BNDES - SEGURANÇA DA INFORMAÇÃO

NOSSA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O BNDES possui uma Política Corporativa de Segurança da Informação (PCSI) aprovada pelo Conselho de Administração do BNDES. A PCSI define os princípios, diretrizes e responsabilidades para garantir a preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações do BNDES, de seus clientes e parceiros.

QUAIS SÃO OS PRINCÍPIOS DA NOSSA PCSI?

- **Privilégio mínimo**, ou seja, acesso só ao que for necessário para execução da atividade do empregado;
- Os controles de segurança devem garantir a **proteção em camadas**;
- As implementações de controles de segurança devem **privilegiar a adoção de padrões abertos**;
- A implantação de controles deve ser **iniciada pelos mais simples** e priorizada de acordo com o resultado de análises de riscos;
- Os **custos** associados à implementação e execução dos controles **não devem ser maiores que os benefícios** esperados; e
- A **aplicabilidade** de controles deve ser **ponderada** diante de sua **efetividade** e do impacto às **necessidades** de negócio.

COMO O BNDES CLASSIFICA AS INFORMAÇÕES?

No BNDES, as informações são classificadas e tratadas de acordo com normativo interno, que, em resumo, prevê a atribuição dos seguintes graus de sigilo:

Reservada ou **Secreta** – para informações cuja divulgação possa comprometer a segurança da sociedade e do Estado, como definido na Lei de Acesso à Informação; e

Controlada ou **Confidencial** – quando houver previsão legal de sigilo, como no caso do sigilo bancário e do sigilo empresarial.

*"No BNDES, a classificação de informações deve observar a **publicidade** como **preceito geral** e a atribuição do **sigilo** como **exceção**."*

O QUE SÃO DADOS SENSÍVEIS PARA NÓS?

No BNDES, são consideradas sensíveis **todas as informações sigilosas classificadas** como **reservada**, **secreta** ou **confidencial,** além de informações controladas que envolvam **dados pessoais, classificação de risco** de empresas, **conceito cadastral, margem** para operar, situação de **adimplência ou inadimplência** de clientes**, saldo devedor** e informações sobre **a estratégia empresarial de clientes**.

RESPONSABILIDADES E ESTRUTURA DE GESTÃO

O Sistema BNDES possui um **Comitê de Segurança da Informação** (CSI), colegiado formado por Superintendentes cuja principal atribuição é promover a governança de Segurança da Informação e o adequado alinhamento estratégico das ações pertinentes ao tema.

Além do CSI, a gestão de segurança da informação conta com a atuação do **Diretor responsável por Segurança da Informação** e do **Gestor de Segurança da Informação**, papel desempenhado pelo Superintendente da Área de Tecnologia da Informação (ATI).

A **Gerência de Segurança da Informação** (ATI/GSEG) é a unidade administrativa responsável por conduzir as ações do Plano Estratégico de Segurança da Informação (PESI), bem como pelo Tratamento de Incidentes de Segurança da Informação, em consonância com o Plano de Resposta a Incidentes de Segurança da Informação (PRISI). De acordo com a PCSI, a segurança da informação é **responsabilidade** de **todos os colaboradores do Banco**, o que inclui empregados, estagiários e prestadores de serviços do Sistema BNDES.

QUE SERVIÇOS SÃO RELEVANTES PARA O BNDES?

O BNDES classifica como **relevante** todo serviço que manipula **dado sensível**, que suporta seus **sistemas principais** ou que é imprescindível para **continuidade de processo crítico**, ou seja, aquele definido como de **recuperação urgente** de acordo com a metodologia de gestão de continuidade de negócios.

COM O QUE DEVO TOMAR MAIS CUIDADO?

Ataques que envolvem técnicas de **engenharia social** são as maiores ameaças hoje em dia. O mais comum são ***phishings***, mensagens falsas em nome de pessoa ou empresa de confiança com intuito de disseminar *links* especialmente preparados para instalação de programas maliciosos e para capturar dados bancários. São frequentes o uso de mensagens por *e-mail*, SMS e até via *WhatsApp*. Fique atento e não clique em *links* em mensagens suspeitas!

TEM ALGUMA DÚVIDA OU SUSPEITA DA OCORRÊNCIA DE ALGUM INCIDENTE? FALE CONOSCO!

Além do canal de denúncias da Ouvidoria do BNDES (www.bndes.gov.br/ouvidoria), a equipe técnica de Segurança da Informação pode ser notificada através do e-mail:

abuse@bndes.gov.br

O QUE É DISCIPLINADO PELA PCSI DO BNDES?

Além dos princípios, diretrizes e responsabilidades, a PCSI é complementada por 10 normas específicas anexas, além de um manual de conceito e cinco modelos de termos de confidencialidade. As normas complementares apresentam diretrizes específicas para:

- ✓ **Controle de acesso à informação**
- ✓ **Uso da Internet**
- ✓ **Uso do correio eletrônico**
- ✓ **Uso de ativos de TI**
- ✓ **Uso de dispositivos pessoais no ambiente corporativo**
- ✓ **Uso de serviços de computação em nuvem**
- ✓ **Acesso remoto a ativos de TI**
- ✓ **Acesso a áreas com ativos críticos de TI**
- ✓ **Administração de ativos de TI**
- ✓ **Gestão dos serviços de segurança da informação**

O QUE O BNDES FAZ PARA PRESERVAR A SEGURANÇA DO BANCO E DOS NOSSOS CLIENTES?

O Banco possui **controles de tecnologia** que minimizam o risco das principais ameaças cibernéticas, entre eles controles contra programas maliciosos e controles contra ameaças de rede. A **implantação** de **sistemas** em regime de **produção** é **controlada** e os sistemas considerados mais expostos ou críticos sofrem **testes** de **segurança** periodicamente. O Banco **monitora** as **vulnerabilidades** e possui rotina para garantir a **atualização** de **segurança** de todo seu parque tecnológico. O Banco possui sua infraestrutura tecnológica de execução dos sistemas principais replicada em ambiente de **contingência**. Há **planos** para **responder** aos **incidentes** de segurança e, periodicamente, são executados **testes** para garantir a **continuidade** dos processos críticos ainda que ocorra evento grave.

COMO VOCÊ PODE NOS AJUDAR?

- ✓ Mantenha seu **computador** sempre **atualizado**!
- ✓ **Troque suas senhas** regularmente e **revise** os **perfis** de **acesso** dos funcionários de sua empresa nos **nossos sistemas online**!
- ✓ Os sistemas do BNDES são publicados por meio de canais seguros **com uso de criptografia**. Confira se o acesso ao site do Banco está sendo feito por conexão **HTTPS** e se não há nada estranho ou indício de tratar-se de página falsa! **Na dúvida, fale conosco**!
- ✓ O **BNDES não reconhece nem credencia consultores** (pessoas físicas ou jurídicas) como intermediários para facilitar, agilizar ou aprovar operações de crédito. Não caia em golpes!
- ✓ Prefira acessar os sites do Banco a partir da digitação do endereço ***https://www.bndes.gov.br*** no seu navegador. **Evite acessos a partir de anúncios em sites de busca, pois** podem ser falsos e remeterem a sites fraudulentos!