Incidentes cibernéticos

Observações gerais:

Âmbito: Empresas de seguros e sociedades gestoras de fundos de pensões sujeitas à supervisão da ASF.

Periodicidade: Mensal

Definição de incidentes cibernéticos: Para efeitos do presente modelo de reporte, define-se incidente cibernético como um evento com um efeito adverso real na segurança das redes e dos sistemas de informação.

ELEMENTO	INSTRUÇÕES
Cabeçalho	
Data de Reporte	Data de referência do reporte (por exemplo, 31-03-2022).
Nome da entidade	Nome da entidade 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 questionário (vd. informação a prestar aos titulares dos dados na folha "Informação Geral").
Endereço *email* da pessoa responsável	Endereço *email* da pessoa responsável pelo preenchimento do questionário (vd. informação a prestar aos titulares dos dados na folha "Informação Geral").
LEI	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	
Classe de incidentes	Classificação dos incidentes de acordo com a Taxonomia Comum da Rede Nacional de CSIRT (https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf).
Indicação dos tipos mais frequentes	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_v3.0.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 seguinte tabela (por exemplo, «6.1,6.3»):

	Classes de Incidentes	**Tipos de Incidentes**
	1 - Código Malicioso	1.1 - Sistema Infetado
		1.2 - Distribuição de *Malware*
		1.3 - Servidor C2
		1.4 - Configuração de *Malware*
	2 - Disponibilidade	2.1 - Negação de Serviço (DoS)
		2.2 - Negação de Serviço Distribuída (DdoS)
		2.3 -Configuração Incorreta
		2.4 - Sabotagem
		2.5 - Interrupção
	3 - Recolha de Informação	3.1 - *Scanning*
		3.2 - *Sniffing*
		3.3 - Engenharia Social
	4 - Intrusão	4.1 - Compromisso de Conta Privilegiada
		4.2 - Compromisso de Conta Não Privilegiada
		4.3 - Compromisso de Aplicação
		4.4 - Arrombamento ("*brute force*")
	5 - Tentativa de intrusão	5.1 - Exploração de Vulnerabilidade
		5.2 - Tentativa de *Login*
		5.3 -Nova Assinatura de Ataque
	6 - Segurança da Informação	6.1 - Acesso Não Autorizado
		6.2 - Modificação Não Autorizada
		6.3 - Perda de Dados
	7 - Fraude	7.1 - Direitos de Autor
		7.2 - Utilização Iligítima de Nome de Terceiros
		7.3 - *Phishing*
		7.4 - Utilização Indevida ou Não Autorizada de Recursos
	8 - Conteúdo Abusivo	8.1 - SPAM
		8.2 - Discurso Nocivo
		8.3 - Exploração Sexual de Menores, Racismo e Apologia da Violência
	9 - Vulnerabilidade	9.1 - Criptografia fraca
		9.2 - Amplificador DDoS
		9.3 - Serviços Acessíveis Potencialmente Indesejados
		9.4 - Revelação de Informação
		9.5 - Sistema Vulnerável
	10 - Outro	10.1 - Sem Tipo
		10.2 - Indeterminado
Dados gerais		
N.º de incidentes cibernéticos (aproximadamente)	N.º (aproximado) de incidentes cibernéticos que ocorreram durante o período de referência, para a mesma classe de incidentes.	
Frequência dos incidentes (aproximadamente)	Frequência (aproximada) com que ocorreram incidentes cibernéticos durante o período de referência, para a mesma classe de incidentes.	
Impacto dos incidentes		
Necessidade de ativação do plano de continuidade de negócio	Sim - caso tenha sido necessário ativar o plano de continuidade de negócio da entidade. Não - caso contrário.	
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.	
Medidas tomadas		
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 sistémico	
Perceção sobre o possível impacto sistémico do incidente	Perceção da entidade sobre a possibilidade de pelo menos um dos incidentes cibernéticos de que foi alvo poder afetar outras entidades e, no limite, o sistema financeiro em geral.
Detalhe (caso seja selecionado "Outro")	Detalhar, no caso de a opção selecionada na coluna anterior ser "Outro".
Outros dados	
Outras informações consideradas relevantes	Neste campo podem ser incluídas outras informações consideradas relevantes. Em especial, solicita-se informação adicional sobre os incidentes classificados como "10 - Outro", no campo relativo às classes de incidentes, e 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.