DIÁRIO OFICIAL DO ESTADO DE SÃO PAULO
Publicado na Edição de 1 de julho de 2026 | Caderno Executivo | Seção Atos Normativos

DELIBERAÇÃO DIREX Nº 10, DE 23 DE JUNHO DE 2026

DELIBERAÇÃO DIREX Nº 10 DE 23 DE JUNHO DE 2026

Plano de Resposta a Incidentes de Segurança da Informação

DELIBERAÇÃO - DIREX Nº 10/2026

Assunto: Aprova o **Plano de Resposta a Incidentes de Segurança da Informação** da Fundação de Previdência Complementar do Estado de São Paulo – SP-PREVCOM

A **Diretoria Executiva** da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM, em sua **698ª Reunião Ordinária**, realizada em 13 de maio de 2026, por unanimidade, resolve:

Artigo 1º. Fica aprovado **Plano de Resposta a Incidentes de Segurança da Informação** da Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM, na forma do Anexo, que integra esta Deliberação para todos os fins.

Parágrafo único. Nos termos dos itens 2.2 e 2.3 da Política Interna de Elaboração e Gestão de Normativos da Prevcom este documento é classificado internamente como Regulamento.

Artigo 2º. Esta Deliberação entra em vigor na data de sua publicação.

Sumário

1. Introdução

2. Objetivo

3.Referência

4. Abrangência

5. Ciclo de vida de um incidente de segurança

6. Classificação de incidentes

7. Grupo de Resposta a Incidentes (GRI)

8. Acionamento do “Plano de Resposta a Incidentes (PRI)”

9. Atualização do “Plano de Resposta a Incidentes (PRI)”

10. Disposições Finais

11. Glossário

12. Anexos

1. Introdução

1.1. O planejamento de resposta a incidentes é essencial para a compreensão de um incidente, identificação e aquisição correta das evidências, prever e descrever situações de possíveis incidentes de segurança visando a mitigação dos riscos, acionamento da equipe de Segurança da Informação e retorno operacional dentro de um tempo razoável no intuito de garantir a menor perda financeira possível.

1.2. O Plano de Resposta a Incidentes (PRI) é formado pelo mapeamento dos serviços e consequentemente dos ativos críticos para o negócio, o conjunto de respostas aos incidentes de segurança da informação para os serviços críticos, os testes de continuidade a serem executados, o plano de comunicação para acionamento das pessoas corretas durante um incidente e as ações para melhoria contínua do "Plano de Resposta a Incidentes (PRI).

2. Objetivo

2.1. Estabelecer diretrizes e procedimentos para a identificação, registro, análise e resposta a incidentes de segurança da informação no ambiente da PREVCOM, assegurando uma atuação tempestiva, coordenada e eficaz, com o objetivo de minimizar impactos aos processos críticos e à continuidade dos negócios.

2.2. O Plano define os principais riscos e cenários de incidentes, as ações necessárias para sua mitigação, os responsáveis pelo tratamento, os fluxos de comunicação e os processos críticos envolvidos, bem como as atividades necessárias para a contenção, erradicação e recuperação dos serviços afetados.

3. Referência

3.1. O documento foi elaborado com base nas seguintes normas e legislações:

3.2. ISO/IEC 27001 – Sistemas de Gestão da Segurança da Informação;

3.3. ISO/IEC 27002 – Controles de Segurança da Informação;

3.4. ISO/IEC 27035 – Gestão de Incidentes de Segurança da Informação;

3.5. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

3.6. Resolução CD/ANPD nº 15, de 24 de abril de 2024.

4. Abrangência

4.1. Este Plano de Resposta a Incidentes tem como principal cobertura os serviços críticos da PREVCOM, bem como seus processos e ativos de informação necessários à manutenção do ambiente de negócios.

4.2. Os serviços críticos e ativos-chave encontram-se definidos nos documentos institucionais de continuidade, especialmente no Plano de Continuidade de Negócios (PCN).

4.3. Este Plano aplica-se aos empregados, agentes públicos e, quando aplicável, a prestadores de serviço que tratem dados pessoais em nome da PREVCOM.

5. Ciclo de vida de um incidente de segurança

O ciclo de vida de um incidente de segurança é composto por 5 fases:

5.1. Preparação e Planejamento: envolve o treinamento e delimitação dos empregados e das atividades que serão executadas em caso de incidentes.

5.2. Detecção e Registro: envolve a identificação através de monitoramento dos ativos e relato de um incidente.

5.3. Avaliação e Decisão: envolve o detalhamento, decisões sobre como serão tratados.

5.4. Resposta: envolve as atividades realizadas para mitigar os danos causados pelo incidente e a retomada das funcionalidades comprometidas.

5.5. Lições Aprendidas: envolve a coleta de informações relativas ao incidente para aprendizado e sua incorporação nas resoluções de próximos incidentes no intuito de melhoria contínua.

5.5.1. Preparação e Planejamento

5.5.1.1. O Regulamento de Respostas a Incidentes de Segurança da informação deve ser divulgada e publicada, além da necessidade de prover conhecimento aos membros da TI em formato de palestras e aculturamento de segurança de informação no que tange à gestão de resposta a incidentes. Dessa forma, devem ser elaborados dois workshops anuais executivos, táticos e operacionais da área de TI, com o objetivo de:

5.5.1.2. Reciclagem de conhecimento de funcionários atuais

5.5.1.3. Abordagem de novas técnicas de mercado e boas práticas

5.5.1.4. Inovação tecnológica e novos ferramentais de segurança de informação

5.5.1.5. Inclusão de novos funcionários no ciclo de gestão de resposta a incidentes

5.5.1.6. Adicionalmente, deverão ser observadas as diretrizes de gestão de pessoas relacionadas à segurança da informação, incluindo:

5.5.1.7. Verificação de antecedentes, quando aplicável, conforme normativos internos;

5.5.1.8. Revisão periódica de acessos;

5.5.1.9. Cancelamento automático nos casos previstos conforme normativos;

5.5.2. Detecção e Registro

5.5.2.1. Através dos recursos disponíveis para detecção de incidentes, seja no monitoramento da rede, dos ativos ou problemas relatados por usuários, devem ser relatados à equipe de resposta a incidentes para análise e tomada das ações necessárias para o tratamento do incidente e encaminhamento do problema para os gestores.

5.5.2.2. Tipos de eventos considerados incidentes de segurança:

5.5.2.3. Violação da disponibilidade de equipamentos, confidencialidade e integridade das informações e de dados pessoais e dados pessoais sensíveis;

5.5.2.4. Inconformidade das políticas, Regulamentos e procedimentos de segurança;

5.5.2.5. Alterações de sistema não autorizadas e sem controle;

5.5.2.6. Funcionamento indevido de hardwares, software ou software desconhecido nos equipamentos;

5.5.2.7. Violação de acesso digital.

5.5.2.8. Registro de Evento de Segurança da Informação e Manutenção do Histórico:

5.5.2.9. Todos os eventos devem ser analisados mesmo que sejam apenas suspeitos. Após a validação do evento, ele deverá ser registrado, assim como todas as informações necessárias para que sirvam como um banco de dados de conhecimento para consultas futuras. Para todos os incidentes devem ser registrados:

5.5.2.10. Nome da pessoa que identificou;

5.5.2.11. Data e hora da identificação;

5.5.2.12. Tipo do evento;

5.5.2.13. Descrição;

5.5.2.14. Ativos afetados conhecidos;

5.5.2.15. Coletar, Documentar e Preservar Evidências de Eventos de SI:

5.5.2.16. A coleta de evidências deve ser a mais cautelosa e cuidadosa possível para que não haja alterações ou fraudes em seus resultados, para isso é sempre importante verificar o horário da coleta com o horário do sistema e confrontar com o horário de registro do log para que se tenha a hora exata do fato de coleta.

5.5.2.17. Responsabilidades no tratamento de incidentes

5.5.2.18. A gestão de incidentes de segurança da informação deverá observar as responsabilidades definidas ao longo de seu ciclo de vida, conforme descrito a seguir:

5.5.2.18.1. Preparação e Planejamento

5.5.2.19. Compete à Diretoria de Tecnologia da Informação, em conjunto com a área de Gestão de Riscos, Controles Internos e Conformidade:

5.5.2.20. estabelecer diretrizes, procedimentos e fluxos de resposta a incidentes;

5.5.2.21. promover ações de capacitação e conscientização dos empregados;

5.5.2.22. definir os papéis e responsabilidades das áreas envolvidas;

5.5.2.23. manter atualizados os instrumentos, modelos e registros necessários à gestão de incidentes.

5.5.2.23.1. Detecção e Registro

5.5.2.23.2. Qualquer agente público que identificar ou suspeitar de um incidente de segurança da informação deverá reportá-lo imediatamente à área de Tecnologia da Informação;

5.5.2.23.3. Compete à Diretoria de Tecnologia da Informação realizar o registro formal do incidente, incluindo sua classificação preliminar, consolidação das informações e abertura de chamado ou registro em ferramenta específica;

5.5.2.23.4. As áreas responsáveis pelos ativos de informação deverão apoiar na coleta de evidências e informações necessárias.

5.5.2.24. Avaliação e Decisão

5.5.2.25. Compete à área de Tecnologia da Informação realizar a análise inicial do incidente, incluindo sua classificação quanto à criticidade e impacto;

5.5.2.26. Nos casos de maior criticidade, a avaliação e decisão deverão ser submetidas ao Grupo de Resposta a Incidentes (GRI), que poderá deliberar sobre o acionamento do PRI e as diretrizes de tratamento;

5.5.2.27. A Assessoria Jurídica e o Encarregado de Dados (DPO) deverão ser acionados nos casos que envolvam riscos legais ou incidentes com dados pessoais.

5.5.2.28. Resposta

5.5.2.29. Compete às áreas técnicas responsáveis pelos ativos afetados executar as ações de contenção, erradicação e recuperação, sob coordenação da área de Tecnologia da Informação;

5.5.2.30. O Grupo de Resposta a Incidentes (GRI), quando acionado, deverá orientar a priorização das ações e deliberar sobre medidas adicionais;

5.5.2.31. A comunicação institucional e, quando aplicável, externa, deverá ser realizada com o apoio da área de Comunicação/Relacionamento Institucional, com validação da Assessoria Jurídica e do Encarregado de Dados (DPO).

5.5.2.32. Lições Aprendidas

5.5.2.33. Compete à área de Tecnologia da Informação consolidar o relatório do incidente, incluindo causa raiz, impactos e ações adotadas;

5.5.2.34. As áreas envolvidas deverão contribuir com informações para análise do incidente;

5.5.2.35. Compete à área de Tecnologia da Informação, em conjunto com Gestão de Riscos, promover a incorporação das lições aprendidas, visando à melhoria contínua dos controles, processos e do próprio Plano de Resposta a Incidentes.

5.5.3. Avaliação e Decisão

5.5.3.1. Os eventos de segurança devem ser triados em pelo menos 5 situações, são elas:

5.5.3.2. Eventos que causam degradação de performance;

5.5.3.3. Eventos que causam indisponibilidade;

5.5.3.4. Eventos que causam adulteração ou fraude;

5.5.3.5. Eventos que causam destruição de ativos ou documentos;

5.5.3.6. Eventos que causam vazamento de dados pessoais.

5.5.3.7. Os incidentes devem ser registrados e catalogados, os relatórios de incidentes devem ter um modelo definido e publicados para o Grupo de Resposta a Incidentes (GRI) e diretoria administrativa. Caso mais de um ativo tenha sido envolvido no incidente, é nessa fase que devem ser definidas a ordem de Prioridade de resposta.

5.5.3.8. Além de sua comunicação, os incidentes devem ser analisados e elaborados planos de ação para que não haja recorrência, e assim aumentar a resiliência dos negócios da PREVCOM.

5.5.4. Resposta

5.5.4.1. Esta fase é executada imediatamente após a confirmação de um incidente. O objetivo é controlar o incidente, eliminar sua causa e restaurar os serviços afetados, com o mínimo impacto possível.

5.5.4.2. Contenção

5.5.4.3. A contenção busca impedir que o incidente se espalhe ou cause mais danos antes da resolução definitiva.

5.5.4.4. Ações:

5.5.4.5. Isolamento de sistemas afetados (retirar da rede ou desconectar da internet).

5.5.4.6. Bloqueio de contas ou credenciais comprometidas.

5.5.4.7. Interrupção temporária de serviços impactados (por segurança).

5.5.4.8. Alteração de permissões de acesso de usuários ou serviços.

5.5.4.9. Criação de backups de evidências (para forense e auditoria).

5.5.4.10. Redirecionamento de tráfego ou uso de ambientes de contingência.

5.5.4.11. Comunicação de Incidentes de Segurança da Informação

5.5.4.12. Os comunicados dos incidentes de segurança de informação devem conter informações claras sobre o serviço / processo que foi afetado e qual o impacto causado, além da previsão do retorno e ações previstas.

5.5.4.13. Encerramento de Incidentes de Segurança da Informação

5.5.4.14. Após retornado à normalidade, devem-se registrar os eventos e ações relacionados ao incidente, dessa forma catalogados e entregues ao Grupo de Resposta a Incidentes (GRI) para a elaboração de planos de ações e investimentos para evitar novos problemas.

5.5.4.15. Identificação de Exposição de Dados

5.5.4.16. Utilizar os registros de auditoria dos sistemas para identificar possíveis exposições de dados e preparar as medidas cabíveis, incluindo comunicados e estabelecimento de questões jurídicas necessárias.

5.5.4.17. Notificação de Partes Interessadas

5.5.4.18. A comunicação da ocorrência de um incidente deve ser realizada quando gerar riscos ou danos relevantes aos envolvidos, em especial aos Titulares dos Dados em caso de um incidente de dados pessoais. Entre as partes que devem ser notificadas estão fornecedores, clientes, participantes, patrocinadores, autoridades (Ministério Público, Procon, ANPD).

5.5.4.19. Em situações que envolvam dados pessoais, a LGPD dispõe no seu artigo 48 sobre a obrigação do controlador de comunicar a autoridade nacional e o titular dos dados sobre a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares. Essa comunicação deve ser feita em prazo razoável, o qual é recomendado pela Autoridade Nacional de Proteção de dados (ANPD) que seja de até 3 (três) dias úteis.

5.5.4.20. Para que essa comunicação seja realizada tempestivamente, o Grupo de Resposta a Incidentes (GRI) de crises irá desenvolver modelos de comunicação que deverão ser elaborados e validados pelo membro do Departamento de Marketing e o Encarregado de Dados.

5.5.4.21. Descarte seguro de mídias e ativos de informação

O descarte de mídias e ativos de informação deverá ser realizado de forma segura, observando diretrizes que garantam a impossibilidade de recuperação dos dados.

5.5.4.21.1. Devem ser adotadas práticas como:

5.5.4.21.2. destruição física de mídias;

5.5.4.21.3. sanitização de dados;

5.5.4.21.4. descarte por empresas especializadas, quando aplicável;

5.5.4.21.5. registro do descarte realizado.

5.5.4.21.6. Essas medidas visam mitigar riscos de vazamento ou exposição indevida de informações.

5.5.5. Lições Aprendidas

5.5.5.1. Relatório forense

5.5.5.2. Após investigação da causa raiz, exposição de dados e possíveis vazamentos, deve ser consolidado o relatório forense, contendo toda a cadeia de causalidade do incidente, quando for possível, ou justificativa quando não for possível. Esse relatório permite a prevenção de incidentes que tenham a mesma origem e deve conter, no mínimo:

5.5.5.3. Atividades de investigação executadas;

5.5.5.4. Artefatos coletados e seus hashes (cadeia de custódia);

5.5.5.5. Timestamps dos eventos encontrados; e

5.5.5.6. Causa raiz e vetor de ataque.

5.5.5.7. Transformação de Experiência em Estratégia

5.5.5.7.1. Após todo o processo deve-se ter como análise todo a massa de dados gerada de forma a gerar uma estratégia de TI em relação a investimentos e posicionamentos para manter a continuidade de negócios.

6. Classificação de incidentes

6.1. Os incidentes devem ser classificados de acordo com os impactos em funcionalidade, informação e recuperabilidade. O cálculo final da severidade do incidente, que vai definir a ordem de Priorização dos incidentes, pode ser realizado através da seguinte equação:

6.2. S=If+Ii+Ir

6.2.1. Sendo:

6.2.2. S = Severidade (varia de 1 a 10)

6.2.3. If = Impacto em funcionalidade

6.2.4. Ii = Impacto em informação

6.2.5. Ir = Impacto em recuperabilidade

6.3. Impacto em funcionalidade: envolvem os impactos na funcionalidade de sistemas de negócio, que resultam em experiência negativa aos usuários.

6.3.1. Seus níveis são:

NÍVEL DE IMPACTO	PONTUAÇÃO	DESCRIÇÃO
Nenhum	0,0	Não há efeito na disponibilização dos serviços de negócio.
Baixo	1,0	Efeito mínimo na disponibilização dos serviços de negócio. Ainda é possível fornecer serviços críticos, mas com menos eficiência.

Médio	2,0	Efeito médio na disponibilização dos serviços de negócio. Não é possível fornecer serviços críticos a um grupo de usuários.
Alto	3,0	Efeito máximo. Não é possível fornecer serviços críticos para nenhum usuário.

6.4.1. Seus níveis são:

NÍVEL DE IMPACTO	PONTUAÇÃO	DESCRIÇÃO
Nenhum	0,0	Nenhuma informação foi extraviada, modificada, excluída ou comprometida de outra forma.
Perda de integridade	1,0	Informação foi alterada ou excluída.
Violação de propriedade	2,0	Informações proprietárias, como dados protegidos de infraestrutura da organização, foram acessadas ou exfiltrados.
Violação de Privacidade	3,0	Dados pessoais (sensíveis ou não) de clientes, funcionários ou cooperados foram acessados ou exfiltrados.

6.5. Impacto em recuperabilidade: envolvem o tamanho do incidente e os tipos de recursos que isso afeta, resultando na variação do tempo gasto para recuperação.

6.5.1. Seus níveis são:

NÍVEL DE IMPACTO	PONTUAÇÃO	DESCRIÇÃO
Regular	1,0	Tempo para recuperação é previsível com os recursos existentes.
Suplementada	2,0	Tempo de recuperação é previsível com recursos adicionais.
Estendida	3,0	Tempo de recuperação é imprevisível e ajuda externa é necessária.
Irrecuperável	4,0	Não é possível se recuperar do incidente (ex: dados sensíveis exfiltrados e publicados)

6.6. A nota final de severidade define a criticidade do incidente como um todo, sendo:

6.6.1. · $1 \leq S < 3$: Criticidade baixa.

6.6.2. · $3 \leq S < 6$: Criticidade média.

6.6.3. · $6 \leq S < 8$: Criticidade alta.

6.6.4. · $8 \leq S \leq 10$: Criticidade muito alta.

6.7. Todos os incidentes classificados devem ser registrados para efeitos de aprendizado e melhoria contínua.

6.8. Para fins de controle, rastreabilidade e melhoria contínua, deverá ser mantido registro de incidentes de segurança da informação, contendo, no mínimo:

6.9. identificador do incidente;

6.10. data e hora;

6.11. descrição;

6.12. ativos afetados;

6.13. classificação de severidade;

6.14. responsáveis;

6.15. ações adotadas;

6.16. status do incidente.

7. Grupo de Resposta a Incidentes (GRI)

7.1. O Grupo de Resposta a Incidentes (GRI) consiste em uma instância de coordenação não permanente, acionada conforme a criticidade do incidente, com a finalidade de avaliar, deliberar e direcionar as ações necessárias para resposta a incidentes de segurança da informação.

7.2. O GRI será composto por representantes das áreas impactadas, podendo incluir, conforme a natureza do incidente:

7.3. Diretoria de Tecnologia da Informação;

7.4. Diretoria Administrativa;

7.5. Diretoria de Seguridade;

7.6. Diretoria de Investimentos;

7.7. Diretoria Comunicação/Relacionamento Institucional.

7.8. Assessoria Jurídica;

7.9. Encarregado de Dados (DPO);

7.10. A convocação do GRI será realizada pela área de Tecnologia da Informação, ou por outro responsável designado, sempre que houver acionamento do Plano de Resposta a Incidentes (PRI).

7.11. O GRI poderá se reunir de forma presencial ou remota, com o objetivo de:

7.12. Avaliar a criticidade e os impactos do incidente;

7.13. Deliberar sobre o acionamento do PRI;

7.14. Definir as diretrizes de resposta e priorização das ações;

7.15. Autorizar comunicações institucionais e externas, quando aplicável.

7.16. O Grupo de Resposta a Incidentes (GRI) deve se reunir e tomar decisões quando o gatilho de crise for acionado. A reunião pode ocorrer à distância, ou seja, pode ser por telefone ou conferência, não necessitando ocorrer presencialmente. Como qualquer acionamento do “Plano de Resposta a Incidentes (PRI)" deverá gerar custos importantes para a PREVCOM, foram definidos “gatilhos” na seção “Acionamento do “Plano de Resposta a Incidentes (PRI)” para limitar e direcionar o acionamento do Grupo de Resposta a Incidentes (GRI).

7.17. Na incidência de um evento que possa requisitar o acionamento do “Plano de Resposta a Incidentes (PRI)”, o Grupo de Resposta a Incidentes (GRI) deverá se reunir e poderá aprovar o acionamento do “Plano de Resposta a Incidentes (PRI)”, realizando inicialmente 3 ações básicas:

7.17.1. Contatar e reunir os profissionais necessários para executar o Plano (seção “Grupos de Execução do PRI”).

7.17.2. Informar o grupo de execução do “Plano de Resposta a Incidentes (PRI)” que o Plano está sendo acionado (“gatilho”), fornecendo o “Plano de Resposta a Incidentes (PRI)” e os procedimentos de recuperação a este grupo.

7.17.3. Indicar ao grupo de execução do “Plano de Resposta a Incidentes (PRI)” quais dos procedimentos deverão ser executados e em qual sequência.

7.18. Grupos de execução do “Plano de Resposta a Incidentes (PRI)”

7.18.1. Avaliar os tipos de crises e eventos é importante para que o Grupo de Resposta a Incidentes (GRI) possa definir as responsabilidades de cada membro do Grupo de Execução do “Plano de Resposta a Incidentes (PRI)”. O grupo pode ser dividido em diferentes equipes, cada uma envolvida com o acionamento de procedimentos de contingência e/ou recuperação distintos. As equipes podem ser também divididas em áreas específicas, por exemplo:

7.19. Equipe de disponibilização ou recuperação de infraestrutura física:

7.19.1. responsável pela disponibilização de um local ou de mais locais de contingência, além de mobiliário, para que os funcionários e demais empregados da Prevcom possam executar as atividades de negócios e fornece os serviços críticos. A equipe de infraestrutura física deverá também indicar ou fornecer os recursos de mobilidade para que as pessoas possam se deslocar ao(s) local(is) de contingência. Os recursos de conectividade com os sistemas da Prevcom no(s) local(is) de contingência devem ser instalados, disponibilizados ou recuperados pela equipe de infraestrutura de TI.

7.20. Equipe de disponibilização ou recuperação de Infraestrutura e

7.20.1. Serviços de TI: responsável pela contingência e/ou recuperação da infraestrutura de TI, correspondente às plataformas de hardware (equipamentos, sistemas operacionais, sistemas de clusterização e virtualização, rede LAN, links WAN, Internet, E-Mail e outros serviços de mensageria e comunicação, dispositivos de segurança, bancos de dados, centrais telefônicas e aparelhos de telefonia etc.

7.21. Equipe de disponibilização ou recuperação de softwares/aplicativos: responsável pela contingência e/ou recuperação de softwares/aplicativos, tanto de uso interno como de clientes da PREVCOM.

7.22. Cabe ao Grupo de Resposta a Incidentes (GRI), no acionamento do “Plano de Resposta a Incidentes (PRI)”(“gatilho”), definir as diferentes equipes do Grupo de Execução do PRI, dependendo do evento que ocorreu e dos serviços críticos que devem ser recuperados.

8. Acionamento do “Plano de Resposta a Incidentes (PRI)”

8.1. No intuito de limitar o acionamento do Grupo de Resposta a Incidentes (GRI), devido ao esforço operacional e orçamento necessário para isso, foram delimitados os eventos críticos que podem ocorrer dentro e fora da PREVCOM, envolvendo ou não o ambiente de TI, para avaliar se o PRI e respectivos procedimentos de recuperação devem ou não ser acionados.

8.2. O Grupo de Resposta a Incidentes (GRI) só será acionado e deverá iniciar o PRI caso pelo menos uma das consequências abaixo ocorra:

8.2.1. Incidentes de Alta Gravidade ou Impacto Crítico

8.2.1.1. Vazamento de grande volume de dados pessoais sensíveis ou estratégicos.

8.2.1.2. Ataques cibernéticos com paralisação de sistemas críticos (ex: sistemas financeiros, operacionais, atendimento).

8.2.1.3. Casos de ransomware com impacto em larga escala, exigência de resgate ou exposição de dados.

8.2.2. Risco à Imagem e Reputação da Organização

8.2.2.1. Exposição pública de incidentes em mídia, redes sociais ou imprensa.

8.2.2.2. Envolvimento da organização em escândalos com repercussão negativa.

8.2.2.3. Notificações ou denúncias recebidas de clientes, fornecedores ou autoridades com repercussão externa.

8.2.3. c) Possibilidade de Multas, Processos ou Penalidades Regulatórias

8.2.3.1. Notificação da ANPD, Tribunal de Contas, PREVIC, TCU, CGU, MP ou outros órgãos de fiscalização.

8.2.3.2. Falhas graves que possam violar leis como LGPD, Lei Anticorrupção ou Marco Civil da Internet.

8.2.3.3. Descumprimento de contratos ou SLAs com impacto jurídico relevante.

8.2.4. d) Afetação Direta à Continuidade de Negócios

8.2.4.1. Paralisação de serviços essenciais por tempo superior ao previsto no Plano de Continuidade de Negócios (PCN).

8.2.4.2. Indisponibilidade de pessoas, instalações ou sistemas sem previsão de retorno.

8.2.4.3. Situações de desastres naturais, pandemias, sabotagem, incêndios ou falhas estruturais.

8.2.4.4. Demais eventos e falhas devem ser tratados pelos processos normais de suporte técnico e operações de infraestrutura e não deverão acionar o “Plano de Resposta a Incidentes (PRI)”, salvo em casos especiais, que poderão ser também objeto de análise do Grupo de Resposta a Incidentes (GRI).

8.2.4.5. As comunicações de incidentes de segurança da informação deverão ser elaboradas pelo Grupo de Resposta a Incidentes garantindo que ela seja objetiva e transparente, zelando pela imagem da PREVCOM.

9. Revisão e Atualização do "Plano de Resposta a Incidentes (PRI)"

9.1. O Plano de resposta a incidentes deverá ser revisado e atualizado frequentemente, para que mantenha sua efetividade. A cada revisão/atualização, o responsável deverá documentar a data em que a revisão foi feita, o responsável pela revisão e um "change log", para facilitar o entendimento das mudanças e prever as eventuais inclusões/alterações a serem inseridas nos próximos testes a serem executados.

9.2. A formalização das alterações poderá ser executada no próprio plano, num capítulo adicional contendo o histórico das versões e revisões, ou num documento à parte, que deverá ser anexado ao plano. É imprescindível que o plano seja atualizado sempre que ocorrer algum incidente, incorporando os aprendizados e desafios do que foi executado.

9.3. Eventos que demandam atualização do plano

9.4. O Plano de Resposta a Incidentes da PREVCOM deverá ser revisado e atualizado sempre que ocorrer uma ou mais das situações abaixo:

9.5. Mudança significativa na infraestrutura de TI (exemplos: troca/upgrade de máquinas com novas tecnologias ou substituição de tecnologia, mudança nas ferramentas de replicação, clusterização, virtualização e/ou backup/restore, mudança nos datacenters, mudança de sistemas operacionais etc.)

9.6. Mudança significativa nos serviços críticos cobertos pelo PRI (por exemplo, caso a Prevcom passe a oferecer um novo produto ou prestar um novo serviço, e este seja considerado um novo serviço/atividade crítica a ser considerada no PRI).

9.7. Mudança significativa nos RTOs – Tempos de Recuperação (por exemplo, caso um dos serviços críticos precise ser recuperado num tempo menor ou maior, devido a mudanças nas criticidades, por novas demandas de um ou mais clientes, por mudanças contratuais, ou mudanças nas diretrizes estratégicas da PREVCOM).

9.8. Depois de decorridos 24 (vinte e quatro) meses da última atualização/revisão do PRI, mesmo que nenhum dos eventos de mudança acima tenha ocorrido, será necessário fazer uma revisão do documento.

10. Disposições Finais

10.1. Este Plano entra em vigor 120 (cento e vinte) dias após sua aprovação, período no qual deverão ser realizadas ações de divulgação, capacitação e adequação dos processos internos.

10.2. Durante o período de vacatio legis, as áreas envolvidas deverão promover o treinamento das equipes, especialmente aquelas que tratam dados pessoais e dados pessoais sensíveis.

11. Glossário

11.1. Hash: valor criptográfico utilizado para garantir integridade de evidências.

11.2. Timestamp: registro temporal de um evento.

11.3. Vetor de ataque: meio utilizado para exploração de vulnerabilidades.

11.4. Causa raiz: origem principal do incidente.

11.5. Exfiltração: extração não autorizada de dados.

11.6. Ransomware: tipo de malware que restringe acesso a dados mediante resgate.

11.7. Clusterização: técnica de alta disponibilidade baseada em agrupamento de sistemas.

12. Anexos

12.1. Os anexos deste Regulamento consistem em modelos referenciais destinados a apoiar o registro, tratamento e comunicação de incidentes de segurança da informação, podendo ser ajustados, adaptados ou substituídos de acordo com as ferramentas, sistemas e aplicações adotados pela PREVCOM.

12.2. Eventuais adequações deverão preservar, no mínimo, as informações essenciais e requisitos estabelecidos neste Regulamento, garantindo a rastreabilidade, padronização e integridade do processo de gestão de incidentes.

ANEXO I – MODELO DE REGISTRO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

1. Identificação do Incidente

• Código do Incidente:

• Data/Hora da Identificação:

• Identificado por (nome/área):

• Forma de identificação:

( ) Monitoramento

( ) Relato de usuário

( ) Auditoria

( ) Outro: _____

2. Descrição do Incidente

• Tipo de incidente:

• Descrição detalhada:

• Ativos afetados:

• Localização (sistema/rede/unidade):

3. Classificação Inicial

• Impacto em funcionalidade: (Baixo / Médio / Alto)

• Impacto em informação: (Baixo / Médio / Alto)

• Impacto em recuperabilidade: (Baixo / Médio / Alto)

• Severidade estimada:

• Envolve dados pessoais? ( ) Sim ( ) Não

• Envolve dados pessoais sensíveis? ( ) Sim ( ) Não

4. Ações Iniciais

• Medidas adotadas:

• Área responsável:

• Data/Hora da ação:

5. Registro e Encaminhamento

• Responsável pelo registro:

• Área responsável pelo tratamento:

• Encaminhado ao GRI? ( ) Sim ( ) Não

• Data do encaminhamento:

6. Status do Incidente

• ( ) Aberto

• ( ) Em tratamento

• ( ) Encerrado

• Data de encerramento:

ANEXO II – MODELO DE RELATÓRIO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

1. Identificação

- Código do Incidente:
- Data de ocorrência:
- Data de detecção:
- Data de encerramento:

2. Resumo Executivo

- Descrição sintética do incidente:
- Impacto geral:
- Áreas afetadas:

3. Detalhamento do Incidente

- Descrição completa:
- Linha do tempo (timeline):
- Sistemas/ativos impactados:

4. Análise Técnica

- Causa raiz:
- Vetor de ataque:
- Vulnerabilidades exploradas:
- Evidências coletadas (hash, logs, etc.):

5. Impactos

- Operacional:
- Financeiro:
- Reputacional:
- Regulatório (LGPD, ANPD, etc.):

6. Ações Executadas

- Contenção:
- Erradicação:
- Recuperação:

7. Comunicação

- Comunicação interna realizada:
- Comunicação externa realizada:
- Notificação à ANPD: ( ) Sim ( ) Não
- Notificação a titulares: ( ) Sim ( ) Não

8. Lições Aprendidas

- Falhas identificadas:
- Oportunidades de melhoria:
- Controles a serem implementados:

9. Plano de Ação

AçãoResponsávelPrazoStatus

10. Aprovação

- Responsável pela elaboração:
- Responsável pela validação:
- Data:

ANEXO III – MODELO DE COMUNICAÇÃO DE INCIDENTE

1. Comunicação Interna

Assunto: Incidente de Segurança da Informação – [Descrição]

Prezados,

Informamos a ocorrência de um incidente de segurança da informação identificado em [data], que afetou [sistemas/processos].

Resumo do incidente:
[Descrição objetiva]

Impacto identificado:
[Impactos operacionais, sistemas afetados]

Medidas adotadas:
[Ações de contenção/mitigação]

Próximos passos:
[Recuperação / monitoramento]

Solicitamos atenção às orientações da área de Tecnologia da Informação e eventuais medidas adicionais.

Atenciosamente,
[Área responsável]

2. Comunicação Externa (Autoridades / Titulares)

Assunto: Comunicação de Incidente de Segurança da Informação

Prezados,

Em atendimento à legislação vigente, informamos a ocorrência de incidente de segurança da informação envolvendo dados pessoais, identificado em [data].

Descrição do incidente:
[Descrição objetiva]

Dados afetados:
[Tipo de dados envolvidos]

Medidas adotadas:
[Ações realizadas pela PREVCOM]

Riscos envolvidos:
[Possíveis impactos aos titulares]

Providências recomendadas (se aplicável):
[Orientações aos titulares]

A PREVCOM permanece à disposição para esclarecimentos adicionais.

Atenciosamente,
Fundação de Previdência Complementar do Estado de São Paulo – PREVCOM
[Contato do DPO / canal oficial]

3. Observações

- A comunicação deverá ser realizada em prazo razoável, preferencialmente em até **3 (três) dias úteis**, conforme regulamentação da ANPD;
- O conteúdo deverá ser validado pela Assessoria Jurídica e pelo Encarregado de Dados (DPO);
  A comunicação externa deve observar critérios de clareza, transparência e proteção da imagem institucional