)* O incidente deu origem a múltiplas reclamações por parte de diferentes clientes; *c)* Os dados exfiltrados da entidade financeira foram divulgados sem o seu consentimento; *d)* A entidade financeira não poderá ou é provável que não possa cumprir as exigências regulamentares na sequência do incidente; *e)* A entidade financeira é ou poderá ser suscetível de perder clientes com impacto material na sua atividade em resultado do incidente.	Obrigatório (se aplicável)
Contextualização do em termos de reputação	Informação detalhada de como o incidente afetou ou poderia afetar a reputação da entidade, tais como, violações legais, exigências regulatórias não cumpridas, número de reclamações de clientes, entre outros. As informações contextuais podem incluir informações adicionais, como o tipo de meios de comunicação social (por exemplo, meios de comunicação social tradicionais, sociais, blogues, redes sociais, plataformas de	Campo alfanumérico	Obrigatório (se aplicável)

	streaming) e a cobertura mediática, incluindo o alcance dos meios de comunicação social (local, nacional, internacional). Note-se que a cobertura mediática, neste contexto, não significa apenas alguns comentários negativos de seguidores ou utilizadores de redes sociais. A entidade financeira deve também indicar se a cobertura mediática destacou riscos significativos para os seus clientes em relação ao incidente, como o risco de insolvência da entidade financeira ou o risco de perda de fundos.		
Duração do incidente	A duração do incidente relacionado com as TIC é medida a partir do momento em que o incidente ocorre até ao momento em que o incidente é resolvido. Caso as entidades não saibam ainda o momento em que o incidente será resolvido, devem aplicar estimativas.	DD:HH:MM	Obrigatório
Tempo de indisponibilidade do serviço	Tempo em que o serviço esteve indisponível, medido a partir do momento em que o serviço está total ou parcialmente indisponível(eis) para os clientes até ao momento em que as atividades/operações regulares são restabelecidas. Quando vários serviços são afetados, o tempo de indisponibilidade do serviço deve ser medido até que todos os serviços sejam restabelecidos.	DD:HH:MM	Obrigatório (se aplicável)
Perda de dados	Tipo de perdas de dados que o incidente envolve em relação à disponibilidade,	Escolha múltipla: *a)* Disponibilidade; *b)* Autenticidade;	Obrigatório (se aplicável)

	autenticidade, integridade e confidencialidade dos dados.	*c)* Integridade; *d)* Confidencialidade.	
Descrição da perda de dados	Descrição do impacto do incidente na disponibilidade, autenticidade, integridade e confidencialidade dos dados críticos.	Campo alfanumérico	Obrigatório (se aplicável)
Outras autoridades informadas	Indicação das autoridades que, além da ASF, foram informadas sobre o incidente.	Escolha múltipla: *a)* Comissão Nacional de Proteção de Dados; *b)* Outras autoridades de supervisão; *c)* Centro Nacional de Cibersegurança; *d)* Outras (especifique, por favor); *e)* Nenhuma.	Obrigatório

Relatório final

Os campos seguintes são campos adicionais a juntar à informação constante da notificação inicial e do relatório intercalar.

Dados Gerais da Entidade			
Campo	**Descrição**	**Observações**	**Etiqueta**
ID do Reporte	Identificador único atribuído a cada reporte. O Identificador único deverá apresentar deverá apresentar o seguinte formato: RI_CE_Ano-Mês-Numeração do reporte (ex. RI-1234-202404-01-NI), sendo que: RI – Reporte de Incidentes; CE – Código Estatístico da entidade (a preencher pela entidade); Ano – Ano atual do reporte de incidentes; Mês – Mês atual do reporte de incidentes (a preencher pela entidade); Numeração do reporte – Número de identificação do reporte incidentes indicado pela entidade, a iniciar na numeração "01" (a preencher pela entidade); RF – Relatório Final.	RI-XXXX-YYYYMMNN-RF	Pré-preenchido
Data e hora da notificação	Data e hora da submissão do relatório final.	dd/mm/aaaa hh:mm	Obrigatório
Descrição do Incidente			
Principal causa do incidente	Classificação da principal causa do incidente.	Escolha múltipla: **1. Ações dolosas** *a)* Ações internas deliberadas; *b)* Dano físico / manipulação/ roubo deliberado; *c)* Ações fraudulentas. **2. Falha de processo**	Obrigatório

		a) Monitorização e controlo deficientes e/ou insuficientes *b)* Funções e responsabilidades insuficientes e/ou imprecisas; *c)* Falha no processo de gestão de risco associado às TIC; *d)* Insuficiência e/ou deficiência das operações de TIC e das operações de cibersegurança: *e)* Inadequação de projetos, políticas, procedimentos e documentação interna; *f)* Inadequação do desenvolvimento e manutenção de TIC; *g)* Outros (especifique por favor). **3. Falha no funcionamento do sistema** *a)* Problemas de hardware (capacidade, desempenho, manutenção); *b)* Problemas de software (incompatibilidade, desempenho) *c)* Problemas de rede *d)* Dano físico à infraest; *e)* Outros (especifique por favor). **4. Erro humano** *a)* Formação insuficiente, deficiente e/ou inexistente; *b)* Negligência ou má interpretação; *c)* Falha de comunicação;	

		d) Insuficiência de recursos humanos; *e)* Outros (especifique, por favor). **5. Evento externo** *a)* Desastres naturais; *b)* Falhas de terceiros prestadores de serviços; *c)* Outros (especifique, por favor).	
Montante total de custos/perdas diretos/ indiretos	Montante total dos custos e perdas diretos e indiretos decorrentes do incidente (em euros): *a)* Montante de fundos ou ativos financeiros expropriados pelos quais a entidade é responsável; *b)* Montante dos custos de substituição ou realocação de *software*, *hardware* ou infraestrutura de rede; *c)* Montante dos custos com pessoal, incluindo custos associados à substituição ou realocação de pessoal, contratação de pessoal adicional, remuneração de horas extraordinárias e recuperação de habilidades perdidas ou prejudicadas do pessoal; *d)* Montante de taxas devidas pelo incumprimento de obrigações contratuais; *e)* Montante de custos de reparação e compensação aos clientes; *f)* Montante de perdas devido a receitas não auferidas; *g)* Montante de custos associados à comunicação interna e externa;	Campo alfanumérico (monetário)	Obrigatório (se aplicável)

	h) Montante de custos em consultoria externa, incluindo custos associados a serviços forenses e serviços de remediação.		
Impacto económico	Detalhe adicional sobre os custos e perdas diretos e indiretos decorrentes do incidente.	Campo alfanumérico	Obrigatório (se aplicável)
Resolução permanente do incidente	Descrição das ações/medidas tomadas/planeadas que pretendem resolver permanentemente o incidente e evitar que o mesmo ocorra novamente no futuro.	Campo alfanumérico	Obrigatório
Data e hora da resolução permanente do incidente	Data e hora em que o incidente foi classificado como resolvido.	dd/mm/aaaa hh:mm	Obrigatório
Inconsistência entre a data de resolução permanente do incidente e a data prevista.	Justificação para a inconsistência entre a data de resolução permanente do incidente e a data inicialmente prevista.	Campo alfanumérico	Obrigatório (se aplicável)
Reclassificação do incidente como não severo	Justificação para a reclassificação de um incidente como não severo.	Campo alfanumérico	Obrigatório (se aplicável)