POLÍTICA DE SEGURANÇA CIBERNÉTICA

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

SUMÁRIO

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

1. OBJETIVO

Esta política tem como objetivo estabelecer as diretrizes necessárias para assegurar a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas de informação utilizados pela **Credi Nestlé** e direcionar um programa efetivo de prevenção, detecção e redução de impactos gerados pelos incidentes relacionados ao ambiente cibernético, em conformidade com as melhores práticas de mercado e legislação aplicada.

É objetivo desta política, ademais, estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética.

2. ABRANGÊNCIA

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores, parceiros e fornecedores da **Credi Nestlé**.

3. DEFINIÇÕES

Backup ou Salvaguarda: Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada.

Colaborador: Empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venham a ter relacionamento profissional, direta ou indiretamente com a organização.

Confidencialidade: Garantia de que a informação é acessível apenas para pessoas ou processos devidamente autorizados.

Disponibilidade: Garantia de que usuários ou processos devidamente autorizados tenham acesso à informação e aos recursos associados sempre que forem requisitados.

Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

Informação: É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

Integridade: Garantia quanto à exatidão da informação, sem quebras e sem alterações não autorizadas, e dos respectivos métodos de processamento. Refere-se à confiabilidade.

Internet: Rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente.

Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC): hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

Risco: Combinação dos impactos advindos da ocorrência de um evento indesejado relacionado à segurança da informação e da probabilidade de sua ocorrência.

Segurança da informação: É a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

4. PRINCÍPIOS DE SEGURANÇA CIBERNÉTICA

4.1. Confidencialidade: Garantir de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento de terceiros não autorizados;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

4.2. Integridade: Garantir que a informação seja mantida em seu estado original, visando protegê-la, no armazenamento ou transmissão, contra alterações indevidas, intencionais ou acidentais;

4.3. Disponibilidade: Garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário.

5. DIRETRIZES GERAIS

5.1. Avaliação de Riscos Cibernéticos de Produtos ou Serviços

a) Compreender os riscos da segurança cibernética associados à condução do negócio e administrar esses riscos de forma eficaz são a base para uma gestão da segurança eficiente.

b) Os riscos devem ser avaliados e administrados pela Gerência Administrativa em conjunto com o diretor responsável pela Política de Segurança Cibernética da **Credi Nestlé**, bem como os controles de proteção e as respostas, proporcionais aos riscos identificados.

c) A Gerência Administrativa, apoiada pela Área de Segurança da Informação da apoiadora Nestlé, deve ser envolvida nas recomendações sobre controles e proteções de segurança cibernética no desenvolvimento de novos produtos ou serviços da **Credi Nestlé** bem como na avaliação de riscos, buscando identificar ameaças e impactos sobre os ativos de informação.

5.2. Classificação da Informação

A informação é um importante ativo da **Credi Nestlé** e deve ser preservada e salvaguardada, em conformidade com suas políticas, normas, procedimentos e controles internos, bem como, com as leis e regulamentos dos órgãos reguladores e autorreguladores sobre o tema. As informações devem ser classificadas e tratadas de acordo com os requisitos especificados no Norma para Classificação da Informação da **Credi Nestlé**

5.3. Proteção de Dados e Privacidade

A **Credi Nestlé** tem o compromisso de promover a aderência às leis de privacidade e de proteção de dados pessoais de seus clientes.

A **Credi Nestlé** compartilha o seu compromisso com tais questões junto aos seus colaboradores.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

A proteção de dados e da privacidade das pessoas naturais devem ser administradas em conformidade com a com os requisitos especificados em todo o conjunto Normativo de Políticas e Procedimentos da **Credi Nestlé** bem como, nas leis e regulamentos de órgãos reguladores e autorreguladores sobre o tema.

A **Credi Nestlé** visa garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, por meio de:

a) Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente;

b) Adoção de medidas de segurança para proteger os dados pessoais de acesso não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito;

c) Armazenamento de modo seguro, controlado e protegido;

d) Processos de anonimização e pseudonimização, sempre que necessário;

e) Protocolos de criptografia na transmissão e armazenamento, sempre que necessário;

f) Registro lógico das operações de tratamento;

g) Descarte seguro dos dados pessoais ao término de sua finalidade e sua conservação de acordo com as hipóteses legais e regulatórias;

h) Transferência à terceiros de modo seguro e contratualmente previsto;

i) Avaliação de impacto e sistemática à privacidade dos titulares de dados;

j) Gestão e tratamento adequado de incidentes que envolvam dados pessoais;

k) Testes, monitoramento e avaliações periódicas de sua efetividade.

5.4. Gestão de Identidades, Acessos e senhas

A **Credi Nestlé** controla o acesso físico e lógico aos seus ambientes, dados e dispositivos, identificando cada Colaborador com uma identidade digital de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo, para que tenha o acesso a tais ativos adequadamente.

A **Credi Nestlé** faz a gestão de senhas em seus ambientes, desde o armazenamento, troca e definição de senhas padrão.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

5.5. Acesso físico aos data centers

Controles devem ser implementados nos data centers para proteger as informações e as instalações corporativas contra acesso físico não autorizado bem como contra danos. O acesso físico aos data centers deve ser realizado somente após autorização e autenticação da pessoa para acessar o local, sendo formalizado o seu acesso pela Área de Tecnologia da Informação da Nestlé.

5.6. Proteção da rede, informações e sistemas

Visando assegurar a proteção das informações bem como a confiabilidade e qualidade dos serviços e sistemas da **Credi Nestlé**, os seguintes mecanismos devem ser adotados:

a) Sistemas de rede virtual;

b) Monitoramento do volume de dados trafegados;

c) Gestão e resposta na identificação de picos de tráfego e uso de portas “incomuns” na rede;

d) Isolamento de redes ou sistemas na identificação de uma atividade “incomum”;

e) Monitoramento de atividades por ponto de inteligência na rede, como filtros de pacote e mensagens;

f) Grupos com direitos em comum;

g) Restrição de horário de “login”;

h) Sistemas de detecção e prevenção de intrusão.

A Gerência Administrativa da cooperativa, em consonância com as diretrizes estabelecidas pela Área de Segurança das Informações da Nestlé, deve estabelecer procedimentos de controles na rede corporativa da **Credi Nestlé** contra acessos não autorizados por tecnologias devidamente atualizadas, revisadas e testadas periodicamente de forma independente.

5.7. Acesso externo (remoto)

Os procedimentos internos para Gestão de Identidade e Controle de Acessos devem estabelecer controles que visam a obrigatoriedade de autenticação individual, a aprovação prévia de Gestor competente e o seu monitoramento. As tentativas de uso indevido devem ser imediatamente registradas como incidente de segurança.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

a) Acessos administrativos realizados de forma remota devem possuir fator duplo de autenticação.

b) Serviços de rede terceirizados

c) Em caso de terceirização, deve ser estabelecido procedimento de análise de redes visando documentar e analisar os serviços de rede de terceiros sob o ponto de vista de segurança.

5.8. Gestão de dispositivos e inventário de ativos

Os equipamentos, mídias, licenças de software, ou qualquer outro ativo de informação da **Credi Nestlé** não podem ser retirados sem autorização do Gestor responsável. Os ativos devem ser transportados em condições adequadas que assegurem a integridade física e lógica do material.

A **Credi Nestlé** deve estabelecer e avaliar os requisitos de segurança cibernética nos processos de aquisição, operação, manutenção e descarte de ativos corporativos (hardware ou software), de acordo com as melhores práticas do setor para garantir a sua disponibilidade, a integridade e confidencialidade dos dados armazenados ou transmitidos por eles.

5.9. Controles dos recursos de tecnologia

Os recursos de tecnologia utilizados pelos colaboradores, sejam eles móveis ou não, e com possibilidade de envio de informações por mensagens, voz ou dados, devem ser protegidos por controles de prevenção ao vazamento de dados.

Os recursos de tecnologia devem ser configurados de acordo com a última atualização de segurança fornecida pelo fabricante, homologados pela Área de Segurança da Informação da apoiadora Nestlé e aplicados pela Área de Tecnologia da Informação, para que não seja possível que os colaboradores de tais recursos de tecnologia, sem auxílio do usuário administrador, desabilitem as configurações de segurança.

5.10. Proteção de Informações e Criptografia

Os recursos de tecnologia portáteis ou transportáveis que contenham informação confidencial devem possuir ferramentas de criptografia ativas e configuradas de acordo com normas e procedimentos internos da **Credi Nestlé.**

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

5.11. Monitoramento

Os ambientes físicos e lógicos da **Credi Nestlé** devem ser monitorados visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança cibernética.

5.12. Cópia de Segurança

Os usuários devem ser orientados e controles devem ser estabelecidos pela Gerência Administrativa da cooperativa, apoiada pela Área de Segurança da Informação para execução de cópias de segurança das informações armazenadas em computadores portáteis sob sua responsabilidade.

5.13. Governança de servidores e sistemas

A **Credi Nestlé** deve ter procedimento de monitoramento de seu ambiente para controlar a infraestrutura de TI, bem como a performance e a capacidade de processamento atual dela.

5.14. Controles lógicos na camada de servidores

Para proteger os servidores utilizados, a **Credi Nestlé** segue integralmente as regras estabelecidas pela àrea de Segurança de Informação da empresa apoiadora Nestlé, no que tange a formalizar controles contra acesso não autorizado e armazenamento indevido, em especial:

a) Configuração, incluindo sistemas operacionais, de acordo com um as orientações da Área de Segurança da Informação;

b) Testar e implementar as atualizações de segurança (patches) no sistema operacional e demais sistemas instalados no servidor e assegurar que estejam aptos para atualizar, sempre que novos patches estejam disponíveis;

c) Monitorar o desempenho de segurança por meio de revisões regulares das trilhas de auditoria;

d) Estabelecer revisões periódicas nas configurações de segurança;

e) Implementar e executar controles contra softwares maliciosos;

f) Verificar periodicamente a inclusão de conteúdo indevido;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

g) realizar periodicamente avaliações de vulnerabilidade e testes de segurança nos sistemas implementados no servidor visando à manutenção da segurança do ambiente.

5.15. Gestão de vulnerabilidades

A Gerência Administrativa da cooperativa, apoiada pela Área de Segurança da Informação Nestlé deve avaliar, analisar e documentar as vulnerabilidades em seus sistemas relevantes, bem como comunicar os responsáveis e cobrar a correção das vulnerabilidades identificadas.

5.16. Gestão de mudança

O andamento e o resultado de uma mudança em sistema relevante ou em infraestrutura tecnológica relevante, devem zelar pela preservação dos controles relacionados à disponibilidade, integridade, confidencialidade e autenticidade dos dados, devendo ser realizados ou administradas pela Gerência Administrativa da cooperativa, apoiada pela Área de Segurança da Informação Nestlé , conforme procedimentos internos.

Qualquer alteração em sistema relevante deve ser sistematicamente planejada, aprovada, testada e documentada pela Área de Tecnologia da Informação e acompanhada pela Área de Segurança da Informação, ambas da Nestlé, conforme procedimentos internos.

5.17. Gestão de configuração de segurança

A Gerência Administrativa da cooperativa, apoiada pela Área de Segurança da Informação Nestlé deve estabelecer e monitorar se as configurações básicas de segurança, controle e monitoramento a fim de verificar se foram aplicadas de modo adequado.

Backup e Restore

A **Credi Nestlé** deve manter processo de salvaguarda dos dados necessários para completa recuperação dos seus sistemas relevantes, a fim de atender aos requisitos operacionais e legais, assegurar a continuidade do negócio em caso de falhas ou incidentes, além de auxiliar em sua ágil recuperação conforme definido em procedimentos internos.

A execução e gestão dos procedimentos de salvaguarda devem ser realizados conforme os requisitos especificados em procedimentos internos.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

5.18. Aquisição, desenvolvimento e manutenção de sistemas

O desenvolvimento interno e externo de softwares, tal qual aquisição destes no mercado devem garantir o cumprimento dos requisitos de segurança da informação e controles de acesso previstos nesta Política e demais normativos internos de Segurança da Informação da **Credi Nestlé** além de serem realizadas somente pela Área de Tecnologia da Informação

5.19. Continuidade do negócio

As informações confidenciais e sistemas relevantes devem ser assegurados de erros ou perdas por meio de um plano de continuidade do negócio, cópias de segurança e planos de contingência que contemplará cenários de incidentes relevantes a serem considerados nos testes de continuidade de negócios.

5.20. Gestão de prestadores de serviços de Tecnologia relevantes

A **Credi Nestlé** deve estabelecer controles de segurança apropriados para assegurar que as informações tratadas por seus fornecedores estejam devidamente protegidas, de acordo com instruções estabelecidos em normativos internos.

5.21. Monitoramento e inspeção

A Gerência de Administrativa e, se necessário, com o apoio de outras áreas da empresa apoiadora Nestlé, pode monitorar ou inspecionar os recursos de tecnologia que estiverem em suas dependências ou que interajam com os ambientes lógicos da **Credi Nestlé** sempre que considerar necessário, atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores.

5.22. Registro e resposta de incidente

A resposta a um incidente deve ser administrada de acordo com os critérios e parâmetros adotados na avaliação de um incidente bem como estabelecer um canal de comunicação para os colaboradores reportarem possíveis casos de incidentes de segurança cibernética.

O registro de um incidente relevante deve conter a análise da causa do incidente, o impacto do incidente e os efeitos gerados pelo incidente para operação da **Credi Nestlé.**

A **Credi Nestlé** deve acompanhar e avaliar as iniciativas criadas que visam o compartilhamento de informações sobre os incidentes relevantes com órgãos regulatórios.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

5.23. Plano de Ação

A Gerência Administrativa da cooperativa deve manter o Plano de Ação que contemple as ações a serem desenvolvidas pela **Credi Nestlé** visando adequar as estruturas organizacionais e operacionais bem como as rotinas, procedimentos, controles e tecnologias a serem utilizados na prevenção e no tratamento de incidentes, de acordo com os princípios e às diretrizes estabelecidas nesta política. Este plano foi desenvolvido e pode ser encontrado no item 7 do presente documento.

Este Plano deve ser revisado anualmente para garantir sua aplicabilidade ao ambiente da **Credi Nestlé**

5.24. Exceções

As exceções devem ser tratadas caso a caso, devendo ser temporárias e aprovadas previamente pelo Conselho de Administração da cooperativa para surtirem efeito.

As solicitações de exceção devem ser encaminhadas por escrito pelo Gestor do Colaborador e, quando pertinente, remetidas à Conselho de Administração da cooperativa para análise de sua viabilidade.

As exceções podem ser revogadas a qualquer tempo por mera liberalidade do Gestor do Colaborador ou do Conselho de Administração da cooperativa , devendo as áreas envolvidas serem comunicadas para a efetiva implementação das medidas necessárias, sob pena de responsabilização de quem se omitiu de eventuais prejuízos sofridos pela **Credi Nestlé**, seus clientes ou terceiros.

5.25. Dúvidas

Qualquer dúvida relativa a esta Política deve ser encaminhada à Gerência Administrativa da cooperativa por meio do endereço eletrônico: protecaodedados11@br.nestle.com

5.26. Revisão e Atualização

A Política deve ser revisada, no mínimo, anualmente pela Gerência Administrativa da cooperativa, ou sempre que existir a necessidade de alterações nos critérios definidos na Política e normas específicas.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

5.27. Alterações

As alterações desta Política e das normas complementares devem ser devidamente comunicadas aos colaboradores.

6. CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

6.1. Treinamento de segurança da informação

A **Credi Nestlé** deve estabelecer e manter um plano anual de capacitação direcionado ao desenvolvimento e manutenção das habilidades dos colaboradores em relação à segurança cibernética.

A **Credi Nestlé** deve aplicar testes periódicos para determinar a aderência e cumprimento desta Política e demais normas de segurança cibernética junto aos seus colaboradores.

6.2. Orientações sobre segurança da informação

A **Credi Nestlé** tem o dever de orientar seus clientes na utilização de seus produtos e serviços, bem como de determinadas precauções relacionadas ao ambiente cibernético na utilização de seus produtos e serviços, disponibilizando publicamente e divulgando os dados de contato para eventuais dúvidas.

A **Credi Nestlé** deve disponibilizar aos seus clientes uma versão resumida com linhas gerais desta política.

7. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA

7.1. Equipe de Resposta ao Incidente

A Equipe de Resposta ao incidente será composta de representantes da Credi Nestlé, preferencialmente com cargo de gestão (gerente e coordenadores) e representantes da equipe de IT Nestlé – Cyber Security.

7.2. Identificação do Incidente

Consiste em detectar ou identificar de fato a existência de um incidente de segurança Cibernética. A Equipe de Resposta ao Incidente baseia-se na identificação de incidentes internos ou externos, seja na detecção de alertas provenientes dos sistemas de monitoramento da rede da **Credi Nestlé** ou por notificações realizadas por qualquer pessoa relatando ser de

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

seu conhecimento ou mesmo vítima de atividade suspeita ou em desacordo com a Política de Segurança Cibernética.

As notificações internas ou externas devem ser realizadas por meio de:

a) Registro de Denúncia ou suspeita de incidente no e-mail: protecaodedados11@br.nestle.com ou telefone: (11) 5102.1849.

b) Registro de chamado através do Rise Webform: 

Ou acesso pelo link: Reporting Information Security Events - Portal do Serviço (service-now.com)

Toda notificação ou denúncia deve ser formalmente registrada pela Gerência Administrativa – Credi Nestlé. Este registro deve estar associado a alguma referência numérica (ID único) para que possa ser gerenciado pela Equipe de Resposta ao Incidente, conforme modelo de formulário.

7.3. Triagem do Incidente

Etapa onde a Equipe de Resposta ao Incidente deve realizar a análise inicial do evento, notificação ou denúncia visando a sua confirmação como incidente e classificando a sua relevância sobre as atividades da **Credi Nestlé**. Nesta Etapa deve ser identificados os sintomas do evento, suas características e os potenciais danos causados.

Confirmado que um incidente foi detectado, ele deve ser analisado antes de qualquer ação seja tomada, principalmente para confirmar se é um incidente válido.

7.4. Análise do Incidente

A análise realizada pela Equipe de Resposta ao Incidente consiste na coleta, aquisição e análise de dados, informações e demais evidências sobre o incidente para investigar o ativo de rede ou sistema de informação que gerou o incidente detectado ou denunciado.

Essa investigação passa pela identificação de ativos compreendendo endereços IP, endereços MAC da interface de rede, nomes, switches. Essas informações devem ser levantadas pelas trilhas de auditoria dos diversos sistemas e serviços disponíveis pela **Credi Nestlé.**

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

7.5. Categorização e Priorização do Incidente

Confirmado o incidente, a Equipe de Resposta ao Incidente deve categorizar e priorizar com base: (i) no impacto potencial que pode ter sobre a Credi Nestlé; (ii) no tempo e recursos necessários para recuperar ativos impactados. O impacto potencial deve ser identificado com base na tabela indentificada na Política de Segurança da Informação da Credi Nestlé.

Todo incidente categorizado como sendo de severidade crítica deve ser notificado imediatamente ao Diretor de Riscos Cibernéticos, que pode realizar a escalação deste incidente e realizar a alocação dos profissionais necessários para resolução do incidente.

Caso o incidente detectado envolva ou tenha a suspeita de envolver o tratamento não autorizado de dados pessoais, a Equipe de Resposta ao Incidente deve notificar imediatamente o Encarregado pelo Tratamento de Dados Pessoais (DPO) para avaliar se o incidente informado se trata de uma violação de dados pessoais.

Confirmado que o incidente é uma violação de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais (DPO) deve ser adicionado na Equipe de Resposta ao Incidente para orientar e acompanhar as medidas a serem tomadas.

Se mais de um incidente estiver ocorrendo ao mesmo tempo, os incidentes devem ser priorizados, pois não haverá o tempo e recursos para atuar simultaneamente.

Nesta etapa, a Equipe de Resposta ao Incidente deve apresentar as ações que serão priorizadas com base na categoria e no impacto do cenário encontrado e realizar as comunicações necessárias.

7.6. Mitigação do Incidente

Etapa que busca a solução do incidente por meio de um ciclo básico composto pelas seguintes fases: (i) análise dos dados, (ii) pesquisa de solução, (iii) ação proposta e realizada (contenção), (iv) comunicação, (v) solução efetiva ou de contorno e (vi) recuperação do ambiente.

7.7. Contenção do Incidente

Devem ser realizados procedimentos iniciais para contenção do incidente visando evitar a sua propagação e posteriormente em restabelecer o ativo, mesmo que com uma solução temporária, até que a solução definitiva seja implementada.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

A Equipe de Resposta ao Incidente deve assegurar que as comunicações com Partes Internas e Externas Interessadas ocorram no momento oportuno e estejam coordenadas de acordo com as diretrizes de gestão de crises da **Credi Nestlé.** As Partes Interessadas Internas devem ser informadas sobre as ações que precisam ser realizadas durante o estágio de recuperação.

7.8. Identificação de Causa e Solução

A Equipe de Resposta ao Incidente deve buscar a solução definitiva, ou seja, identificar a causa raiz de um incidente e eliminá-lo para assegurar que o ativo esteja seguro e confiável para que os procedimentos de recuperação sejam iniciados. A Equipe de Resposta ao Incidente pode solicitar o envolvimento e suporte das demais Áreas da **Credi Nestlé** afetadas para assegurar que os vetores do incidente sejam solucionados.

A Equipe de Resposta ao Incidente deve acompanhar os processos de recuperação dos ativos até o pleno funcionamento.

Os sistemas relevantes da **Credi Nestlé** devem retomar a funcionalidade básica de modo prioritário. As interdependências sistêmicas também devem ser conhecidas, já que alguns sistemas só podem ser recuperados após outros.

Durante a recuperação, os sistemas devem ser reconstruídos, reinstalados ou restaurados pela área de TI usando dados de backup e sistemas e patches atualizados, se necessário com apoio da Equipe de Resposta ao Incidente. Os sistemas recuperados devem ser testados e monitorados para assegurar que não ocorra novamente o incidente e que os ativos estejam funcionando de modo adequado.

7.9. Resposta ao Incidente

Equipe de Resposta ao Incidente deve documentar e arquivar as conclusões do tratamento do incidente, descrevendo:

a) o que aconteceu;

b) como o incidente foi detectado, ou seja, foi relatado por pessoal natural ou por um alerta de sistema automatizado;

c) as etapas tomadas pela Equipe de Resposta ao Incidentea partir da detecção do evento até o estágio de recuperação dos ativos;

d) o status do incidente à medida que ele se move ao longo do processo de solução;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

e) qualquer dado que seja coletado durante o processo de solução que possa ser usado como evidência;

f) definir a categorização final do incidente;

g) comentários e sugestões da Equipe de Resposta ao Incidente.

Esta documentação deve servir como referência para pós-incidente.

A coleta e preservação de prova na etapa de solução do incidente, bem como dados e informações que possibilitaram a identificação do incidente são importantes e devem ser documentadas no registro final do incidente. A coleta de provas deve ser avaliada conforme a necessidade pela Equipe de Resposta ao Incidente, devendo acionar o Jurídico em caso de dúvidas quanto à sua necessidade.

Quando um incidente for categorizado como severidade crítica deve ser realizada a coleta e preservação das provas envolvidas.

7.10. Ações pós-incidente

A etapa de pós incidente tem o seu início após a resolução e encerramento do incidente, onde serão analisadas pela Equipe de Resposta ao Incidenteas causas que motivaram a sua ocorrência e quais são as medidas que podem ser tomadas com objetivo que o fato não ocorra novamente.

O objetivo desta etapa é melhorar os procedimentos realizados na etapa de resposta e aprimorar os ativos para protegê-los de futuros incidentes.

A Equipe de Resposta ao Incidente deve comunicar as partes interessadas do resultado da análise.

Os incidentes ocorridos devem ser analisados em conjunto com os procedimentos de continuidade de negócio e governança de dados pessoais da **Credi Nestlé**. Esta análise visa identificar aprimoramento dos indicadores de probabilidade e consequência dos incidentes previstos e as ocorrências reais de incidentes.

Com base no relatório e nas informações obtidas durante a solução do incidente, a Equipe de Resposta ao Incidente deve criar um plano de ação que incluam os responsáveis, datas de

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

vencimento e entregas para garantir que todas as partes interessadas saibam o que se espera delas. As ações devem ser categorizadas como curto ou longo prazo.

8. RELATÓRIO ANUAL SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO DE RESPOSTA A INCIDENTES

A Equipe de Resposta a Incidentes em conjunto com o DPO e com apoio das áreas relacionadas elaborarão um relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro.

O relatório deverá conter, no mínimo:

a) a efetividade da implementação das ações descritas no Plano de Resposta a Incidentes de Segurança Cibernética (item 7);

b) o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

c) os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

d) os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório deverá ser apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição até 31 de março do ano seguinte ao da data-base.

9. RESPONSABILIDADES

9.1. Conselho de Administração/Diretoria Executiva

Aprovar a política de segurança cibernética e suas atualizações.

9.2. Diretor Responsável pela Política de Segurança Cibernética

a) Analisar, aprovar e declarar formalmente o seu comprometimento com esta política e assuntos relacionados à segurança cibernética;

b) Apoiar na divulgação da política de segurança cibernética;

c) Aprovar os investimentos em segurança cibernética, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

d) Analisar e deliberar sobre as recomendações apresentadas nos relatórios de incidentes de segurança cibernética;

e) Auxiliar, sempre que necessário, a Gerência Administrativa da cooperativa junto ao na capacitação dos colaboradores em segurança cibernética;

f) Aprovar o Plano de ação e o Procedimento de tratamento de incidentes em segurança da informação elaborados pela Gerência Administrativa da cooperativa;

g) Aprovar o relatório anual sobre a implementação do plano de ação e de respostas a incidentes elaborado pela Gerência Administrativa da cooperativa;

h) Analisar e deliberar a respeito de situações de exceção a essa política.

9.3. Comitê de Privacidade de Dados

a) Promover a cultura de segurança cibernética;

b) Analisar e recomendar ações necessárias, balanceando custo e benefício, sempre que acionado;

c) Apoiar, quando acionado, o Diretor Responsável pela Política de Segurança Cibernética na análise e deliberações sobre demandas relacionadas à segurança cibernética;

d) Orientar para que as atividades desempenhadas pela Gerência Administrativa da cooperativa estejam adequadas ao negócio, quando acionado.

9.4. Gerência Administrativa

a) Fazer cumprir esta política e demais documentos complementares por todos os colaboradores da **Credi Nestlé.**

b) Propor, junto ao Diretor Responsável pela Política de Segurança Cibernética as normas relativas à segurança cibernética;

c) Identificar e avaliar os riscos relacionados à segurança cibernética e propor melhorias e recursos necessários às ações de segurança cibernética;

d) Recomendar investimentos em segurança cibernética ao Diretor Responsável pela Política de Segurança Cibernética, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio;

e) Definir, analisar e priorizar ações necessárias, balanceando custo e benefício;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

f) Realizar e acompanhar estudos de tecnologias quanto a possíveis impactos na segurança cibernética;

g) Avaliar riscos e apresentar recomendações sobre controles e proteções de segurança cibernética no desenvolvimento de novos produtos ou serviços relevantes à Área de TI da empresa apoiadora Nestlé, quando demandada;

h) Analisar os incidentes de segurança cibernética reportados e submeter relatório para deliberação ao Diretor Responsável pela Política de Segurança Cibernética, sempre que necessário;

i) Instituir mecanismos de acompanhamento e controle visando assegurar a implementação e a efetividade desta política, do plano de ação e de resposta a incidentes;

j) Estabelecer e monitorar se as configurações básicas de segurança, de controle e de monitoramento nos recursos estão aplicadas de modo adequado pelas áreas responsáveis;

k) Estabelecer e acompanhar os requisitos para contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;

l) Avaliar e acompanhar se os requisitos de segurança cibernética estão presentes na aquisição sistemas relevantes;

m) Acompanhar a manutenção dos requisitos de segurança nas alterações dos sistemas relevantes realizados ou sob supervisão pela Área de TI da empresa apoiadora;

n) Disponibilizar e realizar a gestão das identidades digitais de acesso ao ambiente lógico;

o) Realizar o registro e o monitoramento dos acessos aos ambientes lógicos;

p) Estabelecer plano de ação e o procedimento de tratamento de incidentes e submetê-los à aprovação da Diretoria Executiva da cooperativa;

q) Elaborar relatório anual sobre a implementação do plano de ação e de respostas a incidentes;

r) Auxiliar a Gerência Administrativa na capacitação dos colaboradores em segurança cibernética;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

s) Elaborar conteúdo para avaliações periódicas a ser realizada pela Gerência Administrativa visando a identificação do nível de conscientização e cumprimento desta política e demais normas de segurança cibernética pelos colaboradores;

t) Apoiar, quando couber, procedimento disciplinar para apuração de responsabilidades dos envolvidos em violações de segurança cibernética junto à Auditoria Interna;

u) Auxiliar a Unidade de Governança e Compliance na elaboração de cenários de incidentes cibernéticos bem como na manutenção do plano de continuidade de negócios com os requisitos de segurança cibernética para avaliação da relevância dos incidentes, do fluxo de acionamento e dos testes periódicos para continuidade de negócio.

v) Realizar a gestão, manutenção e administração dos recursos de tecnologia de propriedade ou sob a responsabilidade da Credi Nestlé;

w) Assegurar que os recursos de tecnologia relevantes utilizados na Credi Nestlé atendam às recomendações da Área de Segurança da Informação da empresa apoiadora do grupo Nestlé, de seus fabricantes e desenvolvedores;

x) Auxiliar a Área de Segurança da Informação da empresa apoiadora do grupo Nestlé na análise dos incidentes de segurança cibernética, sempre que solicitado;

y) Assegurar que o desenvolvimento de sistemas, sua qualidade e segurança sejam administrados de acordo com as recomendações de segurança da Área de Segurança da Informação da empresa apoiadora do grupo Nestlé bem como estejam aderentes as boas práticas do mercado;

z) Auxiliar para que o andamento e o resultado de mudanças nos sistemas relevantes e na infraestrutura tecnológica da Credi Nestlé preservem os controles relacionados à disponibilidade, integridade, confidencialidade;

aa) Manter procedimentos de salvaguarda e armazenamento das informações e dados necessários para recuperação dos sistemas relevantes;

bb) Auxiliar a recuperação em situações de contingência dos sistemas relevantes e processos que envolvam os recursos de tecnologia, de acordo com os tempos de recuperação definidos pela Credi Nestlé;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

cc) Assegurar que os procedimentos para continuidade dos serviços de TI estejam alinhados com as diretrizes da Unidade de Compliance, conforme as recomendações dos órgãos fiscalizadores e regramentos legais vigentes;

dd) Assegurar a implementação e gestão de controles ambientais e de segurança física nos Data Centers da Credi Nestlé.

ee) Realizar treinamentos para capacitação e divulgação de boas práticas de segurança cibernética;

ff) Disponibilizar as políticas da Credi Nestlé além de coletar assinatura e custodiar o termo de responsabilidade no momento da admissão de novos colaboradores;

gg) Realizar avaliações periódicas para identificar a aderência e cumprimento desta política e demais normas de segurança cibernética pelos colaboradores;

hh) Auxiliar na análise dos incidentes de segurança por meio da apresentação das trilhas de auditoria dos sistemas sob sua gestão;

ii) Áreas responsáveis pelo gerenciamento de mudanças;

jj) Caso o tratamento do incidente envolva impactos no ambiente de produção a equipe de gerenciamento de mudanças deve ser comunicada para notificar os gestores e usuários do recurso em questão sobre o ocorrido;

kk) Se o incidente tiver consequências legais deve ser estabelecido um contato com os órgãos responsáveis pela apuração e aplicação de penalidades (Agências Reguladoras e/ou Delegacias, se for o caso) para relato dos fatos e a apresentação de indícios relativos ao incidente;

ll) Para os incidentes de segurança da informação que envolva desvio de conduta do colaborador ou em desacordo com o código de ética, o mesmo será encaminhado para área de recursos humanos, a qual poderá se aprofundar na investigação.

mm) No caso de incidentes que tiverem desdobramentos para fora da Credi Nestlé e que envolvam a imprensa ou comunidade externa.

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

9.5. Área Jurídica

a) Participar, apoiar e orientar, no que tange aos aspectos jurídicos, os processos de contratação, bem como, na análise das exigências legislativas dos órgãos reguladores e autorreguladores relacionadas à segurança cibernética;

b) Prestar, quando necessário, orientações jurídicas nas tratativas dos incidentes de segurança cibernética;

c) Analisar e validar as minutas que atendam aos controles de segurança cibernética aplicáveis, especialmente às minutas referentes aos serviços de processamento de dados e computação em nuvem.

9.6. Área de Auditoria

Instaurar, quando couber, procedimento disciplinar para apuração de responsabilidades dos envolvidos em violações de segurança cibernética, e recomendar as penalidades a Gerência Administrativa da cooperativa, quando aplicável.

9.7. Área de Gestão de Continuidade de Negócio

a) Gerenciar plano de continuidade de negócios para contemplar os cenários de incidentes de segurança cibernética com apoio da Área de Segurança da Informação da empresa apoiadora Nestlé;

b) Definir em conjunto com a Área de Segurança da Informação da empresa apoiadora Nestlé, os requisitos a serem utilizados na avaliação de relevância dos incidentes, fluxo de acionamento e testes periódicos de continuidade de negócio;

c) Apoiar as ações de resposta e reestabelecimento de situações em que ocorram incidentes relevantes de segurança cibernética até a completa normalização das operações.

9.8. Gestores

a) Gerenciar o cumprimento desta política e demais documentos complementares pelos seus colaboradores;

b) Identificar vulnerabilidades ou ameaças nos processos e atividades sob sua responsabilidade, tratando-as de forma diligente, a fim de reduzir os impactos ao negócio;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

c) Assegurar que os ativos de propriedade ou sob a responsabilidade da **Credi Nestlé** sejam utilizados de acordo com o dever de cuidado e de acordo com as regras estabelecidas em seus normativos;

d) Identificar violações ou eventual ação em desconformidade às regras de segurança cibernética praticada por pessoa no uso da informação ou sistemas e comunicar à Área de Segurança da Informação da empresa apoiadora Nestlé;

9.9. Colaboradores

a) Ter ciência e manter-se atualizado com esta política e demais documentos complementares;

b) Preservar a integridade, a disponibilidade, a confidencialidade das informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive pela Internet;

c) Não revelar qualquer informação de propriedade ou sob a responsabilidade da **Credi Nestlé** sem a prévia e formal autorização do Encarregado de Dados da cooperativa;

d) Utilizar-se dos ativos de propriedade ou sob a responsabilidade da **Credi Nestlé** com dever de cuidado e zelo, de acordo com as regras estabelecidas nos normativos, somente para fins profissionais, de forma ética e íntegra, respeitando os direitos e as permissões de uso;

e) Zelar pela segurança da sua identidade digital, não a compartilhando, transmitindo ou divulgando a terceiros;

f) Responder por toda atividade realizada por meio dos recursos de tecnologia mediante o uso de sua identidade digital;

g) Reportar formalmente à Área de Segurança da Informação da empresa apoiadora Nestlé; e do Encarregado de Dados da cooperativa, sobre quaisquer eventos relativos à violação ou eventual ação em desconformidade às regras de segurança cibernética praticada por pessoa no uso da informação ou sistemas.

9.10 Encarregado pelo Tratamento de Dados Pessoais (DPO)

a) Analisar as notificações de incidentes de segurança da informação que possívelmente envolvam o tratamento não autorizado de dados pessoais e dados pessoais sensíveis;

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

b) Liderar as salas de crise no caso de incidentes quem envolvam o tratamento não autorizado de dados pessoais;

c) Iniciar processo de gestão de incidentes envolvendo dados pessoais.

9.11 Equipe de Resposta a Incidentes

Monitorar continuamente o ambiente tecnológico do ponto de vista de segurança da informação, visando eventos que possam causar impacto na disponibilidade, integridade e confidencialidade dos sistemas críticos e dos dados sensíveis da **Credi Nestlé;**

10. PENALIDADES

10.1. Violações

Qualquer atividade que desrespeite as disposições estabelecidas nesta Norma ou em quaisquer dos documentos complementares da **Credi Nestlé** deve ser considerada como uma violação e tratada pela **Credi Nestlé** a fim de apurar as responsabilidades dos envolvidos de acordo com as “Medidas Disciplinares” da **Credi Nestlé** visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente

10.2. Tentativa de Burla

A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

11. DISPOSIÇÕES FINAIS

Esta Política deve ser revisada, no mínimo, anualmente, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da **Credi Nestlé**.

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as normas e procedimentos aplicáveis pela **Credi Nestlé.**

Este documento bem como os demais documentos que a complementam encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao Encarregado pelo Tratamento de Dados Pessoais da **Credi Nestlé.**

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

Qualquer dúvida relativa a esta Política deve ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais da **Credi Nestlé** por meio do e-mail protecaodedados11@br.nestle.com

Esta Política entra em vigor na data de sua publicação.

12. CONTROLE DE ATUALIZAÇÕES

Alteração/atualização realizada	Capitulação	Data de aprovação
Instituição do normativo		
Atualização das informações do Plano de resposta a Incidentes, alteração do e-mail de contato,	Item 7 e todos seus subitens	27/06/2023
inclusão da informação sobre a composição da equipe de Resposta a incidente e controles de atualizações	Itens 7.1 e 12	27/06/2023

Rua Dr. Rubens Gomes Bueno nº 691, Conjunto 221, Bloco A, Condomíno 17.007 Nações Unidas - Cep 04730-903 - São Paulo/SP
Tels.: (011) 5508-9070– CNPJ: 62.562.012/0001-67
Reg. no Banco Central nº 279 – Inscrição Estadual Isenta

PROTOCOLO DE AÇÕES

Este é um documento assinado eletronicamente pelas partes, utilizando métodos de autenticações eletrônicas que comprovam a autoria e garantem a integridade do documento em forma eletrônica. Esta forma de assinatura foi admitida pelas partes como válida e deve ser aceito pela pessoa a quem o documento for apresentado. Todo documento assinado eletronicamente possui admissibilidade e validade legal garantida pela Medida Provisória nº 2.200-2 de 24/08/2001.

Data de emissão do Protocolo: 30/06/2023

Dados do Documento

Tipo de Documento	POLÍTICAS_Normativos Internos
Referência Contrato	Política de Segurança Cibernética_27.06.2023
Situação	Vigente / Ativo
Data da Criação	28/06/2023
Validade	28/06/2023 até Indeterminado
Hash Code do Documento	B0375EB863E1DC3D72621E76D852F9665E12EC29653018F5E94A461A9721575D

Assinaturas / Aprovações

Papel (parte) Diretoria (Outorgantes Procuração NÃO Eletrônica)
Relacionamento 62.562.012/0001-67 - Credi Nestlé

Representante	CPF
Francisco Gonçalves Neto	144.039.528-44

Ação:	Assinado em 28/06/2023 03:55:57 - Forma de assinatura: Usuário + Senha	**IP:**	172.70.54.168
Info.Navegador	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.42		
Localização	Não Informada		
Tipo de Acesso	Normal		

Representante	CPF
Marcos Valentim Baccarin	027.765.218-98

Ação:	Assinado em 28/06/2023 04:34:15 - Forma de assinatura: Usuário + Senha	**IP:**	172.70.55.185
Info.Navegador	Mozilla/5.0 (iPhone; CPU iPhone OS 15_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148		
Localização	Latitude: -23.6403730981601/ Longitude: -46.7226683096572		
Tipo de Acesso	Normal		

Enquanto estiver armazenado no Portal, a autenticidade, validade e detalhes de cada assinatura deste documento poderá ser verificada através do endereço https://www.qualisign.com.br/portal/dc-validar, utilizando o código de acesso (passcode) abaixo:

Código de Acesso (Passcode): **OGHCQ-TGZT9-15FPD-GPW1A**

No caso de assinatura com certificado digital também pode ser verificado no site https://validar.iti.gov.br/, utilizando-se o documento original e o documento com extensão .p7s.

Os serviços de assinatura digital deste portal contam com a garantia e confiabilidade da **AR-QualiSign**, Autoridade de Registro vinculada à ICP-Brasil.

Validação de documento não armazenado no Portal QualiSign

Caso o documento já tenha sido excluído do Portal QualiSign, a verificação poderá ser feita conforme a seguir;

a.) Documentos assinados exclusivamente com Certificado Digital (CADES)

A verificação poderá ser realizada em https://www.qualisign.com.br/portal/dc-validar, desde que você esteja de posse do documento original e do arquivo que contém as assinaturas (.P7S). Você também poderá fazer a validação no site do ITI – Instituto Nacional de Tecnologia da Informação através do endereço https://validar.iti.gov.br/

b.) Documentos assinados exclusivamente com Certificado Digital (PADES)

Para documentos no formato PDF, cuja opção de assinatura tenha sido assinaturas autocontidas (PADES), a verificação poderá ser feita a partir do documento original (assinado), utilizando o Adobe Reader. Você também poderá fazer a validação no site do ITI – Instituto Nacional de Tecnologia da Informação através do endereço https://validar.iti.gov.br/

c.) Documentos assinados exclusivamente SEM Certificado Digital ou de forma híbrida (Assinaturas COM Certificado Digital e SEM Certificado Digital, no mesmo documento)

Para documento híbrido, as assinaturas realizadas COM Certificado Digital poderão ser verificadas conforme descrito em (a) ou (b), conforme o tipo de assinatura do documento (CADES ou PADES).

A validade das assinaturas SEM Certificado Digital é garantida por este documento, assinado digitalmente pelo {*PortalNome3*}.

Validade das Assinaturas Digitais e Eletrônicas

No âmbito legal brasileiro e em também em alguns países do Mercosul que já assinaram os acordos bilaterais, as assinaturas contidas neste documento cumprem, plenamente, os requisitos exigidos na Medida Provisória 2.200-2 de 24/08/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e transformou o ITI – Instituto Nacional de Tecnologia da Informação em autarquia garantidora da autenticidade, integridade, não-repúdio e irretroatividade, em relação aos signatários, nas declarações constantes nos documentos eletrônicos assinados, como segue:

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º. As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.

§ 2º. O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Pelo exposto, o presente documento encontra-se devidamente assinado pelas Partes, mantendo plena validade legal e eficácia jurídica perante terceiros, em juízo ou fora dele.