**Pelouro de Estabilidade Financeira**

**Circular n.º ……../EFI/2024**

**Maputo, ……. de ….. de 2024**

O Banco de Moçambique, no cumprimento das suas funções de supervisor das instituições de crédito e sociedades financeiras e no que resulta do previsto no artigo 7 do Aviso n.º xxx, que estabelece as directrizes de reporte de incidentes cibernéticos, determina que:

1. As instituições devem remeter ao Banco de Moçambique o reporte de incidentes cibernéticos de acordo com o modelo de reporte constante no Anexo 1.
2. A relação agregada dos incidentes cibernéticos deve ser remetida ao Banco de Moçambique, de acordo com o modelo de reporte constante no Anexo 2.
3. O modelo a que se refere no número 1 deve ser remetido através do Portal BSA (*Banking Supervision Application*) e outros meios indicados pelo Banco de Moçambique.
4. Nos casos em que a instituição não possua temporariamente capacidade operacional para assegurar a comunicação do incidente por via dos meios indicados no número anterior, ou nos casos em que os mesmos estejam indisponíveis, o reporte deve ser efectuado, a título excepcional, através de correio electrónico: **dsp\_riscocibernético@bancomoc.mz**
5. As dúvidas na interpretação e aplicação da presente Circular devem ser submetidas ao Departamento de Supervisão Prudencial do Banco de Moçambique.
6. A presente Circular entra imediatamente em vigor.

**Anexo I - Modelo de Reporte de Incidentes Cibernéticos**

|  |
| --- |
| Preliminar Até 24 horas, contadas do momento da sua ocorrência |
| Intermédio Até 48 horas, contadas do momento da  submissão do relatório preliminar |
| Final Até 30 dias úteis, após o reporte preliminar |

Identificação do Incidente:

|  |  |  |
| --- | --- | --- |
| Código da Instituição |  |  |
| Ano económico |  |
| Data |  |
| Hora de reporte ao BM |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A -Relatório Preliminar** | | | | | | | | | | | | |
| **Detalhes de contacto (1)** | | | | | | | | | | | | |
| **Pessoa 1** | | | | | | | | | | | | |
| Nome: |  | | | | | | | | | | | |
| Cargo: |  | | | | | | | | | | | |
| E-mail |  | | | | | | | | | | | |
| Telefone: |  | | | | | | | | | | | |
| **Pessoa 2 (se disponível)** | | | | | | | | | | | | |
| Nome: |  | | | | | | | | | | | |
| Cargo: |  | | | | | | | | | | | |
| E-mail |  | | | | | | | | | | | |
| Telefone: |  | | | | | | | | | | | |
| **Detalhes do Incidente (2)** | | | | | | | | | | | | |
| Data da ocorrência | **DD/MM/AAAA** | | | | | | | | | | | |
| Hora | **HH:MM** | | | | | | | | | | | |
| (2.1) Componentes afectados | 🞎 Estações de trabalho (*laptops*, PCs, dispositivos móveis)  🞎 Sistemas Operativos  🞎 Aplicativos computacionais  🞎 Sistemas principais (suportam as áreas de negócio)  🞎 Sistemas periféricos (suportam as áreas de controlo e de suporte) 🞎 Canais digitais (*internet banking*, mobile app)  🞎 Sistemas de gestão de dados e de armazenamento(*file* *servers*, bases de dados, *data warehouse*)  🞎 Aplicações de escritório  🞎 Correio electrónico  🞎 Redes e telecomunicações (*switches, routers, firewalls,* PBX, VoIp, *call center*)  🞎 Outros. Especificar: \_\_\_\_\_\_\_ | | | | | | | | | | | |
| (2.2) Áreas de negócio afectadas | 🞎 Finanças/contabilidade  🞎 Área comercial (corporativa e retalho)  🞎 Mercados financeiros (mercado monetário interbancário, cambial e *forex*)  🞎 Canais digitais/electrónicos (transacções com cartões, *Internet Banking*, *Mobile banking*, carteiras móveis)  🞎 Gestão de operações (de balcão, estrangeiro, gestão de contas de clientes, operações de compensação e liquidação)  🞎Tesouraria  🞎 Gestão de crédito (originação, análise, administração e recuperação/monitoramento de crédito)  🞎 Outros. Especificar: \_\_\_\_\_\_\_ | | | | | | | | | | | |
| (2.3) Áreas de controlo afectadas | 🞎 Risco  🞎 *Compliance*  🞎 Auditoria interna  🞎 Controlo interno  🞎 Segurança de Sistemas/Cibernética  🞎 Gestão de fraudes  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| (2.4)Áreas de suporte afectadas | 🞎 Recursos Humanos  🞎 Tecnologia de Informação  🞎 Aquisição de bens e serviços  🞎 Jurídico/legal  🞎 Gestão de reclamações de clientes  🞎 *Marketing*    🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| (2.5)localização e  **Indicadores de Compromisso (IoCs)** | 2.5.1. Endereços IP(*Se capturados do incidente*)   |  |  |  |  | | --- | --- | --- | --- | | Endereços IP | Envolvimento | Nome de Domínio a partir do qual o endereço de IP foi resolvido | Data/Hora da resolução do endereço de IP a partir do nome de Domínio | |  |  |  |  | |  |  |  |  |   2.5.2. Nome de Domínio (*Se capturados do incidente*)   |  |  | | --- | --- | | Nome de Domínio | Envolvimento do Nome do Domínio | |  |  | |  |  |   2.5.3. Endereços de correio electrónico (*Se capturados do incidente*)   |  |  | | --- | --- | | Endereço Electrónico | Envolvimento do Endereço Electrónico | |  |  | |  |  |   2.5.4. Ficheiros Maliciosos (*Se capturados do incidente*)   |  |  |  |  | | --- | --- | --- | --- | | Nome do ficheiro | Tamanho | MD5 hash | Análise Técnica (Sim/Não) | |  |  |  |  | |  |  |  |  | | | | | | | | | | | | |
| (2.6) Classificação do incidente quanto à natureza | Conteúdo abusivo  🞎 *SPAM*  🞎 Crime de ódio  🞎 Pornografia  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| Código malicioso  🞎 *Worm*  🞎 *Trojan*  🞎 *Spyware*  🞎 *Dialler*  🞎 *Rootkit*  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| Recolha de informações  🞎 *Scanning*  🞎 *Sniffing*  🞎 Engenharia social  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| Tentativa de intrusão  🞎 Exploração de vulnerabilidades conhecidas  🞎 Tentativa de acesso com violação de credenciais  🞎 Ataque desconhecido  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| Intrusão  🞎 Comprometimento de conta privilegiada  🞎 Comprometimento de uma conta sem privilégios  🞎 Comprometimento de aplicações  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| Disponibilidade  🞎 DoS (*Denial-of-Service*)  🞎 DDoS (*Distributed Denial-of-Service*)  🞎 Má configuração  🞎 Sabotagem  🞎 Interrupções  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| Comprometimento de informações  🞎 Acesso não autorizado a informações  🞎 Alteração não autorizada de informações  🞎 Perda de dados  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| Fraude  🞎 Utilização não autorizada de recursos  🞎 Direitos de autor  🞎 Falsificação de identidade  🞎 *Phishing*  🞎 Outros. Especificar:\_\_\_\_\_\_\_ | | | | | | | | | | | |
| APT (*Advanced Penetration Threat*) | | | | | | | | | | | |
| Outros (por especificar) | | | | | | | | | | | |
| (2.7) Classificação do incidente quanto a gravidade | 🞎 Crítico  🞎 Alto  🞎 Médio | | | | | | | | | | | |
| (2.8) Que acções ou respostas foram tomadas pela instituição |  | | | | | | | | | | | |
| (2.9) Incidente identificado por: | 🞎 Segurança cibernética ou de SI  🞎 Tecnologias de Informação  🞎 Auditoria interna  🞎 Auditoria externa  🞎 Prestador de serviços  🞎 Cliente  🞎 Trabalhador  🞎 Outros. Especificar: \_\_\_\_\_\_\_ | | | | | | | | | | | |
| **B - Relatório Intermédio** | | | | | | | | | | | | |
|  | | | | | | | | | | | | |
| 1. Informações sobre o (s) atacante (s) | 🞎 Trabalhador 🞎Provedores de serviço  🞎 *Hackers*  🞎Utente do serviço  🞎 Desconhecido  Outros. Especificar: \_\_\_\_\_\_\_ | | | | | | | | | | | |
| 1. Existe relação com outro incidente reportado anteriormente? | 🞎 Sim | | Fornecer detalhes:  Data:  Hora: | | | | | | | | | |
| 🞎 Não | | | | | | | | | | | |
| 1. **Impacto do incidente** | | | | | | | | | | | | |
| **(3.1) Impacto na reputação** | Nível de visibilidade | | | | | | | | | | | 🞎 Nacional |
| 🞎 Internacional |
| Houve alguma cobertura a nível dos meios de comunicação? | | | | 🞎 Sim | | | | | | | |
| 🞎 Não | | | | | | | |
| Se sim especifique | | | | | | | |
| Houve fuga de informação relacionada com a Instituição ou informações de clientes? | | | | 🞎 Sim | | | | | | | |
| 🞎 Não | | | | | | | |
| Se sim especifique | | | | | | | |
|  | Nível de confiança dos clientes face ao produto ou serviços providos pelo banco | | | |  | | | | | | | |
| **(3.2) Impacto Financeiro** | 🞎 Custos de aquisição, substituição ou actualização de *hardware* e/ou *software* | | | | | | | | | | | |
| 🞎 Potenciais custos legais e de correcção | | | | | | | | | | | |
| 🞎 Perda de receitas devido a oportunidades de negócio perdidas | | | | | | | | | | | |
| Outros. Especificar: \_\_\_\_\_\_\_ | | | | | | | | | | | |
| **(3.3) Impacto Operacional** | 🞎 Interrupção de serviços críticos que excedam o SLA e/ou RTO instituídos  Especificar o(s) serviço(s) crítico(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Indique as horas de interrupção por serviço: \_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | | |
| 🞎 Utilizadores afectados (em termos percentuais ou absolutos). Número de utilizadores: \_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | | |
| 🞎 Operações afectadas (em termos percentuais ou absolutos):  Volume de operações afectadas: \_\_\_\_\_\_\_\_\_\_\_\_\_  Volume de transacções financeiras afectadas: \_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | | |
| **(3.4) Impacto legal** | 🞎 Não | | | | | | | | | | | |
| 🞎 Sim | Especificar | | | | | | | | | | |
|  | | | | | | | | | | |
| 🞎 Possibilidade de aplicação de sanções por autoridades competentes, em resultado de incumprimento da legislação. | | | | | | | | | | |
| 🞎 Possibilidade de os incidentes resultarem em quebra de confidencialidade e integridade de dados sensíveis ou confidenciais | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
| 🞎 Volume de acções judiciais em número significativo de casos. | | | | | | | | | | |
| 🞎 Outros. Especificar: \_\_\_\_\_\_\_ | | | | | | | | | | |
|  |  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | |
| 1. Provedores de serviços originário do incidente | 🞎 Não | | | | | | | | | | | |
| 🞎 Sim | | | | | | | | | | Identificação do provedor | |
|  | |
| 1. O incidente foi resolvido? | 🞎 Sim | | | | | | | | | | Medidas tomadas para resolução do incidente | |
| 🞎 Não | | | | | | | | | | Acções de remediação propostas   |  | | --- | | Acção de Remediação | |  | |  | |  | |  | | |
| **C - Relatório Final** | | | | | | | | | | | | |
| **(1)Investigação e resolução do incidente** | | | | | | | | | | | | |
| 1. **Ordem sequencial dos eventos** | | | | | | | | | | | | |
| (1.1) Duração da interrupção | **HH:MM** | | | | | | | | | | | |
| (1.2) Descrição do invasor |  | | | | | | | | | | | |
| (1.3) Qual foi o vector de entrada do incidente? | 🞎 Rede de *Internet*  🞎 Mensagem instantânea  🞎 Telefone  🞎 Competências administrativas  🞎 *E-mail*  🞎 Rede de terceiros  🞎 Dispositivos não autorizados  🞎 Dispositivos perdidos/roubados  🞎 Redes sociais  🞎 Vulnerabilidades de segurança  🞎 *Phishing* ou *pop-ups* em formulários da *Web*  🞎 Engenharia social  🞎 Ameaças internas mal-intencionadas  🞎 *Spoofing*  🞎 Ataques baseados em identidade  🞎 Ataques de injecção de código  🞎 Outro (por favor, especifique) \_\_\_\_\_\_\_ | | | | | | | | | | | |
| (1.4) Vulnerabilidades/fraquezas expostas:  (possivel Múltipla escolha) | 🞎 Gestão inadequada de *patches*  🞎 Uso da versão anterior do sistema  🞎 Gestão inadequada de contas previlegiadas  🞎 Protecção inadequada de e-mail/navegador da *web*  🞎 Defesas inadequadas contra *malware*  🞎 Gestão inadequada de acessos  🞎 Inadequadas configurações de segurança para hardware em dispositivos, laptops, estações de trabalho, servidores  🞎 Inadequadas configurações de segurança para software em dispositivos, laptops, estações de trabalho, servidores  🞎 Inadequada defesa do perimetro  🞎 Controlo inadequado de portas, protocolos e serviços de rede  🞎 *Backup* inadequado de sistemas ou arquivos  🞎 Dispositivos de rede não seguros (*firewalls*, roteadores, *switches*)  🞎 Controles de segurança de *software* de aplicativo inadequados (aplicativos baseados na *web* e outros)  🞎 Defesa DDoS inadequada  🞎 Testes de penetração e segurança inadequados  🞎 Segmentação de rede inadequada  🞎 Falta de conscientização e/ou conformidade da equipe  🞎 Manutenção e monitoramento inadequados de *logs*  🞎 Falta de pessoal e/ou conformidade  🞎 Criptografia fraca  Outros. Especificar: \_\_\_\_\_\_\_ | | | | | | | | | | | |
| (1.5) Incidente foi escalado internamente para a gestão de topo, ao nível de grupo, para açcões fora dos procedimentos habituais? | 🞎 Não | | | | | | | | | | | |
| 🞎 Sim | | | A quem? (incluir também o papel na estrutura de governação, quando aplicável) | | | | | | | | |
|  |  | | | | | | | | | | | |
| (1.6) Partes interessadas informadas ou envolvidas | 🞎 Não | | | | | | | | | | | |
| 🞎 Sim | | | | | | | Como foram envolvidos ou informados? | | | | |
| (1.7) Medidas de escalonamento tomadas, incluindo aprovações solicitadas sobre medidas provisórias para mitigar o evento e razões para tomar tais medidas |  | | | | | | | | | | | |
| (1.8) A ocorrência obrigou a activação de procedimentos de gestão de crise | 🞎 Não | | | | | | | | | | | |
| 🞎 Sim | | | | 🞎 Planos de resposta e gestão de incidentes cibernéticos, tendo em conta o previsto nas Directrizes de Gestão do Risco e Resiliência Cibernética, aprovadas pelo Aviso n.º 2/GBM/2024, de 15 de Março. | | | | | | | |
| 🞎 Seguros ou outros instrumentos similares de cobertura de perdas relacionadas com o incidente | | | | | | | |
| 🞎 Planos de emergência | | | | | | | |
| 🞎 Outros processos ou módulos de crise relevantes da instituição: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | |
| (1.9) Quem está a liderar a investigação do incidente? | 🞎 A instituição | | | | | | | | | | | |
| 🞎 Provedor do serviço | | | | | | | | | | | |
| 🞎 Autoridades policiais ou outras agências de segurança | | | | | | | | | | | |
| 🞎 Se outro especificar: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | | |
|  |  | | | | | | | | | | | |
| (1.10) Quem está liderar as acções de remediação | 🞎 A instituição | | | | | | | | | | | |
| 🞎 Provedor do serviço | | | | | | | | | | | |
| 🞎 Se outro especificar:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | | |
|  | | | | | | | | | | | | |
| (1.11) Factores que causaram o problema/ Razões para ocorrer, causa e efeitos do incidente |  | | | | | | | | | | | |
| (1.12) O plano de acção definido para a resolução do incidente foi cumprido na totalidade | 🞎 Sim | | | | | | | | | | | |
| 🞎 Não | | | | | | | | Se não indique as razões | | | |
| (1.13) Acções correctivas tomadas para evitar ocorrências futuras de tipos semelhantes de incidentes | 🞎 Não | | | | | | | | | | | |
| 🞎 Sim | | | | | | | | | Etapas identificados ou a serem tomadas para resolver o incidente a longo prazo. | | |
| 1. **Avaliação final e remediação:** | | | | | | | | | |  | | |
| (2.1) Perdas financeiras directas e indirectas em meticais |  | | | | | | | | | | | |
| (2.2) Conclusão sobre causa |  | | | | | | | | | | | |
| (2.4) Resumo de incidentes semelhantes causados pela mesma causa raiz nos últimos 12 meses |  | | | | | | | | | | | |
| (2.5) Outras informações complementares |  | | | | | | | | | | | |
| (2.6) Houve notificação ao cliente/anúncio público/relatório a outros órgãos reguladores relevantes sobre a resolução do incidente | 🞎 Não | | | | | | | | | | | |
| 🞎 Sim | | | | | | Descrição do mecanismo adoptado para a comunicação do incidente ao cliente/anúncio público/relatório a outros órgãos reguladores | | | | | |
| 1. O incidente foi resolvido? | 🞎 Sim | | | | | | | | | | Indique a data de resolução | |
| 🞎 Não | | | | | | | | | | Remeter ao Banco um plano de acções com propostas para a resolução do incidente e respectivos prazos para acompanhamento   |  |  |  |  | | --- | --- | --- | --- | | Acção de Remediação | Prazo | Status | Observações | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  |   ­ | |

**Notas explicativas:**

1. As instituições devem preencher a secção do modelo de relatório, dependendo da fase de comunicação em que se encontram. Todos os campos são de preenchimento obrigatório, e devem conter informação clara, verdadeira, completa e actualizada de forma a permitir uma leitura fácil.
2. Os campos de preenchimento são passíveis de escolhas múltiplas.
3. A secção A corresponde ao relatório preliminar

**Anexo II – Modelo de Reporte de Incidentes Cibernéticos Agregado**

|  |  |  |
| --- | --- | --- |
| Código da Instituição |  |  |
| Ano económico |  |
| Data |  |
| Hora de reporte ao BM |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | | | |
| **(2) Classificação do Incidente** | | **(3 )Vulnerabilidade exposta** | **(4)Frequência dos incidentes** | **(5)ID dos Incidentes reportados** | **(6)Vector de Entrada** | **(7)Componentes afectadas** | | **(8)Serviços afectados (área de suporte, controlo ou de negócio)** | **(9)Nº Transacções comprometidas** | **(10)Nº de utilizadores afectados** | | **(11)Estado (Resolvido/**  **Em processo de resolução/**  **Não Iniciado)** |
| **(2.1) Quanto**  **a natureza** | **(2.2) Quanto**  **a gravidade** |  |  |  |  |  |  | |  |  |  | |
| *<Exemplo de preenchimento: Spam>* | *<alto>* | *<criptografia fraca>* | *<2>* | *<dim01>* | *<rede de internet>* | *SO* | *IT* | | *<10>* | *<1000>* | *<resolvido>* | |
| *<dim02>* | *<mensagem instantânea>* | *sistema principal* | *mercados* | | *<5>* | *<500>* | *<em processo de Resolução>* | |
|  |  |  |  |  |  |  |  | |  |  |  | |
| 1. **ANÁLISE DO IMPACTO DOS INCIDENTES REPORTADOS NO PERÍODO**   <Coloque a descrição global do impacto dos incidentes com base na tabela que se segue>   |  |  | | --- | --- | | **(12) Reputacional** |  | | **(13)Financeiro** |  | | **(14)Operacional** |  | | **(15)Legal** |  | | | | | | | | | | | | | |
| 1. **INFORMAÇÕES ADICIONAIS**  |  |  | | --- | --- | | (16) Outras informações consideradas relevantes: |  | | | | | | | | | | | | | |

*Declaramos que a informação contida no Anexo II – Modelo de Reporte de Incidentes Cibernéticos Agregado está de acordo com o registo de incidentes cibernéticos que ocorreram na instituição no período reportado.*

|  |  |  |
| --- | --- | --- |
| Assinatura do membro do Conselho de Administração  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | Assinatura do responsável pela Segurança Cibernética  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

<*Local*>, aos <*Data*>

1. **Notas explicativas ao Modelo de Reporte de Incidentes Cibernéticos**
2. **Relatório Preliminar**

|  |  |  |
| --- | --- | --- |
| Coluna | Descrição | Tipo de dados |
| (1) | Detalhes dos contactos dos responsáveis pela informação | Texto |
| (2) | Descrição do incidente quanto aos componentes afectados e principais acções implementadas |  |
| (2.1) | Indicação dos componentes e sistemas afectados | Texto |
| (2.2) | Indicação da área de negócio afectada | Texto |
| (2.3) | Indicação da área de controlo afectada | Texto |
| (2.4) | Indicação da área de suporte afectada | Texto |
| (2.5) | Indicação da localização, IP e domínios afectados |  |
| (2.5.1) | Indicação da lista de endereços IP capturados do incidente | Alfanumérico |
| (2.5.2) | Indicação da lista dos domínios capturados do incidente | lista de endereços IP capturados do incidente |
| (2.5.3) | Indicação da lista de e-mails capturados do incidente. | lista de endereços IP capturados do incidente |
| (2.5.4) | Descrição da informação sobre os ficheiros maliciosos capturados no incidente | lista de endereços IP capturados do incidente |
| (2.6) | Classificação do incidente quanto a natureza nos termos do anexo II do aviso de reporte de incidentes | Texto |
| (2.7) | Classificação do incidente quanto a gravidade nos termos do anexo I do aviso de reporte de incidentes | Texto |
| (2.8) | Descrição das acções tomadas para a resolução do incidente | Texto |
| (2.9) | Indicação do mecanismo usado para a identificação do incidente | Texto |

1. **Relatório Intermédio**

|  |  |  |
| --- | --- | --- |
| (1) | Indicação da origem do incidente | Texto |
| (2) | Indicação da relação do incidente reportado com outros incidentes | Texto |
| (3) | Descrição do impacto a nível reputacional, financeiro, operacional e legal | Texto |
| (3.1) | Descrição da magnitude do impacto (quer a nível nacional ou internacional) e do nível de divulgação nos meios de comunicação do incidente | Texto |
| (3.2) | Montante de perdas financeiras directas e indirectas decorrentes da ocorrência de incidente | Texto |
| (3.3) | Descrição do impacto em termos de tempo de indisponibilidade, volume de operações, transacções financeiras e utilizadores afectadas, | Texto |
| (3.4) | Descrição das Implicações legais e regulamentares incluindo o não cumprimento de imposições e possível aplicação de sanções | Texto |
| (4) | Indicação da origem do incidente e do provedor de serviço afectado | Texto |
| (5) | Indicação do estado do incidente tendo em conta o nível e o tempo de resolução do mesmo | Texto |
|  |  |  |
|  |  |  |

1. **Relatório Final**

|  |  |  |
| --- | --- | --- |
| (1) | Descrição detalhadas das investigações efectuadas tendo em conta a origem, vulnerabilidades expostas as acções tomadas para a sua resolução |  |
| (1.1) | Indicação do tempo de duração do incidente em horas | Numero inteiro |
| (1.2) | Descrição detalhada do invasor que esteja na origem do incidente | Texto |
| (1.3) | Indicação dos mecanismos usados na invasão | Texto |
| (1.4) | Indicação das fraquezas/ vulnerabilidades que o sistema esteve exposto | Texto |
| (1.5) | Descrição do nível de escalonamento na gestão do incidente | Texto |
| (1.6) | Indicação dos intervenientes envolvidos na resolução do incidente | Texto |
| (1.7) |  |  |
| (1.8) | Descrição dos procedimentos de gestão de crise activados para a mitigação do incidente | Texto |
| (1.9) | Indicação da parte interessada responsável pela investigação do incidente | Texto |
| (1.10) | Indicação da parte interessada responsável pela remediação do incidente | Texto |
| (1.11) | Descrição da causa do incidente | Texto |
| (1.12) | Indicação do nível de cumprimento do plano de acção na resolução do incidente | Texto |
| (1.13) | Descrição das acções correctivas implementadas para que o incidente não se repita | Texto |
| (2) | Descrição detalhada doa natureza do incidente, impactos económicos, lições aprendidas |  |
| (2.1) | Montante de perdas financeiras directas e indirectas decorrentes da ocorrência de incidentes | texto |
| (2.2) | Descrição detalhada sobre a origem do incidente | Texto |
| (2.3) | Descrição das melhorias implementadas | Texto |
| (2.4) | Descrição dos incidentes com a mesma causa raiz ocorridos nos últimos 12 meses | Texto |
| (2.5) | Descrição de Outras informações consideradas relevantes não captadas nos números anteriores | Texto |
| (2.6) | Descrição do tipo de notificação efectuada após a resolução do incidente | Texto |

1. Notas explicativas ao  **Modelo de Reporte de Incidentes Cibernéticos Agregado**
2. **INFORMAÇÃO ESTATÍSTICA (QUANTITATIVA)**

|  |  |  |
| --- | --- | --- |
| coluna | Descrição | Tipo de dados |
| (1) | *Indicação do nº de incidentes reportados no período em referência* | Numero inteiro |
| (2.1) | Classificar o incidente quanto a natureza nos termos do anexo II do aviso de reporte de incidentes | texto |
| (2.2) | Classificar o incidente quanto a gravidade nos termos do anexo I do aviso de reporte de incidentes | Texto |
| (3) | Indicação das fraquezas/ vulnerabilidades que o sistema esteve exposto | Texto |
| (4) | Indicação do numero de vezes que o incidente ocorreu | Numero inteiro |
| (5) | Indicação do numero de identificação do incidente reportado | Numero inteiro |
| (6) | Indicação do mecanismo utilizado pelo invasor | Texto |
| (7) | Indicação dos componentes e sistemas afectados | Texto |
| (8) | Indicação dos serviços afectados, área de negócio, suporte e controle afectada | Texto |
| (9) | Indicação do numero total de transacções afectadas pelo incidente | Número inteiro |
| (10) | Indicação do numero total de utilizadores afectadas pelo incidente | Numero inteiro |
| (11) | Indicação do estado do incidente tendo em conta o nivel de resolução do mesmo. | Texto |

1. **ANÁLISE DO IMPACTO DOS INCIDENTES REPORTADOS NO PERÍODO**

|  |  |  |
| --- | --- | --- |
| (12) | *Descrição da magnitude do impacto agregado (quer a nível nacional ou internacional) e do nível de divulgação nos meios de comunicação dos incidentes ocorridos no período* | Texto |
| (13) | *Montante total de perdas financeiras directas e indirectas decorrentes da ocorrência de incidentes* | Número |
| (14) | *Indicação do número Total de horas de indisponibilidade de serviços* | Número |
| (15) | Descrição das *Implicações legais e regulamentares incluindo o não cumprimento de imposições e possível aplicação de sanções* | Texto |

1. **INFORMAÇÕES ADICIONAIS**

|  |  |  |
| --- | --- | --- |
| (16) | Descrição de Outras informações consideradas relevantes não captadas nos números anteriores | Texto |