Data de Publicação: 01/2026
Versão: 01.1

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Emissor: Governança, Riscos e Compliance | Revisor: Gerência Financeira |
Aprovador: Diretoria Executiva.

Sumário

1. OBJETIVO

A presente Política visa definir os princípios, diretrizes e responsabilidades sobre os aspectos relacionados à segurança cibernética, na intenção de assegurar a proteção das informações e o uso aceitável dos ativos de informação do Z-ON, baseado nos princípios de confidencialidade, integridade e disponibilidade.

2. ABRANGÊNCIA

A presente Política se aplica de forma sistêmica, ou seja, aplica-se a todos os diretores, gestores, colaboradores, prestadores de serviços, fornecedores e parceiros que possuam relações com o Z-ON.

3. DEFINIÇÕES

- **Dado:** conjunto de informações que não foram tratadas, organizadas ou interpretadas, de forma que não tem um significado claro.
- **Informação:** conjunto de dados organizados, que podem ser utilizados para produção e transmissão de conhecimento, contidos em meio físico ou digital.
- **Segurança da informação:** proteção de ativos de informação, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação a confidencialidade, a integridade e a disponibilidade.
- **Segurança cibernética:** conjunto de ações sobre pessoas, tecnologias e processos contra os ataques cibernéticos. Por vezes nomeada segurança digital ou segurança de TI, é uma ramificação na segurança da informação.
- **Ativo de informação:** são os meios, locais, equipamentos e sistemas de armazenamento, transmissão e processamento da informação.
- **Confidencialidade:** garantia de que o acesso aos dados e informações estejam disponíveis apenas para pessoas autorizadas e quando eles de fato forem necessários.
- **Integridade:** garantia da exatidão e da completude dos dados e informações tratados pelas instituições.
- **Disponibilidade:** garantia de que os dados e informações estejam disponíveis para as pessoas autorizadas sempre que necessários.
- **Vulnerabilidade:** qualquer fator que possa contribuir para gerar invasões, roubos de dados ou acessos não autorizados a ativos de informação.
- **Incidente:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos de informação.

- **Phishing:** técnica de crime cibernético que usa fraude, truque ou engano para manipular as pessoas e obter informações confidenciais.
- **Malware:** proveniente do inglês *"malicious software"* (software malicioso), é um software destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações.

4. DIRETRIZES

O Z-ON, por meio desta política aprovada pela sua Diretoria Executiva, estabelece as seguintes diretrizes relacionadas à segurança de informação e cibernética:

- Todas as decisões que afetam a segurança da informação e cibernética tomadas pelo Comitê de Riscos (CORIS) ou pela Diretoria Executiva, ocorrerá mediante ao devido assessoramento especializado sobre o tema;
- Tratamento de informações do Z-ON, cliente, parceiros e público em geral respeitando os princípios de confidencialidade, integridade e disponibilidade.
- Identificação única, pessoal e intransferível de pessoas autorizadas a acessar informações, de forma que seja possível qualificar o responsável pelas ações realizadas em ativos de informação.
- Concessão de acessos a ativos de informação restrita aos recursos indispensáveis para o pleno desempenho das atividades da pessoa autorizada.
- Segregação entre as funções de gerenciamento de ativos de informação e gerenciamento do risco cibernético.
- Identificação contínua dos riscos relacionados à segurança da informação e cibernética, e atuação para mantê-los em níveis considerados aceitáveis, sendo o seu gerenciamento realizado de forma integrada com os demais riscos do Z-ON.
- Estabelecimento de procedimentos e controles para a redução de vulnerabilidades, gestão de incidentes, classificação de informações, rastreabilidade de informações sensíveis, entre outros, por meio de normativos específicos.
- Desenvolvimento e manutenção de controles efetivos, de forma a garantir a proteção de ativos de informação em todo o seu ciclo de vida.
- Aplicação dos procedimentos e controles de segurança da informação e cibernética nos ativos de informação desenvolvidos internamente e nos adquiridos de terceiros.
- Homologação, pelo CORIS, dos prestadores de serviços, parceiros ou fornecedores que sejam considerados relevantes para as instituições ou que manuseiam dados ou informações do Z-ON, clientes ou público em geral;
- Promoção da cultura de segurança da informação e cibernética em todos os níveis do Z-ON, incluindo a prestação de informações a cliente

e público em geral sobre precauções na utilização de produtos e serviços financeiros.

4.1 Procedimentos e Controles

Para reduzir a vulnerabilidade do Z-ON, prevenir o vazamento de informações e atender ao objetivo de segurança da informação e cibernética são adotados procedimentos e controles, conforme o porte e perfil, tais como:

- **Gestão de Acessos:** as concessões, revisões e exclusões de acessos utilizam as ferramentas e os processos definidos pela estrutura centralizada, incluindo as regras para controlar a complexidade e a qualidade das credenciais de acesso aos ativos de informação do Z-ON.
- **Gestão de ativos de informação:** os ativos de informação são identificados de forma individual, inventariados e protegidos, fisicamente, nos casos aplicáveis, por meio de salas com acesso controlado, e logicamente, por meio de hardening, monitoramentos, autenticação e autorização, além de recursos para evitar a ação de malware, controles de criptografia, atualização de sistema operacional e outros softwares e a adoção de configurações de segurança.
- **Classificação da informação:** as informações, mantidas em meio eletrônico ou físico, são classificadas quanto à sua relevância, nos níveis Pública, Interna e Confidencial. Para tanto, são considerados os requisitos legais, as necessidades do negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida.
- **Gestão de incidentes:** o ambiente tecnológico do Z-ON é monitorado continuamente para identificação de eventos e incidentes de segurança da informação e cibernética. Os alertas, gerados de acordo com os critérios definidos nos procedimentos específicos, devem ser analisados, classificados, tratados e comunicados.
- **Gravação de trilhas de auditoria:** os acessos em ativos de informação e outros eventos de segurança são gravados por meio de trilhas de auditoria, de forma a permitir a identificação da pessoa que acessou as informações, quando e como o acesso foi realizado, além das principais ações realizadas. As gravações são protegidas contra modificações e acessos não autorizados.
- **Proteção de perímetro:** a infraestrutura de tecnologia da informação é protegida contra negação de serviço (DoS), Spam, Phishing, Malware e outros ataques externos, por meio de soluções definidas pela estrutura centralizada. Além disso, são utilizadas ferramentas para prevenir vazamento de dados, instaladas em estações de trabalho, e-mail, navegadores de internet, impressoras, bem como em dispositivos móveis e qualquer recurso corporativo utilizado no Z-ON.
- **Gestão de Riscos de Segurança da informação:** anualmente, ou sempre que necessário, o Z-ON realiza a Avaliação Interna de Risco de Segurança da Informação que tem como objetivo identificar, classificar,

avaliar e tratamento de riscos voltados a segurança da informação e cibernética.

- **Gestão de Terceiros:** durante o processo de contratação de terceiros, parceiros e prestadores de serviço, o Z-ON realiza diligências necessárias buscando identificar e classificar os riscos de Segurança de Informação e Cibernética, bem como estabelece cláusulas contratuais voltados a mitigação dos supracitados riscos, conforme procedimentos específicos.
- **Política de Continuidade de Negócios:** as diretrizes e os princípios que envolvem o plano de continuidade de negócio, bem como, o planejamento e aplicação de testes de segurança são definidos e estabelecidos em políticas e documentos específicos.
- **Treinamentos e Cultura:** todos os diretores, colaboradores e prestadores de serviços que atuem em atividades internas do Z-ON, participam de treinamentos e avalições, periódicas, voltadas para Segurança da Informação e Cibernética, conforme Política de Treinamento do Z-ON.
- **Relatório de Implementação:** anualmente, a Área de Governança, Risco e Compliance elabora o Relatório de Implementação de Segurança de Informação e Cibernética e encaminha para o Comitê de Risco, que deve aprová-lo ou não.

4.2 Resolução CMN nº 5.274/2025

Adicionalmente ao disposto na Política, os procedimentos e controles de segurança cibernética devem abranger, no mínimo: (i) autenticação; (ii) criptografia; (iii) prevenção e detecção de intrusão; (iv) prevenção de vazamentos de informações; (v) proteção contra softwares maliciosos; (vi) rastreabilidade; (vii) gestão de cópias de segurança; (viii) avaliação e correção de vulnerabilidades; (ix) controles de acesso; (x) perfis de configuração segura de ativos de tecnologia; (xi) mecanismos de proteção de rede; (xii) gestão de certificados digitais; (xiii) requisitos de segurança para integração de sistemas por interfaces eletrônicas; e (xiv) ações de inteligência no ambiente cibernético, incluindo monitoramento de informações de interesse da instituição na internet, na Deep Web e na Dark Web, além de grupos privados de comunicação.

Esses controles devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias, bem como verificados, no que couber, em sistemas adquiridos ou desenvolvidos por terceiros quando executados com recursos computacionais da Instituição.

Os mecanismos de rastreabilidade devem abranger transações e operações, contemplando trilhas de auditoria fim a fim (logs para identificar falhas ou comportamentos atípicos), definição de tempo de retenção e retenção segura. A avaliação e correção de vulnerabilidades deve contemplar testes e análises periódicos, varreduras para identificar dispositivos indevidamente conectados à rede corporativa, análises periódicas de vulnerabilidades, testes

de intrusão e correção tempestiva; os testes de intrusão devem ter periodicidade mínima anual, ser realizados com independência e imparcialidade, e ter resultados e planos de ação documentados. Os controles de acesso devem incluir limitação de acesso à rede corporativa a usuários credenciados e dispositivos autorizados, revisão periódica e tempestiva de permissões (especialmente de terceirizados) e MFA para acesso externo.

Os mecanismos de proteção de rede devem contemplar segmentação (especialmente produção e processos críticos), regras de firewall e monitoramento de conexões, critérios e monitoramento de conexões com ambientes externos (inclusive em horários noturnos e dias não úteis), medidas para identificar/prevenir conexões indevidas e processos/ferramentas para tratar eventos atípicos em produção (ex.: VPN e tentativas de acesso privilegiado). A gestão de certificados digitais deve prever monitoramento do uso (com rastreabilidade), guarda de informações e controles sobre chaves privadas, prevenção de compartilhamento indevido e validação tempestiva de certificados revogados.

Como parte integrante desta Política, aplicam-se requisitos adicionais: no caso de comunicação eletrônica de dados na RSFN, incluem MFA para acesso administrativo aos ambientes Pix e STR, isolamento físico e lógico dos ambientes Pix e STR (com instância dedicada em nuvem quando aplicável), monitoramento e guarda de credenciais/certificados (especialmente no SPI), validação de integridade fim a fim das transações antes da assinatura das mensagens e vedação de acesso de terceiros às chaves privadas usadas para assinatura; e, no caso de conexão como participante de SMF autorizados a operar, controles de prevenção, detecção e resposta a fraudes, observados os requisitos técnicos do Catálogo/Manuais do SFN/RSFN.

Considerando que a Instituição utiliza plataforma SaaS provida pela Matera para componentes relevantes de sua infraestrutura tecnológica, parte dos procedimentos e controles previstos nesta Política poderá ser executada pelo fornecedor, conforme a arquitetura e o modelo de prestação do serviço. Nessas situações, a Instituição assegurará o cumprimento dos requisitos aplicáveis por meio de governança sobre o fornecedor, incluindo avaliação de risco, cláusulas contratuais e SLAs de segurança, acompanhamento periódico, tratamento de não conformidades e obtenção de evidências (relatórios, atestados, resultados de testes, informações de incidentes e demais comprovações pertinentes), sem prejuízo da responsabilidade da Instituição pelos controles sob sua própria governança e pela supervisão dos serviços terceirizados.

5. PAPÉIS E RESPONSABILIDADE

5.1 Diretoria

Compete à Diretoria:

- Aprovar e revisar anualmente as políticas e estratégias de segurança da informação e cibernética;
- Assegurar a aderência do Z-ON às políticas e estratégias de segurança da informação e cibernética;
- Designar o diretor responsável pela segurança da informação e cibernética do Z-ON;
- Promover a disseminação da cultura de segurança da informação e cibernética.
- Assegurar a disponibilização de estrutura e recursos necessários ao desenvolvimento e manutenção do Sistema de Segurança de Informação e Cibernética;
- Supervisionar, com o auxílio do Comitê de Riscos, o cumprimento desta Política;

5.2 Comitê de Riscos (CORIS)

Compete ao CORIS:

- Aprovar as normas, procedimentos, medidas e orientações, de caráter corporativo, relacionados à segurança da informação e cibernética;
- Submeter à Diretoria propostas para adoção ou alterações de políticas e manuais aplicáveis ao tema;
- Propor as atribuições para as áreas operacionais diretamente afetadas pelas regras de segurança da informação e cibernétic designação das correlatas responsabilidades;
- Acompanhar a efetividade das atividades e das ações relacionadas à segurança da informação e cibernética;
- Garantir o cumprimento de todas as regras e procedimentos estabelecidos na Política, normas e nos manuais relacionados a à segurança da informação e cibernética;
- Apreciar os relatórios e comunicações emitidos pelos órgãos reguladores, autorreguladores, pela auditoria interna e auditoria externa, determinando as ações e providências necessárias para atendimento das demandas;
- Deliberar sobre os procedimentos de segurança da informação e cibernética e recomendar ações mitigatórias de risco que assegurem a correta realização das atividades do Z-ON;
- Analisar e decidir sobre aceitação ou veto para relacionamentos com clientes, colaboradores, fornecedores, parceiros e prestadores de serviços que apresentem alta risco à segurança da informação e cibernética, em razão dos riscos envolvidos.
- Revisar anualmente a presente política e submeter à aprovação da Diretoria;

5.3 Área de Governança, Riscos e Compliance

- Identificar, comunicar e monitorar os riscos relacionados à segurança da informação e cibernética, atuando na segunda linha de defesa do Z-ON;
- Definir os critérios para geração de alertas de eventos e incidentes de segurança da informação e cibernética;
- Monitorar os eventos e incidentes de segurança da informação e cibernética;
- Comunicar incidentes de segurança da informação e cibernética às partes interessadas no Z-ON e conforme estabelecido nas resoluções em vigor;
- Conduzir as ações de resposta a incidente de segurança da informação e cibernética;
- Desenvolver e manter a política e os normativos de segurança da informação e cibernética;
- Homologar os prestadores de serviços a terceiros considerados relevantes ou que manuseiem dados e informações das instituições, cooperados e público em geral;
- Desenvolver e manter o programa educacional em segurança da informação e cibernética;
- Elaborar e apresentar indicadores e relatórios de segurança da informação e cibernética considerados relevantes para apoiar o processo de tomada de decisão.

6. VIGÊNCIA E HISTÓRICO DE APROVAÇÕES

Os normativos vigentes que abordam temas de abrangência sistêmica, permanecem validos até que Área de Compliance publique uma documentação sistêmica relacionada. Após esta publicação, a política anterior será considerada revogada, podendo existir normas e manuais internos ou específicos complementares ao assunto.

A presente política passa a vigorar a partir de sua aprovação, sendo parte integrante do ambiente normativo interno do Z-ON. Os regramentos complementares, quando aplicáveis, a esta política estão estabelecidos nas normas sistêmicas.

Complementam a presente política e a ela se subordinam todas as normas e procedimentos operacionais que regulam os procedimentos e processo de segurança da informação e cibernética do Z-ON.

DATA	DESCRIÇÃO	APROVADOR
05/01/2024	Criação da Política	Diretoria Executiva
10/01/2026	Revisão da Política	Diretoria Executiva