BNP PARIBAS
CARDIF

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Segurança Global | BNP Paribas Cardif do Brasil

INDEX

1. ABSTRACT

The aim of this document is the establishment of a working scope; a policy and its objectives for the Information Security Management System of BNP Paribas Cardif of Brazil, providing guide and support to executive management in giving adequate support and resources to Information Security.

2. OBJETIVO

O Sistema de Gestão de Segurança da Informação tem como objetivo a minimização sistemática dos riscos.

Para cumprir com esse objetivo, este documento estabelece um escopo de trabalho para a BNP Paribas Cardif do Brasil no âmbito da segurança da informação.

Também é objetivo deste documento definir aspectos gerais do Sistema de Gestão de Segurança da Informação, tais como:

- Definição de Segurança da Informação e sua importância para a BNP Paribas Cardif do Brasil;
- Estabelecimento do comprometimento da Alta Gestão com a Segurança Global;
- Estrutura para Gerenciamento de Riscos;
- Explicação geral dos princípios e políticas que norteiam o Sistema de Gestão de Segurança da Informação (SGSI);
- Governança (Papéis e Responsabilidades) dentro do SGSI e estrutura organizacional da empresa.

3. ESCOPO DE APLICAÇÃO

As políticas e procedimentos de Segurança da Informação e Cibernética aplicam-se para todos[1] os funcionários, contratados, terceirizados, trabalhadores temporários, e aqueles empregados por outros para executar trabalhos nas instalações da BNP Paribas Cardif do Brasil, ou com acesso a qualquer informação, sistema, computador, rede de computadores, telecomunicação, mensagem ou serviço de informações pertencentes à BNP Paribas Cardif do Brasil em todas as divisões, subsidiárias, filiais e parcerias onde as leis locais, estatutos e regulamentações do governo não se sobreponham a essas políticas e procedimentos e de acordo com o escopo definido.

4. INTRODUÇÃO

A BNP Paribas Cardif do Brasil entende que a **Informação**, sua criação, processamento, armazenamento e transferência (compartilhamento) são componentes indispensáveis para o cumprimento da sua **missão** de **desenvolver soluções de relacionamento de longo prazo**, e sua visão de **ser a maior seguradora de afinidades do país**.

Devido à informação ser um ativo chave, devem ser tomadas todas as precauções razoáveis para sua proteção.

A proteção da informação requer que sejam preservadas sua confidencialidade, integridade e disponibilidade[2]. A correta proteção dessas características permitirá à BNP

[1] Este grupo de pessoas é designado em todos os documentos como "Colaboradores"

[2] Para definição dessas características, ler o documento "Guia - Definições e Terminologias", que faz parte do SGSI.

Paribas Cardif do Brasil gerar maior valor para os seus clientes, funcionários, fornecedores e acionistas.

A política é de obrigatório cumprimento por parte de todos os colaboradores da BNP Paribas Cardif do Brasil.

5. DECLARAÇÃO DE COMPROMISSO DA ALTA GESTÃO

A BNP Paribas Cardif do Brasil, ciente da importância da informação para o desenvolvimento da sua missão de desenvolvimento de soluções de relacionamento de longo prazo na área de seguros de afinidades, está altamente comprometida com a preservação da segurança dessa informação.

Como parte desse compromisso, a BNP Paribas Cardif do Brasil praticará os esforços razoáveis e cumprirá com os requerimentos exigidos pela lei para proteger a confidencialidade, integridade e disponibilidade das informações criadas, processadas, armazenadas e transmitidas como parte das suas atividades comerciais.

6. RISCO

O Sistema de Gestão de Segurança da Informação da BNP Paribas Cardif do Brasil está voltado para a minimização do risco de segurança de Informação.

A BNP Paribas Cardif do Brasil entende que o gerenciamento dos riscos em segurança da informação é um processo cíclico e dinâmico que requer uma constante participação de todas as pessoas. Devido ao fato de ser um processo cíclico, está em constante evolução e aprimoramento mediante a comparação dos resultados do processo com os resultados esperados e ajuste das entradas para melhorar os seguintes resultados.

O processo de gerenciamento do risco está baseado nas seguintes etapas:

- Levantamento e avaliação dos riscos de segurança de informação;
- Criação de um plano para o tratamento desses riscos;
- Execução do plano de tratamento de riscos.

O processo é cíclico no sentido de que após a execução do plano de tratamento de riscos, o novo nível de risco deve ser comparado (chamado de risco residual) com o nível avaliado inicialmente.

A informação resultante dessa comparação deve ser utilizada para iniciar novamente o processo.

A descrição detalhada do processo de Análise de Risco está no documento Procedimento - Análise de Riscos, que faz parte do SGSI. Esse documento define a metodologia que deve servir como base para a condução de qualquer análise de risco relacionada à Segurança da Informação.

A lista de controles utilizados pela BNP Paribas Cardif do Brasil para o tratamento do risco está no documento SoA[3] (Statement of Applicability), que faz parte do SGSI.

7. ESTRUTURA ORGANIZACIONAL

[3] O documento em português seria Declaração de Aplicabilidade. Devido a que o nome do documento é reconhecido amplamente como SoA, foi mantida a sua nomenclatura em inglês.

7.1. GESTORES

7.1.1. RESPONSABILIDADES

- A responsabilidade funcional sobre as áreas de operação;
- Responsabilidade de manter atualizada a definição dos ativos de informação e notificar em qualquer alteração no inventário de ativos de sua área;
- Implantar e monitorar a eficácia de procedimentos, instruções de trabalho e documentos quanto à proteção da Segurança da Informação;
- Informar/comunicar todos os fatos relacionados ao SGSI às áreas de operação sob sua responsabilidade;
- Contribuir para implantação dos Objetivos de gestão de Segurança da Informação e efetuar as medições necessárias por processos;
- Implantar as oportunidades de melhoria;
- Planejar a adoção de procedimentos do SGSI e monitorar sua eficácia;
- Garantir a contínua eficácia dos controles implantados para satisfazer os requisitos do SGSI.

7.2. COLABORADORES

Todos os funcionários, terceiros e prestadores de serviço com funções dentro da estrutura da BNP Paribas Cardif do Brasil.

7.2.1. RESPONSABILIDADES

- Responsabilidade de notificação em qualquer alteração no inventário de ativos de sua área;
- Conhecer e seguir os procedimentos pertencentes ao SGSI;
- Recomendar melhorias no SGSI para melhoria do processo;
- Identificar qualquer incidente de segurança e reportá-lo ao seu gestor/contato direto dentro da BNP Paribas Cardif do Brasil. No caso de terceirizados e prestadores de serviço, reportar diretamente para a área de Segurança Global;
- Todos os colaboradores, têm a responsabilidade de cuidar pela proteção dos ativos de informação aos que tiverem acesso.

8. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

8.1. DEFINIÇÃO E MANUTENÇÃO

8.1.1. OBJETIVOS ESPECÍFICOS

- Garantir a segurança da informação e padronizar as práticas a serem aplicadas por todo o pessoal com responsabilidade para a segurança da informação;
- Ter consciência dos riscos que ameaçam o sistema de informação e os meios disponíveis para controlá-los;

- Criar uma estrutura geral para projetar e executar medidas de segurança dos sistemas de informação;
- Promover a cooperação entre os departamentos da BNP Paribas Cardif do Brasil para criar, aplicar e verificar as instruções, procedimentos e medidas de segurança relacionadas ao negócio.

8.1.2. CONTROLES DE SEGURANÇA DA INFORMAÇÃO

Os controles de segurança consistem em um **conjunto amplo de medidas de segurança**, visando minimizar os riscos presentes nos ativos de Informação. Os controles são baseados na norma de segurança aceita internacionalmente (**ISO 27001**), nas especificações de segurança impostas pelo **HO (Head Office)** e declarados no SoA (Statement of Applicability).

8.1.3. IMPLANTAÇÃO E AVALIAÇÃO

A BNP Paribas Cardif do Brasil deve estar em conformidade com os requisitos desta política. Os requisitos podem ser revisados para atender as necessidades de parceiros e da própria companhia. O processo de verificação da conformidade desta deve ser conduzido pelo departamento de Segurança Global obedecendo às políticas, normas e procedimentos definidos no **SGSI.**

8.1.4. EXCEÇÃO À POLÍTICA

As exceções serão avaliadas pelo Security Officer e devem ser reportadas por escrito ao Comitê de Segurança Global. O comitê irá avaliar as exceções conforme as justificativas de negócio fornecidas pelo solicitante e definir o tratamento adequado.

8.2. SEGURANÇA CIBERNÉTICA

8.2.1. OBJETIVOS DA SEGURANÇA CIBERNÉTICA

Os objetivos da política derivam dos valores ou ambições do Grupo demonstrada pela Diretoria Executiva nos principais programas: garantir qualidade de serviço de primeira classe, melhorando o desempenho operacional; contribuir para o crescimento e desenvolvimento do Grupo, preservando os fatores históricos de sucesso; aumentar as habilidades ao mesmo tempo em que incentiva o compartilhamento de práticas e uma cultura comum.

Os objetivos da política também são:

- Manter um capital de alta confiança tendo em vista a profissionalização das “Ameaças cibernéticas”, ao garantir a proteção de infraestruturas essenciais para o desempenho de atividades e dados cuja divulgação, furto ou alteração teriam graves consequências para clientes, parceiros ou colaboradores;
- Apoiar a estratégia de desenvolvimento do Grupo e seus Negócios e acomodar as práticas de mudança (Trabalho Digital, mobilidade, teletrabalho, redes sociais, espaços de trabalho colaborativos, dispositivos conectados, computação em nuvem, atividades de terceirização, etc.), recomendando sistemas de segurança

inovadores que abordem a aberta natureza do ambiente digital (assinatura eletrônica, trocas seguras, etc.);

- Contribuir para o desempenho geral do Grupo e cumprir com seus compromissos pela busca de sinergias internas, mantendo a eficácia dos recursos de TI, melhorando a capacidade do Grupo de detectar e responder a novas ameaças e garantir um nível de segurança “aceitável” e de baixo custo;

- Cumprir as obrigações legais e regulamentares (proteção de dados pessoais, propriedade intelectual, combate à fraude informática, Lei de Programação Militar, etc.) e os requisitos aos quais as entidades do Grupo BNP aderem em função da sua atividade empresarial. Apesar do fortalecimento das leis, regulamentos e “rótulos”.

9. DEFINIÇÕES E APÊNDICE

Ativo - Todos os dados e recursos dos sistemas de informação (tangíveis ou intangíveis) que representem valor ou uma participação (ganho ou perda) para o Grupo e suas entidades. Por exemplo: os serviços de produção, infraestrutura (redes, mensagens, etc.), software aplicativo, software de sistema, ferramentas de desenvolvimento, hardware de TI (servidores, estações de trabalho, etc.) e hardware de comunicação (roteadores, smartphones e tablets), salas de TI, etc.

Requisito de segurança – Requisito / necessidade expressa quanto aos critérios de segurança: Disponibilidade, Integridade, Confidencialidade e Rastreabilidade.

Funcionário - Pessoa física que trabalha na Cardif como agente permanente ou temporário, no Brasil, com contrato de trabalho, destacamento, transferência temporária ou nomeação corporativa, ou com contrato equivalente no exterior.

Comunidade de Segurança Cibernética - Corresponde a uma cadeia funcional gerida pelo Group IT & Cyber Risk Officer, em linha com a sua posição de CISO, reunindo os gestores de segurança, correspondentes e oficiais dos sistemas de informação destacados no Grupo para coordenar a adaptação e a implantação do procedimento de segurança cibernética. Essa comunidade é supervisionada pela comunidade de gerenciamento de riscos de TI dentro do Banco.

Confidencialidade - Capacidade do sistema de informação de proteger dados sensíveis de qualquer divulgação não autorizada e reservar acesso a pessoas devidamente autorizadas.

Segurança Cibernética - é a atividade de implementação de recursos humanos, sua formação, processos, políticas e ferramentas para proteger o BNP Paribas e os interesses dos seus clientes contra as ameaças internas e externas do ambiente digital.

Essas ameaças, que incluem, por exemplo, acesso não autorizado ou destruição de dados, negação de serviço ou danos à reputação da empresa, enfocam a confidencialidade, disponibilidade e integridade dos Sistemas de Informação e dos sistemas relacionados. Esta atividade cobre toda a cadeia de valor, desde a identificação de ameaças, a implementação e manutenção de medidas de proteção até a detecção e processamento de incidentes.

Disponibilidade – Capacidade do sistema de informação para garantir a execução do processamento e acesso aos dados de acordo com as condições pré-definidas de tempo.

Dado sensível - Os dados sensíveis correspondem aos dados classificados como secretos ou confidenciais com base na escala de classificação de dados.

Grupo – "BNP Paribas" ou o "Banco" ou o "Grupo": BNP Paribas S.A. e todas as suas subsidiárias diretas e indiretas, consolidado total ou proporcionalmente, ou todas as suas entidades organizacionais, operacionais ou funcionais, em conjunto ou individualmente.

Integridade - Capacidade do sistema de informação para garantir que os dados sejam inalteráveis no tempo e no espaço.

Rastreabilidade – Capacidade do sistema de informação de fornecer trilhas de auditoria e comprovar as ações realizadas por meio de três mecanismos complementares que são rastreamento, alocação e não repúdio.

Incidente grave de segurança de TI - Um incidente de segurança de TI deve ser classificado como grave no nível do Grupo quando uma das seguintes condições for atendida:

- O CSIRT1 responsável pelo escopo classificou o incidente como nível 4 (Muito alto) na matriz de impacto.

- O CSIRT responsável pelo escopo ativou seu sistema de gestão de crise.

Um único incidente afeta várias entidades ou é provável que tenha um impacto colateral em outras entidades (por exemplo, propagação de malware na rede, intrusão em uma rede local compartilhada por várias entidades).

Ambiente digital – Todos os sistemas usados para suportar recursos digitais, como smartphones, tablets, caixas eletrônicos e objetos conectados.

Propriedade das regras - O proprietário das regras emitidas nesta política é o chefe do Grupo de Gerenciamento de Risco de TI.

10. CONTROLE DE REGISTROS

Versão externa: 1.0 – Data de publicação: 11/04/2023

Versão externa: 2.0 – Data de publicação: 11/12/2024