PLANO DE CONTINGENCIA PARA INCIDENTES DE SEGURANÇA DA COOPERTAR

1. FINALIDADE E ALCANCE

O objetivo deste plano de contingência para incidentes de segurança da COOPERTAR é assegurar a proteção dos dados pessoais e a continuidade dos negócios em caso de violações de segurança, desastres naturais ou outros eventos inesperados.

Este plano se aplica a todas as operações e atividades da COOPERTAR, incluindo seus escritórios, instalações, veículos, sistemas de informação e rede de comunicação.

Definições:

Incidente de segurança: Qualquer evento ou situação que possa causar danos ou interrupção à continuidade dos negócios ou aos dados pessoais armazenados e tratados pela cooperativa.

Equipe de resposta a incidentes: O grupo de funcionários designados pela cooperativa para gerenciar e responder a incidentes de segurança.

Recuperação de dano: O processo de restaurar as operações normais após um incidente de segurança.

2. IDENTIFICAÇÃO DE RISCOS E VULNERABILIDADES

A COOPERTAR possui um processo fomentado para identificar e avaliar riscos e vulnerabilidades relacionados à segurança de dados. Para tanto se considera a realização de avaliações regulares de segurança, feedback dos funcionários, monitoramento de ameaças externas e revisão das ferramentas utilizadas.

Os riscos identificados serão classificados conforme sua probabilidade de ocorrência e impacto potencial, permitindo a focar nas áreas mais críticas.

Uma vez realizada a classificação dos riscos, a COOPERTAR prima pelas áreas que requerem medidas de mitigação mais urgentes ou emergentes, o que assegura que a cooperativa esteja preparada para lidar com os riscos mais críticos primeiro.

3. PLANOS DE AÇÃO

Medidas Preventivas: Para minimizar a possibilidade e os impactos de incidentes de segurança, o Plano de Contingência da COOPERTAR contém medidas preventivas. Estas medidas incluem a implementação de medidas de segurança física e lógica, treinamento e testes de continuidade de negócios, e a contratação de consultores especializados.

Medidas de Resposta: O Plano de Contingência também contém medidas de resposta para lidar com incidentes de segurança, caso ocorram. Isso inclui a criação de um plano de comunicação de incidentes, a ativação de um plano de continuidade de negócios e a implantação de medidas de segurança temporárias.

Medidas de Recuperação: O Plano de Contingência inclui medidas de recuperação para restaurar a operação normal da cooperativa após um incidente de segurança. Isso envolve a revisão e aprimoramento dos processos internos, auditorias de segurança e a implementação de medidas de segurança permanentes. O Plano de Ação deve ser revisado e atualizado regularmente para garantir que as medidas preventivas permaneçam eficazes.

4. COMUNICAÇÃO E COLABORAÇÃO

O objetivo do plano de comunicação interna da COOPERTAR é manter todos os funcionários informados sobre os incidentes de segurança, bem como as medidas preventivas, de resposta e de recuperação adotadas. Isso envolve o estabelecimento de canais de comunicação internos, como alertas por e-mail, reuniões de crise e treinamentos regulares para os funcionários.

O plano de comunicação externa tem como objetivo manter os clientes, parceiros e outras partes interessadas informados sobre os incidentes de segurança. Isso envolve a criação de canais de comunicação externos, como

comunicados à imprensa, atualizações nas redes sociais e comunicações com os parceiros.

Colaboração com Outras Organizações: A COOPERTAR estabelece relações de colaboração com outras organizações para garantir uma resposta rápida e eficaz a incidentes de segurança. Isso inclui acordos de compartilhamento de informações, participação em grupos de trabalho de segurança e treinamentos regulares com outras organizações.

5. EXERCÍCIOS E TESTES

Para garantir que o plano de contingência da COOPERTAR seja eficaz, serão realizados testes regulares, incluindo testes de continuidade de negócios, recuperação de desastres e resposta a incidentes de segurança. Os resultados desses testes serão registrados e usados para melhorar o plano de contingência.

Além dos testes regulares, a cooperativa também promoverá treinamentos de simulação de incidentes de segurança para sua equipe de resposta a incidentes. Esses treinamentos serão realizados em conjunto com outras organizações, incluindo autoridades locais e organizações do setor, com o objetivo de aprimorar a preparação e a resposta da cooperativa em situações de crise.

A COOPERTAR avaliará o desempenho dos testes e treinamentos de simulação, com o objetivo de identificar lacunas e aprimorar continuamente seu plano de contingência. Essa avaliação garantirá que a cooperativa esteja sempre preparada para lidar com incidentes de segurança e minimizar seus impactos.

6. TREINAMENTO E CONSCIENTIZAÇÃO

A COOPERTAR implementou um programa de treinamento para garantir que todos os funcionários estejam cientes dos riscos de incidentes de segurança e saibam como lidar com eles. O treinamento inclui informações sobre a identificação de incidentes, a comunicação interna e externa, medidas preventivas e de resposta, bem como procedimentos internos e regulamentos aplicáveis.

A cooperativa também implementou um programa de conscientização para garantir que todos os funcionários estejam conscientes dos riscos de incidentes de segurança e saibam como evitá-los. Isso inclui campanhas internas para conscientizar os funcionários sobre os riscos, além de informações regularmente atualizadas sobre incidentes de segurança e como lidar com eles.

A cooperativa também fornece treinamento específico para líderes da organização para garantir que eles estejam cientes dos riscos de incidentes de segurança e saibam como lidar com eles. O treinamento inclui liderança em situações de crise, comunicação efetiva e gerenciamento de incidentes.

7. REVISÃO E ATUALIZAÇÃO

Frequência de revisão: O plano de contingência para incidentes de segurança da COOPERTAR será revisado e atualizado anualmente ou sempre que necessário, a fim de garantir que esteja sempre atualizado com as últimas tendências e práticas de segurança.

Responsabilidade pela revisão e atualização: O Comitê de Governança Corporativa da cooperativa será responsável pela revisão e atualização do plano, composto por representantes de diferentes áreas da empresa.

Comunicação de mudanças no plano: As mudanças no plano serão comunicadas a todos os funcionários por meio de treinamentos e atualizações no manual de procedimentos de segurança. Também serão realizadas comunicações internas para garantir que todos estejam cientes das mudanças e estejam preparados para implementá-las.

Testes regulares de implementação: A COOPERTAR realizará testes regulares para avaliar a implementação do plano de contingência em situações reais, incluindo simulações de incidentes de segurança. Eles serão utilizados para identificar áreas que precisam de melhorias no plano e no treinamento dos funcionários.

Revisão pós-incidente: A COOPERTAR realizará uma revisão pós-incidente sempre que ocorrer um incidente de segurança significativo. A revisão será conduzida pela equipe de resposta a incidentes, a fim de identificar as causas

do incidente, avaliar a eficácia do plano de contingência e implementar ações corretivas para evitar futuros incidentes.

Atualização de políticas e procedimentos: A COOPERTAR revisará regularmente suas políticas e procedimentos de segurança, a fim de garantir que estejam alinhados com as melhores práticas de governança corporativa e com as leis e regulamentações aplicáveis. As atualizações serão comunicadas a todos os funcionários e incluídas no treinamento de segurança.

Gestão de fornecedores e terceiros: A COOPERTAR gerenciará seus fornecedores e terceiros para garantir que cumpram as políticas e procedimentos de segurança da cooperativa. Isso inclui a avaliação da segurança dos sistemas de informação dos fornecedores, a implementação de acordos de confidencialidade e a realização de treinamentos para os fornecedores sobre as políticas e procedimentos de segurança da cooperativa.

Monitoramento contínuo: A COOPERTAR monitorará continuamente sua infraestrutura de segurança para identificar possíveis ameaças e vulnerabilidades, incluindo o monitoramento de logs, o uso de ferramentas de detecção de intrusão e a realização de testes de penetração regulares.

7. CONCLUSÃO

A implementação do Plano de Contingência para Incidentes de Segurança é fundamental para a COOPERTAR e suas práticas de governança corporativa. O plano tem como objetivo proteger os dados pessoais e garantir a continuidade dos negócios em casos de incidentes de segurança. Ele inclui uma série de medidas, desde a identificação de riscos até o monitoramento contínuo, que devem ser implementadas de forma eficaz para garantir a proteção dos funcionários, clientes e parceiros da cooperativa. A implementação bem-sucedida do plano de contingência permitirá que a cooperativa esteja preparada para lidar com incidentes de segurança e manter a integridade dos seus negócios.

8. SOBRE OS ANEXOS

A comunicação de incidentes de segurança é fundamental para garantir que todas as partes envolvidas estejam cientes do incidente e das medidas tomadas para resolvê-lo. Isso inclui notificar titulares de dados, autoridades reguladoras e outras partes interessadas, quando necessário. A comunicação efetiva pode ajudar a minimizar o impacto do incidente e prevenir problemas futuros.

O formulário de registro de incidentes de segurança é uma ferramenta importante para garantir que todas as informações relevantes sejam coletadas e comunicadas de forma clara e precisa. Ele deve conter informações sobre a natureza do incidente, as medidas tomadas para lidar com ele e as ações implementadas para evitar incidentes semelhantes no futuro. Além disso, pode incluir informações sobre os possíveis impactos do incidente e recomendações para as partes interessadas.

É importante destacar que a comunicação de incidentes de segurança deve ser rápida e efetiva, pois quanto mais cedo as partes interessadas forem notificadas, mais cedo medidas podem ser tomadas para minimizar o impacto do incidente. Além disso, a comunicação transparente e honesta pode ajudar a garantir a confiança dos titulares de dados e outras partes interessadas na capacidade da organização de lidar com incidentes de segurança.

O relatório de incidente de segurança é um documento importante para a COOPERTAR, pois permite registrar e avaliar os incidentes de segurança de dados ocorridos na cooperativa. Ele é utilizado para identificar as causas e os efeitos do incidente, bem como planejar e implementar medidas para prevenir incidentes semelhantes no futuro.

A estrutura do relatório inclui a identificação do incidente, a descrição detalhada do incidente, análise de causas, análise de impacto, medidas de resposta, recomendações e anexos. É essencial garantir que o relatório seja preciso, completo e claro, escrito de forma objetiva e sem informações desnecessárias. O relatório deve ser revisado e aprovado pelo Comitê de Ética e pela equipe de resposta a incidentes antes de ser entregue aos órgãos reguladores e titulares de dados afetados.

É importante coletar todas as informações relevantes e apresentá-las de maneira organizada e clara. O relatório deve ser entregue dentro do prazo estabelecido pelas autoridades reguladoras e deve atender às exigências regulatórias. Para isso, é importante ter um processo claro e bem definido para elaboração, revisão e aprovação do relatório.

Garantir que o relatório seja mantido em sigilo e acessível apenas às pessoas autorizadas é fundamental. Isso pode ser feito por meio de sistemas de segurança, como criptografia e controle de acesso. Por fim, a equipe de resposta a incidentes e a equipe de governança da cooperativa devem ser bem treinadas e preparadas para lidar com incidentes de segurança. Isso inclui treinamentos regulares para aumentar a conscientização sobre segurança cibernética e práticas de segurança, bem como exercícios de simulação para testar a eficácia do plano de contingência e identificar possíveis melhorias. Com um plano de contingência sólido e uma equipe bem treinada, a cooperativa estará mais preparada para lidar com incidentes de segurança e minimizar seu impacto. A implementação desses formulários e relatórios é uma parte crucial da preparação da cooperativa para lidar com incidentes de segurança. Eles ajudam a garantir que todas as informações relevantes sejam coletadas e comunicadas de forma clara e eficaz, permitindo uma resposta rápida e coordenada a incidentes de segurança.

No entanto, a preparação para incidentes de segurança não é uma tarefa única, mas sim um processo contínuo. A cooperativa deve revisar e atualizar regularmente seus planos de contingência e procedimentos de segurança para garantir que estejam alinhados com as últimas tendências e práticas de segurança. Além disso, a conscientização e o treinamento dos funcionários devem ser constantes, com campanhas regulares para garantir que todos estejam cientes dos riscos e saibam como lidar com incidentes de segurança. A COOPERTAR deve também monitorar continuamente sua infraestrutura de segurança para identificar possíveis ameaças e vulnerabilidades, bem como realizar testes regulares de implementação de seus planos de contingência para garantir que estejam funcionando corretamente.

Em resumo, a preparação para incidentes de segurança é um processo contínuo que envolve a implementação de planos de contingência sólidos, a coleta e comunicação eficaz de informações relevantes e a conscientização e treinamento constantes dos funcionários. Com essas medidas em prática, a

COOPERTAR estará mais bem preparada para lidar com incidentes de segurança e proteger seus funcionários, clientes e parceiros.

Responsáveis pela elaboração:

_____

José Ribeiro Primo

_____

Aline da Conceição de Almeida

_____

Lucas Alexander da Silva Mendes

_____

Bruno Leite Casciano

ANEXO I

Comunicação de Incidente de Segurança
Formulário de Comunicação de Incidente de Segurança

Informações gerais: Data e hora do incidente: _____
Local do incidente:

_____ Descrição breve do incidente: _____ Informações sobre o incidente: Tipo de incidente: _____ Fonte do incidente: _____
Impacto do incidente: _____

Medidas tomadas: Medidas imediatas tomadas para contornar o incidente: _____

Medidas adicionais planejadas para lidar com o incidente: _____

Data prevista para conclusão das medidas: _____

Informações de contato: Nome do funcionário responsável pelo relatório: _____ Cargo: _____ Telefone: _____ E-mail: _____

Anexos (se aplicável) Prints de tela, arquivos de log, outros documentos relevantes.

Assinatura do responsável pelo relatório: _____

Data: _____

Observações: Este formulário deve ser preenchido e encaminhado imediatamente após a identificação de um incidente de segurança. Ele deve ser enviado para o Comitê de Governança, através do e-mail **coopertar.coop@gmail.com**, para avaliação e tomada de ação adequada.

ANEXO II

Relatório de Incidente de Segurança
Modelo de Relatório de Incidente de Segurança

Identificação do Incidente: Data e hora do incidente: _____ Local do incidente: _____
Tipo de incidente: _____

Nome do funcionário(s) envolvido(s): _____

Descrição do Incidente: Forneça uma descrição detalhada do incidente, incluindo as circunstâncias que o levaram a ocorrer e as ações tomadas imediatamente após o incidente.

Impacto do Incidente: Identifique qual foi o impacto do incidente nos dados pessoais armazenados e tratados pela cooperativa. Identifique qual foi o impacto do incidente nas operações da cooperativa.

Ações Tomadas: Liste as ações tomadas para contornar o incidente e minimizar seu impacto. Indique quais medidas foram tomadas para prevenir que o incidente ocorra novamente.

Informações Adicionais: Forneça quaisquer outras informações relevantes sobre o incidente.

Assinatura: Funcionário responsável pelo preenchimento do relatório: _____ Data: _____

Nota: Este modelo de relatório deve ser preenchido e enviado ao Comitê de Ética assim que o incidente ocorrer e deve ser revisado e aprovado pelo Comitê antes de ser arquivado.

ANEXO – III
Modelo e Orientação de Relatório de Acompanhamento de Incidente de Segurança

Modelo de Relatório de Acompanhamento de Incidente de Segurança

I. Identificação do incidente: data, hora e local do incidente, bem como a descrição detalhada do incidente, incluindo as evidências coletadas.

II. Análise de risco: uma avaliação dos riscos e impactos potenciais do incidente, incluindo a classificação do incidente de acordo com a gravidade e a probabilidade de ocorrência.

III. Medidas preventivas: Após a identificação de um incidente de segurança, é fundamental que medidas preventivas sejam tomadas para evitar incidentes similares no futuro. Essas medidas podem incluir:

1. Revisão e atualização das políticas de segurança da informação da cooperativa, com o objetivo de garantir que elas sejam claras, abrangentes e estejam alinhadas com as melhores práticas de segurança da informação.

2. Implementação de controles adicionais para garantir a segurança da informação, como autenticação de dois fatores, criptografia, entre outros.

3. Treinamento e conscientização dos funcionários em relação à segurança da informação e boas práticas de segurança cibernética.

4. Realização de testes de penetração regulares para identificar vulnerabilidades e ameaças à segurança da informação.

5. Melhoria contínua dos processos e procedimentos da cooperativa, com foco em garantir a segurança da informação.

É importante que essas medidas preventivas sejam implementadas o mais rápido possível, para minimizar o risco de futuros incidentes de segurança.

Além disso, elas devem ser revisadas regularmente para garantir que a

cooperativa esteja sempre protegida contra novas ameaças e vulnerabilidades.

Para documentar as medidas preventivas implementadas, recomenda-se a elaboração de um plano de ação de segurança da informação. Esse plano deve incluir as medidas tomadas, as datas de implementação e os responsáveis pela implementação. O plano deve ser revisado e atualizado regularmente para garantir que as medidas preventivas permaneçam eficazes.

Além disso, é importante que haja uma política clara de segurança da informação que estabeleça as diretrizes e os procedimentos para garantir a proteção dos dados da cooperativa. Essa política deve ser divulgada a todos os funcionários e revisada periodicamente para garantir sua atualização.

Outras medidas preventivas que podem ser implementadas incluem:

1. Autenticação forte: garantir que todas as contas de usuário tenham senhas fortes e que a autenticação de dois fatores seja utilizada sempre que possível.

2. Controle de acesso: limitar o acesso aos dados somente a usuários autorizados, com base no princípio do "menor privilégio".

3. Monitoramento de segurança: implementar ferramentas de monitoramento de segurança para detectar atividades suspeitas e identificar possíveis ameaças.

4. Treinamento e conscientização: fornecer treinamento regular para todos os funcionários sobreas melhores práticas de segurança da informação e como reconhecer possíveis ameaças.

5. Atualização de software: garantir que todo o software utilizado pela cooperativa seja atualizado regularmente para corrigir possíveis vulnerabilidades de segurança.

6. Criptografia de dados: implementar a criptografia de dados sensíveis para garantir que eles não possam ser acessados por usuários não autorizados.

7. Gestão de fornecedores: implementar processos de due diligence para avaliar a segurança da informação dos fornecedores da cooperativa e garantir que eles estejam em conformidade com as políticas de segurança da informação da cooperativa.

Essas medidas preventivas devem ser implementadas de forma integrada e devem ser consistentes com o plano de segurança da informação da cooperativa. A monitoração regular e a avaliação da eficácia das medidas preventivas são essenciais para garantir a segurança dos dados da cooperativa.