POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TERMO DE RESPONSABILIDADE(ANEXO I)

1. INTRODUÇÃO

A **Credi Nestlé** reconhece a importância da Segurança da Informação como ferramenta para cumprimento da sua missão, aspiração e valores, bem como investe constantemente no crescimento profissional de seus colaboradores e em tecnologias que garantam a excelência de seus produtos e serviços, principalmente pelo modelo de negócio voltado para a utilização da inteligência artificial para a solução de problemas complexos e organização de dados para empresas.

Por isso, é essencial a proteção dos seus ativos, uma vez que quando utilizados de modo indevido podem gerar danos irreparáveis à cooperativa**,** além de afetar a sua imagem perante o mercado. Deste modo, preservar ativos como: a informação, equipamentos tecnológicos e a sua reputação torna-se essencial.

Desta forma, a Política de Segurança da Informação foi elaborada para garantir a sua aderência à legislação vigente e aos requisitos do negócio.

É responsabilidade de todos, independentemente de cargo ou função, estarem cientes e cumprirem a Política de Segurança da Informação da **Credi Nestlé,** além de aplica-la constantemente nas suas atividades diárias, respeitando e disseminando o seu conteúdo.

2. OBJETIVO

Esta Política de Segurança da Informação (PSI) tem como objetivos:

Declarar formalmente o comprometimento da Direção da **Credi Nestlé** na promoção de diretrizes estratégicas, responsabilidades, competências e apoio ao Sistema de Gestão de Segurança da Informação (SGSI), a fim de garantir a proteção dos seus ativos tangíveis e intangíveis;

Estabelecer as responsabilidades e os limites de atuação dos colaboradores da **Credi Nestlé** em relação à segurança da informação, reforçando a cultura interna e priorizando as ações necessárias conforme o negócio.

3. 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.**

4. DEFINIÇÕES

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano.

Aplicativos de Comunicação: Conjunto de código e instruções compiladas, executados ou interpretados por um Recurso de Tecnologia da Informação e Comunicação, armazenados em um dispositivo ou na nuvem, que são usados para troca rápida de mensagens, conteúdos e informações multimídia.

Ativo: É qualquer coisa que tenha valor e precisa ser adequadamente protegido.

Ativo Intangível: Todo elemento que possui valor e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à dados, reputação, imagem, marca e conhecimento.

Autenticidade: Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

Backup: 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 as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.

Disponibilidade: Garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

Dispositivos Móveis: Equipamentos que podem ser facilmente transportados devido a sua portabilidade, com capacidade de registro, armazenamento ou processamento de

informações, além da possibilidade de estabelecer conexões com a Internet e outros sistemas, redes ou qualquer dispositivo.

Dispositivos Removíveis de Armazenamento de Informação: Dispositivos capazes de armazenar informações que pode ser removida do equipamento, possibilitando a portabilidade dos dados, como CD, DVD e pen drive.

Gestor da informação: Colaborador responsável pela criação/recebimento, classificação, divulgação, compartilhamento, eliminação e destruição da informação. Também é incumbido da gestão de validação, liberação e cancelamento dos acessos à informação destes. Vale ressaltar que tais atividades podem ser delegadas para outro colaborador, desde que concedidas pelo Gestor da informação.

Homologação: Processo de avaliação e aprovação técnica de Recursos de Tecnologia da Informação e Comunicação para serem utilizados dentro do ambiente da organização.

Identidade Digital: É a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.

Incidente de Segurança da Informação e Comunicação: 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.

Informação: 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 de que as informações estejam íntegras durante o seu ciclo de vida.

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.

Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

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.

Repositórios Digitais (Cyberlockers): Plataformas de armazenamento na Internet, a exemplo de Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd.

Risco: Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

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.

5. PRINCÍPIOS

Preservar e proteger a informação da **Credi Nestlé** ou sob sua responsabilidade, em todo o seu ciclo de vida, contida em qualquer suporte ou formato, de vulnerabilidades e ameaças;

Prevenir e reduzir impactos gerados pelos incidentes de segurança da informação, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade no desenvolvimento das atividades profissionais;

Zelar por relações transparentes e éticas e coibir toda forma de corrupção, fraude, suborno, favorecimento e extorsão praticados por colaboradores;

Cumprir a legislação brasileira e os demais instrumentos regulamentares relacionados ao negócio no que diz respeito à segurança da informação.

6. DIRETRIZES GERAIS

Interpretação: Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, as atividades que não estão tratadas nos normativos só devem ser realizadas após prévia e formal autorização do gestor do colaborador.

Publicidade: Esta PSI e seus documentos complementares devem ser divulgados aos colaboradores pela Gerência Administrativa, visando dar publicidade para todos que se relacionam profissionalmente com a **Credi Nestlé.**

Propriedade: As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade ou estão sob a responsabilidade e direito de uso exclusivo da **Credi Nestlé** e devem ser utilizados unicamente para fins profissionais.

Propriedade Intelectual: A utilização de obras intelectuais, softwares, desenhos industriais, marcas, identidade visual ou qualquer outro sinal distintivo atual ou futuro da **Credi Nestlé** em qualquer suporte, inclusive na Internet e mídias sociais, deve ser previamente autorizada pela empresa e vinculada as atividades profissionais.

Classificação da Informação: Todas as informações de propriedade ou sob a responsabilidade da **Credi Nestlé** devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida.

Sigilo: É vedada, a qualquer tempo, a revelação de informação de propriedade ou sob a responsabilidade da **Credi Nestlé** sem a prévia e formal autorização do Gestor da Informação, excetuando-se a informação pública.

Uso dos Ativos: Os ativos de propriedade ou sob sua responsabilidade da **Credi Nestlé** devem ser utilizados somente para fins profissionais e de acordo com as orientações dos fabricantes e da empresa.

Uso dos Recursos de TIC: Os Recursos de TIC de propriedade ou sob a responsabilidade da **Credi Nestlé** devem ser utilizados somente para fins profissionais, de modo lícito, ético e moral e conforme as regras da **Credi Nestlé**.

Manutenção dos Ativos: A gestão dos ativos na **Credi Nestlé** deve atender às recomendações dos fabricantes e desenvolvedores, sendo que qualquer necessidade de manutenção, atualização ou correção de falhas técnicas somente pode ser realizada pelo Departamento de TI, de acordo com o tipo de ativo.

Inventário dos Ativos: A **Credi Nestlé** deve realizar inventário de hardwares e softwares que possuir, devendo a Gerência Administrativa, com apoio da área de TI da Nestlé, indicar as informações necessárias e ser a responsável pelo seu registro, armazenamento e atualização.

Dispositivos Móveis Corporativos: Os dispositivos móveis devem ser utilizados quando fornecidos ou autorizados prévia e expressamente pelo gestor, no caso de colaboradores, ou Diretor Presidente, no caso de gestores, conforme a função do colaborador/Gestor e as necessidades do negócio.

Uso dos Recursos de TIC/Dispositivos Móveis Particulares: Não é permitido o uso de Recursos de TIC/Dispositivos Móveis particulares na execução de qualquer atividade profissional, exceto quando autorizado e fundamentado pela Gerência Administrativa.

Repositórios Digitais e Dispositivos Removíveis: É vedado aos colaboradores o uso de repositórios digitais ou dispositivos removíveis não autorizados ou homologados pela **Credi Nestlé** para armazenar ou transmitir informações de propriedade ou sob a responsabilidade da empresa.

Aplicativos de Comunicação Instantânea: O uso de aplicativos de comunicação instantânea para troca de informações corporativas deve atender as regras estabelecidas pela Gerência Administrativa da cooperativa, conjugada com as orientações gerais da área de TI da Nestlé.

Mídias Sociais: O uso das mídias sociais para realização das atividades profissionais em favor da **Credi Nestlé** deve ocorrer somente quando necessário e de forma restrita aos objetivos do negócio, de acordo com o Código de Conduta e Ética vigente. Tais atividades devem ser executadas por meio dos Recursos de TIC da **Credi Nestlé.**

Conduta do Colaborador no Uso das Mídias Sociais: O colaborador deve ser cauteloso, ético e seguro em relação à sua exposição de modo que não afete a reputação da **Credi**

Nestlé, a exemplo de rotinas, trajetos e contatos, além do dever de preservar o sigilo profissional nas mídias sociais.

Controle de Acesso: A **Credi Nestlé** controla o acesso físico e lógico aos seus ambientes, ativos e informações. Desse modo, o colaborador recebeu uma identidade digital de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

O colaborador é responsável pelo uso, proteção e sigilo de sua identidade digital, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de suas credenciais, tal qual de terceiros.

Para garantir o controle de acesso aos ambientes físicos e lógicos, a **Credi Nestlé** utiliza os critérios do mínimo conjunto necessário (least privilege) e estritamente necessários (need to know) ao definir os acessos de cada colaborador.

Ambientes Lógicos: Os sistemas e Recursos de TIC que suportam os processos e as informações da **Credi Nestlé** devem ser confiáveis, íntegros, seguros e disponíveis a quem deles necessitem para execução de suas atividades profissionais. Para garantir a segurança acima estabelecida, a **Credi Nestlé** utiliza os seguintes sistemas de proteção, ativos e atualizados:

Contra programas maliciosos e acessos indevidos, como antivírus e firewall;

Para indicar tentativas de intrusão realizada aos ambientes lógicos, como Sistemas de Detecção a Intrusão (Intrusion Detection Systems) ou IPS (Intrusion Protection Systems);

Contra mensagens eletrônicas indesejadas ou não autorizadas, como AntiSpam.

Ambientes Físicos: A **Credi Nestlé** deve estabelecer perímetros de segurança para proteção de seus ativos, especialmente aqueles que processam ou armazenam informações/ativos críticos para o negócio, e implementar controles para identificação e registro de acessos aos seus ambientes.

Áudio, Vídeos e Imagens: É vedado aos colaboradores qualquer atividade relacionada a captura de áudio, vídeo ou imagens dentro das dependências da **Credi Nestlé** sem a prévia e formal autorização da Gerência Administrativa da cooperativa, exceto em eventos oficiais da empresa.

Contratação de Colaboradores e Prestadores de Bens e Serviços: As contratações em que ocorram o compartilhamento de informações de propriedade ou sob a responsabilidade da **Credi Nestlé** ou a concessão de acesso aos seus ambientes ou ativos críticos, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à segurança da informação.

Desenvolvimento e Aquisição de Software: Tanto o desenvolvimento interno e externo de softwares como aquisições de mercado devem garantir o cumprimento dos requisitos de segurança da informação e controles de acesso previstos nesta PSI e demais Normas Complementares, além de serem acompanhadas pela área de TI da Nestlé, para que os requisitos e exigências de compliance sejam observadas e atendidas de forma integral.

Salvaguarda (backup): A **Credi Nestlé** mantém um processo de salvaguarda das informações e dos dados necessários para completa recuperação dos seus sistemas (backup), a fim de atender os requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes ou sua recuperação o mais rápido possível.

Análise dos Processos e Recursos de TIC: Os coordenadores de unidades da cooperativa devem analisar seus processos e Recursos de TIC, em intervalos regulares, visando assegurar que estejam devidamente inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança mapeadas.

Monitoramento: A **Credi Nestlé** monitora seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio, a reputação e a identificação de eventos ou alertas de incidentes referentes à segurança da informação.

Auditoria e Inspeção: A **Credi Nestlé** pode auditar ou inspecionar os Recursos de TIC que estiverem em suas dependências ou que interajam com seus ambientes lógicos sempre que considerar necessário, atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores.

Gestão de Risco: A gerência Administrativa, com o apoio da área de TI da Nestlé, deve identificar e avaliar os riscos relacionados à segurança da informação e adotar as melhores práticas para o seu gerenciamento.

Gestão de Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e na infraestrutura tecnológica da **Credi Nestlé**, devem preservar os controles

relacionados a disponibilidade, integridade, sigilo e autenticidade das informações e realizados somente com supersição integral da Gerência Administrativa da cooperativa.

Continuidade do Negócio: Os procedimentos de gestão de Continuidade do Negócio devem ser executados em conformidade com os requisitos de segurança da informação da **Credi Nestlé**.

Investimentos: Os investimentos em segurança da informação na **Credi Nestlé** devem ser estudados e deliberados pela Gerência Administrativa da cooperativa junto à Diretoria Executiva, alinhado com as áreas de negócio da Nestlé, considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio.

Comitê de Segurança da Informação (CSI): A **Credi Nestlé** pode estabelecer um CSI responsável por assessorar e gerenciar a implementação dos controles estabelecidos pelo SGSI, analisar questões específicas ao tema, auxiliar com a melhoria constante dos padrões e observância dos normativos de segurança da informação, além de tratar questões relacionadas ao uso indevido dos ativos da empresa, interno ou externo.

O CSI deve ser composto por uma equipe multidisciplinar, submetido à Diretoria da **Credi Nestlé**, com atuação permanente, reunindo-se periodicamente, conforme a necessidade, para tratar de pautas relacionadas à segurança da informação.

Comunicação de Incidentes: A **Credi Nestlé** possui um canal de comunicação divulgado aos seus colaboradores para reportar possíveis casos de incidentes de segurança da informação:protecaodedados11@br.nestle.com

Proteção de Dados Pessoais: A **Credi Nestlé** respeita a privacidade. Assim deve garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais. A **Credi Nestlé** deve avaliar as seguintes medidas de segurança da informação quanto à tratamento de dados pessoais:

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

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;

Elaboração de plano de análise e resposta às violações de dados pessoais;

Armazenamento de modo seguro, controlado e protegido, especialmente quanto se tratarem de dados pessoais sensíveis;

Processos de anonimização e pseudonimização, sempre que necessário;

Protocolos de criptografia na transmissão e armazenamento, quando verificado necessário;

Registro lógico das operações de tratamento de dados pessoais;

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

Transferência aos Agentes de Tratamento de modo seguro e contratualmente previsto;

Mapeamento e manutenção de inventário de fluxos de dados pessoais;

Elaboração de relatórios de impacto à proteção de dados pessoais, quando necessário;

Gestão e tratamento adequado de incidentes que envolvam dados pessoais;

Capacitação: A **Credi Nestlé** deve estabelecer um plano periódico e anual de capacitação direcionado ao desenvolvimento e manutenção das habilidades dos colaboradores sobre segurança da informação.

Revisão e Atualização: A **Credi Nestlé** deve possuir e manter um programa de revisão/atualização desta PSI e das Normas Complementares sempre que se fizer necessário, desde que não exceda o período máximo de 12 (dozes) meses, visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos e atualizados.

Alterações: As alterações desta PSI e das Normas Complementares devem ser devidamente comunicadas aos colaboradores.

Exceções: As exceções somente são admitidas de forma excepcional a essa PSI, devendo ser temporárias e aprovadas previamente pela Diretoria Executiva para produzirem efeito.

Os pedidos de exceção devem ser encaminhados por escrito ao Gestor do colaborador e, se julgado pertinente, será remetido ao Diretor responsável para análise de viabilidade. Se necessário, o pedido de exceção será submetido à Diretoria Executiva para aprovação ou denegação.

As exceções podem ser revogadas a qualquer tempo por mera liberalidade do Gestor do colaborador ou do Diretor, devendo as unidades relacionadas serem informadas imediatamente da denegação por quem a fez para providências, sob pena de responsabilização de quem se omitiu de eventuais prejuízos sofridos pela **Credi Nestlé**, seus clientes ou terceiros.

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

7. RESPONSABILIDADES

7.1. Conselho de Administração e Diretoria Executiva

a) Analisar, aprovar e declarar formalmente o seu comprometimento com esta PSI;

b) Aprovar os investimentos em segurança da informação na **Credi Nestlé**, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio;

c) Analisar e aprovar, ou não, as exceções de forma excepcional a essa PSI.

d) Analisar e aprovar esta PSI e demais Normas Complementares;

7.2. Comitê de Segurança da Informação (CSI), quando instalado

a) Estar ciente desta PSI e demais documentos complementares **Credi Nestlé**;

b) Promover e realizar a gestão do SGSI, garantindo a implementação de controles, modelos, padrões e recursos necessários para a proteção da informação;

c) Promover cultura de segurança da informação na **Credi Nestlé**;

d) Analisar e priorizar ações necessárias, balanceando custo e benefício;

e) Auxiliar, sempre que necessário, a Gerência Administrativa na capacitação dos colaboradores em Segurança de Informação;

f) Orientar para que as todas as atividades desempenhadas estejam adequadas ao negócio da **Credi Nestlé**;

g) Analisar os incidentes de segurança da informação reportados e submeter relatório para deliberação da Diretoria Executiva, sempre que necessário;

h) Instaurar, quando couber, procedimento disciplinar para apuração de responsabilidades dos envolvidos em violações de segurança da informação, e aplicar as penalidades, quando necessário.

7.3. Gerência Administrativa, com apoio da TI Nestlé

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

b) Identificar e avaliar os riscos relacionados à segurança da informação e propor melhorias e recursos necessários às ações de segurança da informação;

c) Realizar e acompanhar estudos de tecnologias, com o apoio do Comitê de Segurança da Informação, quanto a possíveis impactos na segurança da informação;

d) Elaborar e manter atualizado os documentos que compõem o SGSI, além de submetê-los à aprovação da Diretoria ou do CSI;

e) Propor, junto com o CSI, normas e procedimentos internos relativos à segurança da informação na **Credi Nestlé**;

f) Realizar a gestão, manutenção e administração dos Recursos de TIC de propriedade ou sob a responsabilidade da **Credi Nestlé**;

g) Garantir que todos os Recursos de TIC utilizados na **Credi Nestlé** atendam as recomendações de seus fabricantes ou desenvolvedores;

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

i) Realizar o registro e o monitoramento dos acessos aos ambientes lógicos da **Credi Nestlé**;

j) Disponibilizar e realizar a gestão das identidades digitais de acesso ao ambiente lógico da **Credi Nestlé**;

k) Analisar ou auxiliar na análise dos incidentes de segurança da informação reportados;

l) Avaliar se os requisitos de segurança da informação estão presentes antes da aquisição, manutenção ou desenvolvimento de softwares;

m)Garantir andamento e o resultado de mudanças preservem os controles relacionados à disponibilidade, integridade, confidencialidade, autenticidade e legalidade das informações, sobretudo nos sistemas e na infraestrutura tecnológica da **Credi Nestlé;**

n) Garantir a rápida recuperação em situações de contingência de seus sistemas e processos que envolvam os Recursos de TIC da **Credi Nestlé**;

o) Elaborar e/ou manter procedimentos de salvaguarda das informações e dos dados necessários para recuperação dos sistemas da **Credi Nestlé**;

p) Assegurar que os procedimentos de Gestão da Continuidade do Negócio sejam executados em conformidade com os requisitos de segurança da informação;

7.4. Encarregado pelo Tratamento de Dados Pessoais (DPO)

a) Analisar e aprovar contratos que envolvam tratamento de dados pessoais, seguindo a legislação vigente e aplicável a cada situação em suas particularidades;

b) Apoiar em sindicâncias para apuração de responsabilidade dos envolvidos em violações de dados pessoais e auxiliar na definição de aplicação das penalidades internas, quando necessário;

c) Avaliar e auxiliar na elaboração de Relatórios de Impacto à Proteção de Dados Pessoais;

d) Manter Mapeamento de Fluxos de Dados Pessoais atualizado;

e) Desenvolver Plano de Análise e Resposta a Violações de Dados Pessoais que identifique o tipo de violação, o número de registros afetados, quais registros foram afetados e as categorias de dados pessoais envolvidas, as notificações apropriadas e plano de mitigação dos efeitos da violação.

f) Garantir que o tratamento de Dados Pessoais tenha o mesmo nível de tratamento que informações consideradas confidenciais.

7.5. Gerência Administrativa com apoio do escritório Jurídico contratado

a) Participar, apoiar e orientar, de acordo com os aspectos jurídicos, os processos de contratação e as exigências legislativas relacionadas à segurança da informação;

b) Validar as minutas que devem atender aos controles de segurança da informação aplicáveis aos contratos.

7.6. Gerência Administrativa

a) Realizar campanhas de capacitação e divulgação da segurança da informação;

b) Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores;

c) Garantir a publicidade e disponibilidade dos documentos que compõe o SGSI na **Credi Nestlé;**

d) Disponibilizar os normativos da **Credi Nestlé**, além de custodiar e colher assinatura do "Termo de Ciência e Responsabilidade" na admissão de novos colaboradores.

e) Autorizar ou não, o uso das marcas, identidade visual e qualquer outro sinal distintivo atual ou futuro da **Credi Nestlé**;

f) Autorizar ou não, a gravação de áudio, vídeo ou foto das dependências da **Credi Nestlé**;

g) Autorizar ou não, a revelação de qualquer informação de propriedade ou sob a responsabilidade da **Credi Nestlé**;

h) Identificar violações ou qualquer ação duvidosa praticada pelos colaboradores no uso da informação da **Credi Nestlé** e comunicar ao CSI e ao Gestor do colaborador;

i) Garantir e gerenciar o cumprimento desta PSI e demais documentos complementares pelos seus colaboradores;

j) Identificar e medir as vulnerabilidades e ameaças nos processos e atividades de sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir os impactos ao negócio;

k) Autorizar, ou não, a utilização de Recursos de TIC ou dispositivos móveis particulares por seus colaboradores para execução de qualquer atividade profissional na **Credi Nestlé**;

l) Aplicar, após definição com o Departamento de Recursos Humanos, as sanções de violação desta PSI e documentos complementares;

m)Identificar incidentes de segurança da informação ou qualquer ação duvidosa praticada por seus colaboradores, comunicando o CSI imediatamente.

7.7. Colaboradores

a) Estar ciente e manter-se atualizado com esta PSI e demais documentos complementares;

b) Conhecer e assinar o "Termo de Ciência e Responsabilidade";

c) Utilizar os ativos de propriedade da **Credi Nestlé** ou sob sua responsabilidade de acordo com as orientações do fabricante, do desenvolvedor e da empresa, com cuidado e zelo;

d) Utilizar os ativos e informações da **Credi Nestlé** somente para fins profissionais, de forma ética e legal, respeitando os direitos e as permissões de uso concedidas;

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

f) Não revelar qualquer informação de propriedade ou sob a responsabilidade da **Credi Nestlé** sem a prévia e formal autorização;

g) Utilizar as marcas e outros sinais distintivos, patentes, desenhos industriais, softwares e demais direitos de propriedade intelectual de titularidade da **Credi Nestlé** somente para finalidades profissionais e autorizadas pela empresa, de acordo com a atividade e função exercida;

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

i) Responder por toda e qualquer atividade realizada nos Recursos de TIC da **Credi Nestlé** realizada mediante o uso de sua identidade digital;

j) Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais;

k) Reportar formalmente ao seu Gestor quaisquer eventos relativos à violação ou possibilidade de violação de segurança ou atividades suspeitas.

8. PENALIDADES

Violações: Qualquer atividade que desrespeite as disposições estabelecidas nesta Política 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.

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

9. 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 (DPO) da **Credi Nestlé.**

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

Esta Política entra em vigor na data de sua publicação.

ANEXO I - TERMO DE CIÊNCIA E RESPONSABILIDADE

Formato Disclaimer (para ciência eletrônica)

Deve ser coletada a ciência do colaborador por meio de barreira de navegação no login da rede ou publicado na Intranet com envio para o correio eletrônico corporativo de todos, conforme descrito abaixo:

Termo de Ciência e Responsabilidade

Confirmo que estou ciente do conteúdo da Política de Segurança da Informação da **Credi Nestlé**, e reafirmo meu dever de cumprir, disseminar e manter-me sempre atualizado com as regras lá estabelecidas.

Formato Impresso (para assinatura)

Termo de Ciência e Responsabilidade

Eu, _____, pelo presente, confirmo que estou ciente do conteúdo da Política de Segurança da Informação da **Credi Nestlé,** e reafirmo meu dever de cumprir, disseminar e manter-me sempre atualizado com as regras lá estabelecidas.

_____, __/___/_____
Local, Data

_____
Assinatura do Colaborador

Código de Crachá do Colaborador

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: 07/06/2024

Dados do Documento

Tipo de Documento	POLÍTICAS_Normativos Internos
Referência Contrato	CNestle_PoliticaSegurancaInformacao
Situação	Vigente / Ativo
Data da Criação	31/05/2024
Validade	31/05/2024 até Indeterminado
Hash Code do Documento	4D4A37AD10F9C1C8FCF0FA7742716AFC9A037B63DD75FBA78A79E8D59E7E6CE0

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 07/06/2024 09:20:26 - Forma de assinatura: Usuário + Senha	**IP:**	186.204.80.133
Info.Navegador	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36 Edg/125.0.0.0		
Localização	Não Informada		
Tipo de Acesso	Normal		

Representante	CPF
Marcos Valentim Baccarin	027.765.218-98

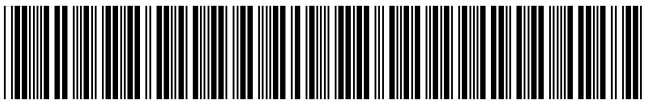
Ação:	Assinado em 31/05/2024 10:22:35 - Forma de assinatura: Usuário + Senha	**IP:**	200.79.187.88
Info.Navegador	Mozilla/5.0 (iPhone; CPU iPhone OS 15_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148		
Localização	Latitude: -22.1319689464823/ Longitude: -47.471185439247		
Tipo de Acesso	Normal		

Representante	CPF
TIAGO CASTILLO E SOUSA	094.209.376-31

Ação:	Assinado em 31/05/2024 11:24:00 - Forma de assinatura: Usuário + Senha	**IP:**	179.98.213.48
Info.Navegador	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0		
Localização	Latitude: -23.627643/ Longitude: -46.742621		
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): **QU7TZ-5PFTY-7FV2B-QHFQR**



No caso de assinatura com certificado digital também pode ser verificado no site https://verificador.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://verificador.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://verificador.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 e certificado pela QualiSign.

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.