

# RELATÓRIO ANUAL DE SEGURANÇA CIBERNÉTICA BASE 2022-2023

Documento assinado eletronicamente. Verificação em <https://www.qualisign.com.br/portal/dc-validar>  
através do código TMQIV-LXHIK-ZJTKM-K6XES enquanto armazenado no Portal

## 1. APRESENTAÇÃO

A **Cooperativa de Economia e Crédito Mútuo dos Funcionários da Nestlé – Credi Nestlé** em caráter preventivo, busca manter a estrutura organizacional, composta pelo Conselho de Administração e pela Diretoria Executiva, pelo Conselho Fiscal, empregados e prestadores de serviços cientes das responsabilidades sob suas atividades que norteiam a segurança cibernética.

Para isso, alguns procedimentos devem ser cumpridos de forma a garantir a confidencialidade, a integridade e a disponibilidade das informações da Cooperativa.

## 2. AÇÕES DE TREINAMENTO E CONSCIENTIZAÇÃO

Como uma de suas responsabilidades, a Cooperativa identifica as necessidades relativas a treinamento e conscientização em toda sua estrutura funcional e propõe ações que possam suprir essa necessidade.

Dentre essas ações, no período de junho/2022 a junho/2023 foram realizadas as seguintes ações:

- a) conscientização de toda equipe funcional sobre o tema de Riscos Cibernéticos, como podemos identificar indícios, ferramentas de apoio e denúncia, a quem devemos recorrer e cuidados no tratamento de dados;
- b) divulgação da Política de Segurança Cibernética , tanto para colaboradores como para órgãos de administração;
- c) atualização das diretrizes básicas da Política de Segurança Cibernética;
- d) confecção e aprovação do Plano de Ação e Resposta a Incidentes Relevantes os quais são documentos base para a elaboração desse relatório (item 7 da Política de Segurança Cibernética);
- e) realização de capacitação on line sobre Data Privacy com todo equipe funcional da cooperativa;

### 3. AÇÕES EM INFRAESTRUTURA

A Cooperativa com o apoio da IT Nestlé Brasil, busca continuamente a melhoria dos equipamentos que compõem seu parque tecnológico com o intuito de assegurar a integridade das informações e disponibilidade dos serviços prestados e disponibilizados, dentre eles:

- a) manutenção das máquinas no padrão estabelecido pela IT Nestlé, incluindo soluções de Firewall, Fastly e AKamai, para manutenção da segurança, permitindo aumento de capacidade, recursos de segurança e VPN para acesso remoto seguro;
- b) contratação de novos e modernos notebooks no mês de junho/2023, com maiores capacidades e recursos de segurança de informação;
- c) elaboração execução do teste de ativação do Backup do site e seu Banco de Dados, com realização de backup de 2 em 2 horas e armazenamento por 3 meses de todos conteúdo. Os backups não são armazenados no mesmo servidor por segurança;
- d) atualização do sistema operacional é realizada diariamente, conforme definição da Facil Tech. O conteúdo tem armazenamento em nuvem da Amazon;
- e) gerenciamento da concessão de acessos aos módulos do Sistema Operacional Fácil, conforme as atribuições exigidas pelo cargo;
- f) envio de e-mails testes de phishing para avaliação se a equipe está ciente das ações de segurança cibernética.

### 4. REGISTRO DE EVENTOS OCORRIDOS

No período de 01 de junho de 2022 a 30 de junho de 2023 não foram identificados a ocorrência de incidentes que impediram as atividades da Cooperativa.

#### 4.1. INFORMAÇÕES DO RELATORIO DE INCIDENTES RELEVANTES

Não foram registrados eventos de incidentes relevantes, portanto, não há informações a serem preenchidas no **Relatório de Incidentes de Segurança Cibernética (RISC)**:

RELATÓRIO DE INCIDENTES DE SEGURANÇA CIBERNÉTICA (RISC)

Item	Descrição	Ação
------	-----------	------

1	Nº do registro do incidente	
2	Data da ocorrência do evento:	
3	Relevante	( ) Sim - <i>Obs: Impede a execução das atividades da Cooperativa</i>
		( ) Não - <i>Obs: Não impede a execução das atividades da Cooperativa</i>
4	Área / Unidade responsável pelo registro e acompanhamento do tratamento	

	Descrição	<i>Identificar resumidamente sobre o incidente</i>
5	Período em que ocorreu o incidente	Data início: _____ Data fim: _____
		Hora início: _____ Hora fim: _____
6	Severidade do incidente	( ) Alta ( ) Média ( ) Baixa
7	Tipo de Impacto	( ) Confidencialidade ( ) Integridade ( ) Disponibilidade
8	Origem do alerta	<i>Informar quem ou qual sistema alertou do incidente</i>
9	Comunicação do incidente	<i>Informar a quem ou a quais setores o incidente foi informado</i>

10	Detalhamento do Incidente	<i>Descrição do ocorrido, o que foi impactado (ex. sistema), informações do prestador de serviço, o que foi afetado e demais informações importantes.</i>
----	---------------------------	---

Documento assinado eletronicamente. Verificação em <https://www.qua.lisboa.gov.brl/portal/dc-VALIDAR> através do código: TMCQW-LXHIK-ZJTKM-K6KES enquanto armazenado no Portal

11	Tratamento do Incidente	<i>Descrever ações executadas para contenção e/ou contorno do problema/incidente, equipes/pessoas envolvidas, sistemas/ferramentas utilizadas para controle do incidente.</i>
12	Análise e Encerramento do Incidente	<i>Descrever se necessárias outras ações e recursos necessários para finalizar o tratamento do incidente e/ou para evitar que o incidente volte a ocorrer.</i>

#### 4.1.1. DETALHAMENTO DO INCIDENTE

No período de 01 de junho de 2022 a 30 de junho de 2023 não foram identificados a ocorrência de incidentes que impediram as atividades da Cooperativa.

#### 4.1.2. TRATAMENTO DO INCIDENTE

No período de 01 de junho de 2022 a 30 de junho de 2023 não foram identificados a ocorrência de incidentes que impediram as atividades da Cooperativa.

#### 4.1.3. ANÁLISE E ENCERRAMENTO DO INCIDENTE

No período de 01 de junho de 2022 a 30 de junho de 2023 não foram identificados a ocorrência de incidentes que impediram as atividades da Cooperativa.

#### 4.1.4. RESULTADO DO TESTE DE CONTINUIDADE

No período de 01 de junho de 2022 a 30 de junho de 2023 não foram identificados a ocorrência de incidentes que impediram as atividades da Cooperativa.

#### 4.1.5. DATA DE EXECUÇÃO

No período de 01 de junho de 2022 a 30 de junho de 2023 não foram identificados a ocorrência de incidentes que impediram as atividades da Cooperativa.

### 5. CONCLUSÃO

Não há conclusão a ser expressa, uma vez que no período de 01 de junho de 2022 a 30 de junho de 2023, não foram registrados a ocorrência de incidentes relacionados com riscos cibernéticos.

Entretanto, a cooperativa mantém procedimentos de prevenção, conforme padrão estabelecido pela IT da Nestlé Brasil e também conforme as regulamentações específicas do segmento de atuação.

# 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: 11/08/2023

## Dados do Documento

Tipo de Documento	POLÍTICAS_Normativos Internos
Referência Contrato	Relatório Anual de Segurança Cibernética_04.08.2023
Situação	Vigente / Ativo
Data da Criação	08/08/2023
Validade	08/08/2023 até Indeterminado
Hash Code do Documento	D69C01A15E41D5C1F1194B4884FA6358CC1DBF315151FE7B9E8D661304EADD55

## Assinaturas / Aprovações

**Papel (parte)** Diretoria (Outorgantes Procuração NÃO Eletrônica)

**Relacionamento** 62.562.012/0001-67 - Credi Nestlé

Representante	CPF
<b>Francisco Gonçalves Neto</b>	144.039.528-44
<b>Ação:</b>	Assinado em 08/08/2023 02:12:26 - Forma de assinatura: Usuário + Senha <b>IP:</b> 172.70.254.173
<b>Info.Navegador</b>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Edg/114.0.1823.82
<b>Localização</b>	Não Informada
<b>Tipo de Acesso</b>	Normal

Representante	CPF
<b>Marcos Valentim Baccarin</b>	027.765.218-98
<b>Ação:</b>	Assinado em 08/08/2023 10:57:05 - Forma de assinatura: Usuário + Senha <b>IP:</b> 108.162.210.148
<b>Info.Navegador</b>	Mozilla/5.0 (iPhone; CPU iPhone OS 15_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148
<b>Localização</b>	Latitude: -23.6403773977641/ Longitude: -46.7226660834898
<b>Tipo de Acesso</b>	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): **TMQIV-LXHIK-ZJTKM-K6XES**



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.