POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1 OBJETIVO 3

2 ABRANGÊNCIA 3

3 REFERÊNCIAS 3

4 CONCEITOS 3

5 DIRETRIZES 4

6 RESPONSABILIDADES 6

7 DISPOSIÇÕES FINAIS 8

8 INFORMAÇÕES DE CONTROLE 8

1 OBJETIVO

Esta Política tem por objetivo estabelecer os conceitos e as diretrizes de segurança da informação, visando proteger a organização, os clientes e o público em geral.

2 ABRANGÊNCIA

Esta Política aplica-se a administradores, funcionários, estagiários, fornecedores, prestadores de serviços e parceiros da B3 S.A. – Brasil, Bolsa, Balcão, suas controladas no exterior, bem como ao Banco B3, à BSM, à Cetip Info Tecnologia S.A, ao B3 Social e demais associações (Companhia).

3 REFERÊNCIAS

- Código de Conduta e Ética;
- Política de Gestão de Riscos Corporativos;
- Política de Continuidade de Negócios;
- Política de Tecnologia da Informação;
- ABNT NBR ISO IEC 27002:2005;
- CPMI - IOSCO *Guidance on cyber resilience for financial market infrastructures*; e
- NIST - *National Institute of Standards and Technology Framework*.

4 CONCEITOS

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- confidencialidade: garantia de que a informação somente possa ser acessada por pessoas autorizadas, para uso específico e pelo período necessário;

- disponibilidade: garantia de que a informação esteja disponível para as pessoas autorizadas quando se fizer necessária; e

- integridade: garantia de que a informação esteja completa, exata, íntegra e que não tenha sido modificada ou destruída indevidamente, de maneira não autorizada ou acidental durante o seu ciclo de vida.

5 DIRETRIZES

A informação constitui-se ativo valioso de extrema importância para a Companhia e fundamental para o sucesso dos seus negócios, merecendo, portanto, proteção adequada.

Segurança da informação consiste na adoção de medidas para proteger a propriedade, confidencialidade, disponibilidade e integridade da informação, em qualquer forma e suporte que se apresente – física ou digital –, das diversas ameaças existentes, a fim de evitar seu uso indevido, inadequado, ilegal ou em desconformidade com as políticas e os procedimentos internos. Para tanto, devem ser observadas as diretrizes a seguir indicadas.

Os riscos de segurança da informação seguem a metodologia de riscos corporativos da B3.

5.1 Propriedade, monitoramento e classificação da informação

As informações produzidas pelos colaboradores abrangidos por esta Política (em formato físico ou digital) são de propriedade exclusiva da Companhia, bem como as informações a ela disponibilizadas, de maneira autorizada, por terceiros, devendo ser utilizadas exclusivamente para o atendimento dos objetivos do negócio.

Os equipamentos, meios de comunicação e sistemas da Companhia estão sujeitos a monitoramento, sendo certo que eventuais informações de cunho pessoal tratadas por esses meios ou fornecidas à Companhia serão abrangidas por referido controle. O monitoramento aqui previsto é de conhecimento de todos os colaboradores abrangidos por esta Política.

Deve existir método para a classificação da informação de acordo com o nível de confidencialidade e criticidade para o negócio da Companhia.

As informações devem ser atribuídas a proprietários, formalmente designados como responsáveis pela autorização de acesso às informações sob a sua responsabilidade.

As informações devem estar adequadamente protegidas e rotuladas em observância às diretrizes de segurança da informação da Companhia em todo o ciclo de vida, que compreende: geração, acesso, manuseio, armazenamento, reprodução, transporte e descarte.

5.2 Acessos e identidades

Os acessos às informações e aos ambientes tecnológicos da Companhia devem ser controlados de acordo com sua classificação e revisados periodicamente, de forma a serem disponibilizados apenas às pessoas autorizadas e com os privilégios necessários para o desempenho de suas atividades.

5.3 Descarte de informações

O descarte da informação deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital. A informação deve ser descartada considerando prazos mínimos legais ou regulatórios, bem como sua necessidade para o negócio ou a área, o que for maior.

5.4 Fornecedores e partes externas

Os contratos com as empresas prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ao ambiente da Companhia devem conter cláusulas que assegurem o cumprimento das regras de segurança da informação, bem como penalidades no caso de descumprimento.

Para os participantes, devem ser prestadas informações sobre precauções na utilização de produtos e serviços oferecidos.

5.5 Continuidade de negócios

A gestão de continuidade de negócios estabelece e mantém estrutura estratégica e operacional preparada para gerenciar e responder à interrupção nos processos que suportam os negócios da Companhia. Este é disciplinado pela Política de Continuidade de Negócios e de Gestão de Crises.

5.6 Treinamento de Segurança da Informação e Proteção de Dados

Os administradores, funcionários, estagiários, fornecedores e prestadores de serviços, obrigatoriamente, devem realizar o treinamento de Segurança da Informação e Proteção de Dados, anualmente.

5.7 Plano Diretor

As estratégias de cibersegurança são definidas no Plano Diretor de Segurança e Privacidade e devidamente avaliadas pelo Comitê de Segurança da informação, que também são responsáveis por monitorar os controles de segurança, direcionar e priorizar as ações de segurança.

6 RESPONSABILIDADES

6.1 Colaboradores abrangidos por esta Política

- Cumprir as regras de Segurança da Informação;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados;
- Assegurar que os recursos tecnológicos, as informações e os sistemas a sua disposição sejam utilizados apenas para as finalidades de negócio;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir, citar ou compartilhar assuntos confidenciais em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo comentários e opiniões em blogs e redes sociais;

- Não compartilhar informações confidenciais de qualquer tipo; e
- Comunicar imediatamente à Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas normas e procedimentos.

6.2 Gestores

- Reforçar e orientar a equipe em relação a práticas, processos de segurança e acessos a sistemas.

6.3 Diretoria de *Cyber Security*

- Prover ampla divulgação da Política e das Normas de Segurança da Informação;
- Promover ações de conscientização e treinamento sobre segurança da informação para os administradores, funcionários, estagiários, fornecedores e prestadores de serviços;
- Propor ações de aperfeiçoamento da segurança da informação; e
- Estabelecer normas e procedimentos relacionados à instrumentação da segurança da informação, dispondo sobre a propriedade e o uso da informação, a gestão de acessos e identidades e os incidentes de segurança da informação.

6.4 Diretoria de Contabilidade e Administração

- Assegurar que contratos com as empresas prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ao ambiente da Companhia contenham cláusulas que assegurem o cumprimento desta Política e das Normas de Segurança da Informação, bem como penalidades no caso de descumprimento.

6.5 Diretoria Colegiada

- Realizar o treinamento de Segurança da Informação e Proteção de Dados anualmente.

6.6 Conselho Fiscal

- Realizar o treinamento de Segurança da Informação e Proteção de Dados anualmente.

6.7 Conselho de Administração

- Aprovar a presente Política de Segurança da Informação, bem como suas revisões.
- Realizar o treinamento de Segurança da Informação e Proteção de Dados anualmente.

7 DISPOSIÇÕES FINAIS

O disposto acima se aplica, imediatamente, para toda a Companhia, a partir da publicação da presente Política.

8 INFORMAÇÕES DE CONTROLE

Vigência: a partir de 26 de abril de 2024.

1ª versão: 16/02/2009.

Responsáveis pelo documento:

Responsável	Área
Elaboração	Gerência de Governança e Riscos de Segurança
Revisão	Diretoria Executiva de Governança, Gestão Integrada e Segurança Cibernética Diretoria Executiva Jurídica Comitê de Governança e Indicação
Aprovação	Comitê Interno de Segurança Cibernética Conselho de Administração

Ciência	Diretoria Colegiada

Registro de alterações:

Versão	Item Modificado	Motivo	Data
01	Versão Original	N/A	16/02/2009
01.1	Diversos	Primeira revisão da Política	10/08/2009
01.2	Diversos	Inclusão da abrangência da Política, atualização das nomenclaturas das áreas e revisão na aplicação da Política.	27/12/2010
02	Diversos	Ampliação das diretrizes, substituição de glossário por definições, remoção de regras da Política.	08/03/2011
03	Diversos	Revisão geral, foco nas diretrizes corporativas para a Segurança da Informação.	15/05/2013
04	Diversos	Inclusão dos conceitos e gestão de incidentes, simplificação das diretrizes e responsabilidades.	06/05/2014
05	Diversos	Adequação para B3 S.A. – Brasil, Bolsa, Balcão	12/05/2017

06	Diversos	Restruturação dos tópicos e remoção de regras similares. Inclusão de cláusulas que assegurem o cumprimento de regras de segurança da informação nos contratos firmados com fornecedores e partes externas. Inclusão de responsabilidades para a Superintendência de Administração, Suprimentos e Patrimônio e para os gestores. Determinação do descarte das informações de modo a impedir sua reconstituição, respeitados os prazos legais e regulatórios. Reavaliação dos pontos de sobreposição com a Política de Tecnologia da Informação.	01/06/2018
07	Abrangência Formatação	Adequação à nova estrutura de governança de controladas B3 Adequação ao novo *template*	17/08/2020
08	Referências Formatação	Inclusão do *National Institute of Standards and Technology Framework* nas referências	12/04/2021
09	Responsabilidades	Atualização do nome da área Diretoria de *Cyber Security* Inclusão de responsabilidade ao Conselho de Administração	08/12/2022
10	Treinamento de Segurança da Informação e Proteção de Dados Responsabilidades	Atualização do tópico 5. Diretrizes Inclusão do tópico 5.6 Treinamento de Segurança da Informação e Proteção de Dados Inclusão do tópico 5.7 Plano Diretor Atualização do tópico 6.3. Atualização de responsabilidade do Conselho de Administração	08/12/2023

11	5.4 Fornecedores e partes externas	Inclusão de informações sobre precauções na utilização de produtos e serviços oferecidos aos participantes	26/04/2024