POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

NOVA

SOBRE O DOCUMENTO:

Revisão	Data	Elaborador / Revisor
01	Dez./2021	Daniel Ribeiro – Tecnologia David Joaquim – Tecnologia Otávio Venturini – Jurídico
02	Nov./2024	Daniel Ribeiro – Tecnologia David Joaquim – Tecnologia Otávio Venturini – Jurídico

SUMÁRIO

1. OBJETIVO

Estabelecer diretrizes, controles e princípios relacionados à segurança da informação na NOVA, com o intuito de reduzir riscos e promover a melhoria contínua dos sistemas de informação. Isso inclui garantir os princípios fundamentais da segurança da informação, que são a confidencialidade, a integridade e a disponibilidade dos dados. Além disso, busca-se assegurar a conformidade com a legislação vigente, bem como aderir a normas e boas práticas de mercado.

2. APLICABILIDADE DA POLÍTICA

A todos os colaboradores e as partes externas que estejam envolvidos no uso e tratamento da informação de propriedade ou sob custódia da NOVA, contemplando os sistemas de informação físicos e/ou lógicos, os recursos de processamento de dados e as redes de comunicações.

3. DEFINIÇÕES

Ativo(s) de TI: ativo(s) de tecnologia, *hardware* e *software* que suportam a prestação de serviços e o negócio da NOVA.

Canal de comunicação: ferramenta ou meio eletrônico que permite aos clientes ou às partes externas reportarem incidentes de segurança, inconsistências ou violações de dados diretamente à NOVA.

Colaborador: para fins desta política, entende-se como colaborador qualquer pessoa que trabalhe para a NOVA, seja este funcionário com registro em carteira de trabalho, terceiro, *trainee*, estagiário ou aprendiz.

Conformidade: cumprimento de um requisito.

Controle: qualquer recurso ou medida que assegure formas de tratamento de riscos. A implantação e a manutenção adequada de controles materializam os princípios de segurança da informação (confidencialidade, integridade e disponibilidade). Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, *software*, *hardware*, entre outros.

Criptografia: mecanismo de segurança e privacidade que torna determinada comunicação ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem.

Direção: pessoa ou grupo de pessoas que dirige e controla uma organização em seu nível mais alto. Responsável pela visão, pelas decisões estratégicas e pela coordenação de atividades para dirigir e controlar a organização.

Incidente de segurança da informação: são considerados incidentes de segurança da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que possam levar ao comprometimento de um ou mais princípios de segurança da informação (confidencialidade, integridade e disponibilidade), colocando o negócio em risco.

Informação: é o conjunto de dados e conhecimentos.

Infraestrutura: sistemas de instalações, equipamentos e serviços necessários para a operação de uma organização.

Mitigação: adoção de medidas corretivas e preventivas que visam reduzir ou eliminar os impactos de vulnerabilidades e incidentes de segurança.

Objetivo: resultado a ser atingido.

Partes externas: fornecedores de serviços/produtos e parceiros de negócios.

Política: diretrizes de uma organização expressadas formalmente pela sua direção.

Procedimento: maneira específica de conduzir uma atividade ou um processo.

Processo: conjunto de atividades relacionadas que envolvem pessoas, equipamentos, procedimentos e informações e, quando executadas, transformam entradas (insumos) em saídas (produtos ou serviços); atendem à necessidade de um cliente interno ou externo; e agregam valor e produzem resultados para uma organização.

Proprietário da informação: colaborador da área de negócio ou formalmente delegado por este, responsável pela informação

criada, armazenada, processada, transmitida, compartilhada ou descartada nos sistemas de informação.

Recursos: todos os ativos, pessoas, competências, tecnologia (incluindo instalações e equipamentos), locais, suprimentos e informação (eletrônica ou não) que uma organização deve ter disponíveis para uso, quando necessário, a fim de operar e atingir seus objetivos de negócio.

Relatório de segurança: documento formal que descreve as medidas de segurança implementadas, os resultados de auditorias internas ou externas, e as ações corretivas adotadas em resposta a vulnerabilidades ou incidentes.

Requisitos: necessidade ou expectativa, geralmente implícita ou obrigatória.

Spam: termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para muitas pessoas. *Spams* estão diretamente associados à disseminação de golpes e venda ilegal de produtos.

Terceiros autorizados: entidades externas, como fornecedores e parceiros, que possuem autorização formal para acessar ou utilizar dados e informações da NOVA, seguindo as diretrizes e políticas de segurança da organização.

Usuário: pessoa que utiliza ou consome um produto, equipamento ou serviço.

Violações de dados pessoais: acesso, divulgação, alteração ou destruição não autorizada de dados pessoais, seja de forma acidental ou intencional, que afete a confidencialidade, integridade ou disponibilidade dos dados.

4. INTRODUÇÃO

4.1. POR QUE A SEGURANÇA DA INFORMAÇÃO É NECESSÁRIA?

As organizações são expostas a diversos tipos de ameaças, que podem causar incidentes e comprometer as informações e seus ativos por meio da exploração de vulnerabilidades,

materializando riscos que afetam a confidencialidade, integridade e disponibilidade da informação. Consequentemente, causam impactos negativos tangíveis ou intangíveis aos negócios, tais como: perda operacional, financeira ou de imagem, aplicação de multas, quebra contratual, entre outros.

Nesse contexto, definir, estabelecer, manter e aprimorar a segurança da informação são atividades essenciais para mitigar riscos que podem causar prejuízos à organização, buscando a proteção da informação e a continuidade de seus negócios.

5. ORGANIZAÇÃO E FUNÇÕES DE SEGURANÇA DA INFORMAÇÃO

A estrutura funcional e os papéis de gestão para o estabelecimento, a implementação, a manutenção e a melhoria contínua dos sistemas de informação estão relacionados a seguir.

5.1. DIREÇÃO

5.1.1. Prover o adequado direcionamento e suporte para as iniciativas de segurança da informação.

5.1.2. Assegurar a designação de papéis e responsabilidades para a segurança da informação.

5.1.3. Apoiar, difundir e alavancar o cumprimento das políticas e os controles de segurança da informação por meio da organização, provendo os recursos humanos e orçamentários necessários.

5.2. COLABORADORES

5.2.1. Ler e aceitar os termos da Política de Segurança da Informação, bem como praticar as diretrizes estabelecidas, conforme disposto no **ANEXO I – TERMO DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO**.

5.2.2. Participar das campanhas, dos *workshops* e dos treinamentos de segurança.

5.2.3. Cumprir com as responsabilidades descritas na política de segurança da informação e nas demais normas, políticas e procedimentos relacionados.

5.2.4. Notificar a direção sobre possíveis incidentes e violações de segurança que venha a ter conhecimento.

5.3. PARTES EXTERNAS (PRESTADORES DE SERVIÇOS OU PARCEIROS)

5.3.1. Notificar a direção sobre possíveis incidentes e violações de segurança que venha a ter conhecimento.

5.3.2. Cumprir as diretrizes da Política de Segurança da Informação e as normas internas estabelecidas pela NOVA, além de assinar o termo de confidencialidade em casos de acesso a informações internas ou confidenciais da NOVA, conforme descrito no **ANEXO III – CLÁUSULAS CONTRATUAIS DE SEGURANÇA DA INFORMAÇÃO**, abrangendo, mas não se limitando à apresentação de ideias de negócios, dados financeiros, projetos, auditorias, infraestrutura, tecnologias implementadas, relatórios gerenciais, entre outros.

6. SEGURANÇA EM RECURSOS HUMANOS

6.1. SEGURANÇA EM RECURSOS HUMANOS

6.1.1. Devem ser definidas e formalizadas as obrigações e recomendações de segurança às quais estão submetidos colaboradores e partes externas que estejam envolvidos no uso e tratamento da informação de propriedade ou sob custódia da NOVA.

6.1.2. Nos contratos assinados por colaboradores e partes externas, deve ser incluída cláusula referente ao cumprimento das políticas de segurança da NOVA.

6.1.3. Devem ser realizadas campanhas de treinamento e conscientização referentes à segurança da informação para os colaboradores da NOVA.

6.1.4. Devem ser definidas e formalizadas as obrigações e recomendações de segurança às quais estão submetidos colaboradores e partes externas que estejam envolvidos no uso e tratamento da informação de propriedade ou sob custódia da NOVA.

7. CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Todos os dados armazenados na NOVA devem receber um nível adequado de proteção, de acordo com o seu valor, grau de sigilo, sensibilidade e criticidade para o negócio. O nível de proteção é utilizado para determinar quais colaboradores têm acesso autorizado aos dados.

7.1. PROPRIETÁRIO DA INFORMAÇÃO

7.1.1. Classificar a informação de acordo com o seu valor, requisitos legais, grau de sigilo, sensibilidade e criticidade para o negócio.

7.1.2. Identificar e notificar os riscos, as vulnerabilidades inerentes aos ativos à direção e assegurar o tratamento dos riscos.

7.1.3. Identificar e notificar incidentes de segurança inerentes aos ativos de informação à direção.

7.1.4. Avaliar as solicitações de acesso de usuários aos ativos de informação.

7.1.5. Disponibilizar os meios e recursos necessários para o cumprimento dos controles de segurança, alinhados aos requisitos de negócio.

7.1.6. Zelar pelo cumprimento dos controles de segurança aplicáveis aos ativos de informação.

7.2. CATEGORIAS DE INFORMAÇÃO

As informações devem ser classificadas pelo proprietário, considerando os seguintes critérios:

7.2.1. CONFIDENCIAL: informação de alta sensibilidade que deve ser protegida por sua relevância sobre decisões estratégicas, impacto financeiro, oportunidades de negócio, potencial de fraude ou requisitos legais. Tal informação deve ser utilizada estritamente dentro da NOVA, onde a divulgação não autorizada pode impactar séria ou negativamente a empresa, os parceiros de negócio ou seus clientes. Exemplos de informações confidenciais incluem senhas, chaves criptográficas, informações de portadores de cartão, informações sobre contas bancárias, entre outros.

7.2.2. INTERNA: informação sem restrição que deve ser mantida no âmbito interno da NOVA. A divulgação não autorizada pode afetar negativamente a empresa ou seus funcionários. Exemplos de informações privadas incluem políticas e procedimentos, propriedade intelectual, entre outros.

7.2.3. PÚBLICA: informação cuja divulgação não gere prejuízos financeiros ou de imagem aos negócios da NOVA e dos parceiros. Para classificar uma informação como pública, é necessário consultar e obter a autorização expressa da direção.

7.2.4. Qualquer informação sem classificação explícita deve ser tratada como interna.

7.3. RESPONSABILIDADE PELO ARMAZENAMENTO DE DADOS

A NOVA é totalmente responsável pelo armazenamento seguro de todas as informações sob sua custódia, assegurando que todos os dados sigam os mais altos padrões de proteção. Além disso, a empresa garante que qualquer terceiro autorizado a acessar ou utilizar essas informações siga estritamente as diretrizes de segurança da NOVA e esteja alinhado com as exigências contratuais. Para garantir a conformidade:

7.3.1. Contratos com terceiros devem incluir cláusulas de segurança que exijam o cumprimento desta Política de Segurança da Informação, conforme descrito no **ANEXO III – CLÁUSULAS CONTRATUAIS DE SEGURANÇA DA INFORMAÇÃO**.

7.3.2. Auditores internos e externos devem verificar a aderência dos terceiros autorizados às políticas de segurança.

7.3.3. Os processos de revisão do desempenho de terceiros, se aplicável, devem incluir verificações sobre o uso adequado e seguro das informações.

8. GESTÃO DE ACESSO LÓGICO

8.1. Deve ser estabelecida uma norma que direcione os controles adequados para as etapas de solicitação, autorização, provisionamento, revogação e revisão periódica de acessos lógicos aos sistemas de informação, aos recursos e às redes de comunicações da NOVA.

8.2. Tal norma deve estar de acordo com os requisitos do negócio e basear-se no princípio da "necessidade de conhecer e necessidade de fazer", ou seja, os usuários devem acessar somente as informações e os recursos necessários para realizar suas funções de trabalho, a serviço exclusivo da NOVA.

8.3. A norma de gestão de acesso lógico considera os seguintes itens:

I. A legislação aplicável.

II. As obrigações contratuais com partes externas.

III. Os requisitos de segurança aplicáveis a cada sistema de informação ou recurso.

IV. Todo acesso está proibido, salvo se estiver expressamente permitido.

9. GESTÃO DE ATIVOS

9.1. Deve ser estabelecido e gerenciado um inventário dos ativos de processamento e recursos de informação.

9.2. Os ativos inventariados devem possuir um proprietário designado.

9.3. Devem ser estabelecidas as diretrizes e regras para o uso aceitável dos ativos de informação, considerando que eles devem ser utilizados única e exclusivamente como ferramentas de trabalho a serviço da NOVA.

9.4. Todos os ativos de informação sob a posse de colaboradores ou partes externas devem ser devolvidos à NOVA após o encerramento de suas atividades, seu contrato ou seu acordo de trabalho.

10. RELATÓRIOS E MEDIDAS DE SEGURANÇA

Com o objetivo de atender às exigências contratuais e regulamentares, a NOVA implementa e mantém processos para a geração e disponibilização de relatórios detalhados acerca das medidas de segurança da informação em vigor. Os relatórios serão disponibilizados sob demanda, tanto para clientes e parceiros quanto para autoridades competentes. Eles devem incluir informações detalhadas sobre os controles de segurança implementados, as auditorias realizadas, e as medidas de mitigação adotadas em resposta a vulnerabilidades identificadas. A criação dos relatórios de segurança seguirá as seguintes diretrizes:

10.1. Periodicidade e solicitação: os relatórios serão gerados conforme solicitado por partes interessadas ou de forma periódica, de acordo com os requisitos contratuais ou regulamentares.

10.2. CONTEÚDO DOS RELATÓRIOS:

10.2.1. Descrição das medidas de segurança implementadas para assegurar a **confidencialidade, integridade e disponibilidade** das informações.

10.2.2. Resultados de auditorias internas e externas relacionadas à segurança da informação, quando aplicáveis.

10.2.3. Medidas de correção adotadas em resposta a incidentes ou vulnerabilidades detectadas.

10.2.4. Informações sobre os processos e controles de segurança aplicáveis a terceiros autorizados que utilizam ou armazenam dados da NOVA.

10.3. Revisão e aprovação: os relatórios serão revisados pelo responsável pela segurança da informação e aprovados pela direção antes de serem disponibilizados às partes interessadas, conforme estabelecido no **ANEXO IV – AUDITORIAS E RELATÓRIOS DE SEGURANÇA DA INFORMAÇÃO**.

Esse processo assegura que a NOVA esteja preparada para fornecer documentação precisa e tempestiva sobre suas práticas de segurança, mantendo a transparência e o cumprimento das obrigações contratuais.

11. REDES E COMUNICAÇÕES

Devem ser definidos e implantados controles, mecanismos e procedimentos operacionais de segurança necessários para a implantação, configuração, manutenção e gestão da infraestrutura de redes e comunicações da NOVA, tais como: roteadores, *firewalls*, *switches*, entre outros. Nesse contexto, cabe destacar os seguintes aspectos:

11.1. Manter instalados e habilitados somente os serviços que são utilizados.

11.2. Segregar rede, física e lógica, por meio dos mecanismos e das tecnologias aplicáveis, assegurando a confidencialidade, integridade e disponibilidade das informações trafegadas.

11.3. Controlar o acesso lógico de uso e administração dos serviços.

11.4. Configurar os serviços de modo seguro, minimizando o risco de exploração de eventuais vulnerabilidades.

11.5. Instalar periodicamente as atualizações de segurança recomendadas pelos fabricantes.

12. SEGURANÇA EM PROJETOS

Os projetos associados a sistemas de informação, às redes de comunicação e à infraestrutura de tecnologia da informação

que suportam os serviços e processos de negócio devem considerar a aderência às políticas e aos controles de segurança da informação, desde os estágios iniciais do projeto. E quando necessário, realizar alinhamentos com a direção, com o objetivo de avaliar os riscos inerentes ao escopo do projeto.

13. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Os requisitos de segurança da informação devem ser identificados e considerados nas iniciativas ou demandas de aquisição e desenvolvimento de sistemas de informação proprietários, ou sempre que houver alterações significativas nos sistemas já existentes.

13.1. Os responsáveis pela aquisição, pelo desenvolvimento e pela manutenção de sistemas devem garantir o envolvimento de um profissional de segurança da informação para garantir a consistência da segurança dos sistemas e processos.

13.2. Deve ser utilizada uma metodologia de desenvolvimento apropriada ao escopo, à magnitude e à complexidade do projeto, da iniciativa e/ou da demanda.

13.3. Além dos testes funcionais e operacionais, testes de segurança devem ser contemplados para validar se as melhores práticas de desenvolvimento e os requisitos de segurança foram devidamente implantados. Quaisquer vulnerabilidades identificadas nessa fase devem ser corrigidas antes que o sistema seja disponibilizado em produção.

14. CRIPTOGRAFIA

É necessário implementar controles de criptografia robustos para assegurar que a comunicação e o tráfego de informações sejam realizados de maneira segura e protegida. Esses controles devem abranger tanto os dados em trânsito quanto os dados em repouso, garantindo que informações sensíveis sejam adequadamente criptografadas para prevenir acessos não autorizados. Além

disso, a escolha dos métodos criptográficos deve estar alinhada com as melhores práticas do setor e ser regularmente revisada para se manter atualizada frente às evoluções tecnológicas e às novas ameaças emergentes.

15. PLANO DE RESPOSTA À INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A NOVA possui um plano de resposta a incidentes de segurança que descreve as ações a serem tomadas para garantir a contenção rápida, eliminação da ameaça e recuperação após um incidente. O procedimento detalhado de resposta a incidentes está descrito no **ANEXO II – PROCEDIMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**. As etapas desse plano são:

15.1. Notificação: após a detecção de um incidente de segurança, a equipe de segurança deve comunicar à direção, em até 2 horas, para que a notificação ao contratante seja realizada dentro do prazo de 24 horas;

15.2. Identificação: o incidente será analisado para determinar sua natureza, sua origem e seu impacto.

15.3. Erradicação: as ameaças associadas ao incidente serão identificadas e eliminadas para evitar danos adicionais aos sistemas e dados da NOVA.

15.4. Recuperação: após a eliminação da ameaça, os sistemas afetados serão restaurados ao seu estado normal de funcionamento, e as operações da NOVA continuarão normalmente.

15.5. Mitigação: medidas corretivas serão implementadas para corrigir vulnerabilidades que possibilitaram o incidente e prevenir sua recorrência.

O plano é revisado e testado periodicamente para assegurar sua eficácia e conformidade com as exigências contratuais.

16. NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

Em caso de violação de dados pessoais, a NOVA adotará as seguintes medidas:

16.1. A NOVA notificará o contratante dentro de 24 horas após a constatação do incidente de violação de dados. A notificação incluirá:

16.1.1. Uma descrição clara da natureza da violação de dados, especificando quais tipos de dados foram comprometidos.

16.1.2. As consequências prováveis ou já realizadas decorrentes da violação.

16.1.3. Medidas corretivas imediatas adotadas para mitigar os danos, e ações para evitar a recorrência.

16.2. Canal de comunicação para reporte de incidentes pelo contratante:

Com o intuito de fortalecer a comunicação e agilizar a identificação de possíveis incidentes de segurança, a NOVA disponibiliza aos seus clientes um canal dedicado para a abertura de chamados, diretamente acessível na página inicial do *site* da NOVA. Esse canal foi desenvolvido para permitir que os clientes notifiquem, de forma rápida e segura, qualquer inconsistência percebida ou suspeita de violação de dados. A partir da notificação, a NOVA iniciará o processo de investigação para verificar a ocorrência e, se necessário, adotar as medidas cabíveis para mitigação e resolução do problema. As diretrizes para o uso desse canal são as seguintes:

I. **Acesso ao canal**: o canal de notificação estará disponível na página inicial do *site* da NOVA, acessível por meio de um formulário seguro, que permitirá aos clientes descreverem o incidente ou a inconsistência detectada.

II. **Informações necessárias**: o contratante deverá fornecer informações detalhadas sobre a suspeita de violação, incluindo:

a) Descrição do incidente ou da inconsistência observada.

b) Data e hora da ocorrência (se possível).

c) Dados ou sistemas afetados (se conhecidos).

III. **Confirmação de recebimento**: após o envio da notificação, o contratante receberá uma confirmação de recebimento, e a NOVA compromete-se a iniciar o processo de verificação do incidente em até 48 horas após o recebimento da notificação.

IV. **Processo de investigação**: todas as notificações enviadas por meio do canal de abertura de chamados serão analisadas pela equipe de segurança da NOVA, que tomará as medidas necessárias para identificar, conter e resolver o incidente reportado.

V. ***Link* do canal de comunicação**: https://canaldenunciacompliance.azurewebsites.net/

17. CÓPIAS DE SEGURANÇA E RECUPERAÇÃO

As definições e os parâmetros de realização de cópias de segurança e recuperação de informações devem considerar os seguintes critérios:

17.1. A natureza da informação (financeira, contratos com clientes, registros de acessos, entre outros) e a legislação vigente aplicável.

17.2. A necessidade do negócio e as definições do proprietário da informação.

17.3. Os requisitos de disponibilidade e os níveis de serviço acordados.

17.4. Os requisitos de segurança da informação.

18. USO DA INTERNET

Com o objetivo de estabelecer as diretrizes gerais para a utilização da Internet por meio dos ativos da empresa, utilizando-

se da rede corporativa ou das redes particulares, e garantir a proteção adequada das informações, os colaboradores ou as partes externas devem seguir as diretrizes a seguir, mas não se limitar a elas:

18.1. Todos os colaboradores ou partes externas devem utilizar a Internet de forma ética e profissional, sendo responsável por todas as ações realizadas por meio das credenciais de acesso disponibilizadas para seu uso.

18.2. Não é permitido/aceitável quaisquer acessos, transferência ou exibição de informações que possam ser consideradas pornográficas, eróticas, obscenas, discriminatórias, ilegais, ofensivas, perturbadoras, racistas, imorais, e que violem a legislação vigente, o direito de pessoas, empresas ou órgãos governamentais, inclusive os de propriedade intelectual, autorais, marcas, patentes e privacidade, bem como utilizar-se da Internet e de outros serviços disponibilizados com o intuito de cometer fraude.

18.3. O acesso à Internet deve ser utilizado apenas para as finalidades lícitas, éticas e autorizadas; portanto, a NOVA *não assume qualquer responsabilidade civil ou criminal pelo uso indevido* dela. A responsabilidade pelos atos é exclusiva do usuário responsável pela credencial de acesso.

18.4. Toda informação acessada ou transmitida está sujeita a auditorias, sem aviso prévio, e caso identificados desvios será passível de aplicação de penalidades de acordo com a gravidade, conforme normas internas existentes, contratos firmados, dispositivos constantes na Consolidação das Leis do Trabalho (CLT) ou em outros dispositivos legais cabíveis.

19. USO DE DISPOSITIVOS MÓVEIS

O uso de dispositivos móveis e outros equipamentos fornecidos pela NOVA é regido por normas e diretrizes específicas que garantem a proteção dos dados e o alinhamento às políticas de segurança da informação da empresa. A seguir, estão os requisitos para o uso adequado e seguro desses dispositivos, tanto no ambiente corporativo quanto fora dele:

19.1. REGRAS PARA USO DE DISPOSITIVOS MÓVEIS E EQUIPAMENTOS CORPORATIVOS:

19.1.1. Utilização permitida: dispositivos fornecidos pela NOVA são destinados exclusivamente a atividades profissionais. Seu uso para atividades pessoais ou que não estejam relacionadas ao trabalho é estritamente proibido.

19.1.2. Aprovação de aplicativos: é proibido instalar aplicativos ou *softwares* que não tenham sido previamente aprovados e homologados pela área técnica da NOVA. Somente a equipe de Tecnologia da Informação poderá realizar ou autorizar a instalação, manutenção e remoção de *softwares*.

19.1.3. Criptografia e segurança de dados: qualquer comunicação que contenha dados sensíveis da NOVA ou de seus clientes deve ser realizada usando métodos de comunicação criptografados e homologados pela NOVA, evitando o uso de aplicativos de terceiros, como o WhatsApp, para a comunicação de informações confidenciais.

19.2. MONITORAMENTO E ACESSO A DADOS EM DISPOSITIVOS DA NOVA: para garantir a segurança da informação e o cumprimento das normas internas, a NOVA reserva-se o direito de acessar e monitorar dispositivos e dados corporativos. Esse monitoramento aplica-se a:

19.2.1. Programas e aplicativos: a NOVA pode monitorar o uso de programas e aplicativos nos dispositivos fornecidos pela agência para verificar a conformidade com as políticas de segurança.

19.2.2. *E-mails* e comunicações: todas as comunicações, incluindo *e-mails* enviados e recebidos, estão sujeitas a monitoramento para prevenir vazamento e uso indevido de dados.

19.2.3. Tráfego de rede: dispositivos conectados à rede da NOVA podem ter seu tráfego monitorado, incluindo o acesso a recursos internos, com o objetivo de identificar e prevenir potenciais ameaças à segurança.

19.3. REGRAS PARA CONEXÃO DE DISPOSITIVOS EXTERNOS À REDE DA AGÊNCIA: qualquer dispositivo pessoal ou de terceiros conectado à rede da NOVA deve seguir as normas e políticas de segurança aplicáveis aos dispositivos corporativos, estando sujeito a monitoramento e verificação de conformidade, tais como:

19.3.1. Verificação de conformidade: a NOVA poderá inspecionar dispositivos externos conectados à sua rede para assegurar o cumprimento das políticas de segurança e evitar ameaças.

19.3.2. Monitoramento de tráfego: dispositivos conectados poderão ter seu tráfego monitorado para garantir que todas as atividades estejam em conformidade com os padrões de segurança da empresa.

19.3.3. Consentimento para monitoramento: colaboradores e terceiros, ao conectarem dispositivos externos à rede da NOVA, consentem automaticamente com o monitoramento enquanto esses dispositivos estiverem conectados, aceitando todas as políticas de segurança aplicáveis.

19.4. DISPOSIÇÕES GERAIS:

19.4.1. Responsabilidade pelo dispositivo: o colaborador é responsável por manter a integridade física e a segurança das informações contidas nos dispositivos móveis fornecidos pela NOVA, devendo comunicar imediatamente qualquer incidente de segurança ou perda do equipamento.

19.4.2. Sanções e penalidades: o uso inadequado dos dispositivos fornecidos pela NOVA, o descumprimento das diretrizes de uso e a violação das normas de segurança resultarão em medidas disciplinares, de acordo com as políticas internas e a legislação aplicável.

20. USO DE *SOFTWARE*

Com o objetivo de estabelecer as diretrizes para o uso adequado de *softwares* de propriedade ou sob custódia da NOVA. As regras abaixo devem ser seguidas, mas não se limitando a:

20.1. Apenas *softwares* homologados devem ser utilizados nos ativos de propriedade da NOVA.

20.2. *É proibida a instalação, desinstalação, parada de serviços nos dispositivos ou qualquer tipo de manutenção; apenas a área técnica da* NOVA tem autorização para realizar tais procedimentos.

21. CREDENCIAIS E SENHAS

Tem como objetivo estabelecer as regras de segurança para o gerenciamento e uso adequado das credenciais e senhas de acesso aos ativos da NOVA. As regras a seguir devem ser seguidas, mas não se limitando a elas:

21.1. As credenciais de acesso e senhas são individuais e intransferíveis e não podem ser reveladas ou compartilhadas.

21.2. O colaborador é responsável por todas as ações realizadas por meio das credenciais de acesso disponibilizadas para seu uso.

21.3. É proibido o uso de lembretes de senhas em blocos de notas, cadernos, planilhas ou em quaisquer outros meios passíveis de identificação (eletrônicos ou físicos). A confidencialidade relativa à não divulgação da senha é de responsabilidade exclusiva dos colaboradores e das partes externas.

21.4. A complexidade mínima de senhas a ser adotada nos sistemas da NOVA segue os padrões de mercado, incluindo os seguintes requisitos obrigatórios:

21.4.1. Quantidade mínima de 8 caracteres.

21.4.2. Deve conter letra maiúscula.

21.4.3. Deve conter letra minúscula.

21.4.4. Deve conter números.

21.4.5. Deve conter caracteres especiais (ex: !@#$%&*).

21.5. As senhas não devem conter:

21.5.1. Nomes próprios.

21.5.2. Datas.

21.5.3. Sequências crescentes ou decrescentes de letras ou números.

21.6. As regras de complexidade mínima de senha só podem ser descumpridas caso o sistema em questão não permita manter a complexidade solicitada.

22. USO DE CORREIO ELETRÔNICO

Com o objetivo de estabelecer as diretrizes de segurança para o uso adequado do correio eletrônico, as regras abaixo devem ser seguidas, mas não se limitando a:

22.1. Todo colaborador é responsável por qualquer informação trafegada e/ou armazenada através de sua conta de correio eletrônico.

22.2. O correio eletrônico deve ser utilizado apenas para envio de mensagens relacionadas ao negócio da NOVA, de forma legal e ética, de acordo com o código de conduta da empresa.

22.3. É proibido incluir ou divulgar o endereço de correio eletrônico da NOVA em listas de discussões, *chat*, notícias, *sites* de compras, entre outros.

22.4. É proibido divulgar, enviar, transmitir qualquer conteúdo que seja ilegal, difamatório, evasivo à privacidade, abusivo, ameaçador, prejudicial, vulgar, obsceno, ofensivo, preconceituoso ou de qualquer formal censurável.

22.5. É proibido o envio de arquivos anexos às mensagens, que possam infectar computadores e dispositivos móveis com vírus ou outros códigos maliciosos.

22.6. Ao receber *e-mails* caracterizados como *SPAM*, eles devem ser imediatamente reportados e encaminhados para o Lixo Eletrônico.

22.7. As credenciais de acesso à caixa de *e-mail* não devem ser compartilhadas. Tais credenciais são de uso exclusivo do colaborador, pessoal e intransferível.

23. CASOS OMISSOS

23.1. Toda e qualquer atividade que não seja claramente permitida é proibida. Em caso de dúvida, o colaborador deve consultar seu gestor ou a direção.
23.2. Cabe à direção avaliar os riscos das atividades não previstas nas políticas de segurança da NOVA.

24. ALEGAÇÃO DE DESCONHECIMENTO

24.1. Em nenhuma circunstância será permitido que colaboradores ou partes externas aleguem desconhecimento das diretrizes de segurança da informação como justificativa para violações ou descumprimentos dessas diretrizes, resultando na ocorrência de incidentes de segurança, sejam eles acidentais ou deliberados.
24.2. Todo e qualquer caso de descumprimento ou inobservância da documentação normativa será passível de aplicação de penalidades, conforme normas internas existentes, contratos firmados, dispositivos constantes na Consolidação das Leis do Trabalho (CLT) ou em outros dispositivos legais aplicáveis.

25. ANEXOS

ANEXO I – TERMO DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

Este documento formaliza o compromisso de colaboradores, parceiros e terceiros com a confidencialidade e a segurança das informações da NOVA. Ao assinar este termo, o signatário compromete-se a:

Manter sigilo: manter sigilo absoluto sobre quaisquer informações confidenciais às quais tiver acesso no exercício de suas funções. Informações confidenciais incluem, mas não se limitam a dados financeiros, estratégias de negócios, informações pessoais de clientes e colaboradores, e qualquer outra informação que a NOVA classifique como confidencial.

Cumprir políticas de segurança: cumprir integralmente as políticas internas de segurança da informação da NOVA, incluindo, mas não se limitando ao uso adequado de credenciais, dispositivos e sistemas. O signatário deve assegurar que suas ações não comprometam a segurança das informações.

Notificação de incidentes: notificar imediatamente a direção sobre qualquer incidente de segurança, seja ele suspeito ou confirmado, relacionado a informações sob sua responsabilidade. Exemplos de incidentes incluem acesso não autorizado, vazamento de informações e falhas de segurança em sistemas.

Responsabilidade: assumir total responsabilidade pelas consequências de qualquer violação de segurança causada por negligência ou descumprimento das diretrizes estabelecidas neste termo. O signatário reconhece que a violação das obrigações de confidencialidade pode resultar em sanções disciplinares, incluindo rescisão de contrato, e em ações legais, conforme a legislação vigente.

Sanções: sanções serão aplicadas em casos de descumprimento das obrigações aqui estabelecidas, de acordo com as normas internas da empresa e a legislação vigente. Tais sanções podem incluir advertências, suspensão, rescisão contratual e/ou ações judiciais, conforme a gravidade da infração.

ANEXO II – PROCEDIMENTO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Este anexo descreve o plano de resposta a incidentes de segurança que deve ser seguido em caso de violação da segurança da informação, conforme estabelecido na Seção 15 da Política de Segurança da Informação (Rev. 2):

Notificação inicial: qualquer incidente de segurança detectado deve ser comunicado à equipe de segurança da NOVA no prazo máximo de 2 (duas) horas após sua detecção. A notificação ao cliente ou contratante deverá ocorrer em até 24 (vinte e quatro) horas, conforme a natureza e a gravidade do incidente.

Identificação: a equipe de segurança da informação da NOVA realizará uma análise detalhada do incidente para determinar sua origem, sua natureza e seu impacto. Essa avaliação é fundamental para entender a extensão do problema e desenvolver uma resposta adequada.

Erradicação: medidas corretivas devem ser implementadas de forma imediata para eliminar a ameaça identificada e prevenir novos danos. Isso pode incluir a remoção de *malwares*, o bloqueio de acessos não autorizados e outras ações necessárias para garantir a segurança.

Recuperação: os sistemas afetados devem ser restaurados ao seu estado normal de operação o mais rápido possível, garantindo a continuidade dos serviços. A recuperação deve ser realizada de acordo com os procedimentos estabelecidos e com a supervisão adequada da equipe de segurança.

Mitigação: após a erradicação e recuperação, a equipe de segurança da informação implementará ações preventivas para evitar a recorrência do incidente. Isso pode incluir a atualização de sistemas, o reforço das medidas de segurança e o treinamento adicional para os colaboradores.

Revisão e testes: este procedimento deve ser revisado e testado periodicamente para garantir sua eficácia e adequação às novas ameaças e vulnerabilidades. A revisão incluirá a avaliação de incidentes anteriores e a atualização das práticas de resposta conforme necessário.

ANEXO III – CLÁUSULAS CONTRATUAIS DE SEGURANÇA DA INFORMAÇÃO

Estas cláusulas devem ser incluídas em todos os contratos firmados com terceiros que tenham acesso às informações da NOVA, assegurando o cumprimento das diretrizes de segurança da informação:

DA CONFIDENCIALIDADE

Compromisso de confidencialidade: a CONTRATADA obriga-se a manter todas as informações a que tiver acesso na execução do presente contrato em caráter de absoluta confidencialidade. Essa obrigação se estende a qualquer informação, documento, dado ou conhecimento que, por sua natureza, seja considerado confidencial.

Uso das informações: a CONTRATADA compromete-se a não divulgar, reproduzir ou utilizar as informações confidenciais a que tiver acesso, exceto para os fins específicos do presente contrato e em conformidade com as instruções da CONTRATANTE.

Acesso às informações: a CONTRATADA deverá restringir o acesso às informações recebidas apenas aos seus empregados e consultores que estiverem diretamente envolvidos na execução do presente contrato e que necessitem desse acesso para o desempenho de suas funções. A CONTRATADA deve assegurar que todos os envolvidos estejam cientes e concordem com os termos de confidencialidade estabelecidos neste documento.

Devolução de informações: ao término da vigência do contrato, a CONTRATADA compromete-se a devolver ou destruir, de forma imediata e completa, todos os documentos e materiais que contenham informações confidenciais, incluindo cópias, resumos ou qualquer outro suporte em que tais informações estejam registradas.

Duração do compromisso: a obrigação de confidencialidade da CONTRATADA permanecerá em vigor durante a vigência do contrato e se estenderá por um período de cinco (5) anos após a sua rescisão, independentemente do motivo.

Responsabilidade por violação: a CONTRATADA reconhece que a violação de quaisquer disposições deste anexo poderá resultar em danos irreparáveis à CONTRATANTE. Assim, a CONTRATADA concorda que, em caso de descumprimento, a CONTRATANTE terá o direito de buscar medidas cautelares, além de outros recursos legais disponíveis.

Exceções à confidencialidade: o dever de sigilo não se aplicará a informações que: (i) sejam ou se tornem de domínio público sem violação deste contrato; (ii) tenham sido legitimamente recebidas de terceiros sem obrigação de confidencialidade; ou (iii) sejam exigidas por lei, regulamento ou ordem judicial, desde que a Parte que deve divulgar a informação notifique a outra Parte previamente, permitindo que esta tome as medidas adequadas para proteger a informação.

DAS MEDIDAS DE SEGURANÇA

A CONTRATADA compromete-se a adotar todas as medidas técnicas e organizacionais necessárias para garantir a segurança das informações recebidas, conforme exigido pela NOVA. Essas medidas devem incluir, mas não se limitar a, controles de acesso, criptografia e procedimentos de segurança física e lógica.

DAS AUDITORIAS

Direito de auditoria: a NOVA se reserva o direito de realizar auditorias periódicas e/ou extraordinárias para verificar o cumprimento das diretrizes de segurança estabelecidas neste Anexo. A CONTRATADA deverá fornecer acesso irrestrito a todas as informações e aos documentos necessários para a realização dessas auditorias.

Relatórios de auditoria: a CONTRATADA compromete-se a apresentar relatórios detalhados sobre a segurança da informação, sempre que solicitado pela NOVA, incluindo informações sobre incidentes de segurança, medidas corretivas adotadas e quaisquer outros dados que demonstrem conformidade com as políticas de segurança.

DAS CONSEQUÊNCIAS DE VIOLAÇÃO

Em caso de descumprimento das obrigações contratuais, poderão ser aplicadas sanções, que incluem, mas não se limitam a, rescisão contratual, indenização por danos diretos e indiretos, e obrigação de reparar qualquer dano causado à NOVA ou a terceiros.

ANEXO IV – AUDITORIAS E RELATÓRIOS DE SEGURANÇA DA INFORMAÇÃO

Este anexo define as diretrizes para auditorias e relatórios de segurança mencionados na Seção 10 da Política de Segurança da Informação (Rev. 2), estabelecendo as seguintes diretrizes:

Periodicidade das auditorias: auditorias de segurança da informação devem ser realizadas, no mínimo, uma vez ao ano. No entanto, auditorias adicionais poderão ser realizadas conforme solicitado por clientes, partes interessadas ou em resposta a incidentes de segurança.

Notificação prévia: a NOVA deverá notificar ao contratante com antecedência mínima de trinta (30) dias sobre a realização de auditorias programadas, permitindo tempo suficiente para a preparação e organização dos documentos necessários.

Informações dos relatórios: os relatórios de auditoria devem incluir, mas não se limitar a:

- Avaliação das medidas de segurança implementadas e sua eficácia.
- Resultados de auditorias anteriores, incluindo questões identificadas e o *status* das ações corretivas.
- Ações corretivas aplicadas em resposta a qualquer não conformidade identificada durante a auditoria.
- Recomendações para melhorias nas práticas de segurança da informação.

Formato dos relatórios: os relatórios devem ser apresentados em um formato claro e compreensível, com a inclusão de gráficos,

tabelas e outros recursos visuais que facilitem a análise das informações apresentadas;

Processo de revisão de relatórios: todos os relatórios devem ser revisados pela equipe de segurança da informação da NOVA. A revisão deve incluir a verificação da precisão das informações, a consistência dos dados apresentados e a adequação das ações corretivas propostas.

Aprovação pela direção: após a revisão, os relatórios devem ser submetidos à aprovação da direção da NOVA antes de serem compartilhados com terceiros, garantindo que todos os resultados e as recomendações sejam validados pelas partes responsáveis.

Registro de incidentes de segurança: qualquer incidente de segurança identificado, independentemente de sua gravidade, deve ser documentado detalhadamente. A documentação deve incluir:

- Descrição do incidente.
- Data e hora do ocorrido.
- Impacto na segurança da informação.
- Medidas corretivas adotadas para mitigar os efeitos do incidente e evitar recorrências.

Inclusão nos relatórios: as informações sobre incidentes de segurança documentados devem ser incluídas nos relatórios de auditoria, garantindo que a NOVA tenha uma visão abrangente da eficácia das medidas de segurança implementadas.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

/SP
Rua Nazaré Paulista, 297
05448-000 • São Paulo/SP
+55 11 3066-5400

/DF
SCN Quadra 2 • Bloco A • 7º andar
Ed. Corporate Financial Center
70712-900 • Brasília/DF
+55 61 3329-8200

/RJ
Rua México, 3 • Ed. Civitas A • 19º andar
20031-903 • Rio de Janeiro/RJ
+55 21 3554-1720

/MT
Av. André Antônio Maggi, 487 • Sala 1.004
Loteamento Parque Eldorado
78049-080 • Cuiabá/MT
+55 65 4052-9180/9186/9187

NOVA