POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TORRA SOCIEDADE DE CRÉDITO DIRETO

Sumário

1. OBJETIVO

A Política de Segurança da Informação (PSI) estabelece diretrizes essenciais para proteger dados e ativos tecnológicos da Torra ACC, garantindo confidencialidade, integridade e disponibilidade das informações. A Torra ACC mantém um Programa de Segurança Cibernética alinhado à Resolução 4.893/2021, que contempla controles preventivos, monitoramento contínuo, gestão de vulnerabilidades, treinamento e resposta a incidentes.

2. APLICAÇÃO

Esta política se aplica a todos os colaboradores, prestadores de serviço, parceiros e fornecedores que tratem informações da Torra ACC. Seu cumprimento é obrigatório em qualquer ambiente corporativo, incluindo computação em nuvem e sistemas sob gestão de terceiros.

3. REFERÊNCIAS

Baseada nas normas ISO/IEC 27001, 27002, 27701, Resoluções Bacen 4.893/2021 e 4.98/2025, além da Lei Geral de Proteção de Dados (LGPD).

4. DEFINIÇÕES

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

Informações – As informações são definidas como todos os documentos, desenhos, dados eletrônicos e conhecimentos obtidos através de negócios, tangíveis ou intangíveis, de qualquer forma.

SI – Segurança da Informação.

TI – Tecnologia da Informação.

Usuário – Todos que recebem acesso a informações, recursos e ativos de informação.

5. RESPONSABILIDADES

Alta Administração: aprova a política, aloca recursos e supervisiona riscos e segurança cibernética.

Comitê de Segurança: avalia incidentes, vulnerabilidades e eficácia dos controles.

Diretor de Segurança Cibernética: coordena o Programa de Segurança e comunicação com o Bacen.

TI/SI: implementa controles, monitora ambientes, realiza backups e gerência acessos.

Usuários: seguem as diretrizes, protegem informações e reportam incidentes.

6. DIRETRIZES

Para assegurar o atendimento e conformidade às diretrizes desta política são estabelecidas regras de negócios específicas para cada tópico relacionado a segurança da informação, conforme segue:

6.1 Gestão e Uso Aceitável De Ativos Da Informação

Ativos são inventariados, monitorados e devem ser usados apenas para fins corporativos. É proibido subir dados confidenciais ou pessoais em serviços públicos de IA ou ferramentas externas. Softwares só podem ser utilizados se homologados pela TI.

6.2 Mesa e Tela Limpa

Manter o sigilo das informações, bloquear o equipamento ao se ausentar, evitar impressões desnecessárias e descartar documentos de forma segura.

6.3 Classificação da Informação

Informações devem ser classificadas conforme sua sensibilidade e utilizadas somente por quem tem autorização e necessidade de acesso.

6.4 Gestão de Incidentes

Todo incidente ou suspeita deve ser reportado imediatamente pelos canais oficiais. Incidentes críticos são comunicados ao Bacen, e registros são mantidos por no mínimo cinco anos.

6.5 Gestão De Acessos Lógico

A Torra ACC para concessão de acessos segue o princípio do menor privilégio, com revisões periódicas e uso obrigatório de autenticação multifator em sistemas críticos.

6.6 Segurança Física

Ambientes físicos são controlados e monitorados, garantindo proteção contra acessos indevidos, danos e perdas.

6.7 Gestão de Riscos e Controles Internos

A Torra ACC adota uma estrutura de gestão de riscos integrada, conforme Resolução 4.98/2025, contemplando riscos cibernéticos, financeiros, operacionais, de terceiros e de conformidade.

6.8 Gestão de Terceiros e Provedores De Serviço

Os relacionamentos com terceiros e prestadores de serviços devem garantir a proteção das informações, dados e ativos tecnológicos acessados, processados ou armazenados, conforme as diretrizes das Resoluções Bacen nº 4.893/2021 e nº 498/2025.

Os riscos associados à cadeia de suprimentos devem ser identificados, avaliados, mitigados e monitorados de forma contínua, considerando os controles e responsabilidades contratuais definidos entre as partes.

6.9 Aquisição e Desenvolvimento de Sistemas

Toda a aquisição de novos sistemas e produtos devem ser avaliadas considerando a adoção do conceito de "Privacy e Security by Design e by Default", considerando as medidas de segurança e privacidade desde a definição do escopo do projeto e deve ser acompanhado pelo time de TI e Privacidade de Dados.

Não é permitido uso de softwares ou ferramentas particulares para atividades corporativas, que não tenham sido autorizados formalmente pela Torra ACC.

6.10 Controles Criptográficos

Para devida proteção das informações visando assegurar sua integridade, confidencialidade e disponibilidade controles criptográficos devem ser usados em informações armazenadas ou em trânsito.

6.11 Backup e Restore

Cópias de segurança de informações devem ser realizadas e testadas a intervalos regulares, conforme os critérios de cópia serão estabelecidos pelo responsável ou custodiante considerando: frequência de realização, conteúdo, recuperação, armazenamento e tempo de retenção.

6.12 Continuidade De Negócios E Recuperação Cibernética

O processo de gestão de continuidade de negócios deve compreender todos os elementos-chave necessários para a correta identificação de ameaças e a escolha e aplicação adequada de controles visando evitar e/ou reduzir impactos no ambiente da Torra ACC.

6.13 Conscientização e Treinamento

A Torra ACC promove programas de conscientização e capacitação anual sobre segurança da informação,

privacidade e prevenção de fraudes;

Devem ser conduzidas simulações de phishing e campanhas sobre comportamento seguro.

6.14 Monitoramento

Para assegurar a conformidade aos requisitos desta política serão estabelecidos procedimentos de monitoramento dos serviços críticos, como serviços de e-mail, internet e outros recursos que forem disponibilizados para atendimento a seus clientes.

6.15 Conformidade, Requisitos Legais e Regulatórios

A Torra ACC deve atender a todos os requisitos legais, tais como: estatutos, regulamentações ou obrigações contratuais aplicáveis aos processos de negócio.
Estes requisitos devem ser explicitamente definidos, documentados e atualizados. Além disso, devem ser estabelecidos e documentados os responsáveis internos por manter o cumprimento destes requisitos.

6.16 Propriedade Intelectual

A Torra ACC assegura a proteção adequada da propriedade intelectual em conformidade com as diretrizes estabelecidas pela ISO/IEC 27001, por meio da implementação de medidas que preservem os direitos de propriedade intelectual, incluindo patentes, marcas, direitos autorais e segredos comerciais

6.17 Auditoria dos Controles de Segurança da Informação

A Torra ACC deve realizar auditorias anuais dos controles de segurança da informação e privacidade conforme diretrizes da ISO/IEC 27001, Resoluções 4.983/2021 e 498/25 do Banco Central. As auditorias poderão ser realizadas por auditores internos qualificados ou por terceiros independentes, com frequência definida com base na criticidade dos processos e nas mudanças no ambiente de risco, garantindo a avaliação integral dos controles de segurança, processos e sistemas relevantes.

6.18 Melhoria Contínua do Sistema de Gestão da Segurança da Informação

A melhoria contínua do Sistema de Gestão da Segurança da Informação é crucial para manter a eficácia e a relevância das práticas de segurança em um ambiente dinâmico e em constante evolução.

7. SANÇÕES E PENALIDADES

Todas as ações que possam infringir as documentações da Torra ACC, assim como quaisquer legislações, estão

sujeitas a sanções administrativas conforme prevista no contrato de trabalho e prestação de serviços.

8. REVISÃO E ATUALIZAÇÃO

Esta política deverá ser revisada anualmente ou quando houver mudança significativa no negócio e/ou ambiente.

9. REGISTROS DE VERSÕES

Data	Versão do documento	Responsável	Aprovador
04/11/2025	Ver. 01	Anielle Trizzi	