PLANO DE AÇÃO E RESPOSTAS A INCIDENTES CIBERNÉTICOS

1. Introdução

Este Plano visa atender os requisitos da resolução CMN nº 4.893/21 do Banco Central do Brasil e a Política de Segurança Cibernética da Cogem, e estabelece regras para definição de plano de ação e de resposta a incidentes, estratégias e ações a serem realizadas caso ocorram eventos prejudiciais à organização no Ambiente Cibernético.

2. Objetivos

Este plano tem como principais objetivos:

- Orientar a equipe Cogem nas respostas aos incidentes que envolvam os ativos de Tecnologia da Informação (TI) da Cooperativa, de forma documentada, formalizada, rápida e confiável, protegendo as evidências que possam ajudar a prevenir novos incidentes; e
- Dar transparência ao fluxo de procedimentos adequados e os responsáveis, no caso de incidentes.

É importante salientar que este Plano não aborda tipos específicos de incidentes, mas sim estabelece etapas, com comunicação, funções e notificações necessárias para responder a qualquer incidente de segurança de informação envolvendo os ativos de TI da Cooperativa.

3. Termos e definições

Para facilitar o entendimento na compreensão deste Plano de Resposta a Incidentes de Segurança são adotadas as seguintes definições:

- **Ativo:** É tudo aquilo que tenha valor, envolva recursos ou esteja relacionado com a imagem da Cogem em meio digital, neste caso, são considerados ativos os equipamentos, os sistemas, redes e as informações que são tratadas nesses ambientes.
- **Agentes de tratamento**: Corresponde ao Controlador e Operador em conjunto.
- **Anonimização**: É a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- **Ataque**: Evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível.
- **Autoridade Nacional de Proteção de Dados (ANPD)**: É o órgão da administração pública nacional responsável por fiscalizar e zelar pelo

cumprimento da Lei Geral de Proteção de Dados (LGPD) em todo o território brasileiro.

- **Bot**: Código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda.
- **Comunicar**: Refere-se à troca de informações de forma geral, abrangendo uma variedade de situações. Pode ser uma transmissão de informações para informar, relatar ou compartilhar dados com alguém ou um grupo de pessoas. A comunicação pode ser unilateral (de uma parte para outra) ou bilateral (entre duas partes). Pode ou não ser relacionada a eventos ou ações específicas. Se refere ao ato de compartilhar informações sobre incidentes de segurança, políticas de segurança, diretrizes ou qualquer outra informação relevante para a segurança cibernética.
- **Controlador**: É toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais.
- **Dados pessoais sensíveis:** São dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Dados pessoais**: Qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, por conta própria ou quando combinada com outras informações.
- **Encarregado ou *Data Privacy Officer (DPO)***: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Engenharia social**: Técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados.
- **Gestão de ativos:** Processo que envolve planejar, executar, monitorar e avaliar as atividades relacionadas a segurança dos ativos, considerando os objetivos estratégicos, os riscos, os custos e os benefícios ao longo do ciclo de vida deles.
- **Incidente de segurança com dados pessoais**: De acordo com a 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 de dados pessoais;
- **Incidente de segurança**: Qualquer evento adverso, confirmado ou

sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

- **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 de tempo inferior ao tempo objetivo de recuperação.
- **IP**: Protocolo da Internet (*Internet Protocol*), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet.
- **Log**: Processo de registro de eventos relevantes num sistema computacional.
- **Malware**: É um termo genérico para qualquer tipo de "*malicious software*" "software malicioso" projetado para se infiltrar em dispositivos eletrônicos sem o devido conhecimento do usuário. Existem muitos tipos de malware, e cada um funciona de maneira diferente na busca de seus objetivos.
- **Notificação**: Termo mais específico que implica informar ou dar aviso a alguém sobre algo de importância crítica ou eventos específicos. A notificação é frequentemente usada em situações formais ou quando há a necessidade de alertar alguém ou um grupo sobre um evento ou ação iminente que requer atenção imediata. É frequentemente usado para se referir ao ato de informar as partes interessadas, como autoridades regulatórias, clientes ou partes internas, sobre incidentes de segurança, violações de dados ou outros eventos significativos que exijam ação ou acompanhamento imediato.
- **Operador**: É toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.
- **Ponto Focal**: É o servidor designado pelo titular da Unidade, devidamente cadastrado na TI, que atuará como elo entre a Unidade e a TI.
- **Porta**: Uma porta de conexão está sempre associada a um endereço IP de um *host* e ao tipo de protocolo de transporte utilizado para a comunicação. Exemplo: o servidor de e-mail que executa um serviço de SMTP usa a porta 25 do protocolo TCP.
- **Scripts**: Conjunto de instruções para que uma função seja executada em determinado aplicativo.
- **Sistemas**: *Hardware*, *software*, *network* de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pelo Cogem para dar

suporte na execução de suas atividades.

- ***Sniffing***: Corresponde ao roubo ou interceptação de dados capturando o tráfego de rede usando um *sniffer* (aplicativo destinado a capturar pacotes de rede).
- ***Spam***: Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para muitos colaboradores.
- ***Spyware***: Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
- **Tratamento**: Qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização.
- ***Trojan* (Cavalo de Troia)**: Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.
- **Vazamento de dados**: Qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado.
- **Violação de privacidade**: Qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento.
- **Vírus**: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.
- ***Worm***: Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

4. Responsabilidades

Setores que podem operar no tratamento de incidentes cibernéticos, por ocasião da diversidade, complexidade área afetadas por este na Cogem. Dentre estes podemos citar:

- A TI, como principal atuador sobre os incidentes envolvendo ativos de Tecnologia da Informação (TI) da Cogem.
- O Comitê Gestor de Respostas a Incidentes Cibernéticos (CGIC) que deve atuar junto a TI em caso de incidentes de alta criticidade ou impacto.
    - Integrantes:
        - Wanderson Oliveira

- Emerson Pereira
- Carla Ilinski
- Josimara Lima
- Priscila Oliveira

- O Encarregado de Dados, que deve atuar como canal de comunicação entre a Cogem e a ANPD e os titulares.
- Os Pontos focais ou responsáveis técnicos que devem atuar juntamente com a TI na resposta aos incidentes.
- Os Usuários interno e externos, que devem relatar qualquer incidente de segurança da informação a TI e CGIC.

5. Macro etapas do processo de resposta a incidentes

Para simplificar o processo de lidar com incidentes cibernéticos, este capítulo oferece uma visão geral das principais etapas envolvidas na resposta a esses problemas. Começando pelo isolamento dos sistemas afetados (quando possível), passando pela identificação e classificação do incidente, até investigações mais detalhadas e eventual recuperação de dados, se necessário. Também discutimos a importância de notificar as partes interessadas. Ao entender e seguir essas etapas, a Cogem pode se tornar muito mais capaz de lidar com ameaças cibernéticas, limitando os danos financeiros e protegendo sua reputação diante de possíveis incidentes de segurança.

- **Isolamento e contenção**

Nesta fase inicial, o foco principal é conter o incidente para evitar que ele se espalhe e cause mais danos. Isso pode envolver a desconexão de sistemas comprometidos da rede, a interrupção do tráfego malicioso ou o isolamento da parte afetada para impedir que a ameaça se espalhe para outros sistemas. O isolamento é fundamental para controlar o incidente e limitar sua expansão.

- **Identificação e classificação**

Após a contenção, a equipe de resposta a incidentes precisa identificar e classificar o incidente. Isso significa entender o que exatamente aconteceu e qual é a sua gravidade. Os incidentes podem variar amplamente, desde *malware* comum até violações de dados graves. A classificação ajuda a determinar a resposta apropriada e alocar recursos de maneira eficaz.

- **Investigação**

A investigação é uma etapa mais detalhada para entender a origem, os responsáveis e a extensão do incidente. Isso envolve a análise de registros de atividades, o rastreamento de invasões, a identificação de vulnerabilidades exploradas e a coleta de evidências para entender como o incidente ocorreu. A investigação é essencial para identificar o que deve ser corrigido e como prevenir futuros incidentes.

- **Recuperação de dados**

Se os dados foram comprometidos, a recuperação de dados é crítica. Isso pode envolver a restauração de *backups* válidos e a análise da integridade dos sistemas e dados. O objetivo é restaurar os sistemas afetados ao seu estado normal, garantindo que os dados estejam íntegros.

- **Notificação e relatórios**

Dependendo da gravidade do incidente e das regulamentações aplicáveis, pode ser necessário notificar partes interessadas internas e externas. Isso pode incluir autoridades regulatórias, clientes, parceiros de negócios e até o público, dependendo da natureza do incidente e das obrigações.

6. Processo de resposta a incidentes

Esta seção apresenta as etapas do processo de resposta ao incidente.

6.1. Receber chamado

A primeira etapa envolve receber informações sobre um possível incidente de segurança, pode se notificar incidentes de segurança por email:

Incidentes cibernéticos: emerson.pereira@cogem.com.br

Contatos de comunicação exclusivo para tratamento de dados. Lei (13709/2018) LGPD: tratamentodedados@cogem.com.br

Informar o máximo de informações possíveis sobre o ocorrido:

- **Origem do incidente:** Unidade, setor ou organização à qual o dispositivo ou o processo que originou o incidente pertence;
- **Contato da origem:** E-mail, telefone ou outro contato disponível do informante do incidente;
- **Local onde originou o incidente:** O dispositivo ou serviço que originou o incidente;
- **Recursos utilizados pela origem do incidente:** Especificação do tipo do protocolo (IP, TCP, UDP, etc) e portas, ou procedimentos operacionais, adotados na ação do incidente;
- **Endereço do alvo:** Endereço IP (Ipv4 ou Ipv6) do dispositivo ou

endereço de acesso do serviço que foi o alvo do incidente;

- **Protocolos e portas alvos do incidente:** Especificação do tipo do protocolo (IP, TCP, UDP, etc.) e portas utilizados no destino do incidente;
- **Serviços envolvidos:** Especificação do serviço que foi alvo do incidente (http, ftp, smtp, etc.) e versões de sistemas utilizados;
- **Descrição do incidente:** Breve descrição do incidente, tais como tipo do ataque, motivação aparente, ou outras características relevantes;
- **Logs ou evidências:** Anexação das porções de log, imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente.

6.2. Filtrar/triagem – Classificar

Após o recebimento inicial, os incidentes passam por um processo de triagem e classificação com base em critérios como gravidade, impacto potencial e prioridade. Essa classificação ajuda a equipe a determinar quais incidentes requerem intervenção imediata. As classificações sugeridas neste Plano são:

- **Conteúdo abusivo**: *Spam*, assédio, etc.;
- **Código malicioso**: *Bot*, *worm*, vírus, *trojan*, *spyware*, *scripts*;
- **Prospecção por informações**: Varredura, *sniffing*, engenharia social;
- **Tentativa de intrusão**: Tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;
- **Intrusão**: Acesso lógico indesejável, comprometimento de conta de usuário, de aplicação;
- **Indisponibilidade de serviço ou informação**: Negação de serviço, sabotagem;
- **Segurança da informação**: Acesso não-autorizado à informação, modificação não autorizada da informação;
- **Fraude**: Violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;
- **Outros**: Incidente não categorizado.

6.3. Pesquisar incidente e mitigação

A equipe de TI inicia uma investigação aprofundada para compreender a natureza do incidente, sua origem e sua extensão. Simultaneamente, são aplicadas medidas de mitigação imediatas para conter o incidente. Nesse ponto, a equipe começa a documentar e preparar informações técnicas internas para mitigação e correção, além de material de divulgação externa e para fins de prevenção.

Todas as informações novas relativas ao incidente, bem como as medidas de mitigação, são registradas na base de conhecimento da organização para futuras referências.

6.4. Recuperar informações do incidente na base de conhecimento

A equipe verifica se há informações relevantes sobre incidentes semelhantes na base de conhecimento interna, as quais podem ser usadas para orientar a resposta ao incidente.

6.5. É possível barrar o atacante?

Nesta etapa, a equipe avalia se é viável tomar medidas adicionais para bloquear o atacante, rastrear suas atividades ou impedir o acesso não autorizado aos sistemas ou redes afetadas. Isso pode incluir a implementação de contramedidas técnicas, como o bloqueio de endereços IP, restrições de acesso ou análise forense para identificar a origem do ataque. A eficácia dessas medidas é cuidadosamente avaliada para determinar se é possível conter o atacante e evitar futuros ataques.

6.6. Identificar o responsável ou ponto focal e o serviço afetado

Com base nas informações coletadas sobre o incidente, a equipe procura identificar o responsável técnico ou ponto focal do setor afetado. Se não for possível identificá-los imediatamente, a equipe entra em contato com o administrador do setor e registra a informação na base de conhecimento.

6.7. Avaliar criticidade

Nesta etapa, a equipe avalia a criticidade do incidente com base em seu impacto à instituição, na segurança e nos dados sob custódia da Cogem. Também são considerados fatores como o serviço ou sistema afetado e o potencial prejuízo até que o incidente seja mitigado ou corrigido.

Essa classificação ajuda a garantir que os incidentes de segurança da informação na Cooperativa sejam tratados de acordo com sua gravidade, garantindo uma resposta assertiva e eficaz a cada situação.

A TI pode mudar a classificação do incidente de acordo com a investigação.

6.7.1 Incidente de baixa gravidade

Incidentes classificados como de baixa gravidade geralmente envolvem eventos menores que têm impacto mínimo nas operações da Cooperativa. Esses incidentes são tipicamente de fácil resolução e podem não necessitar de uma investigação aprofundada. Exemplos incluem situações como a presença de malware em um único computador ou um incidente de perda de senha.

6.7.2 Incidente de média gravidade

Incidentes de média gravidade são mais sérios e exigem uma investigação mais aprofundada. Eles têm o potencial de afetar uma parte significativa dos sistemas

ou dados da Cooperativa e representam um risco maior para as operações. Exemplos incluem incidentes como violações de dados que afetaram um banco de dados ou ataques de *phishing* que se espalharam para vários funcionários.

6.7.3 Incidente de alta gravidade

Incidentes de alta gravidade são críticos e têm um impacto significativo nas operações da Cooperativa, na segurança de dados e na integridade dos sistemas. Eles representam uma ameaça séria e exigem ação imediata. Exemplos incluem incidentes como ataques de negação de serviço que derrubam a rede da Cooperativa ou violações de dados em larga escala que expõem informações confidenciais de colaboradores e associados.

6.8. Comunicação de incidentes cibernéticos

Na avaliação da criticidade/gravidade do incidente a TI deverá informar o CGIC para que sejam tomadas decisões sobre o bloqueio ou desativação de serviços. O Encarregado de Dados Pessoais (DPO), o Comitê Gestor a Respostas a Incidentes Cibernéticos (CGIC), as autoridades policiais e o solicitante devem ser informados sobre o incidente, as soluções aplicadas e os possíveis impactos. O responsável, o encarregado e/ou os titulares de dados pessoais são informados das medidas de mitigação aplicadas até o momento.

6.9. Impacto! Filtrar internamente?

Na avaliação da criticidade/gravidade do incidente e nas orientações dos responsáveis (quando aplicável), a TI avalia a necessidade de bloquear o sistema, serviço, rede ou dispositivo afetado, e simultaneamente inicia a fase de comunicação de incidentes cibernéticos.

6.10. Solicitação de bloqueio de equipamentos / Redes

Quando necessário, a equipe de TI pode ser solicitada a bloquear ou isolar sistemas, serviços, redes ou dispositivos afetados para evitar a disseminação do incidente.

6.11. Tratamento do incidente

Nesta fase, os responsáveis pelos sistemas, serviços ou redes em questão devem agir com a máxima agilidade para mitigar e resolver o incidente, além de comunicar à TI sobre o status da resolução e as medidas tomadas. Dependendo da tipologia e gravidade do incidente, a TI pode requerer um relatório detalhado sobre o incidente e suas ações corretivas. A Equipe também pode oferecer suporte durante o tratamento do incidente, caso seja solicitado.

Entre as possíveis medidas adotadas nesse processo, estão o isolamento do servidor afetado para evitar a propagação do incidente, a verificação da integridade do sistema, a recuperação de dados perdidos, a condução de

análises forenses para determinar a origem do incidente, a correção de vulnerabilidades identificadas, a documentação das etapas realizadas, a implementação de monitoramento contínuo para garantir a eficácia da resolução. Cada ação é adaptada de acordo com a gravidade e a natureza específica do incidente.

6.12. Esperar resposta

A equipe aguarda uma resposta do responsável ou ponto focal do sistema ou serviço afetado. O prazo estabelecido deve ser respeitado e, caso não haja resposta dentro desse período, se o sistema, serviço, rede ou dispositivo foi bloqueado, este deve ser mantido, e o incidente deve ser sua criticidade reavaliada.

6.13. Notificação de correção / Mitigação

Caso a equipe receba uma notificação de correção ou mitigação por parte do responsável ou ponto focal, essa informação é registrada e verificada para garantir que as ações adotadas sejam eficazes na resolução do incidente.

6.14. Validar resolução / Mitigação

Com base no relatório fornecido pelo responsável ou ponto focal, a equipe verifica e valida, quando possível, a resolução ou mitigação do incidente. Todas essas informações são registradas no registro do incidente para documentação.

6.15. Incidente resolvido / Mitigado?

Se a validação realizada pela TI confirmar que o incidente foi resolvido, este segue para as fases finais de tratamento. Caso não confirme a resolução, o incidente deve ir passar a fase de Reavaliar Incidente, uma vez que esta pode ter sido alterada pelo tempo de atividade.

6.16. Aguardar prazo de resposta

Esse evento é acionado caso o prazo estipulado para a correção ou mitigação do incidente tenha se esgotado sem uma resposta adequada do responsável ou ponto focal.

6.17. Desbloquear Ips / Redes?

Após a conclusão bem-sucedida da mitigação ou correção, a equipe avalia se é apropriado desbloquear sistemas, serviços, redes ou dispositivos previamente bloqueados. Alguns filtros, como bloqueios permanentes em redes consideradas inseguras ou serviços vulneráveis, podem ser mantidos como parte da estratégia de mitigação.

6.18. Solicitação de desbloqueio de equipamentos / Redes

Quando o incidente foi devidamente mitigado ou corrigido, a equipe de resposta a incidentes solicita que as equipes de TI procedam com o desbloqueio de sistemas, serviços, redes ou dispositivos afetados durante a resposta ao incidente. Existem exceções em que determinados bloqueios são mantidos como parte da estratégia de resolução do incidente.

6.19. Fechar chamado

Quando todo o processo de tratamento do incidente está sendo finalizado, a equipe de resposta a incidentes atualiza e fecha o registro do incidente. Isso inclui a verificação de que todas as informações importantes foram registradas.

7. Incidentes de segurança com dados pessoais

Consta no art. 46 da LGPD que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, e tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução.

No caso de incidentes que envolvam dados pessoais e dados pessoais sensíveis devem ser adotadas as seguintes medidas como fundamentais:

1. Preservar todas as evidências possíveis do incidente.
2. Avaliar internamente o incidente e obter informações iniciais sobre:
   - i o impacto do evento; natureza, categoria e quantidade de titulares de dados pessoais afetados;
   - ii categoria e quantidade de dados afetados,
   - iii consequências do incidente para os titulares e a Cogem,
   - iv criticidade e probabilidade;
3. Comunicar à TI em caso de incidentes na rede computacional.
4. Comunicar a Gerência e a Diretoria a existência do incidente
5. Elaborar documentação com todas as informações coletadas, as ações realizadas para o tratamento efetivo do incidente e as considerações necessárias para promover a melhoria contínua no atendimento, para atualizar o RIPD (Relatório de Impacto à Proteção dos Dados Pessoais).

8. Plano de comunicação

A TI deve entrar em contato com o responsável ou Ponto Focal de um ativo de TI sob suspeita de estar envolvido em um incidente de segurança da informação sempre que houver indícios de que esse ativo possa estar comprometido ou afetado pelo incidente. Isso geralmente ocorre como parte da investigação inicial

do incidente. Durante o contato, a TI deve consultar sua base de conhecimentos e compartilhar informações relevantes sobre o incidente, como sua natureza, sintomas, comportamento do ativo afetado e quaisquer medidas de mitigação ou correção que estejam sendo consideradas. O contato com o responsável ou Ponto Focal deve ser colaborativo, visando a coleta de informações, *insights* e sugestões que podem ajudar na resposta ao incidente.

A comunicação com o Responsável ou Ponto Focal deve ser feita utilizando os meios oficiais de comunicação da Cooperativa, e a Base de Conhecimento da TI deve conter essas informações e ser continuamente atualizada.

A comunicação ao Controlador deve ser feita assim que um incidente de segurança de dados pessoais for detectado ou suspeito. Isso se aplica a todos os incidentes, independentemente da gravidade. O objetivo é permitir que o Controlador tome conhecimento do incidente e, se necessário, tome as medidas apropriadas para lidar com a situação.

A comunicação ao Encarregado deve ser feita sempre que for notificado um incidente de segurança de dados pessoais, confirmado ou sob suspeita. O Encarregado é a pessoa ou função responsável por supervisionar a conformidade com a lei de proteção de dados (LGPD).

A comunicação à ANPD deve ser coordenada pelo Encarregado, conforme previsto pela LGPD. A comunicação à ANPD deve seguir os prazos de 2 (dois) dias úteis. É importante que a comunicação seja clara e completa, fornecendo todas as informações necessárias sobre o incidente.

A comunicação pelo encarregado à ANPD deve responder às seguintes questões:

- Quais informações foram objeto do incidente?
- O titular pode ser vítima de fraude em razão do incidente?
- O incidente foi devidamente comunicado às autoridades?
- O que o titular pode fazer em benefício de sua proteção?
- Onde o titular pode obter mais informações sobre o incidente?

A comunicação à ANPD deve ser efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos. Eventual e comprovada subavaliação dos riscos e danos por parte do Controlador pode ser considerada descumprimento da legislação de proteção de dados pessoais.

A decisão de notificar a polícia sobre um incidente de segurança da informação depende da natureza e gravidade do incidente, bem como das leis e regulamentos locais. A notificação à polícia é considerada quando o incidente envolve atividades criminosas, como invasões, ataques cibernéticos graves, roubos de informações confidenciais ou outras atividades ilegais. Incidentes com o potencial de causar danos substanciais ou que já causaram danos significativos geralmente justificam a notificação às autoridades policiais.

É importante considerar a conformidade com as leis locais, regionais e nacionais que regulamentam a segurança da informação e a proteção de dados. Além disso, a presença de evidências sólidas que podem ser utilizadas na investigação

criminal pode influenciar a decisão de notificar a polícia. As políticas internas da Cogem podem conter orientações específicas sobre quando notificar a polícia, mas, em muitos casos, é aconselhável buscar orientação de um departamento jurídico ou advogado especializado em segurança da informação para determinar as obrigações legais e melhores práticas relacionadas à notificação à polícia. A decisão de notificar a polícia sobre um incidente de segurança deve ser tomada pelo CGIC.

A notificação ao solicitante ou denunciante de um incidente de segurança da informação ocorre quando a TI determinar a natureza e a gravidade do incidente. A notificação deve ser conduzida de maneira sensível, clara e transparente, fornecendo informações relevantes sobre o incidente e as medidas tomadas para mitigá-lo. Isso ajuda a construir a confiança com o solicitante ou denunciante e a manter a transparência no processo de resposta ao incidente.

9. Elaborar a documentação

A documentação de um incidente de segurança da informação é fundamental por várias razões:

- **Registro histórico**: A documentação cria um registro histórico de eventos, ações e descobertas relacionadas ao incidente. Isso é valioso para fins de análise pós-incidente, aprendizado organizacional e investigações futuras.
- **Conformidade Legal**: Muitas regulamentações e leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD), exigem que as organizações documentem e relatem incidentes de segurança de dados. A documentação ajuda a cumprir essas obrigações legais.
- **Resposta eficiente**: A documentação ajuda na coordenação e na resposta eficiente ao incidente. As equipes de resposta têm um registro claro do que aconteceu e das medidas tomadas até o momento.
- **Avaliação de impacto**: A documentação ajuda a avaliar o impacto do incidente, incluindo a extensão das violações de segurança e a exposição de dados sensíveis.
- **Melhoria contínua**: A análise dos documentos de incidentes anteriores pode ajudar a identificar áreas de melhoria na segurança e no plano de resposta a incidentes.

9.1. Etapas da elaboração da documentação

Algumas etapas essenciais para documentar um incidente de segurança da informação:

1. **Registro inicial**: Registre detalhes iniciais do incidente, incluindo data, hora, localização, natureza do incidente e pessoas ou sistemas afetados.
2. **Classificação**: Classifique a gravidade do incidente com base em

critérios predefinidos. Isso ajuda a priorizar a resposta.

3. **Descrição detalhada**: Documente uma descrição detalhada do incidente, incluindo como foi descoberto, quem estava envolvido e quais sistemas ou dados foram afetados.
4. **Evidências**: Colete e preserve evidências relevantes, como logs de sistema, registros de eventos e capturas de tela. Isso é crucial para investigações posteriores.
5. **Ações tomadas**: Registre todas as ações tomadas em resposta ao incidente, como isolamento de sistemas afetados, remoção de malware ou interação com autoridades reguladoras.
6. **Comunicações**: Mantenha registros de todas as comunicações internas e externas relacionadas ao incidente, incluindo notificações a autoridades reguladoras, titulares de dados e ações de relações públicas, se aplicável.
7. **Lições aprendidas**: Após a resolução do incidente, conduza uma revisão para identificar lições aprendidas e oportunidades de melhoria.
8. **Relatórios**: Prepare um relatório de incidente de segurança da informação que inclua todas as informações relevantes. Isso pode ser usado para fins de conformidade e como um recurso de aprendizado.
9. **Armazenamento seguro**: Mantenha a documentação em um local seguro e de fácil acesso, de acordo com as políticas de retenção de registros da organização.
10. **Compartilhamento com as partes interessadas**: Compartilhe informações relevantes com as partes interessadas, como autoridades reguladoras, autoridades legais e departamentos internos relevantes.

9.2. Geração de evidências

A geração de evidências em caso de incidente de segurança da informação é uma etapa crucial do processo de resposta. Ela acontece a partir do momento em que um incidente é detectado até a sua resolução final, garantindo que todas as ações tomadas e informações relevantes sejam devidamente documentadas.

- **Responsáveis pela geração de evidências**: A TI é geralmente responsável por coletar, preservar e documentar evidências. Eles devem seguir procedimentos rigorosos para garantir a integridade e autenticidade das evidências coletadas.
- **Tipos de evidências**: Evidências podem incluir registros de logs de sistemas, registros de rede, capturas de tela, informações de identificação de ativos envolvidos, conversas ou correspondências relevantes, análises forenses de dispositivos afetados e qualquer outro dado que possa esclarecer o incidente.
- **Preservação de evidências**: É vital que as evidências sejam preservadas de maneira adequada para evitar qualquer forma de adulteração. A TI deve adotar práticas de preservação sólidas para

garantir que as evidências permaneçam íntegras e possam ser utilizadas em processos subsequentes, como investigações internas ou procedimentos legais.

- **Documentação de cadeia de custódia**: Cada peça de evidência deve ser cuidadosamente registrada e documentada em uma cadeia de custódia, que rastreia quem teve acesso a ela e quando. Isso é essencial para estabelecer a confiabilidade das evidências em um contexto legal.
- **Entrega de evidências**: Quando apropriado, as evidências coletadas podem ser fornecidas a autoridades legais, terceiros de confiança ou partes interessadas para fins de investigação ou ações legais.
- **Armazenamento seguro**: Evidências devem ser armazenadas de forma segura, garantindo que apenas pessoal autorizado tenha acesso a elas. Isso ajuda a evitar a perda ou alteração acidental das evidências.

A geração adequada de evidências é um componente crítico no tratamento de incidentes de segurança da informação, permitindo que a organização compreenda e responda efetivamente a incidentes, além de apoiar investigações futuras, se necessário.

9.2.1 Anexo I – Registro de incidente de segurança da informação.

Anexo I - Registo de Incidente Segurança da Informação

Registro de Evento Número:			
Empresa/ Unidade / Setor:			
Gestor:			
Reporte feito por: Nome:		Cargo:	
Incidente:			
Título/ Identificação:			
Número / Código de Registro:			
Hora e Data da ocorrência:			
Hora e Data do Reporte:			
Hora e Data da Resolução:			
Descrição detalhada do Incidente:			
Equipamento:			
Descrição:		Endereço IP:	
Equipamento:			
Rede / Departamento:		Obs.:	
Sistema ou Aplicativo / Software:			
Objetivo do Sistema:			
Sistema Operacional:			
Porta / meio de Comunicação (se conhecida):			
Localização Física:			
Caminho do Ataque/ acesso			

usado pelo invasor (se conhecido):	
Evidência captada ou recebida:	
Detalhes adicionais:	
Sistema, Rede ou dispositivo paralisado, prejudicado / atingido:	
Serviço prejudicado ou atingido:	
Terceiro / Parceiro prejudicado ou atingido:	
Anexos/ Descrição se obtidos: Logs, Relatórios, Telas Capturadas, informes ou alertas recebidos, etc.):	
Avaliação do Impacto pelo Gestor do Negócio:	
Avaliação do Impacto pela Área Técnica / T. I.:	
Avaliação do Impacto pelo Responsável por Segurança da Informação:	
Ações Corretivas, impactos e danos detectados:	
Planos de ação para prevenção de reincidência:	

Registro de Alteração			
Data	**Versão**	**Páginas alteradas**	**Informações Relevantes**
Mai/25	1ª	-	• Elaboração do Documento.