Brasília, DD MM AAAA

ANEXO VI – A

Modelo ISCF - Incidente de Segurança Cibernética em Fornecedor

ISCF – Incidente de Segurança Cibernética em Fornecedor

ISCF Nº: xxxx/2024	**TICKET Nº: Identificação interna do incidente no ambiente do fornecedor ex.: ID122024, TK012025, TH142026**
Descrição resumida da ocorrência	Ex. Ataque DDoS no sistema XPTO
Período (data/hora) do incidente	Data início: Hora início: Data fim: Hora fim:
Severidade	Crítica ou Alta
Característica da violação de segurança da informação apresentada.	( ) Confidencialidade ( ) Disponibilidade ( ) Integridade
Origem do alerta	Ex. SIEM, E-mail, denúncia interna/externa, Polícia Civil etc.
Serviço afetado: ex.: serviço de cobrança XYZ, url: http://www.teste.com	Gestor operacional CAIXA Área - ex.: CECOT, CESEG, CESET Contrato CAIXA: ex: 01-2024
Comunicado Incidente segurança	abuse@caixa.gov.br
Comunicado ISDP	gerit10@caixa.gov.br

1. INTRODUÇÃO

<Breve descrição ao leitor sobre o objetivo e informações que serão detalhadas a seguir nas fases do processo>.

2. ANÁLISE RESUMIDA DA OCORRÊNCIA

<As informações constantes nas seções que seguem devem ser objetivas, sem pré-julgamentos de fatos e baseada em informações evidenciadas em logs e regras.>

2.1. DETECÇÃO

<Informar como o evento foi detectado (ex.: Email externo ou interno, SIEM, Teams etc.>

2.2. ANÁLISE

<Informar a classificação do incidente, tática utilizada pelo atacante, POP, playbook utilizado etc.>

2.3. CONTENÇÃO

<Informar todas as ações que foram necessárias para conter o incidente (ex: isolamento de máquinas, bloqueio de usuários, bloqueio de IP, takedown de páginas etc.>

2.4. ERRADICAÇÃO

<Caso existam, informar todas as ações que foram necessárias para erradicar as fragilidades que permitiram o incidente (ex.: Atualização de patch, alteração em regras de firewall, alteração em permissionamento de acessos etc.>

2.5. RECUPERAÇÃO

<Caso existam, informar servidores, serviços ou aplicações que foram afetadas e que precisaram ser recuperadas por todas as áreas envolvidas.>

3. CONCLUSÃO

3.1. ANÁLISE FINAL DE PÓS-INCIDENTE

<Breve descrição ao leitor sobre a finalização do incidente relatando outros desdobramentos em função da ocorrência como: comunicados externos realizados, monitoramentos criados, dificuldades encontradas na investigação, queixa crime solicitada via polícia etc.>.

4. INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

4.1. FORMULÁRIO ISDP

<Nas ocorrências em que se observe qualquer tipo de violação de dados pessoais, conforme disposição da LGPD, o fornecedor deverá complementar o comunicado com as informações a seguir para os casos ISDP, comunicando também a equipe da GERIT:

4.1.1 COMUNICAÇÃO

4.1.1.1 Tipo de Comunicação

☐ Completa.

☐ Parcial.

Comentário:

4.1.1.2 Para comunicação parcial

☐ Preliminar

☐ Complementar

Comentário:

4.1.1.3 Critério para comunicação

☐ O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

☐ Não foi identificado riscos relevantes aos titulares

☐ Impacto continua sob avaliação

Comentário:

4.2 IDENTIFICAÇÃO DO AGENTE DE TRATAMENTO

4.2.1 Responsabilidade no tratamento de dados envolvido

☐ Controlador.

☐ Operador.
Comentário:

4.2.2 Comunicação ao Controlador

☐ Não necessária, o notificante é o Controlador.

☐ O Controlador já foi notificado.

☐ O Controlador não foi notificado.
Comentário:

4.2.3 Identificação da empresa

Número do CPF ou CNPJ:
Nome ou Razão Social:
Natureza da Organização (Pública ou Privada):
Endereço:
Cidade:
Estado:
CEP:
E-mail:
Comentário:

4.2.4 Dados do notificante

Nome
E-mail
Telefone

4.2.5 Dados do encarregado

☐ Mesmos do notificante
Nome
E-mail
Telefone

4.3 SOBRE O INCIDENTE DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS

4.3.1.1 Breve Descrição

4.3.1.2 Quando o incidente ocorreu

Data e hora de confirmação
Comentário

4.3.1.3 Quando a organização teve ciência do incidente de segurança

Data e hora de confirmação
Comentário

4.3.1.4 Justificativa quando a comunicação inicial do incidente não ocorrer no prazo sugerido de 2 dias úteis

Comentário

4.3.1.5 Justificativa quando a comunicação não ocorrer de forma imediata

Comentário

4.3.1.6 Qual a natureza dos dados afetados

☐ Origem racial ou étnica

☐ Convicção religiosa

☐ Opinião política

☐ Filiação a sindicato

☐ Filiação a organização de caráter religioso, filosófico ou político.

☐ Dado referente à saúde.

☐ Dado referente à vida sexual.

☐ Dado genético ou biométrico.

☐ Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).

☐ Dado financeiro.

☐ Nomes de usuário ou senhas de sistemas de informação.

☐ Dado de geolocalização.
Comentário

4.3.1.7 Qual a quantidade de titulares afetados

Comentário

4.3.1.8 Qual a categoria dos dados afetados

☐ Funcionários

☐ Prestadores de serviço

☐ Clientes

☐ Consumidores

☐ Usuários

☐ Pacientes de serviço de saúde

☐ Crianças ou adolescentes

☐ Outros (Comentar)

Comentário

5 MEDIDAS DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS

5.1 Medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a ocorrência do incidente de segurança.

Comentário

5.2 Medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança.

Comentário

5.3 Medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados

Comentário

5.4 O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?

Comentário

6 RISCOS RELACIONADOS AO INCIDENTE DE SEGURANÇA

6.1 Quais as prováveis consequências do incidente de segurança para os titulares afetados?

Comentário

6.2 Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

☐ Sim

☐ Não

Comentário

6.3 Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?

☐ Sim

☐ Não

Comentário

6.4 Caso os titulares afetados não tenham sido informados, quais são os motivos que justificam a não comunicação ou o seu retardo?

Comentário