Política de Segurança Cibernética E Segurança da Informação

Janeiro 2025

Contents

1. Objetivo

A BCP Securities Distribuidora de Títulos e Valores Mobiliários Ltda. (BCP DTVM) reconhece a importância da segurança cibernética e da informação como um pilar fundamental para a proteção de seus ativos, clientes e operações. O objetivo desta política é estabelecer diretrizes claras e abrangentes para a implantação e manutenção de práticas de segurança cibernética e de informação, visando preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações. Esta política também busca garantir a conformidade com as regulamentações vigentes e promover uma cultura organizacional que valorize a segurança em todas as suas dimensões

2. Aplicação

Esta política se aplica a todas as áreas, locais e prestadores de serviço da BCP DTVM, que utilizam, armazenam ou processam informações da instituição. É responsabilidade de todos os colaboradores, parceiros e terceiros contratados aderir estritamente às diretrizes estabelecidas neste documento.

3. Referências

Esta política está alinhada com as seguintes normas e frameworks:

- ISO 27000, 27001, 27002 (Segurança da Informação)
- ISO 27701 (Privacidade)
- Frameworks NIST, COBIT, ITIL
- LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709/2018)
- Regulamentações da CVM e Banco Central

4. Definições

Segurança da Informação: Conjunto de medidas para preservar a confidencialidade, integridade, autenticidade e disponibilidade das informações.

Confidencialidade: Garantia de que a informação é acessível somente por pessoas autorizadas.

Integridade: Proteção da exatidão e completude das informações.

Disponibilidade: Garantia de que as informações e os recursos de TI estão disponíveis sempre que necessário.

Autenticidade: Garantia de que as informações são genuínas e provenientes de fontes verificadas.

5. Princípios Gerais

A BCP DTVM adota os seguintes princípios:

Proatividade: Antecipar e mitigar riscos cibernéticos antes que eles se materializem.

Resiliência: Desenvolver e manter a capacidade de resistir e se recuperar rapidamente de incidentes cibernéticos.

Conformidade: Assegurar o cumprimento de todas as regulamentações aplicáveis e padrões da indústria.

Cultura de Segurança: Promover uma cultura organizacional que valorize a segurança cibernética e da informação em todos os níveis da empresa.

6. Responsabilidades

6.1 – Diretoria

- Promover e liderar a cultura de segurança cibernética na instituição.
- Garantir que a política esteja alinhada com as regulamentações vigentes e que seja revisada anualmente ou conforme necessário.
- Aprovar exceções à política e garantir a implementação de medidas corretivas após a identificação de deficiências.

6.2 – Compliance

- Assegurar que a política esteja em conformidade com os regulamentos e diretrizes internas.
- Desenvolver e revisar o relatório anual de implementação do plano de ação e resposta a incidentes.
- Garantir que todos os colaboradores e terceiros estejam cientes desta política e dos requisitos associados.

6.3- Tecnologia da Informação

- Implementar e manter os procedimentos e tecnologias necessários para garantir a conformidade com esta política.
- Realizar testes regulares de recuperação de desastres e manter um plano atualizado de continuidade de negócios.
- Monitorar continuamente o ambiente de TI para identificar e mitigar riscos.

6.4- Colaboradores, Prestadores de Serviços de TI e Terceiros Contratados

- Cumprir integralmente as diretrizes desta política.
- Reportar imediatamente qualquer incidente ou ação que possa comprometer a segurança da informação.

7. Gestão de Riscos e Controles

7.1- Classificação da Informação

- **Confidencial:** Informações que exigem proteção especial devido ao seu potencial impacto em caso de divulgação não autorizada.
- **Restrita:** Informações que, embora sensíveis, possuem impacto menor que as confidenciais.
- **Interna:** Informações destinadas exclusivamente ao uso interno, com impacto moderado em caso de divulgação não autorizada.
- **Pública:** Informações que podem ser divulgadas publicamente sem causar danos à empresa.

7.2- Segurança Física e do Ambiente

- Todas as informações classificadas como confidenciais devem ser armazenadas em áreas seguras, com controle de acesso apropriado.
- Medidas de segurança devem ser implementadas para proteger informações impressas ou armazenadas em mídias físicas contra vazamentos.
- Controle de Acesso e Segregação de Funções
- Implementar políticas de acesso baseado em papéis (RBAC) e revisar periodicamente os direitos de acesso.
- Garantir que as funções críticas sejam segregadas para minimizar o risco de erros ou fraudes.

7.3- Senhas e Autenticação

- Implementar autenticação multifator (MFA) para sistemas críticos.
- Garantir que as senhas sejam únicas, complexas e alteradas regularmente, em conformidade com as melhores práticas de segurança.

7.4- Criptografia

- Utilizar criptografia de ponta a ponta para proteger dados em trânsito e em repouso.
- As chaves criptográficas devem ser gerenciadas de forma segura e revisadas periodicamente.

7.5- Prevenção e Detecção de Intrusão

- Monitorar continuamente o tráfego de rede para identificar e mitigar atividades maliciosas.
- Utilizar sistemas como Sophos e Zabbix para garantir a segurança ativa do ambiente de TI.

7.6- Backup e Recuperação de Dados

- Realizar backups diários e testar regularmente a restauração dos dados.
- Armazenar cópias de backup em locais fisicamente separados para garantir a recuperação em caso de desastre.

8. Conscientização e Treinamento

Todos os colaboradores devem participar de programas anuais de conscientização sobre segurança cibernética, incluindo simulações de phishing e workshops práticos.

A comunicação contínua será mantida por meio de boletins informativos, sessões de Q&A e uma biblioteca de recursos acessível a todos.

9. Monitoramento e Auditoria

Realizar auditorias internas regulares para verificar a conformidade com esta política e revisar periodicamente incidentes para melhorar as práticas de segurança.

Manter um histórico de versões da política, documentando as principais mudanças realizadas.

10. Tratamento de Incidentes

Incidentes de segurança devem ser documentados, analisados e comunicados aos stakeholders relevantes.

Desenvolver e manter um plano de resposta a incidentes para garantir que a BCP DTVM possa responder rapidamente e de forma eficaz a qualquer incidente cibernético.

11. Sanções

O descumprimento desta política poderá resultar em medidas disciplinares proporcionais à gravidade da infração, incluindo advertências, suspensão, demissão e possíveis ações legais.