Notificação inicial

Dados Gerais da Entidade			
Campo	**Descrição**	**Observações**	**Etiqueta**
ID do Reporte	Identificador único atribuído a cada reporte	A ser definido pela ASF	Preenchimento automático
Data da notificação	Data e hora da submissão da notificação inicial.	dd/mm/aaaa hh:mm	Preenchimento automático
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 [*presente norma regulamentar*].	Escolha múltipla: *a)* Empresas de seguros e resseguros; *b)* Sociedades gestoras de fundos de pensões autorizadas em Portugal; *c)* Mediadores de seguros, de resseguros e de seguros a título acessório residentes ou com sede em Portugal, que não sejam microempresas ou pequenas ou médias empresas de acordo com os critérios previstos no Decreto-Lei n.º 372/2007, de 6 de novembro, com exceção dos mediadores de seguros que também sejam instituições de crédito.	Obrigatório
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 [*presente norma regulamentar*].	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 [*presente norma regulamentar*].	Escolha múltipla: *a)* Qualquer acesso doloso, não autorizado e efetivo às redes e sistemas de informação; ou *b)* Afeta serviços críticos, e cumulativamente, 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 reputacional; *iii)* Duração do incidente superior a 24 horas ou tempo de indisponibilidade do serviço crítico superior a 2 horas;	Obrigatório

		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 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.	Obrigatório
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	Campo alfanumérico	Obrigatório (se aplicável)

	continuidade do negócio).		
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)* 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	A ser definido pela ASF	Preenchimento automático
Data e hora da notificação	Data e hora da submissão do relatório intercalar.	dd/mm/aaaa hh:mm	Preenchimento automático
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			
Código de referência do incidente	Indicação do código de referência atribuído pela ASF no seguimento da notificação inicial.	Campo alfanumérico	Obrigatório
Tipo de Incidente	Classificação da tipologia do incidente.	Escolha múltipla: *a)* Cibersegurança; *b)* Falha do processo; *c)* Falha do sistema; *d)* Evento externo; *e)* Outro (especifique, por favor).	Obrigatório
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*);	Obrigatório (se aplicável)

		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).	
Número de clientes afetados	Número de clientes afetados pelo incidente [Artigo 3.º, alínea *a)*].	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; Gestão de produto;	Campo alfanumérico	Obrigatório

	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)* Outros.	Obrigatório
Impacto reputacional	Informação sobre o impacto reputacional 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	Obrigatório (se aplicável)

		material na sua atividade em resultado do incidente.	
Contextualização do impacto reputacional	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 *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.	Campo alfanumérico	Obrigatório (se aplicável)
Duração do incidente	A duração do incidente relacionado com as TIC é medida a partir do	DD:HH:MM	Obrigatório

	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.		
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, autenticidade, integridade e confidencialidade dos dados.	Escolha múltipla: a) Disponibilidade; *a)* Autenticidade; *b)* Integridade; *c)* Confidencialidade.	Obrigatório (se aplicável)
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;	Obrigatório

		c) Centro Nacional de Cibersegurança; *d)* Outras (especifique, por favor); *e)* Nenhuma.	

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	A ser definido pela ASF	Preenchimento automático
Data e hora da notificação	Data e hora da submissão do relatório final.	dd/mm/aaaa hh:mm	Preenchimento automático
Descrição do Incidente			
Código de referência do incidente	Indicação do código de referência atribuído pela ASF no seguimento da notificação inicial.	Campo alfanumérico	Obrigatório
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** *a)* Monitorização e controle deficientes e/ou insuficientes ao nível: *i)* Da adesão à política; *ii)* Dos terceiros prestadores de serviços (incluindo intragrupo); *iii)* Da mitigação de vulnerabilidades;	Obrigatório

		iv) Da gestão de identidade e acesso; *v)* Da criptografia; *vi)* Do registo. *b)* Funções e responsabilidades insuficientes e/ou imprecisas: *c)* Falha no processo de gestão de risco associado às TIC: *i)* Imprecisão da definição dos níveis de tolerância ao risco; *ii)* Insuficiência das avaliações das vulnerabilidades e ameaças; *iii)* Inadequação das medidas de tratamento de risco; *iv)* Deficiência da gestão de riscos residuais de TIC; *d)* Insuficiência e/ou deficiência das operações de TIC e das operações de cibersegurança: *i)* Gestão de vulnerabilidades e *patches*; *ii)* Gestão de mudanças; *iii)* Gestão de capacidade e desempenho; *iv)* Gestão de ativos de TIC e classificação de informações; *v)* *Backup* e restauração; *vi)* Tratamento de erros; *e)* Insuficiência e/ou deficiência na gestão de projetos de TIC;	

		f) Inadequação das políticas, procedimentos e documentação interna; *g)* Inadequação dos sistemas de TIC em desenvolvimento e em manutenção; *h)* Insuficiência e/ou deficiência do teste de *software*; *i)* Outros (especifique por favor). **3. Falha no funcionamento do sistema** *a)* Capacidade e desempenho de *hardware*: incidentes causados por recursos de *hardware* que se revelam inadequados em termos de capacidade ou de desempenho para cumprir os requisitos legais aplicáveis; *b)* Manutenção de *hardware*: incidentes decorrentes de manutenção inadequada ou insuficiente de componentes de *hardware*, e da obsolescência do *hardware* (i.e., de incidentes decorrentes de componentes de *hardware* desatualizados ou obsoletos); *c)* Incompatibilidade de *software*: incidentes causados por componentes de *software* que são incompatíveis com outras configurações de *software*	

		ou do sistema. Inclui, entre outros, incidentes resultantes de conflitos de *software* ou configurações incorretas que afetam a funcionalidade geral do sistema; *d)* Desempenho de *software*: incidentes decorrentes de componentes de *software* que apresentam baixo desempenho ou ineficiências, mas que não são causados por questões de incompatibilidade de *software*. Inclui incidentes causados pela lentidão da resposta, pelo excesso de consumo de recursos ou pela ineficiente execução de consultas *e)* Configuração de rede: incidentes associados a configurações ou infraestrutura de rede incorretas ou mal configuradas. Inclui, mas não se limita a problemas como erros de configuração de rede, dificuldades no encaminhamento de tráfego, configurações inadequadas de *firewall*, e outros problemas de rede que comprometam a conectividade ou a comunicação; *f)* Dano físico: incidentes causados por danos físicos à infraestrutura	

		de TIC que levam a falhas no sistema; *g)* Outros (especifique por favor). **4. Erro humano** *a)* Formação insuficiente, deficiente e/ou inexistente; *b)* Negligência; *c)* Má interpretação *d)* Falha de comunicação; *e)* Insuficiência (quantitativa e/ou qualitativa) de recursos humanos; *f)* 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;	Campo alfanumérico (monetário)	Obrigatório (se aplicável)

	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; *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)