RESUMO POLITICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO DA CREDJUST

OBJETIVO

Este normativo estabelece a Política de Segurança Cibernética da **CREDJUST,** bem como os requisitos para a Contratação, Avaliação e gestão de serviços de processamento e armazenamento de dados e de computação em nuvem visando total observância e adequação ao exigido na resolução nº4.893/21 do Banco Central do Brasil.

O principal objetivo desta Política é assegurar a proteção dos ativos de informação da Cooperativa contra ameaças, internas e externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo de nossos negócios.

RAZÕES, AMEAÇAS E RISCOS CIBERNÉTICOS

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das Instituições Financeiras, permitindo assim agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços.

Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições.

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas, hackers individuais, terroristas, colaboradores, competidores, etc), como por exemplo:

- Ganhos financeiros através de roubo, manipulação ou adulteração de informações;
- Obter vantagens competitivas e informações confidenciais de clientes ou Instituições concorrentes;
- Fraudar, sabotar ou expor a Instituição invadida por motivos de vingança, ideias políticas ou socias;
- Praticar o terror e disseminar pânico e caos;
- Enfrentar desafios e/ou ter adoração por hackers famosos.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada organização. As consequências para as instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem

concorrencial, além de riscos operacionais. Os possíveis impactos dependem também da rápida detecção e resposta após a identificação do ataque.

Tanto instituições grandes como menores podem ser impactadas e por esse motivo os ativos incorporados no espaço cibernético, devem ser protegidos e preservados, sendo também essa necessidade um dos motivos da implementação, desta Política.

Entre três ativos cibernéticos estão:

- Softwares, como um programa de computador;
- Conectividades, como acesso a internet, Banco Central e Receita Federal;
- Informações sigilosas dos cooperados;
- Componentes físicos, como servidores, estações de trabalho, notebooks, etc.

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, reguladores de mercado, incluindo o Banco Central através da resolução nº 4.658, já mencionada, tem voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

ÁREA GESTORA DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Responsável: Diretor responsável pela Política de Segurança Cibernética

Atribuições:
- Responsável pela Política de Segurança Cibernética
- Responsável pela execução do Plano de Ação e da resposta a incidentes

O diretor responsável pela Política de Segurança Cibernética pode desempenhar outras funções na Cooperativa desde que não haja conflitos de interesses.

DIRETRIZES

A política de Segurança Cibernética, que está sendo implementada na CREDJUST baseia-se nos seguintes princípios:

- Assegurar a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) observando as regras de sigilo e confidencialidade vigentes;

- Assegurar a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- Assegurar a disponibilidade dos dados e sistemas de informação utilizados na cooperativa (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário).

A implementação desta Política considera as seguintes compatibilidades da Cooperativa:

a) O porte, perfil de risco e o modelo de nossos negócios;
b) A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais;
c) A sensibilidade dos dados e das informações sob responsabilidade da instituição.

Os ambientes, sistemas, computadores e redes da Cooperativa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Caberá a todos os colaboradores conhecer e adotar as disposições desta política e deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas ao exercício de suas atividades.

Conforme Resolução nº 4.658/18, os serviços de computação em nuvem abrangem a disponibilidade da CREDJUST, sob demanda, e de maneira virtual de ao menos um dos seguintes serviços:

a) Processamento e armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a CREDJUST implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos.
b) Implantação ou execução de aplicativos desenvolvidos ou adquiridos pela CREDJUST utilizando recursos computacionais de seus prestadores de serviços.
c) Execução por meio de internet dos aplicativos implantados ou desenvolvidos por prestadores de serviços da CREDJUST, com utilização de recursos computacionais do próprio prestador de serviços contratado pela Cooperativa.

A CREDJUST é responsável pela gestão dos serviços contratados incluindo as seguintes atividades:

a) Análise de informações e de recursos adequados ao monitoramento dos serviços;
b) Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto a prestadores de serviços;

c) Cumprimento da legislação e da regulamentação vigente.

PLANO DE AÇÃO- RESPOSTAS INCIDENTES

IMPLEMENTAÇÃO DA POLÍTICA

Visando a implementação, das práticas da Política de Segurança Cibernética na CREDJUST, está sendo implementado um Plano de Ação e de resposta a incidentes abrangendo o seguinte:

- As ações a serem desenvolvidas para adequar a estrutura organizacional e operacional aos princípios e diretrizes da Política de Segurança Cibernética;
- Os procedimentos, rotinas, controles e tecnologias a serem utilizadas na prevenção e na resposta a incidentes;
- Área responsável pelo registro e controle dos efeitos de incidentes relevantes.

O Plano de Ação e de Resposta a Incidentes será aprovado pelo Diretor responsável pela Política de Cibernética e será revisado no mínimo anualmente.

RELATÓRIO SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

Será emitido anualmente, com data base 31 de dezembro, relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes.

Esse relatório deve contemplar, no mínimo, as seguintes informações:

- A efetividade da implementação das ações relativas à implementação da Política de Segurança Cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório deve ser elaborado até 31 de março do ano seguinte ao da data base devendo será aprovado pelo Diretor responsável pela Segurança Cibernética.

CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

Os prestadores e parceiros de serviços de processamento de dados e armazenamento em nuvem podem representar uma fonte significativa de riscos de cibersegurança.

A computação em nuvem considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações, envolve determinados riscos que são levados em conta pela Cooperativa, demandando assim cuidados proporcionais a esta identificação de ameaças.

COMUNICAÇÃO AO BANCO CENTRAL

A CREDJUST deverá informar previamente ao Banco Central a contratação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem.

Essa comunicação deve ser realizada 60 dias antes da contratação dos serviços e deve conter as seguintes informações:

a) Denominação da empresa a ser contratada;
b) Os serviços relevantes a serem contratados;
c) A indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, nos casos de contratação no exterior.

As alterações contratuais que impliquem modificações das informações devem ser comunicadas ao Banco Central no mínimo 60 dias antes da alteração contratual.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a ser realizada pela CREDJUST, deve observar os seguintes requisitos:

a) A existência de convênio para troca de informações entre o Banco Central e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
b) Assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;
c) Definir, previamente a contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
d) Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio citado nos itens anterior a CREDJUST deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações já mencionadas.

A CREDJUST deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes do Banco Central do Brasil aos dados e às informações.

PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO

MITIGAÇÃO DOS RISCOS

Está sendo estabelecido um conjunto de medidas buscando mitigar os riscos de forma a impedir previamente a ocorrência de um ataque cibernético.

A Cooperativa oferece aos colaboradores uma completa estrutura tecnológica para exercícios das atividades, sendo responsabilidade de cada Colaborador manter e zelar pela integridade dessas ferramentas de trabalho, e por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade (Computador, notebook, acesso à internet, E-mail, etc.).

Equipamentos e computadores disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender os interesses comerciais legítimos da Cooperativa.

A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da Cooperativa depende de autorização do Diretor responsável pela Política de Segurança Cibernética devendo observar os direitos de propriedade intelectual pertinentes, tais como copyright, licenças e patentes.

As mensagens enviadas ou recebidas através do correio eletrônico corporativo (e-mails corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (internet) através de equipamentos da Cooperativa poderão ser monitoradas.

As senhas para os dados contidos em todos os computadores, bem como nos e-mails, devem ser reconhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgado para quaisquer terceiros. O colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não dedem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, Etc.) compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais como: o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdef”, “87456123”, entre outras.

Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

AVALIAÇÃO INICIAL

Avaliar o incidente em conjunto com a Diretoria para verificar se é provável a sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas.

Analisar motivos e consequências imediatas, bem como a gravidade da situação.

DOCUMENTOS A DISPOSIÇÃO DO BANCO CENTRAL

Os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

- Política de Segurança Cibernética;
- Ata de Reunião da Diretoria Executiva da Cooperativa, implementado a Política de Segurança Cibernética;
- Documento relativo ao Plano de Ação e de resposta a incidentes relativos à implementação da Política de Segurança Cibernética;
- Relatório anual sobre a implementação do Plano de ação e de resposta a incidente;
- Documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- Documentação sobre os serviços relevantes de processamento, armazenamento de dados de computação em nuvem prestados no exterior, caso isso ocorra;
- Contratos de Prestação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem;
- Dados, registros e informações relativas aos mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética; do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

1. REGULAMENTAÇÃO ASSOCIADA

Resolução Bacen nº 4.893 de 26 de fevereiro de 2021.

2. AGRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA

O conteúdo desta Política de Segurança Cibernética aplica-se a todos os colaboradores e prestadores de serviços relevantes da CREDJUST, no âmbito de suas atividades, atribuições e responsabilidades.

Está aprovada pela Diretoria a qual está comprometida com a melhoria contínua do disposto neste normativo.

Está sendo comunicada para todos os colaboradores, empresas contratadas de serviços de cibernética, clientes e partes externas relevantes para o necessário cumprimento.

Um resumo da Política de Segurança Cibernética estará sendo divulgado ao público através do site da Cooperativa.

É obrigação de todo colaborador conhecer e praticar às disposições desta Política e assegurar que, quando necessário, prestadores de serviços sejam informados sobre as regras estabelecidas.

Será implementado um Programa de Capacitação e de avaliação periódica de pessoa, sobre as diretrizes desta Política.

Esta Política, juntamente com o Plano de Ação e respostas a incidentes serão revisadas anualmente ou quando mudanças significativas ocorrerem, assegurando a sua contínua pertinência, adequação e eficácia.

HISTORICO DE REVISÕES Versões	**Data Alteração**	**Alterações**	**Responsável**
01	23/03/2019	Elaboração do Documento	Francisco Carlos Firmino de Sousa
02	20/11/2020	Elaboração do Documento	Joy Allan de Sousa
03	24/01/2022	Revisão	Joy Allan de Sousa
04	02/05/2022	Atualização	Joy Allan de Sousa
05		Atualização	Joy Allan de Sousa

PLANO DE RESPOSTAS A INCIDENTES DE SEGURANÇA EM DADOS PESSOAIS CREDJUST

Sumário

INTRODUÇÃO

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD, tem como um de seus pilares centrais a implementação de medidas de Segurança da Informação que podem trazer às entidades públicas e privadas, uma cultura de maior conscientização na área. A LGPD considera que, mais grave do que sofrer um ataque ou passar por um vazamento de dados, é não se prevenir e nem adotar as medidas e práticas necessárias e possíveis para a proteção dos seus dados e de todos os que são afetados por eventuais acessos não autorizados.

A atividade de adequação às regras da Lei Geral de Proteção de Dados não se resume ao emprego de medidas tecnológicas e padrões de segurança. Inclui, também, a necessidade de elaboração, manutenção e revisão de documentos que, além de garantir a adequação à citada Lei, também são medidas que podem trazer maior organização e otimização aos processos internos, bem como, proteger a Entidade e sua reputação, seus servidores, usuários dos serviços prestados e parceiros.

Na Era Tecnológica, com a popularização dos computadores pessoais e a facilidade do acesso à internet, cada vez mais se observa a dependência de processos digitais para a manutenção de modelos de negócios ou cumprimento de obrigações legais. A praticidade, redução de custos e economia de tempo, advindas da informatização dos processos, traz consigo riscos de segurança que não devem ser negligenciados. Com tempo e recursos suficientes, qualquer sistema pode ser comprometido.

Levando isso em consideração, a criação de estratégias e planos para controle de danos é essencial, e é aí que entram os Planos de Respostas a Incidentes de Segurança em Dados Pessoais.

Incidente de segurança é "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

Resposta a Incidentes é o processo que descreve como uma organização deverá lidar com um incidente de segurança, seja ele um ataque cibernético, uma violação de dados, a presença de um aplicativo malicioso (como um vírus), uma violação das políticas e padrões de segurança da entidade, dentre outros. O objetivo é minimizar os danos que poderiam ser causados pelo incidente, reduzir o tempo de ação e os custos de recuperação.

O Plano de Respostas a Incidentes (PRI) consiste de um documento interno que deve ser amplamente conhecido por todos os servidores/funcionários/colaboradores e que dispõe sobre as medidas que devem ser adotadas no caso de um Incidente de Segurança em Dados Pessoais.

A CREDJUST cujos tratamentos de dados realizados no seu âmbito se dá em função do cumprimento de suas obrigações legais e regulatórias (7º, inciso II, da LGPD), vem passando por todo o processo de adequação à Lei em comento.

Atualmente, grande parte dos processos da CREDJUST são informatizados, imprimindo maior eficiência e agilidade nos serviços que presta. Por isso mesmo, a criação e implementação de medidas de controle e segurança de dados, como o Plano de Resposta a Incidentes, é questão que impõe.

OBJETIVO, ABRANGÊNCIA E VIGÊNCIA DO PLANO DE RESPOSTAS A INCIDENTES (PRI)

O Plano em questão, tem o objetivo geral de orientar a CREDJUST a responder às situações de emergência e exceção, de forma documentada, formalizada, ágil e confiável, além de resguardar as evidências que possam auxiliar na prevenção de novos incidentes e no atendimento às exigências legais de comunicação e transparência.

Neste PRI serão estabelecidas funções e responsabilidades individuais e de equipes, bem como, as medidas a serem adotadas para que a CREDJUST responda adequadamente a um incidente, sempre prezando pela integridade dos sistemas/processos, proteção de informações e privacidade dos seus titulares, possibilitando manter a confiabilidade dos serviços prestados.

O presente PRI se aplica em qualquer caso de incidentes envolvendo Dados Pessoais e deverá ser observado em conjunto com as demais políticas da cooperativa por todas as áreas, diretoria, conselho, colaboradoras e prestadores de serviços que possam vir a ter acesso às informações.

O PRI da CREDJUST entrará em vigor na data de sua publicação, por tempo indeterminado, podendo ser revisto e alterado sempre que identificada a necessidade.

TERMOS E DEFINIÇÕES

- Agentes de tratamento: corresponde ao controlador e operador em conjunto. Não são considerados controladores ou operadores os servidores ou as equipes de trabalho de uma entidade, já que atuam sob o poder diretivo do agente de tratamento;

- 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 em todo o território nacional;
- Controlador: é toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;
- Dados pessoais: qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, ou para entrar em contato, por conta própria ou quando combinada com outras informações;
- Dados pessoais sensíveis: são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, prática ou orientação sexual, informações médicas ou de saúde, como histórico médico e prontuário físico ou eletrônico, informações genéticas ou biométricas, crenças políticas ou filosóficas, filiação política ou sindical, número do seguro social, número da carteirinha do plano de saúde e informações bancárias;
- Incidente: qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse da CREDJUST ou que ela venha a ter acesso;
- IP: Protocolo da Internet (Internet Protocol), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;
- LGPD: acrônimo utilizado para identificação da Lei Geral de Proteção de Dados, a Lei nº 13.709/2018, que regula as atividades de Tratamento de Dados no Brasil.
- Log: processo de registro de eventos relevantes num sistema computacional;
- Operador: é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador. O operador será sempre uma pessoa distinta do controlador;
- Sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pela CREDJUST para dar suporte na execução de suas atividades.
- 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;

- Vazamento de dados: qualquer quebra de sigilo ou disseminação 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.

ATORES E RESPONSABILIDADES

Cada setor da CREDJUST tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, devendo comunicar, imediatamente, ao diretor responsável.

- Notificador: pessoa ou sistema de monitoração que notifica o incidente;
- Gerente: responsável pelo recebimento das notificações e realização do tratamento inicial (triagem) do incidente;
- Responsável por Sistema: indicado, com capacidade de propor soluções de resposta, bem como, autorizar ou vetar procedimentos de emergência;
- Responsável por Processo ou Negócio: gerente organizacional, com capacidade de propor soluções de resposta a serem apreciadas pelo responsável pelo sistema;
- Diretor: principal instância decisória sobre o tratamento de Dados Pessoais no âmbito da CREDJUST. Responde diretamente ao Presidente.

MACRO ETAPAS DO PROCESSO

Este Plano de Resposta a Incidentes está estruturado conforme as macro etapas a seguir descritas.

Identificação

A identificação de qualquer Incidente de Segurança é aspecto chave para a boa implementação de um Plano de Respostas. É importante que se possa dispor das principais medidas de detecção e identificação de Incidentes, como ferramentas de monitoramento, eventos de log, mensagens de erro firewalls, etc. Também deve haver um trabalho maciço de sensibilização e capacitação de servidores/funcionários/colaboradores, para que, proativamente, esses tenham a capacidade de identificar e informar eventual vazamento de dados, de que tenham conhecimento/acesso.

Preparação

Uma resposta a um incidente deve ser decisiva e executada prontamente. Como há pouco espaço para equívocos, é essencial que as práticas de emergência sejam exercitadas e os tempos de resposta medidos. Desta forma, é possível desenvolver uma metodologia que estimule a agilidade e a exatidão, minimizando o impacto da indisponibilidade de recursos e os potenciais danos causados pelo comprometimento do sistema/processos.

Contenção

Após a identificação de um incidente, o mesmo deve ser contido e, se for o caso, isolado, para que outros sistemas/processos não sejam afetados, evitando maiores danos ao ambiente. Essa etapa inclui a contenção de curto prazo, backup do sistema, contenção a longo prazo, dentre outros.

É importante que, durante a etapa de contenção, ocorra simultaneamente a adoção de medidas que permitam a documentação e o registro do incidente, devendo ser evitado que evidências e provas do ocorrido sejam destruídas ou perdidas.

Erradicação

Após a contenção da ameaça, a próxima etapa consiste da remoção da ameaça e restauração dos sistemas/processos afetados para que retornem ao seu estado original antes do incidente.

Recuperação

Nesta etapa, os sistemas/processos afetados retornarão, após testes e validações, ao ambiente de produção, ou, ao habitual andamento, com vistas a garantir que nenhuma ameaça permaneça.

Preceitos assimilados (Lições aprendidas)

Esta última etapa visa atualizar o Plano de Respostas a Incidentes com as ações realizadas para tratar o incidente, contribuindo para o aprendizado da equipe e facilitando as próximas atuações em futuros incidentes.

Documentação do Incidente

O incidente deve ser documentado de forma detalhada, incluindo todas as ações implementadas nas etapas anteriores e as lições aprendidas com o caso.

Comunicações

A ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, deve ser comunicada à Autoridade Nacional de Proteção de Dados – ANPD e ao titular afetado. A depender da situação, as informações a serem prestadas à ANPD poderá ocorrer por meio de solicitações, comunicações ou auditorias, com a finalidade principal de demonstrar, para o órgão fiscalizador, a adequação (ou intenção de adequação) da Entidade aos ditames da lei.

DESCRIÇÃO DO PROCESSO

Início/Detecção

1. Um novo incidente é notificado por pessoa interna/externa à CREDJUST ou por eventual alarme da monitoração. A comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como e-mails, telefone, “Fale Conosco”, Canal de Comunicação, Sistemas internos (incluindo as recebidas pelo Encarregado quando se tratar de notificação

do titular dos dados pessoais), devendo todas serem registradas, diretamente pelo Notificador.

Triagem

2. A Notificação é recebida pela Gerente, que deverá fazer a avaliação preliminar, descartando as notificações nulas ou claramente improcedentes.
3. Na avaliação preliminar, devem ser buscadas informações sobre os sistemas/processos que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravarem se não houver resposta imediata.
4. Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para tramites regulares dos setores pertinentes da Autarquia.

Avaliação

5. Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente pelo diretor, classificando-o e definindo a sua criticidade.
6. A criticidade do incidente pode ser definida de acordo com as seguintes classificações:

Volume de Dados Pessoais expostos	Alto	Alta Gravidade	Alta Gravidade	Alta Gravidade
	Médio	Média Gravidade	Alta Gravidade	Alta Gravidade
	Baixo	Baixa Gravidade	Média Gravidade	Média Gravidade
		Baixa	Média	Alta
		Sensibilidade dos Dados Pessoais afetados		

Volume de Dados Pessoais expostos
Descrição
Volume de Dados Pessoais afetado superior a 10% da base de dados da Controladora.
Volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados da Controladora.
Volume de Dados Pessoais afetado inferior a 2% da base de dados da Controladora.

Sensibilidade dos Dados Pessoais afetados	
Criticidade	Descrição
Alta	Dados Pessoais de crianças/ adolescentes, dados Pessoais Sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais imediatamente identificáveis (Ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (Ex.: histórico de atividades, preferências).
Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (Ex.: IP)

7. Deve-se procurar identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos setores afetados para colaborar e isso deve ser feito a critério da Gerente a qualquer momento que julgar adequado e viável.

Contenção, Erradicação e Recuperação

8. Os responsáveis pelos sistemas/processos impactados, devem ser acionados para se manifestarem sobre os procedimentos de resposta, contenção e erradicação.
9. O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida, poderá ser realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas e colocados avisos de indisponibilidade para manutenção. Todos os cuidados devem ser adotados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

10. Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot (registro do estado de um arquivo, aplicação ou sistema em um certo ponto no tempo) para posterior análise.
11. Em se tratando de incidentes não relacionados a recursos computacionais, mas essencialmente de atividade humana, os procedimentos podem envolver sindicância administrativa, processo administrativo disciplinar, entre outras medidas dispostas na legislação aplicável ao caso.
12. A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema/processo.
13. Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, ou elaboração de novas rotinas processuais.

Comunicações

14. Assim que possível, a situação deve ser encaminhada para análise da Diretoria para avaliar se houve risco ou dano relevante aos titulares dos dados pessoais impactados.
15. Caso do diretor conclua que o incidente acarretou risco ou dano relevante aos titulares de dados pessoais, o Encarregado de Dados (DPO), que deverá fazer as comunicações obrigatórias por Lei. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados e imprensa, bem como relatórios formais para a ANPD.

Preceitos assimilados

16. Com o incidente contido e sua resolução encaminhada, a Gerente deve agendar e conduzir uma reunião de lições aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos - inclusive deste Plano de Resposta a Incidentes.
17. As melhorias sugeridas na reunião devem ser encaminhadas a diretoria para deliberação sobre a adoção.

Documentação

18. O diretor deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações executadas, inclusive as da reunião de lições aprendidas.
19. Após a neutralização da ameaça, o diretor deve elaborar um relatório circunstanciado de todas as medidas que foram adotadas, apresentando todas as informações relevantes, tais como, informações sobre o incidente em si (quando foi identificado, qual sua natureza, danos ou potenciais danos causados, a extensão, a relevância e a repercussão desses danos, etc); providências adotadas para preservação das evidências, procedimentos seguidos para a contenção da crise; medidas de correção técnicas e de Governança adotadas; questionamentos e demandas externas (requerimentos de titulares de dados, autoridades e imprensa, bem como suas respostas).

Observações complementares

Paralelamente à execução do Plano de Respostas a Incidentes, diversas ações devem ser desenvolvidas, antes, durante e depois da ocorrência de um incidente, conforme:

Durante o incidente - Identificação, coleta e preservação das evidências:

Como já mencionado, um aspecto essencial da Resposta aos Incidentes é a coleta e preservação de evidências que possam vir a ser úteis ou necessárias para a Entidade, por exemplo, para demonstrar às autoridades que houve uma resposta adequada e que o incidente foi tratado com a seriedade necessária.

Especialmente no contexto da LGPD e da ANPD, as providências adotadas pela Entidade, para conter o Incidente e seus danos, podem ser definitivas para a minimização das sanções e multas, eventualmente, aplicadas ao caso concreto. Tais evidências também se prestam a possibilitar a identificação/responsabilização do usuário causador do vazamento de dados pessoais. Diversas decisões na União Europeia, em decorrência da GDPR (General Data Protection Regulation ou Regulamentação Geral de Proteção de Dados da União Europeia), demonstram que, mais grave do que o incidente em si, é o fato de a organização desprezá-lo.

Após o incidente - Elaboração de relatório final do incidente e revisão dos procedimentos:

O relatório, além de ter uma função de comprovação das medidas levadas a efeito pela Entidade, é importante para que se possa compreender as causas do incidente, avaliar a aderência e efetividade do Plano de Respostas a Incidentes e analisar a atuação dos responsáveis.

No que tange à Comunicação de Incidente de Segurança, prevista na LGPD, cujo conteúdo mínimo está definido no artigo 48, temos:

> *Art. 48. 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.*
> *I – a descrição da natureza dos dados pessoais afetados;*

Não basta apontar se os dados pessoais são convencionais (art. 5º, I) ou sensíveis (art. 5º, II), mas deve-se arrolar, com precisão, as espécies: contas de e-mail, dados de cartão de crédito, senhas, informações de geolocalização, etc., para que o titular tenha uma ideia, ainda que estimada, dos riscos existentes ou dos danos possíveis.

> *II – as informações sobre os titulares envolvidos;*

É a descrição, precisa ou estimada, de quais e quantos titulares foram afetados.

> *III – a indicação das medidas técnicas e de segurança utilizadas para a proteção;*

Observados os segredos comercial e industrial, a LGPD exige, em seu art. 46, que os agentes de tratamento (controlador e operador) adotem medidas de segurança (técnicas e administrativas) para a proteção de dados pessoais. Tais medidas devem ser descritas, para se demonstrar o compliance com a lei. Obviamente, essa descrição minuciosa admite algumas limitações, como os segredos comercial e industrial, que devem ser poupados para a preservação do negócio. A depender do tipo de incidente e, em havendo o risco de ser repetido, a descrição de determinadas medidas de segurança adotadas também poderia ser ocultada, segundo a técnica da "segurança por obscuridade" (Security Through Obscurity – STO), que teria o condão de privar o adversário/atacante de qualquer informação que possa ajudá-lo a comprometer a organização.

> *IV – os riscos relacionados ao incidente;*

Trata-se de uma análise prospectiva do incidente, levando em consideração, principalmente, os itens I e II. Poderá mencionar, também, os danos que já ocorreram, como a destruição ou codificação de dados.

> *V – os motivos da demora, no caso de a comunicação não ter sido imediata;*

É a justificativa, devidamente fundamentada, da não apresentação imediata da notificação. Poderá decorrer, por exemplo, da complexidade e extensão (número de titulares afetados, quantidade de dados, etc.) do incidente.

VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Aqui devem ser mencionadas, de forma clara e objetiva, e sem exagero de expressões técnicas, as condutas que foram e que serão implementadas para eliminar ou minimizar os efeitos do incidente, como o contato com as autoridades policiais, determinação de troca de senhas pelos usuários, a atualização de sistemas e servidores, etc.

João Pessoa, 20 de junho de 2022.

_____
JOY ALLAN DE SOUSA
DIRETOR

Plano de Ação e de Respostas a Incidentes - Segurança Cibernética					
Ações	Providências a serem tomadas	Medidas adotadas	Prazo	Responsável	Status
Aprovação da Política de Segurança Cibernética	Aprovação em ATA de Reunião Diretoria	Registrar em Ata da Diretoria	2022	Diretoria	Concluído
Apresentação dos Princípios, das Ditrizes e do Tratamento da Informação e do Objetivo da Política de Segurança Cibernética da Cooperativa da Diretoria, Conselho Fiscais, e funcionárias.	Disponibilização do documento no Site da Cooperativa dando livre acesso a qualquer interessado. Recolhimento de Assinatura do Termo do Ciencia da Diretoria, Conselho Fiscais, e funcionárias.	Recolhimento Assinatura do Termo Ciência.	fev/22	Diretor Responsável	Concluído
Aprovação do Plano de Ação e de Resposta a Incidentes visando à Implementação da Política de Segurança Cibernética	Aprovação em ATA de Reunião Diretoria	Registrar em Ata da Diretoria	jun/22	Diretor Responsável	Concluído
Divulgação da aprovação da reforma da Política de Segurança Cibernética e do Piano de Ação e Resposta a Incidentes	Divulgação no site Plano de Ação	Divulgar em site	jul/22	Diretor Responsável	Concluído
Inicio da Gestão da Segurança Cibernética	Acompanhamento se dá através de relatórios do TI e Ata de reunião da diretoria.	Elaboraçào de relatório de acompanhamento de gestão para conferência mensal das rotinas, procedimentos, controles e tecnologias.	ago/22	Gerente ADM	Em tratamento
Necessidade de Investimentos	Açôes Estruturantes	Identificada a necessidade de investimento em Servidor de forma a ampliar a segurança e organização dos dados da cooperativa e seus clientes, e gerenciar o uso das estações e aplicativos internos	dez/22	Diretoria	Em tratamento

Gerenciamento de Incidentes	São etapas do Gerenciamento de Incidentes: I – Recepção da denúncia; II – Medidas de contenção imediata; III – Coleta das informações e evidências; IV – Análise das informações e evidências; V – Notificação dos envolvidos; VI – Análise crítica e medidas de corretivas; VII – Acompanhamento da Diretoria.	Os procedimento de gerenciamento de incidentes estão descrito na política de Segurança Cibernética e acompanhado pela diretoria.	2022	Diretoria	Em tratamento
Prestação de Informação aos associados sobre precaução na utilização de produtos e serviços	Estimular a educação financeiro dos Cooperados	Confecção de material educativo	2022	Gerente ADM	Em tratamento
Elaboração de relatório sobre a implementação do plano de ação e de resposta a incidentes	Elaborar relatório semestral	A analise será feita através dos relatórios de controle	mar/23	Gerente ADM	Em tratamento

Plano 07.2022		
Status	Em tratamento	5
	Concluído	4
Revisando em: 15/07/2022		