GUIA SGI 004 01

Guia de Uso Aceitável (GUA) dos Recursos Tecnológicos

Abrangência: **CNP Seguros *Holding* Brasil**

Atualizado em: 28/06/2022

INFORMAÇÕES GERAIS	
Macroprocesso/ Processo	**Gerir controles internos e auditoria/Gerir riscos**
Alteração em relação à versão anterior (resumo)	**Primeira Versão**
Classe	**Pública**
Normativo interno Vinculado	PO 008 – Política de Segurança da Informação e Segurança Cibernética
Normativos Citados	**Não se aplica**

REFERÊNCIAS NORMATIVAS		
CÓD./ORG.	**Descrição**	**Tipo**
ABNT	NBR ISO/IEC 27002 - Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Gestão da Segurança da Informação	Externa
SUSEP	Circular SUSEP nº 638/2021	Externa
CNP *Assurances*	*Group Information Security Policy*	Externa

ELABORADOR		
DIR./GER.	**Nome**	**Data**
DIRRIS/GESEG	**Darlan dos Santos Ferreira**	27/06/2022

APROVADOR DA UNIDADE DE IMPACTO		
DIR./GER.	**Nome**	**Data**
	Não se aplica	

Sumário

1. Objetivo

1.1. Definir as regras de uso aceitável de recursos tecnológicos disponibilizados aos usuários da CNP Seguros *Holding* Brasil – CNP Brasil, englobando colaboradores, fornecedores, parceiros de negócios e clientes, de forma responsável, ética e segura, com orientações para um comportamento adequado às melhores práticas de Segurança da Informação e segurança cibernética. A CNP Brasil está comprometida em combater ações ilegais ou danos provocados por indivíduos de forma acidental, intencional, ilícita e/ou por falhas em processos.

2. Definições

2.1. **Antivírus:** é um software que detecta, impede e atua na remoção de programas de *software* maliciosos.

2.2. **Aplicação:** trata-se de uma solução de TI capaz de integrar as diversas áreas de negócio da empresa, trazendo automação, integração e armazenando todas as informações do negócio.

2.3. **Ativos:** representam tudo aquilo que a empresa possui e controla, sejam estes bens, créditos ou direitos, tangíveis ou intangíveis, que podem ser convertidos em meios monetários e gerar benefícios econômicos no futuro. Ativos de TI são todos os itens, físicos ou virtuais, que compõem a infraestrutura de TI de uma empresa. Ou seja, tudo que é *hardware*, software, redes e outras tecnologias fundamentais para a continuidade das operações do negócio.

2.4. **Biometria:** toda tecnologia que permite que uma pessoa seja identificada a partir de suas características físicas. O mercado conta com vários tipos de tecnologias biométricas: reconhecimento facial, reconhecimento de voz, impressão digital, leitura da íris, entre outros.

2.5. **Classificação da Informação:** é a definição de níveis de proteção que cada dado deve receber. O seu objetivo é garantir que nenhum dado seja divulgado indevidamente e que apenas as pessoas que têm direito recebam acesso à informação. A classificação da informação faz parte dos requisitos da ISO/IEC 27001 e a CNP Brasil divulga esta informação junto com suas informações.

2.6. **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados.

2.7. **Continuidade do Negócio:** é um processo abrangente que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

2.8. **Custodiante:** o colaborador (empregado, estagiário e o terceirizado alocado) que tem sob a sua responsabilidade a guarda e utilização de qualquer equipamento tecnológico fixo ou móvel, ou informação de propriedade da CNP Brasil.

2.9. **Dados:** uma série de fatos discretos que servem como base para a construção da informação e do conhecimento. Porém, o dado não

apresenta um significado importante e não leva a nenhuma compreensão quando analisado sozinho.

2.10. **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

2.11. **Equipamentos móveis:** são aqueles que possuem características de armazenamento de dados, mobilidade e conectividade, tais como *notebook*, *smartphone*, *tablets*, *pendrive*, cartões de memória, mídias de armazenamento de dados móveis, entre outros.

2.12. ***Firewall:*** são programas de *software* ou dispositivos de *hardware* que filtram e examinam as informações provenientes de uma conexão com a Internet. Eles representam uma primeira linha de defesa porque podem impedir que um programa ou invasor mal-intencionado obtenha acesso à rede e informações antes que qualquer dano potencial seja causado.

2.13. ***Hackers:*** são pessoas com um conhecimento profundo de informática e computação que trabalham desenvolvendo e modificando *softwares* e *hardwares* de computadores, não necessariamente para cometer algum crime. Eles também desenvolvem novas funcionalidades no que diz respeito a sistemas de informática.

2.14. **Incidente:** uma interrupção não planejada de um serviço de TI ou redução da qualidade do serviço de TI ou alguma falha de um item de configuração (ativo) que ainda não causou impacto em um serviço de TI (por exemplo, falha de um disco em um conjunto de discos espelhados). Fonte: *ITIL*.

2.15. **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

2.16. **Irretratabilidade:** característica daquilo que não se consegue tratar; qualidade do que não se pode reproduzir ou fotografar. Particularidade do que é irretratável.

2.17. ***Malwares*:** forma reduzida de *malicious software* (*software* malicioso), é um *software* usado por atacantes para comprometer a operação de um computador, colher informações sensíveis ou ganhar acesso a sistemas computacionais privados.

2.18. ***Patches* (plural de *patch*):** é um programa de computador criado para atualizar ou corrigir um *software* de forma a melhorar sua usabilidade, performance e/ou segurança.

2.19. **Plataforma:** são modelos de negócios baseados em tecnologia. A missão delas é conectar interesses e pessoas, promovendo interações de valor entre os envolvidos (por exemplo: um portal é uma plataforma *web*).

2.20. **Pseudonimização:** é o "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

2.21. **Recursos tecnológicos:** computadores e periféricos móveis ou fixos, equipamentos tecnológicos que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação englobando as atividades de produção, coleta, tratamento, processamento,

armazenamento, transmissão, recepção, comunicação e disseminação de informações e serviços, mídias, documentos eletrônicos, *softwares*, sistemas e bancos de dados.

2.22. **Serviços em Nuvem *(Cloud):*** refere-se a um conceito tecnológico baseado em uma malha de computadores, redes, infraestruturas tecnológicas e serviços espalhados pela internet (nuvem pública) ou em um ambiente privado (nuvem privada), que podem ser rapidamente mobilizados e liberados com o mínimo esforço ou intervenção de um provedor de serviços, e permitir acessar sistemas e aplicações sem que estas estejam instaladas em computadores, celulares, tablets etc.

2.23. ***Spam:*** O *spam* (*Sending and Posting Advertisement in Mass*, na sigla em inglês que significa, envio e publicação de anúncios em massa) são mensagens eletrônicas que são enviadas ou postadas para muitas pessoas sem que elas tenham sido solicitadas.

2.24. ***Software*:** programas de computadores desenvolvidos para interagir com o usuário por meio de sequência de instruções a serem seguidas e/ou executadas, na manipulação, redirecionamento ou modificação de um dado/informação ou acontecimento.

2.25. **Token:** dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta USB.

2.26. **Usuário:** qualquer pessoa física, devidamente autorizada, que utiliza algum recurso computacional ou qualquer rede local ou sistema de acesso remoto para conectar um computador pessoal ou qualquer outro dispositivo, sistema ou serviço, à rede computacional CNP Brasil.

2.27. **Vulnerabilidade:** uma fraqueza de um ativo que poderia ser potencialmente explorada por uma ou mais ameaças. Qualquer causa potencial de um incidente não desejado que possa resultar em dano ao sistema ou organização.

3. Abrangência

3.1. Esta guia se aplica a todos os empregados, estagiários, terceirizados (incluindo fornecedores de bens e serviços), consultores externos, parceiros e clientes, que estejam conectados a um sistema, plataforma ou aplicação, rede de dados, servidores ou computadores (pessoais ou comerciais) localizados em locais pertencentes ou não à CNP Brasil, que acessam, usam, gerenciam, transmitem ou armazenam informações da companhia (incluindo plataformas, *softwares*, serviços de infraestrutura, sistemas e serviços em nuvem de computadores – *Cloud*).

3.2. A guia deve ser divulgada internamente nas empresas da CNP Brasil e externamente através dos seus portais corporativos de *internet*.

3.3. Quando divulgada nos portais corporativos de *internet*, a guia poderá sofrer alterações em seu *layout* a fim de atender aos padrões do portal, desde que mantenha integralmente o conteúdo original.

4. Regras Gerais

4.1. O uso aceitável de recursos tecnológicos da CNP Brasil é sempre ético, honesto, e respeita os direitos individuais, inclusive os direitos à privacidade, personalidade e inviolabilidade.

4.2. O armazenamento e a disponibilização de dados e informações da CNP Brasil observa rigorosos controles de segurança da informação e proteção de dados pessoais com base nas políticas internas, na ABNT ISO 27001 e nas melhores práticas consolidadas pelo mercado.

4.3. Toda informação gerada, processada, armazenada, acessada, divulgada, transmitida, recuperada ou confiada no âmbito da CNP Brasil é tratada como um ativo de sua propriedade, e deve ser protegida dos riscos aos quais está sujeita, em especial os associados à privacidade, confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade.

4.4. São também tratadas como ativo de propriedade da CNP Brasil as informações geradas e/ou mantidas em ambientes de fornecedores e parceiros de negócio, originadas nos processos internos ou externos da CNP Brasil, incluindo os realizados no fornecedor ou parceiro, ou fruto do relacionamento estabelecido.

4.5. Esta guia é aplicada aos equipamentos móveis de propriedade e/ou particulares que venham a se conectar na rede de dados da CNP Brasil, ou que sejam utilizados para acessar, armazenar e/ou processar informações da CNP Brasil.

4.6. Todos os usuários devem cumprir as leis e regulamentações Brasileiras e dos demais países em que atuam, que substituirão quaisquer aspectos conflitantes desta política e padrões relacionados.

4.7. Os empregados, estagiários e terceirizados alocados da CNP Brasil devem conhecer e cumprir os normativos internos que estabelecem os controles de segurança da informação e de continuidade do negócio.

5. Uso Aceitável

5.1. O usuário deve utilizar senhas seguras, de acordo com as orientações apresentadas no momento do seu cadastramento para uso de um recurso computacional, e evitar o uso de dados que possam facilitar a sua revelação indevida, tais quais nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam se relacionadas com o usuário, entre outras informações de cunho pessoal.

5.2. Manter sua senha pessoal em sigilo e não a revelar em nenhuma hipótese.

5.3. Fazer uso responsável das credenciais de acesso (nome do usuário, senha, *token*, biometria etc.) disponibilizadas pela CNP Brasil para permitir o acesso aos recursos tecnológicos dotados deste controle.

5.4. Fazer uso responsável da credencial de acesso que contém privilégios administrativos, conforme os limites e atribuições determinadas para estes acessos, tendo conhecimento que tanto os acessos quanto as operações realizadas são registradas e monitoradas pela CNP Brasil.

5.5. Respeitar a propriedade intelectual e os acordos de confidencialidade.

5.6. Utilizar somente *softwares* licenciados.

5.7. Certificar-se que o equipamento tecnológico que utiliza, seja este particular ou corporativo, está protegido com todos os *patches* e correções de segurança fornecidos pelo fabricante do sistema operacional, *firewall* local ativo e antivírus licenciados, instalados e atualizados.

5.8. Utilizar o correio eletrônico, e quaisquer dispositivos disponibilizados aos custodiantes pela CNP Brasil, para atender exclusivamente aos propósitos profissionais.

5.9. Respeitar a classificação da informação sempre que esta for apresentada no momento do seu acesso ou durante o seu uso.

5.10. Respeitar os controles de segurança aplicados aos recursos tecnológicos da CNP Brasil, sabendo que são disponibilizados para fins estritamente profissionais, e tanto os acessos quanto as operações realizadas pelos usuários são registradas e monitoradas.

5.11. Comunicar imediatamente a ocorrência de qualquer anomalia ou incidente ocorrido durante o uso dos recursos tecnológicos ou acesso às informações da CNP Brasil por meio do canal interno de comunicação de incidente de segurança ou dos canais de comunicação com o cliente disponíveis no portal de Internet (*https://www.cnpbrasil.com.br/*).

6. Uso Não Aceitável

6.1. Compartilhar informações sigilosas, classificadas ou proprietárias, inclusive senhas, com pessoas ou organizações não-autorizadas.

6.2. Compartilhar assuntos restritos ao dia a dia do trabalho e informações relevantes para os negócios nas redes sociais.

6.3. Desviar ou usar informações específicas da empresa para fins que incluem concorrência desleal, fazer declarações falsas, excluir ou modificar indevidamente os dados de propriedade da CNP Brasil.

6.4. Violar ou desativar inadvertidamente sistemas de segurança de quaisquer redes ou recursos tecnológicos da CNP Brasil e de parceiros integrados às nossas plataformas tecnológicas.

6.5. Burlar e/ou violar quaisquer controles de segurança utilizados para a transmissão de dados da CNP Brasil.

6.6. Contornar as restrições de utilização dos recursos tecnológicos que lhe são disponibilizados.

6.7. Enviar mensagens eletrônicas não solicitadas, incluindo, mas não se limitando a, quantidade significativa de mensagens com publicidade comercial ("*spam*") ou anúncios informativos que possam vir a prejudicar os serviços providos pela CNP Brasil.

6.8. Forjar a origem da mensagem de correio eletrônico enviada, de maneira que pareça ter sido enviado por outro usuário.

6.9. Usar os recursos tecnológicos da CNP Brasil ou próprios para obter acesso não autorizado a dados, sistemas ou redes, incluindo, mas não se limitando a qualquer tentativa de investigação, exames ou testes de vulnerabilidade, sem anuência expressa da CNP Brasil.

6.10. Utilizar os recursos tecnológicos da CNP Brasil para finalidades ilegais e/ou não éticos, que violem quaisquer leis locais, estaduais, nacionais e acordos internacionais.

6.11. Utilizar *softwares* não licenciados, sem homologação, maliciosos ou contaminados por vírus ou pragas eletrônicas.

6.12. Instalar ou alterar as configurações dos *softwares* instalados nos recursos tecnológicos da CNP Brasil.

6.13. Difundir *malware* (*software* malicioso) ou qualquer forma de rotinas de programação prejudicial ou danosa aos recursos tecnológicos tanto no âmbito interno da CNP Brasil quanto externo.

6.14. Conduzir qualquer tipo de ataque ou atividade de fim malicioso que vise tornar um serviço indisponível, obter vantagem indevida, escalar privilégios ou prejudicar outros usuários.

6.15. Acessar, por meio dos recursos tecnológicos da CNP Brasil, sítios na *Internet* que tenham cunho e conteúdo criminoso, obsceno, pornográfico, racista, constrangedor, difamatório, *hacker*, jogos online e, que de forma geral, possam gerar riscos à segurança da informação, às pessoas e ao negócio da CNP Brasil.

6.16. Tentar reverter técnicas de pseudonimização que tenham sido aplicadas para proteger dados sensíveis aos quais o usuário pode ter acesso.

7. Sanções

7.1. O usuário é responsável pelas consequências da violação dessas diretrizes, que podem incluir a suspensão de seus acessos e a aplicação da lei na esfera civil e criminal, nacional e internacional.

8. Responsabilidades

8.1. CNP Seguros *Holding* Brasil

8.1.1. Definir as diretrizes de uso aceitável dos recursos tecnológicos disponibilizados e mantê-las disponíveis para seus clientes, colaboradores, fornecedores, parceiros e acionistas.

8.1.2. Garantir que as melhores práticas de segurança da informação estão sendo aplicadas para resguardar a integridade dos recursos tecnológicos e das informações mantidas, transitadas, processadas e disponibilizadas.

8.1.3. Atuar na aplicação das sanções cabíveis, quando necessário.

8.1.4. Disponibilizar um canal para comunicação de incidentes no portal corporativo da empresa na *Internet*.

8.2. Usuário

8.2.1. Fazer bom uso dos recursos tecnológicos e das informações disponibilizados pela CNP Brasil, respeitando os princípios do uso aceitável apresentados neste guia.

8.2.2. Informar imediatamente as violações de segurança identificadas ou suspeitas por meio dos canais de comunicação com o cliente da CNP Brasil disponíveis nos canais internos de comunicação de incidentes de segurança ou no portal de Internet (https://www.cnpbrasil.com.br/).