SESCOOP/SP

RESOLUÇÃO Nº 090/2022 – CONSELHO ADMINISTRATIVO DO SESCOOP/SP

Dispõe sobre a regulamentação da Política de Resposta a Incidentes de Segurança da Informação de Privacidade - PRISIP do Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo - SESCOOP/SP,

O Presidente do Conselho Administrativo do Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo – SESCOOP/SP, no uso das atribuições conferidas nos incisos III e IX do artigo 13 do seu Regimento Interno (Resolução nº 71/2019), torna público que o Conselho Administrativo, 206ª (ducentésima sexta) Reunião Ordinária, realizada em 22 de fevereiro de 2022,

CONSIDERANDO a previsão estabelecida no artigo 4º, inciso III, alínea "a" e inciso IV e artigo 17 do Regulamento da Governança Corporativa (Resolução 078/2020 do Conselho Administrativo do SESCOOP/SP), que dispõem respectivamente sobre o Regulamento de natureza estratégica, que as deliberações do Conselho Administrativo serão instrumentalizadas por meio de Resolução,

CONSIDERANDO o advento da Lei nº 13.709, de 14/08/2018 com as alterações da Lei nº 13.853, de 08/07/2019, Lei Geral de Proteção de Dados, em vigor a partir de 18 de setembro de 2020,

CONSIDERANDO na necessidade de orientar o SESCOOP/SP a responder às situações de emergência e de exceção relacionadas a incidentes de segurança da informação e de privacidade, bem como sobre os eventuais incidentes relacionados a dados pessoais, de forma documentada, formalizada, rápida e confiável, resguardando as evidências, gerando aprendizado de forma a prevenir novos incidentes e, ainda, atendendo às exigências legais de comunicação e transparência.

RESOLVEU

Art. 1º – Aprovar a Política de Resposta a Incidentes de Segurança da Informação de Privacidade do SESCOOP/SP com vistas a estabelecer um plano estruturado e aplicável a todos usuários de informação do SESCOOP/SP e visando estabelecer.

Art. 2º – Esta Política, entra em vigor, na data de sua aprovação pelo Conselho Administrativo do SESCOOP/SP.

São Paulo, 22 de março de 2022.

EDIVALDO DEL GRANDE
Presidente do Conselho Administrativo do SESCOOP/SP

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

SESCOOP/SP

POLÍTICA DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE – SESCOOP/SP

CAPÍTULO I
APRESENTAÇÃO E DIRETRIZES

Art. 1º. Esta Política de Resposta a Incidentes de Segurança da Informação e de Privacidade se aplica ao Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo – **SESCOOP/SP**.

Art. 2º. Este documento institui e regulamenta o Plano de Resposta a Incidentes e Remediação previsto no § 2º, inciso I, letra "g" do artigo 50 da Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais – LGPD.

Art. 3º. Este Plano tem por objetivo orientar o **SESCOOP/SP** responder às situações de emergência e de exceção relacionadas a incidentes de segurança da informação e de privacidade, inclusive àqueles com dados pessoais, de forma documentada, formalizada, rápida e confiável, resguardando as evidências, gerando aprendizado de forma a prevenir novos incidentes e, ainda, atendendo às exigências legais de comunicação e transparência.

Art. 4º. Este Plano de Resposta a Incidentes de Segurança da Informação e de Privacidade abrange todos os recursos computacionais e físicos pertencentes, operados, mantidos e controlados pelo **SESCOOP/SP.**

Art. 5º. Este Plano de Resposta a Incidentes de Segurança da Informação e de Privacidade deve ser observada por todos no **SESCOOP/SP:** conselheiros, presidente, superintendentes, empregados, estagiários, menores aprendizes, prestadores de serviço, fornecedores, parceiros, conveniados, cooperados, público-alvo das ações da entidade e demais partes envolvidas.

CAPÍTULO II
TERMOS E DEFINIÇÕES

Art. 6º. ANPD - Autoridade Nacional de Proteção de Dados. Segundo a LGPD é a entidade responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Art. 7º. Ativo de informação. Qualquer componente (humano, tecnológico, físico ou lógico) que agrega valor e que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

Art. 8º. Controlador. Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Art. 9º. Co-controlador. Quando outra entidade determina em conjunto com o controlador as finalidades e meios de tratamento de dados pessoais.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Art. 10º. DDoS. Acrônimo em inglês para Distributed Denial of Service, negação de serviços distribuída em português. Tem a mesma finalidade do DoS, contudo o ataque é realizado de forma distribuída pela internet, quando milhares de computadores zumbis, comandados por um computador mestre, disparam ataques para um sistema alvo.

Art. 10. DoS. Acrônimo em inglês para Denial of Service, negação de serviços em português. É uma tentativa de tornar indisponíveis os recursos de um sistema através da sobrecarga de requisições.

Art. 11. Dialler. Programas que se conectam a internet, sem o conhecimento do usuário, para cometer fraudes.

Art. 12. Encarregado pelo Tratamento de Dados Pessoais. Membro especial do Grupo de Resposta a Incidentes de Segurança da Informação e de Privacidade, responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais

Art. 13. Fluxo de Tratamento de Dados Pessoais. É a descrição do ciclo de vida do tratamento de dados pessoais, ou seja, a forma como os dados pessoais são coletados, retidos/armazenados, processados/usados e eliminados.

Art. 14. Grupo de Resposta a Incidentes de Segurança da Informação e de Privacidade - GRISP. Grupo multidisciplinar do SESCOOP/SP responsável por coordenar e dar suporte às ações de resposta e remediação dos incidentes de Segurança da Informação e de Privacidade.

Art. 15. Incidente. Evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação.

Art. 16. Incidente de Segurança da Informação. Evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação.

Art. 17. Incidente de Segurança da Informação com Dados Pessoais. De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais.

Art. 18. Incidente de Segurança da Informação e de Privacidade. Inclui os dois tipos de incidentes relacionados nos Art. 16 e Art. 17.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Art. 19. Inventário de Dados Pessoais. O Inventário de Dados Pessoais representa um artefato primordial para documentar o tratamento de dados pessoais realizados pela instituição em alinhamento ao previsto pelo art. 37 da Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais.

Art. 20. Login. É o processo pelo qual o acesso a um sistema da informação é controlado pela autenticação de credenciais do usuário. As credenciais normalmente utilizadas em um processo de login são "Nome" e "Senha".

Art. 21. Log. Processo de registro de eventos relevantes num sistema computacional.

Art. 22. Nome CVE (Common Vulnerabilities and Exposures). Dicionário de vulnerabilidades e exposições de segurança da informação publicamente conhecidas.

Art. 23. Notificador. Qualquer pessoa ou sistema de monitoração que eventualmente notifique um incidente.

Art. 24. Relatório de Impacto à Proteção de Dados Pessoais. Segundo a LGPD é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como as medidas, salvaguardas e mecanismos de mitigação de risco.

Art. 25. Risco de Privacidade. É a perda potencial de controle sobre as informações pessoais. Embora um indivíduo possa consentir com o uso de suas informações pessoais, a perda de controle ocorre quando a organização deixa de fornecer salvaguardas adequadas.

Art. 26. Scanning. Ato de varrer a rede, seus dispositivos e sistemas com a finalidade de encontrar brechas ou vulnerabilidades que possam ser utilizadas para uma invasão.

Art. 27. Sniffing. É o procedimento de interceptar e registrar o tráfego de dados em uma rede de computadores.

Art. 28. Spam. Mensagens de e-mail não solicitadas e enviadas para um grande número de pessoas.

Art. 29. Spyware. Programa automático de computador que secretamente coleta informações sobre o usuário e seus costumes na internet e transmite estas informações para alguma entidade externa.

Art. 30. Titular. Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Art. 31. Trojan. Programa que infecta um computador e libera uma porta para invasão remota.

Art. 32. Vírus. Em Tecnologia da Informação é um software malicioso que infecta um programa, faz cópias de si mesmo e tenta se espalhar para outros computadores.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Art. 33. Worm. Em TI é um programa que se autorreplica e que, diferente dos vírus, não precisa de outro programa para se propagar.

CAPÍTULO III
GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE - ESCOPO, PAPÉIS E RESPONSABILIDADES

Art. 34. O Escopo do Grupo de Resposta a Incidentes de Segurança da Informação e de Privacidade – GRISP é receber, analisar, relatar, indicar soluções e coordenar as atividades necessárias, dentro do **SESCOOP/SP** para o tratamento de um incidente de segurança da informação ou que envolva dados pessoais, bem como a mitigação dos riscos de novos incidentes similares ao tratado.

Art. 35. À Diretoria Executiva cabe instituir e patrocinar o GRISP.

Art. 36. Ao Notificador:

Parágrafo 1º. Quando fizer parte do Pessoal Interno (qualquer pessoa que se enquadre naqueles papéis elencados no Art. 5º deste Plano) do **SESCOOP/SP**:

I. Notificar o GRISP na ocorrência de qualquer suspeita que aponte para um incidente de segurança da informação, relatando todas as informações até então conhecidas sobre o incidente;

II. Processar imediatamente as informações e atividades solicitadas pelo GRISP às demais unidades do **SESCOOP/SP**.

Parágrafo 2º. Quando for o titular ou outra parte interessada externa ao **SESCOOP/SP**:

I. Notificar o GRISP na ocorrência de qualquer suspeita que aponte para um incidente de segurança da informação, relatando todas as informações até então conhecidas sobre o incidente.

Art. 37. Ao Encarregado pelo Tratamento de Dados Pessoais cabe encaminhar comunicações formais à ANPD, ao titular, à controladores e à co-controladores em incidentes envolvendo dados pessoais.

Art. 38. Ao GRISP cabe:

I. Receber, analisar, relatar, indicar soluções e coordenar as atividades necessárias para o tratamento de um incidente de segurança da informação e de privacidade;

II. Acompanhar as atividades de modo a certificar que as ações de resposta foram corretamente implementadas e que o incidente foi devidamente contornado, contido ou solucionado;

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

III. Documentar todo o processo de resposta ao incidente de modo a alimentar a base de conhecimentos do **SESCOOP/SP**.

Art. 39. O GRISP será composto por representantes nomeados por portaria.

Parágrafo 1º. Extraordinariamente, o GRISP poderá convocar representantes de outras unidades do **SESCOOP/SP** ou dispensar algum dos componentes anteriores.

Parágrafo 2º. O tratamento de incidentes de segurança e de privacidade pelo GRISP será sempre considerado prioritário em relação às atividades rotineiras dos componentes do grupo.

Parágrafo 3º. O grupo será coordenado pelo representante da área de Infraestrutura e TI.

CAPÍTULO IV
PROCESSO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE

Seção I
Do Processo de Trabalho

Art. 40. Os recursos a serem utilizados no processo de resposta a incidentes de segurança da informação e de privacidade são:

I. Servidores e dispositivos de rede;

II. Ferramentas de segurança da informação;

III. Contratos, convênios e congêneres com terceiros;

IV. Serviços terceirizados de TI;

V. Planilhas de Inventário de Dados Pessoais;

VI. Planilhas de Riscos de Privacidade;

VII. Fluxos de tratamento de dados pessoais;

VIII. Relatório de impacto à proteção de dados pessoais;

IX. Relatórios prévios de Incidentes de Segurança da Informação e de Privacidade.

Art. 41. O GRISP definirá a metodologia de trabalho a ser utilizada em cada incidente, seguindo as premissas descritas neste capítulo.

Art. 42. Todo o trabalho do grupo deverá ser guiado e embasado pelo seguinte ciclo de vida de um incidente:

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

I. Ocorrência - interrupção não planejada de um serviço;

II. Detecção - processo que ocorre algum tempo após a ocorrência do evento;

III. Diagnóstico - identificação das características de um incidente;

IV. Reparo - processo de reconfigurar itens atacados;

V. Recuperação - processo de restaurar itens em falha ao seu último estado recuperável;

VI. Restauração - processo de disponibilizar ao usuário o serviço afetado;

VII. Encerramento - processo de validar com o usuário se o serviço está completamente disponível.

Art. 43. O ANEXO I apresenta o fluxo completo de todo o processo de resposta a incidentes de segurança da informação e de privacidade.

Art. 44. O GRISP deverá definir as informações a serem coletadas pelas diversas áreas do **SESCOOP/SP** bem como o meio de armazenamento destas informações. As informações coletadas devem conter, no mínimo:

I. Logs completos;

II. Data, horário e fuso horário (timezone) dos logs ou da ocorrência da atividade notificada;

III. Dados completos do incidente e outras informações utilizadas para identificar o evento.

Parágrafo 1º. Após análise do incidente e das informações disponíveis, o GRISP irá definir ações ou atividades a serem realizadas pelas diversas áreas do **SESCOOP/SP**.

Parágrafo 2º. Cada integrante do grupo ficará responsável por levantar informações e acompanhar a execução das ações dentro de sua unidade organizacional.

Parágrafo 3º. O armazenamento das informações coletadas deverá buscar garantir as características de confidencialidade, integridade e disponibilidade daquelas informações.

Art. 45. O GRISP ficará responsável pelo acompanhamento do problema até sua solução, mantendo informada a Diretoria Executiva do **SESCOOP/SP** quanto ao andamento das atividades.

Art. 46. Após a implementação da solução, o GRISP avaliará a eficácia das providências adotadas, verificando os níveis de satisfação obtidos e eventuais efeitos colaterais não esperados.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Seção II
Do Relatório de Incidentes de Segurança da Informação

Art. 47. Após a solução do incidente de segurança, o GRISP deverá gerar um Relatório de Incidentes de Segurança da Informação com, pelo menos, as seguintes informações:

I. Parecer técnico contendo uma análise de impacto, informações levantadas e o escopo do incidente;

II. Classificação do incidente de acordo com a tabela do **ANEXO II**;

III. As ações realizadas para a solução do incidente de segurança;

IV. Os problemas e as dificuldades encontradas para solução do incidente;

V. Sugestão de melhoria do ambiente de TI para prevenção de eventos similares ao ocorrido;

VI. Se o incidente envolver dados pessoais, o Encarregado deverá acrescentar o cálculo do **Art. 49** e a respectiva ação do **Art. 51**, de acordo com o resultado da Gravidade da Violação de Dados Pessoais, **GV**, a fim de evidenciar o motivo de comunicar ou não as partes interessadas sobre o incidente de segurança da informação com dados pessoais.

Parágrafo 1º. Todos os incidentes de segurança da informação, independentemente de envolverem dados pessoais ou não, serão documentados pelo Relatório de Incidentes de Segurança da Informação.

Parágrafo 2º. Após preenchido e executados os devidos procedimentos, o GRISP armazenará o Relatório assinado para consultas futuras.

Parágrafo 3º. O **ANEXO III** contém um modelo para o Relatório de incidente de segurança da informação.

Seção III
Da Avaliação da Gravidade da Violação e da Comunicação de Incidente de Segurança da Informação com Dados Pessoais

Art. 48. Havendo dados pessoais envolvidos no incidente, ou seja, para os Incidentes de Segurança da Informação com Dados Pessoais, o Encarregado de dados procederá com uma avaliação da gravidade da violação de dados pessoais, considerando os potenciais riscos ou danos para os titulares envolvidos.

Parágrafo 1º. A LGPD aduz em seu artigo 48 que "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares".

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Parágrafo 2º. A presente seção tem por objetivo definir uma metodologia objetiva para subsidiar a decisão do Encarregado de Dados e dos Controladores do **SESCOOP/SP** sobre quais incidentes de segurança da informação com dados pessoais devem ser comunicados, em conformidade com a Lei Geral de Proteção de Dados Pessoais.

I. A metodologia é baseada na metodologia recomendada pela Agência da União Europeia para a Cibersegurança -- ENISA[1].

Art. 49. Para o cálculo da Gravidade da Violação de Dados Pessoais, **GV**, será utilizada a fórmula **GV = CP x FI + CV**, onde:

I. Contexto de Processamento de Dados, **CP**. Diz respeito ao tipo dos dados violados, considerando outros fatores relacionados ao contexto geral do processamento. O **ANEXO IV** traz uma tabela com as pontuações possíveis para o critério **CP**;

II. Facilidade de Identificação, **FI**. Relaciona-se com a facilidade de identificação do titular a partir dos dados envolvidos no incidente. O **ANEXO V** traz uma tabela com as pontuações possíveis para o critério **FI**;

III. Circunstâncias de Violação, **CV**. Concernente às circunstâncias da violação de dados pessoais, como a perda de segurança ou a intenção maliciosa envolvida. O **ANEXO VI** traz uma tabela com as pontuações possíveis para o critério **CV**.

Art. 50. Após realizado o cálculo da Gravidade da Violação de Dados Pessoais, **GV**, conforme disposto no **Art. 49**, o valor de **GV** deverá ser confrontado com a tabela do **ANEXO VII**.

Art. 51. De acordo com o valor de Gravidade da Violação (**GV**) encontrado, o Encarregado de Dados executará as seguintes ações:

Parágrafo 1º. Se **GV** < 2, ou seja, se a gravidade de violação for "**Baixa**", o Encarregado de dados encaminhará o relatório e a comunicação de incidente com dados pessoais para:

I. As autoridades competentes do **SESCOOP/SP**;

II. Eventuais controladores e co-controladores dos dados pessoais afetados pelo incidente.

[1] Recommendations for a methodology of the assessment of severity of personal data breaches. Disponível em <https://www.enisa.europa.eu/publications/dbn-severity>. Acessado em 10/11/2021.

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Parágrafo 2º. Se 2 ≤ **GV** < 3, ou seja, se a gravidade de violação for "**Média**", o Encarregado de dados encaminhará o relatório e a comunicação de incidente com dados pessoais para:

I. As autoridades competentes do **SESCOOP/SP**;

II. Eventuais controladores e co-controladores dos dados pessoais afetados pelo incidente;

III. Titular(es) dos dados pessoais afetados pelo incidente.

Parágrafo 3º. Se 3 ≤ **GV** < 4, ou seja, se a gravidade de violação for "**Alta**", o Encarregado de dados encaminhará o relatório e a comunicação de incidente com dados pessoais para:

I. As autoridades competentes do **SESCOOP/SP**;

II. Eventuais controladores e co-controladores dos dados pessoais afetados pelo incidente;

III. O(s) titular(es) dos dados pessoais afetados pelo incidente;

IV. A ANPD.

Parágrafo 4º. Se **GV** ≥ 4, ou seja, se a gravidade de violação for "**Muito Alta**", o Encarregado de dados encaminhará o relatório e a comunicação de incidente com dados pessoais para:

a) As autoridades competentes do **SESCOOP/SP**;

b) Eventuais controladores e co-controladores dos dados pessoais afetados pelo incidente;

c) Titular(es) dos dados pessoais afetados pelo incidente;

d) ANPD.

Art. 52. A comunicação do incidente para a ANPD dar-se-á pelo preenchimento e envio do Formulário de Comunicação de Incidentes de Segurança com Dados Pessoais da ANPD.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo-SP

Parágrafo Único. O envio do Formulário à ANPD dar-se-á pelo Peticionamento Eletrônico do sistema SEI[2].

Art. 53. Até que a ANPD regulamente o prazo para comunicação do incidente de segurança com dados pessoais, a própria Autoridade Nacional recomenda que, havendo risco relevante, a comunicação se dê em até 2 (dois) dias úteis contados da data de conhecimento do incidente.

Art. 54. Ao final do Formulário o Encarregado deverá acrescentar o cálculo do **Art. 49** e a tabela do **ANEXO VII**, a fim de evidenciar o motivo de comunicar ou não as partes interessadas sobre o incidente de segurança da informação com dados pessoais.

Seção IV
Do Formulário de Incidente de Segurança da Informação com Dados Pessoais

Art. 55. Se houver necessidade de comunicar o incidente à ANPD, o Encarregado de Dados preencherá um Formulário de Incidente de Segurança da Informação com Dados Pessoais.

Parágrafo 1º. O Formulário de Incidente de Segurança da Informação com Dados Pessoais a ser utilizado é o disponibilizado pela ANPD, devendo ser baixado diretamente do site[3] da Autoridade Nacional.

Parágrafo 2º. Após preenchido o Formulário e executados os devidos procedimentos, o Encarregado de dados armazenará o Formulário para consultas futuras e para atender a eventuais pedidos lícitos do titular, controlador ou co-controlador envolvidos no incidente ou da ANPD.

Art. 56. Para auxiliar o preenchimento do Formulário, devem ser consultados o Inventario de Dados Pessoais, o Fluxo de Tratamento de Dados Pessoais, a Planilha de Riscos de Privacidade e o Relatório de Impacto à Proteção de Dados Pessoais referentes ao processo de tratamento de dados relacionado ao incidente.

CAPÍTULO V
DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 57. Sempre que o **SESCOOP/SP** mudar a forma de resposta a incidentes de segurança da informação e de privacidade, atualizará este Plano.

---

[2]Peticionamento Eletrônico para Usuário Externo do SEI. Disponível em <https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico>. Acessado em 10/11/2021

[3] Formulário de comunicação de incidentes de segurança com dados pessoais da ANPD, disponível em: <https://www.gov.br/anpd/pt-br/assuntos/atual-formulario-de-comunicacao-de-incidentes-de-seguranca-com-dados-pessoais_01-03-2021-4.docx>. Acessado em 8/11/2021.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Parágrafo 1º. Reservamo-nos o direito de fazer alterações às nossas práticas e a este Plano a qualquer tempo.

Parágrafo 2º. Consulte este Plano frequentemente para verificar quaisquer atualizações ou mudanças.

Art. 58. As dúvidas e casos omissos não abrangidos por esta política serão submetidos para deliberação do Conselho Administrativo do SESCOOP/SP.

Art. 59. Esta Política, entra em vigor, na data de sua aprovação pelo Conselho Administrativo do SESCOOP/SP, podendo ser revista sempre que necessário.

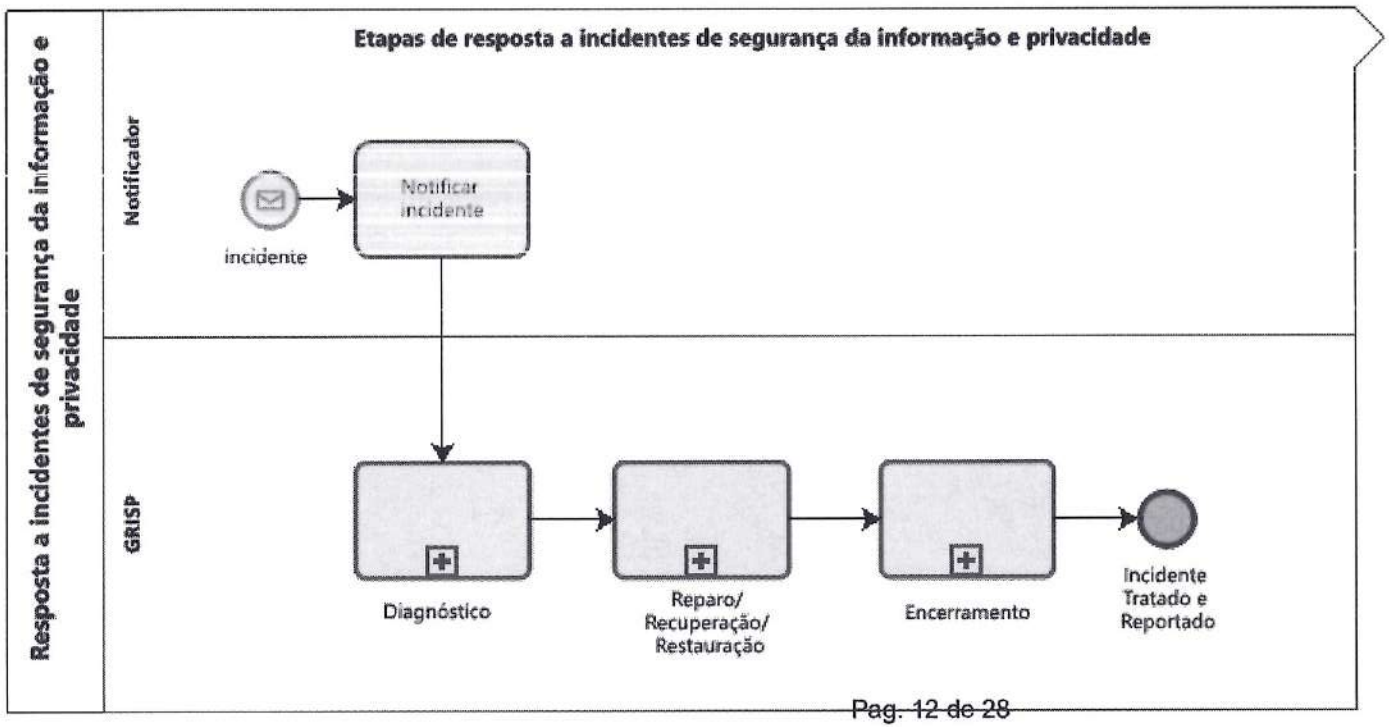
São Paulo, 22 de março de 2022.

EDIVALDO DEL GRANDE
Presidente do Conselho Administrativo do SESCOOP/SP

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO I
PROCESSO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE

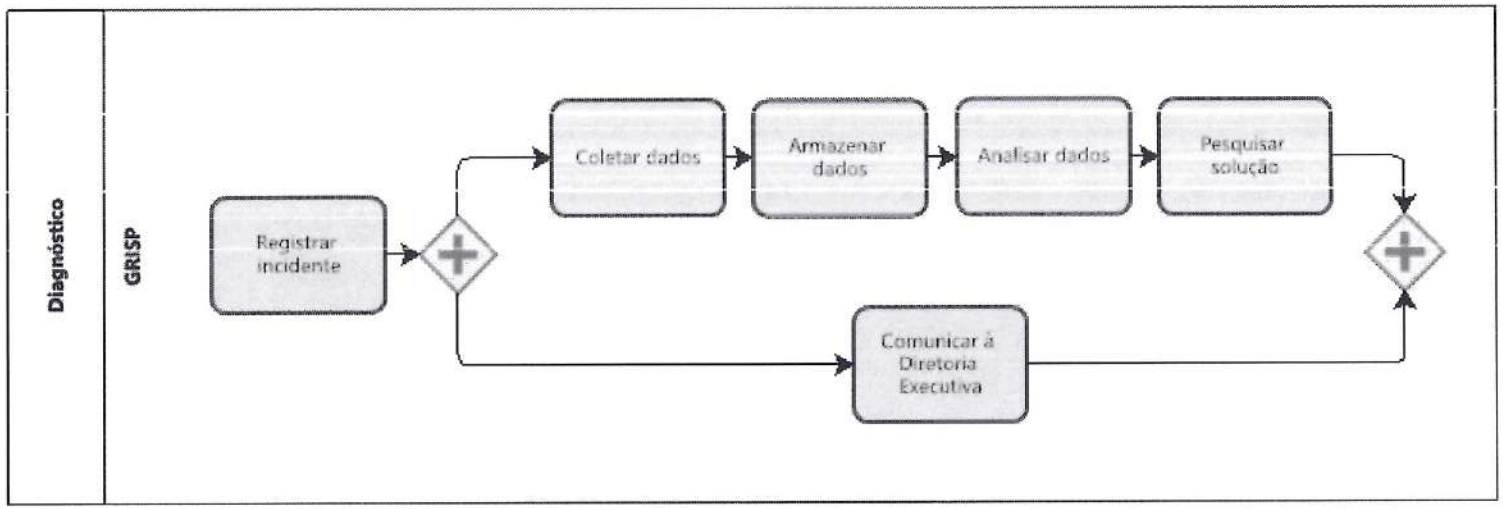
A figura a seguir mostra o Processo de Resposta a Incidentes de Segurança da Informação e de Privacidade. As demais figuras detalham os subprocessos "Diagnóstico", "Reparo/ Recuperação/ Restauração" e "Encerramento".



Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br
sistemaocesp @sistemaocesp Sistema Ocesp

ANEXO I
PROCESSO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE - Continuação

A imagem abaixo detalha o subprocesso "Diagnóstico" do Processo de Resposta a Incidentes de Segurança da Informação e de Privacidade.

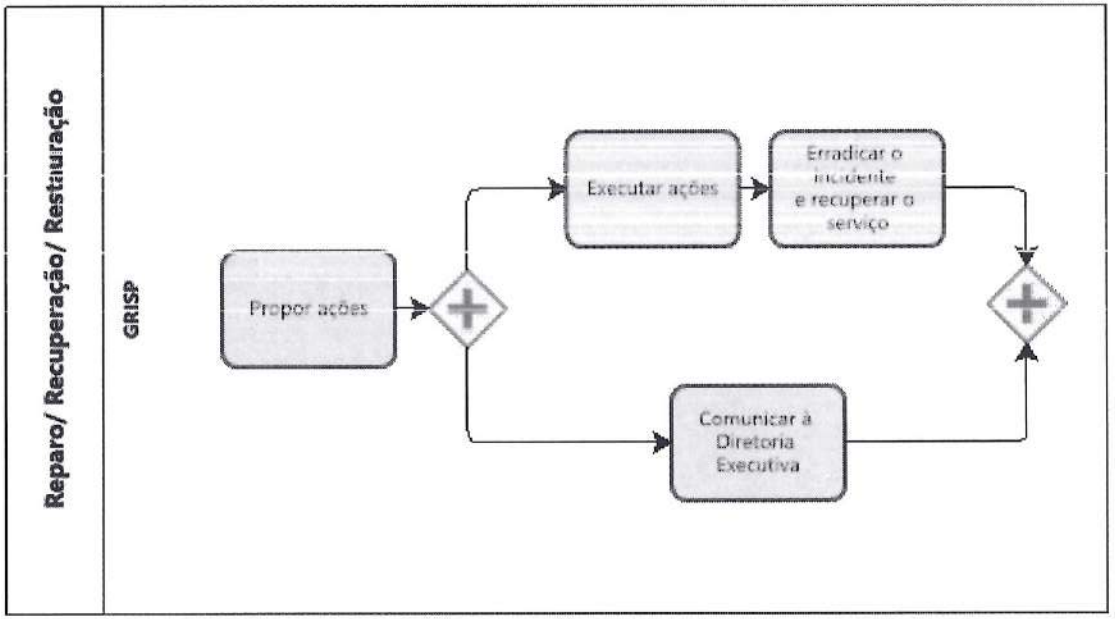


Powered by bizagi Modeler

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br
sistemaocesp @sistemaocesp Sistema Ocesp

ANEXO I
PROCESSO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE - Continuação

A imagem a seguir detalha o subprocesso "Reparo/ Recuperação/ Restauração" do Processo de Resposta a Incidentes de Segurança da Informação e de Privacidade.

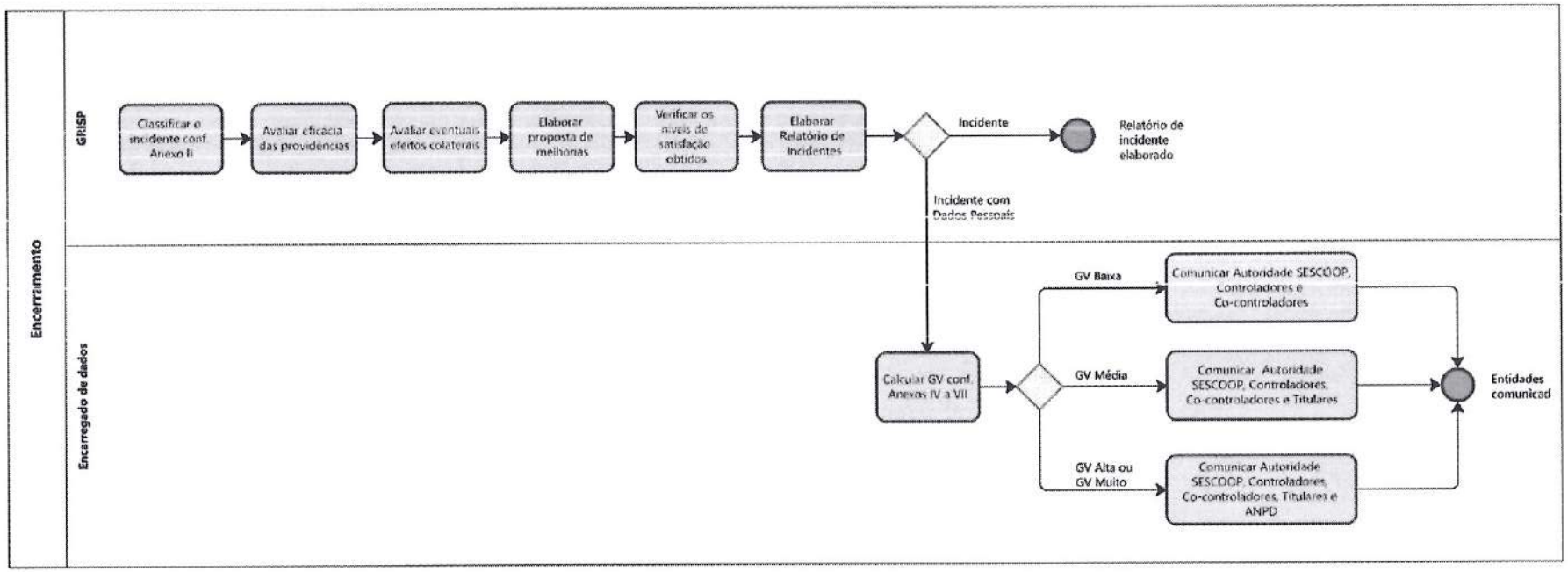


Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO I

PROCESSO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE - Continuação

A imagem a seguir detalha o subprocesso "Encerramento" do Processo de Resposta a Incidentes de Segurança da Informação e de Privacidade.



Powered by Bizagi Modeler

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO II
ESQUEMA DE CLASSIFICAÇÃO DOS INCIDENTES DE SEGURANÇA E DE PRIVACIDADE

Classe do Incidente	Tipo do Incidente	Descrição / Exemplos
Conteúdo Abusivo	*Spam*	Mensagens de e-mail em massa, não solicitadas pelo destinatário, enviadas em grande quantidade.
	Assédio	Desacreditar ou discriminar alguém, perseguição virtual.
	Pornografia, pornografia infantil, violência	Conteúdo sexual, apologia à violência.
Código Malicioso	Vírus	*Software* incluído ou inserido intencionalmente em um sistema com finalidade prejudicial. Normalmente é necessária a interação do usuário para ativar o código.
	Worm	
	Trojan	
	Spyware	
	Dialler	
Coleta de Informações	*Scanning*	Ataque que envia requisições para um sistema com a finalidade de descobrir vulnerabilidades. Exemplos: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, etc.).
	Sniffing	Observação e gravação de tráfego de rede.
	Engenharia social	Coleta de informações junto a usuários de forma não técnica (mentiras, truques, suborno ou ameaças etc.).
Tentativas de Intrusão	Exploração de vulnerabilidades conhecidas	Tentativa de comprometer um sistema ou serviço explorando vulnerabilidades identificadas e normalizadas como um nome CVE (*buffer overflow, backdoors, cross site scripting* etc.).
	Tentativas de *login*	Múltiplas tentativas de *logins* (adivinhando ou quebrando senhas, força bruta)
	Novas assinaturas de ataque	Uma tentativa usando um método desconhecido.
Intrusão	Conta privilegiada comprometida	Comprometimento de um sistema, serviço ou aplicação que pode ter

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Classe do Incidente	Tipo do Incidente	Descrição / Exemplos
Segurança da Informação	Acesso não autorizado à informação	A segurança da informação pode ser ameaçada por uma conta de usuário válida ou aplicação comprometida que permitam acesso não autorizado à informação. Há, ainda, ataques que interceptam e acessam informações durante a transmissão dos dados pela rede.
	Modificação não autorizada à informação	
Fraude	Uso não autorizado de recursos	Uso de recursos para propósitos não autorizados, como uso de e-mail para correntes ou pirâmides.
	Direitos autorais	Venda ou instalação de *software* comercial não licenciado ou material protegido por direitos autorais.
	Mascarado	Tipo de ataque no qual uma entidade assume ilegalmente a identidade de outra para tirar benefícios.
Outros	Incidente não categorizado	Todos os incidentes não categorizados em um dos tipos anteriores devem ser classificados nesta classe. Quando o número de incidentes nesta categoria aumentar, será o momento de rever esta tabela de classificações.

Classe do Incidente	Tipo do Incidente	Descrição / Exemplos
	Conta não privilegiada comprometida	acontecido remotamente ou localmente por meio de acesso não autorizado.
	Aplicação comprometida	
Disponibilidade	DoS	Neste tipo de ataque o sistema é bombardeado com grande quantidade de requisições, a ponto apresentar atrasos nas respostas ou parar completamente de responder.
	DDoS	
	Sabotagem	

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO III
MODELO PARA O RELATÓRIO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE

1. Introdução

(Contextualizar o incidente ocorrido, especialmente nas fases de Ocorrência e Detecção, incluindo: data e hora da detecção, data e hora do incidente e sua duração, resumo do incidente de segurança e se incluiu dados pessoais, com indicação da localização física e meio de armazenamento).

2. Análise de impacto

(Possíveis consequências e efeitos negativos do incidente para o negócio e, em caso de incluir dados pessoais, para os titulares dos dados afetados).

3. Informações levantadas

(Quais informações foram analisadas, descrever o que foi verificado e quais as impropriedades encontradas).

4. Escopo do incidente

(Elencar os sistemas, aplicações, dados, serviços, equipamentos afetados pelo incidente).

5. Classificação do incidente

5.1. Classe do incidente: (verificar a coluna respectiva na tabela do **ANEXO II**).

5.2. Tipo do Incidente: (verificar a coluna respectiva na tabela do **ANEXO II**).

6. Ações realizadas para solução

(Listar as ações realizadas nas fases de Diagnóstico, Reparo, Recuperação, Restauração e Encerramento).

7. Problemas e dificuldades encontrados

(Listar os problemas e as dificuldades encontradas durante a realização de ações nas fases de Diagnóstico, Reparo, Recuperação, Restauração e Encerramento).

8. Sugestão de melhoria do ambiente de TI para prevenção de eventos similares ao ocorrido

(Descrever as novas medidas a serem adotadas par evitar que incidentes semelhantes voltem a ocorrer).

9. Avaliação da Gravidade da Violação (GV)

GV = CP x FI + CV, onde:

CP = A (trocar pelo valor adequado de acordo com a tabela do ANEXO IV)

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

FI = B (trocar pelo valor adequado de acordo com a tabela do **ANEXO V**)
CV = C (trocar pelo valor adequado de acordo com a tabela do **ANEXO VI**)

Logo:
GV = A x B + C
GV = X (resultado do cálculo)

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO III
MODELO PARA O RELATÓRIO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE - Continuação

De acordo com o valor de GV, a ação recomendada é:
(Manter somente o item abaixo adequado, em acordo com o valor de GV)
Se **GV** < 2, ou seja, se a gravidade de violação for "**Baixa**", o Encarregado de dados encaminhará o relatório e a comunicação de incidente com dados pessoais para:

I. As autoridades competentes do **SESCOOP/SP**;

II. Eventuais controladores e co-controladores dos dados pessoais afetados pelo incidente.

Se 2 ≤ **GV** < 3, ou seja, se a gravidade de violação for "**Média**", o Encarregado de dados encaminhará o relatório e a comunicação de incidente com dados pessoais para:

IV. As autoridades competentes do **SESCOOP/SP**;

V. Eventuais controladores e co-controladores dos dados pessoais afetados pelo incidente;

VI. Titular(es) dos dados pessoais afetados pelo incidente.

Se 3 ≤ **GV** < 4, ou seja, se a gravidade de violação for "**Alta**", o Encarregado de dados encaminhará o relatório e a comunicação de incidente com dados pessoais para:

V. As autoridades competentes do **SESCOOP/SP**;

VI. Eventuais controladores e co-controladores dos dados pessoais afetados pelo incidente;

VII. O(s) titular(es) dos dados pessoais afetados pelo incidente;

VIII. A ANPD.

Se **GV** ≥ 4, ou seja, se a gravidade de violação for "**Muito Alta**", o Encarregado de dados encaminhará o relatório e a comunicação de incidente com dados pessoais para:

e) As autoridades competentes do **SESCOOP/SP**;

f) Eventuais controladores e co-controladores dos dados pessoais afetados pelo incidente;

g) Titular(es) dos dados pessoais afetados pelo incidente;

h) ANPD.

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO IV
PONTUAÇÃO PARA O CRITÉRIO CONTEXTO DE PROCESSAMENTO DE DADOS (CP)

Tipo de Dados: Dados simples Por exemplo: dados biográficos, detalhes de contato, nome completo, dados sobre educação, vida familiar, experiência profissional etc.	
Descrição	**Pontuação (CP)**
Pontuação básica: quando a violação envolve "dados simples" e o controlador não tem conhecimento de quaisquer fatores agravantes.	1
A pontuação CP pode ser 2, por exemplo, quando o volume de "dados simples" e / ou as características do controlador são tais que certos perfis do indivíduo podem ser habilitados ou suposições sobre a situação social / financeira do indivíduo podem ser feitas.	2
A pontuação CP pode ser de 3, por exemplo, quando os "dados simples" e / ou as características do controlador podem levar a suposições sobre o estado de saúde do indivíduo, preferências sexuais, crenças políticas ou religiosas.	3
A pontuação CP pode ser 4, por exemplo, quando devido a certas características do indivíduo (por exemplo, grupos vulneráveis, menores), a informação pode ser crítica para sua segurança pessoal ou condições físicas / psicológicas.	4
Tipo de Dados: Dados comportamentais Por exemplo. localização, dados de tráfego, dados sobre preferências e hábitos pessoais etc.	
Descrição	**Pontuação (CP)**
Pontuação básica: quando a violação envolve " dados comportamentais " e o controlador não tem conhecimento de quaisquer fatores agravantes ou atenuantes.	**2**
A pontuação CP pode ser 1, por exemplo, quando a natureza do conjunto de dados não fornece nenhuma visão substancial das informações comportamentais do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes disponíveis publicamente (por exemplo, combinação de informações de pesquisas na web).	1
O escore CP pode ser 3, por exemplo, quando o volume de "dados comportamentais" e / ou as características do controlador permitirem a criação de um perfil do indivíduo, expondo informações detalhadas sobre seu cotidiano e hábitos.	3
A pontuação CP pode ser 4, por exemplo, se um perfil baseado em dados confidenciais de um indivíduo puder ser criado.	4

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO IV
PONTUAÇÃO PARA O CRITÉRIO CONTEXTO DE PROCESSAMENTO DE DADOS (CP) - Continuação

Tipo de Dados: Dados financeiros Qualquer tipo de dados financeiros (por exemplo, receitas, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas etc.). Inclui dados de bem-estar social relacionados a finanças em formação.	
Descrição	**Pontuação (CP)**
Pontuação básica: quando a violação envolve "dados financeiros" e o controlador não tem conhecimento de quaisquer fatores agravantes ou atenuantes.	3
A pontuação CP pode ser 1, por exemplo, quando a natureza do conjunto de dados não fornece nenhuma visão substancial das informações financeiras do indivíduo (por exemplo, o fato de uma pessoa ser cliente de um determinado banco sem mais detalhes).	1
A pontuação CP pode ser 2, por exemplo, quando o conjunto de dados específico inclui algumas informações financeiras, mas ainda não fornece nenhuma visão significativa da situação / situação financeira do indivíduo (por exemplo, números de contas bancárias simples sem mais detalhes).	2
A pontuação CP pode ser 4, por exemplo, quando devido à natureza e / ou volume do conjunto de dados específico, informações financeiras completas (por exemplo, cartão de crédito) são divulgadas que podem permitir fraude ou um perfil social / financeiro detalhado é criado.	4
Tipo de Dados: Dados sensíveis Qualquer tipo de dados confidenciais (por exemplo, saúde, filiação política, vida sexual)	
Descrição	**Pontuação (CP)**
Pontuação básica: quando a violação envolve "dados sensíveis" e o controlador não está ciente de nenhum fator de redução.	4
A pontuação CP pode ser 1, por exemplo, quando a natureza do conjunto de dados não fornece nenhuma visão substancial das informações comportamentais do indivíduo ou os dados podem ser coletados facilmente (independentemente da violação) por meio de fontes disponíveis publicamente (por exemplo, combinação de informações de pesquisas na web).	1
A pontuação CP pode 2, por exemplo, quando a natureza dos dados pode levar a suposições gerais.	2
A pontuação CP pode ser 3, por exemplo, quando a natureza dos dados pode levar a suposições sobre informações confidenciais.	3

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO V
PONTUAÇÃO PARA O CRITÉRIO CONTEXTO DE FACILIDADE DE IDENTIFICAÇÃO (FI)

Identificador: Endereço de e-mail	
Descrição	**Pontuação (FI)**
(Insignificante) quando o endereço de e-mail não revelar nenhuma outra informação de identificação (por exemplo, nome) e não for usado como endereço principal do indivíduo em sites da internet, fóruns ou redes sociais.	0,25
(Significativo) quando o endereço de e-mail não revela nenhuma outra informação de identificação (por exemplo, nome), mas é usado como endereço principal do indivíduo em sites da internet, fóruns ou redes sociais (pesquisáveis na web).	0,75
(Máximo) quando o endereço de e-mail revela o nome do indivíduo e é utilizado como endereço principal em sites, fóruns ou redes sociais (pesquisáveis na web).	1

Identificador: Nome completo (Primeiro nome, sobrenome)	
Descrição	**Pontuação (FI)**
(Insignificante) quando em toda a população do país muitas pessoas compartilham o mesmo nome completo	0,25
(Limitado) quando em toda a população do país poucas pessoas compartilham o mesmo nome completo.	0,5
(Significativo) quando em toda a população de uma pequena cidade poucas ou nenhuma pessoa compartilha o mesmo nome completo.	0,75
(Máximo) usando também a data de nascimento e o endereço de e-mail.	1

Identificador: Número de telefone / endereço residencial	
Descrição	**Pontuação (FI)**

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

(Insignificante) em toda a população de um país quando o número / endereço não está registrado em um registro disponível ao público.	0,25
(Limitada) em toda a população de uma pequena cidade e o número / endereço não está registrado em um registro disponível publicamente (identificação possível por meio de comunicação).	0,5
(Máximo) em toda a população de um país e o número / endereço está incluído no registro disponível publicamente.	1

Identificador: Foto / Vídeo	
Descrição	**Pontuação (FI)**
(Insignificante) quando a imagem não é nítida ou vaga (por exemplo, filmagem de Câmeras de Segurança de longa distância).	0,25
(Limitada) quando a imagem não é clara ou vaga, mas inclui informações adicionais (por exemplo, arredores que mostram um local específico) que podem levar à identificação do indivíduo.	0,5
(Significativo) quando a imagem é nítida, mas nenhuma outra informação de identificação está ligada a ela.	0,75
(Máximo) quando a imagem é nítida e vinculada a alguma informação adicional (por exemplo, informações sobre a adesão a um grupo específico, endereço residencial etc.).	1

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO V
PONTUAÇÃO PARA O CRITÉRIO CONTEXTO DE FACILIDADE DE IDENTIFICAÇÃO (FI) - Continuação

Identificador: Codificação / Aliases / Iniciais	
Codificação é um número de identificação exclusivo a cada indivíduo, como em um contexto de banco de dados, por exemplo. Aliases, ou apelidos, é uma forma de pseudonimização, quando um identificador exclusivo é substituído por um apelido, por exemplo, quando o nome completo de um indivíduo é substituído por um apelido, como suas iniciais.	
Descrição	**Pontuação (FI)**
(Insignificante) quando o código / pseudônimo não revela e não pode ser vinculado a quaisquer outros dados pessoais sobre o indivíduo, a menos que seja obtido acesso à base de dados de referência.	0,25
(Significativo) quando o pseudônimo revela alguns dados sobre o indivíduo (por exemplo, primeiro nome) e está vinculado a outros dados pessoais (por exemplo, o endereço de e-mail do indivíduo).	0,75
(Máximo) quando o alias revela o nome completo do indivíduo ou os dados do banco de dados de referência também estão disponíveis.	1

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO VI
PONTUAÇÃO PARA O CRITÉRIO CONTEXTO DE CIRCUNSTÂNCIAS DE VIOLAÇÃO (CV)

Circunstância: Perda de confidencialidade	
Descrição	**Pontuação (CV)**
Dados expostos a riscos de confidencialidade sem evidências de que o processamento ilegal ocorreu. Exemplos: • Um arquivo de papel ou laptop que é perdido durante o transporte. • Um equipamento que foi descartado sem destruição dos dados pessoais.	0
Dados descartados para uma série de destinatários conhecidos. Exemplos: • Um e-mail com dados pessoais foi enviado por engano a vários destinatários conhecidos. • Alguns clientes podem acessar contas de outros clientes em um serviço online.	0,25
Dados descartados para um número desconhecido de destinatários. Exemplos: • Os dados são publicados em um quadro de mensagens na Internet. • Os dados são enviados para um site P2P. • • Um funcionário vende um CD-ROM com dados pessoais do cliente. • Um site configurado incorretamente torna publicamente acessível os dados da Internet de usuários internos.	0,5

Circunstância: Perda de integridade	
Descrição	**Pontuação (CV)**
Dados alterados, mas sem qualquer uso incorreto ou ilegal identificado. Exemplo: • Os registros de um banco de dados com dados pessoais foram atualizados incorretamente, mas o original foi obtido antes de qualquer uso dos dados alterados.	0
Dados alterados e possivelmente usados de forma incorreta ou ilegal, mas com possibilidade de recuperação. Exemplos: • Foi alterado o cadastro necessário para a prestação do serviço social online e o indivíduo precisa solicitar o serviço offline. • Um registro que é importante para a precisão do arquivo de um indivíduo em um serviço médico online foi alterado.	0,25
Dados alterados e possivelmente usados de forma incorreta ou ilegal, sem possibilidade de recuperar. Exemplo: • Os exemplos anteriores, mas os dados originais não podem ser recuperados.	0,5

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO VI
PONTUAÇÃO PARA O CRITÉRIO CONTEXTO DE CIRCUNSTÂNCIAS DE VIOLAÇÃO (CV) - Continuação

Circunstância: Perda de disponibilidade	
Descrição	**Pontuação (CV)**
Dados que podem ser recuperados sem qualquer dificuldade. Exemplos: • Uma cópia do arquivo foi perdida, mas outras cópias estão disponíveis. • Um banco de dados que está corrompido, mas que pode ser facilmente reconstruído a partir de outros bancos de dados.	0
Dados com indisponibilidade temporal. Exemplos: • Um banco de dados que está corrompido, mas pode ser reconstruído a partir de outros bancos de dados, embora algum processamento seja necessário. • Um arquivo é perdido, mas as informações podem ser fornecidas novamente pelo indivíduo.	0,25
Dados com indisponibilidade total (os dados não podem ser recuperados do controlador ou dos indivíduos). Exemplo: • Um arquivo ou banco de dados foi perdido.	0,5

Circunstância: Intenção maliciosa	
Descrição	**Pontuação (CV)**
A violação ocorreu devido a uma ação intencional, por exemplo, para causar problemas ao controlador de dados (por exemplo, demonstrar perda de segurança) e / ou para prejudicar os indivíduos. Exemplos: • Um funcionário de uma empresa compartilha intencionalmente dados privados de clientes em um site público de mídia social. • Um funcionário de uma empresa vende dados privados de clientes para outra empresa. • Um membro de uma rede social envia intencionalmente informações sobre outros membros para seus familiares a fim de prejudicá-los.	0,5

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

ANEXO VII
GRAVIDADE DE UMA VIOLAÇÃO DE DADOS

Gravidade de uma violação de dados		
Valor da GV	**Descritor da Gravidade**	**Descrição**
GV < 2	**Baixa**	Os indivíduos não serão afetados ou poderão encontrar alguns inconvenientes, que serão superados sem problemas (tempo gasto para reintroduzir informações, aborrecimentos, irritações etc.).
2 ≤ GV < 3	**Média**	Os indivíduos podem encontrar inconvenientes significativos, que serão capazes de superar apesar de algumas dificuldades (custos extras, recusa de acesso aos serviços comerciais, medo, falta de compreensão, estresse, pequenas doenças físicas etc.).
3 ≤ GV < 4	**Alta**	Os indivíduos podem enfrentar consequências significativas, que devem ser capazes de superar, embora com sérias dificuldades (apropriação indébita de fundos, lista negra de bancos, danos materiais, perda de emprego, intimação, piora da saúde etc.).
GV ≥ 4	**Muito Alta**	Os indivíduos podem encontrar consequências significativas, ou até irreversíveis, que eles não podem superar (dificuldades financeiras, como dívidas substanciais ou incapacidade de trabalhar, doenças físicas ou psicológicas de longo prazo, morte etc.).

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br