Banco de la Nación Argentina

INDICE

Banco de la Nación Argentina

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA

A Política de Segurança da informação aponta a obter a segurança total dos ativos de informação do Banco, portanto, está orientada a garantir que esses ativos, dos que depende a Organização para levar adiante suas atividades, estejam adequadamente protegidos.

DECLARAÇÃO DA POLÍTICA

A Política de Segurança da Informação constitui a base do Programa de Segurança da Informação. Todas as iniciativas relacionadas com à gestão da informação obterão apoio desta Política assim como também deverão cumprir com ela. Os procedimentos de segurança deverão integrar-se com os procedimentos de gestão dos ativos de informação existentes e / ou futuros.

OBJETIVO

Estabelecer as responsabilidades, diretivas e requerimentos a fim de garantir a integridade, confidencialidade, disponibilidade e auditabilidade da informação e implementar um razoável nível de amparo dos ativos do Banco. Estas políticas são criadas com o fim de acautelar o mau uso e perdas de bens da Organização, estabelecendo as bases para minimizar os expostos de segurança referidos com a:

- Integridade, entendida como a propriedade de integridade e exatidão de um ativo;
- Confidencialidade, entendida como a propriedade da informação de ser acessível ou revelada unicamente a indivíduos, entidades ou processos autorizados;
- Disponibilidade, entendida como a propriedade de um ativo de ser acessível e utilizável em tempo e forma baixo demanda de indivíduos, entidades ou processos autorizados; e
- Auditabilidade, entendida como a propriedade que permite identificar e rastrear as operações levadas a cabo pelo usuário dentro de um sistema de informação.

Banco de la Nación Argentina

ALCANCE

Esta Política se aplica em todo o âmbito do Banco, a seus recursos e à totalidade dos processos, já sejam internos ou externos vinculados à entidade através de contratos ou acordos com terceiros.

CONTEÚDO

SEGURANÇA DA INFORMAÇÃO

A informação é um dos ativos mais valiosos da organização e como tal deve ser protegida. Os principais riscos que podem afetá-la são a divulgação, modificação ou destruição não autorizadas, sejam acidentais ou deliberadas.

Para minimizar estes riscos é imprescindível implementar a segurança da informação no alcance de toda a organização, de modo tal que se cubram ao menos as seguintes funções mínimas:

A. Proteger a informação, como ativo da Organização, dos riscos a que possa estar exposta independentemente do meio em que se encontre.

B. Assegurar a integridade, confidencialidade, disponibilidade e auditabilidade da informação contemplando os requisitos legais e regulatórios.

COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Deve existir um Comitê que trate os aspectos da segurança da informação com a participação da Diretória e dos representantes das distintas Áreas do Banco com o propósito de garantir o apoio no processo de conscientização e o cumprimento das Políticas de Segurança da Informação.

RESPONSABILIDADE

A Política de Segurança da Informação é de aplicação obrigatória para todo o pessoal que trabalha no Banco, contratado ou externo com desempenho de atividades dentro do âmbito do mesmo, qualquer que seja sua situação atual a área a qual se encontre trabalhando e qualquer que seja o nível das tarefas que desempenhe.

Esta Política é passada pela Diretória em consequência as modificações posteriores resultantes de revisões periódicas, de exigências do negócio ou de mudanças no marco regulatório devem ser autorizadas e aprovadas pela mesma instância.

Deve-se garantir que todos os usuários estejam familiarizados e tenham acesso às Políticas e Normas de Segurança da Informação.

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Banco de la Nación Argentina

As Políticas de Segurança da Informação têm por objetivo definir os esboços gerais dos distintos aspectos de segurança envoltos, ou seja:

ORGANIZAÇÃO DA SEGURANÇA

Deve definir as pautas para administrar a segurança da informação dentro de Banco e estabelecer um marco gerencial para controlar sua implementação, assim como para a distribuição e segregação de funções e responsabilidades e garantir a aplicação de medidas de segurança adequadas nos acessos de terceiros à informação do Organismo.

IDENTIFICAÇÃO E CLASSIFICAÇÃO DE ATIVOS

Deve garantir que os ativos de informação recebam um apropriado nível de amparo possibilitando a identificação e classificação da informação para assinalar sua sensibilidade, criticidade e a definição de níveis de amparo e medidas de tratamento especial de acordo a sua classificação.

SEGURANÇA DO PESSOAL

Deve estabelecer os esboços de segurança que se deve cumprir ao contratar, desenvolver suas atividades ou finalizar a relação trabalhista com todo pessoal do Banco e terceiros relacionados, com o propósito de identificar sua atividade em temas de vinculação com a entidade, reduzindo os riscos de engano humano, comissão de ilícitos, uso inadequado de instalações e recursos, e manuseio não autorizado da informação.

SEGURANÇA FÍSICA E AMBIENTAL

Deve estabelecer as medidas de segurança física e ambiental nas dependências do Banco onde se processe informação, para minimizar os riscos e obter um adequado nível de amparo dos ativos de informação.

GESTÃO DAS COMUNICAÇÕES E AS OPERAÇÕES

Deve estabelecer os esboços para assegurar a integridade, confidencialidade e disponibilidade dos serviços e comunicações para garantir um correto processamento da informação, resguardando a segurança da mesma.

CONTROLE DE ACESSO

Deve estabelecer os esboços para assegurar que o acesso aos ativos informáticos sejam restringidos e controlados, de forma tal que os usuários possam executar as tarefas que lhe designe a organização com uma adequada segregação de funções.

AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Deve estabelecer os esboços para garantir que o desenvolvimento, manutenção e/ou aquisição dos sistemas de informação do Banco incluam controles de segurança referidos a confidencialidade, integridade, disponibilidade e auditabilidade da informação a efeitos de acautelar perdas, modificações ou uso inadequado dos dados e/ou dos sistemas de informação do Banco em todo seu ciclo de vida e na infraestrutura de base na qual se apoiam.

GESTÃO DE INCIDENTES

Deve estabelecer os esboços para assegurar que os incidentes e debilidades de segurança associados com os ativos de informação sejam administrados de uma maneira efetiva, permitindo tomar ações corretivas oportunas, minimizando sua possibilidade de ocorrência no futuro e reduzindo ao máximo possível o impacto para o Banco.

CONTINUIDADE DO NEGÓCIO

Deve estabelecer os esboços para o desenvolvimento e manutenção de procedimentos que garantam a continuidade operativa dos processos críticos de negócio em condições aceitáveis dos sistemas de informação que os suportam.

CUMPRIMENTO LEGAL E NORMATIVO

Deve garantir o cumprimento das leis, disposições normativas e contratuais a fim de evitar prejuízos de índole legal ou administrativa para o Banco e/ou seus empregados, assegurando que os sistemas informáticos e o uso das tecnologias relacionadas cumpram com a política, normas, padrões e procedimentos de segurança do Banco.

PENALIDADES POR DESCUMPRIMENTO

O descumprimento da Política e Normas de segurança deve ser sancionado administrativamente de acordo com as normas estatutárias, escalonarias e convencionais que regem para o pessoal do Banco.

Banco de la Nación Argentina

ORGANIZAÇÃO DA SEGURANÇA

OBJETIVO

Administrar a segurança da informação dentro de Banco e estabelecer um marco gerencial para controlar sua implementação, assim como para a distribuição e segregação de funções e responsabilidades e garantir a aplicação de controles de segurança adequados aos ativos de informação.

ALCANCE

Todos os empregados do Banco e a todas suas relações com terceiros que impliquem o acesso a seus dados, recursos e/ou à administração e controle de seus sistemas de informação.

POLÍTICA

DEFINIÇÕES PRÉVIAS

- A máxima autoridade em relação à aprovação e atualização do manual de segurança será o Comitê de Segurança da Informação, conforme foi definido na Política de Segurança.

- "Proprietários da Informação": devem ser funcionários com autoridade para criar, manter e eliminar a informação dos sistemas aplicativos.

- "Proprietários dos Aplicativos": Devem ser designados por Desenvolvimento de Sistemas. Devem ser funcionários com autoridade para selecionar, criar, e manter os programas e sistemas aplicativos a partir das definições proporcionadas pelos Proprietários da Informação.

- "Proprietários dos Perfis": Devem ser designados por Organização e Processos. Os proprietários devem ser funcionários com autoridade para criar, manter e eliminar perfis funcionais a partir das definições estabelecidas pelos Proprietários da Informação, e a associação dos programas/transações de cada aplicativo realizada pelos Proprietários das Aplicações.

- "Proprietários das Plataformas": Devem ser designados por Tecnologia e Processamento. Os Proprietários das Plataformas devem ser funcionários com autoridade para criar, manter e eliminar as plataformas e seus sistemas operacionais ou produtos utilitários.

- "Usuários da Informação": São os agentes a quem em forma explícita lhes outorgou autorização para ver, criar, modificar e eliminar dados.

Banco de la Nación Argentina

INFRA-ESTRUTURA DA SEGURANÇA DA INFORMAÇÃO

COMITÊ DE SEGURANÇA DA INFORMAÇÃO

- Coordenar as atividades relacionadas com a segurança da informação, assegurando que são realizadas de acordo com a Política de segurança do Banco.

- Emprestar um apoio ativo para a segurança da informação dentro do Banco através de diretrizes claras, um compromisso demonstrado, atribuições explícitas e o reconhecimento das responsabilidades associadas, garantindo que a segurança seja parte do processo de planejamento da informação.

- Aprovar a política e as normas em matéria de segurança da informação.

- Promover a difusão da segurança da informação dentro do Banco.

- Assegurar o alinhamento do Plano Estratégico de segurança da informação com as necessidades do Banco.

- Identificar e/ou alertar sobre situações de riscos.

- Aprovar a atribuição de funções e responsabilidades específicas para a segurança da informação na organização.

- Assegurar a avaliação da informação recebida do monitoramento e revisão de incidentes de segurança, e recomendar ações apropriadas em resposta a eles.

- Aprovar as exceções aos controles definidos no marco normativo.

- Coordenar o processo de administração da continuidade do negócio frente a interrupções imprevistas.

PROPRIETÁRIOS DE ATIVOS INFORMÁTICOS

- Definir uma adequada segregação de funções entre as pessoas a seu cargo, de maneira que nenhuma pessoa em forma individual possa controlar todos os aspectos chave de um processo.

- Definir as regras de acesso à informação a seu cargo de acordo com o princípio de "necessidade de conhecer" e "mínimo privilégio" a modo de garantir o normal desenvolvimento dos processos de negócio.

- Autorizar todos os acessos à informação a seu cargo, verificando previamente que não exista contradição com a segregação de funções.

- Autorizar, em casos excepcionais, privilégios ou atributos especiais à área de Segurança da Informação, considerando como "privilégio de acesso" a qualquer método que permita a um usuário evitar os controles estipulados.

- Assegurar o cumprimento da Política de Segurança do Banco por parte de seus sistemas de informação.

- Identificar as transações críticas de seus sistemas de informação e levar a cabo um estrito controle do uso das mesmas.

- Assegurar que as mudanças introduzidas a seus ativos informáticos respondam a seus requerimentos.

- Autorizar quando fosse necessário a cópia de dados reais que se utilize para provas, assegurando a proteção dos mesmas em condições idênticas ao ambiente de produção.

- Avaliar a análise de risco para determinar o nível de risco a que está exposta a informação e da contramedida para a redução do mesmo.

- Colaborar na definição de controles de auditoria que favoreçam a detecção de desvios, com respeito aos acessos autorizados e os riscos estabelecidos.

- Assegurar a realização de avaliações de riscos sobre seus ativos informáticos e determinar os requerimentos de controle necessários para acessar aos mesmos.

- Controlar periodicamente as permissões outorgadas aos usuários como assim também os registros de auditoria e incidentes de segurança.

- Emitir diretrizes para a retenção, armazenamento, manipulação, guarda e eliminação de sua informação.

- Promover e organizar, com a colaboração da área de Segurança da Informação, campanhas regulares para aumentar a consciência e a disciplina com respeito ao grau de responsabilidade pela segurança e o controle interno, facilitando que todo o pessoal a seu cargo, conheça suas funções e responsabilidades em relação com os sistemas de informação.

- Em caso de considerá-lo conveniente poderá delegar a uma pessoa ou setor dentro de sua mesma área a administração e o controle de seus ativos informáticos, conservando sempre o grau de responsabilidade máximo dos mesmos. Comunicar formalmente esta delegação a todas as áreas envolvidas nos distintos procedimentos.

- Assegurar a existência, manutenção e prova do plano de continuidade correspondente à sua unidade de negócio, garantindo a incorporação de mudanças nas disposições relativas às atividades da mesma.

RESPONSÁVEIS POR ÁREA

- Autorizar o acesso à rede, aos serviços básicos e aos serviços estendidos de modo de assegurar que todas as políticas e requerimentos de segurança relevantes sejam cumpridas.

- Controlar todas as necessidades novas ou existentes em relação ao de acesso à informação por parte do pessoal abaixo de sua responsabilidade.

- Em caso de considerá-lo conveniente poderá delegar a uma pessoa ou setor dentro de sua mesma unidade a gestão de autorizações de acesso à rede, aos serviços e às aplicações, conservando sempre o grau de responsabilidade máximo destas autorizações. Comunicar formalmente esta delegação a todas as áreas envolvidas nos distintos procedimentos.

- Promover entre o pessoal abaixo de sua responsabilidade a cultura de segurança da informação.

ÁREA DE SEGURANÇA DA INFORMAÇÃO

- Definir e manter atualizadas as Normas, Procedimentos e Padrões de Segurança aplicáveis aos distintos setores e plataformas operativas da entidade assessorando sobre seu cumprimento a todos os setores do Banco.

- Colaborar com os Proprietários de Ativos de Informação e Responsáveis por área para o cumprimento de suas responsabilidades.

- Colaborar com a promoção de metodologias de Classificação da Informação e sua correspondente Análise de Riscos.

- Difundir a cultura de segurança da informação e implementar programas de formação.

- Publicar e difundir necessidades relacionadas com aspectos de segurança da informação.

- Manter um registro formal de todas as pessoas habilitadas para autorizar acessos (Proprietários e seus delegados).

- Administrar os acessos aos ativos informáticos do Banco garantindo o cumprimento da normativa vigente.

- Definir os términos e as condições de uso dos ativos informáticos.

- Definir os padrões de configuração de aspectos de segurança dos ativos informáticos.

- Implementar e manter atualizados aspectos de segurança que não possam ser delegados, em função de seu criticidade e/ou impossibilidade de segregação e/ou controle posterior.

- Realizar o monitoramento sobre a aplicação das políticas, normas, procedimentos e padrões nas diferentes plataformas do Banco, assim como também as atividades desenvolvidas pelos usuários.

- Informar periodicamente aos Proprietários os acessos outorgados a seus ativos informáticos.

- Realizar a gestão de vulnerabilidades nos sistemas de informação do Banco.

- Realizar a gestão de incidentes de segurança da informação.

- Elevar periodicamente ao Comitê de Segurança da Informação o relatório de gestão para o estado da segurança do Banco.

ÁREA DE GESTÃO DE RISCO

- E avaliar e monitorar a exposição a risco.

- Coordenar as atividades de análise de riscos adicionados baixo modelos qualitativos e quantitativos, articulando sua atuação com os responsáveis por todas as Unidades.

- Preparar um processo de seguimento da eficácia do sistema de gestão de riscos que poderá identificar riscos de maneira proativa com o propósito de assegurar seu tratamento por parte das unidades que intervêm nos processos relacionados.

- Desenvolver os aspectos relacionados à capacitação e divulgação em matéria de Gestão de Riscos.

ÁREA DE SISTEMAS E ORGANIZAÇÃO

- Homologar os sistemas de informação e a infraestrutura tecnológica que lhe dá suporte em concordância com a política e normas de segurança da informação.

- Aplicar os padrões de configuração de aspectos de segurança dos ativos informáticos definidos pela Segurança da Informação.

- Administrar os meios necessários para manter os registros, logs e pistas de auditoria requeridos pela Segurança da Informação.

- Colaborar no processo de gestão de incidentes.

ÁREA DE RECURSOS DE HUMANOS

- Verificar o cumprimento da presente Política na gestão de todos os contratos, acordos ou outra documentação do Organismo com seus empregados e com terceiros.

- Assessorar em matéria legal ao Organismo, no que se refere à segurança da informação.

- Colaborar nas tarefas de difundir a cultura de segurança da informação e implementar programas de formação.

ÁREA DO AUDITORIA DE SISTEMAS

- Realizar auditorias periódicas sobre os sistemas e atividades vinculadas com a tecnologia de informação, devendo informar sobre o cumprimento das especificações e medidas de segurança da informação estabelecidas por esta Política e pelas normas, procedimentos e práticas que dela surjam.

USUÁRIOS

- Manter-se atualizados e familiarizados com a Política de Segurança da Informação vigente.

- Cumprir e fazer cumprir as Políticas de segurança da Informação.

- Comunicar a Segurança da Informação sobre qualquer incidente ou situação que pudesse suceder em incidente de segurança e denunciar qualquer descumprimento legal ou normativo que possa afetar os interesses do Banco.

EXCEÇÕES

As solicitações de exceções devem ser justificadas em forma escrita e contar com as aprovações necessárias para que se considerem válidas. As exceções qualificadas com nível de risco alto devem ser passadas pela Diretoria e pelo Comitê de Segurança da Informação e devem detalhar os riscos assumidos em sua aprovação.

As exceções aprovadas devem contar com um prazo de validez. Na data de vencimento devem ser novamente avaliadas e em caso de persistir a necessidade de exceção, aprovadas por um novo prazo.

Em caso que as exceções fujam dos controles existentes se devem implementar novos controles para minimizar os riscos ou compensar os controles evadidos. Esta situação deve ser incluída na documentação das exceções detalhando os controles existentes substituídos e os compensatórios implementados.

REVISÃO INDEPENDENTE DA SEGURANÇA DA INFORMAÇÃO

Devem-se realizar, a intervalos específicos, revisões do nível de segurança do Banco incluindo: nível de adesão às normas por parte do pessoal, medidas de segurança implementadas nas redes externas e internas e nível de segurança física.

As revisões devem ser realizadas por Auditoria Interna e/ou auditorias externas.

Os resultados das revisões e sua implementação devem ser documentados em informe que serão apresentados às gerências correspondentes para sua avaliação.

ACESSO A INFORMAÇÃO DO BANCO POR PARTE DE TERCEIROS

O acesso à informação do Banco por parte de terceiros deve ser autorizada formalmente pela Diretoria, quem com colaboração de Segurança da Informação deverão realizar e documentar a avaliação de riscos correspondente.

Devem conformar-se convênios de confidencialidade e acordos de bom uso dos recursos informáticos a efeitos de comunicar convincentemente a obrigação de cumprir com a Política, Normas e Procedimentos de Segurança da informação do Banco.

Não deve dar-se acesso a terceiros à informação, instalações de processamento ou outros serviços críticos até tanto se assinou contratos ou acordos que definam as condições de acesso.

Segurança da Informação deve definir os requerimentos de segurança em contratos ou acordos com terceiros com a participação de Assessoria Legal.

TERCERIZAÇÃO

O Banco não delega responsabilidade quando terceiriza serviços, em consequência devem adotar controles necessários para garantir a adequada da prestação de serviços por parte de terceiros.

Nos contratos do Terceirização devem se ter em conta os níveis de serviço que o Banco requer e todos os requisitos legais e/ou de regulação externa que regem para a Entidade incluindo cláusulas de confidencialidade da informação.

Segurança da Informação deve definir os requerimentos de segurança lógica e física sobre os serviços tercerizados.

Devem estabelecer-se controles sobre os serviços tercerizados e monitoramento do cumprimento dos requisitos de segurança exigidos.

Os serviços tercerizados devem incluir procedimentos de continuidade de serviço de acordo com a criticidade dos serviços envolvidos, e os mesmos devem ser considerados no plano de continuidade de negócios do Banco.

IDENTIFICAÇÃO E CLASSIFICAÇÃO DE ATIVOS

OBJETIVO

OBJETIVO

Estabelecer os esboços gerais para o desenvolvimento de procedimentos que permitam identificar e classificar os ativos de informação do Banco, definindo os níveis de sensibilidade e criticidade que permitam manter uma apropriada proteção dos mesmos.

ALCANCE

Todas as áreas da Organização.

POLÍTICA

TERMOS GERAIS

O Banco deve ter um pleno conhecimento sobre os ativos que possui como parte necessária para a administração de riscos.

A informação adota muitas formas, tanto nos sistemas informáticos como fora deles. Pode ser armazenada (em tais sistemas ou nos meios portáteis), transmitida (através de redes ou entre sistemas) e impressa ou escrita em papel. Cada uma destas formas deve contemplar todas as medidas necessárias para assegurar a confidencialidade, integridade e disponibilidade da informação.

A informação pode passar a ser obsoleta e, portanto, ser necessário eliminá-la. A destruição da informação é um processo que deve assegurar a confidencialidade da mesma até o momento de sua eliminação.

RESPONSABILIDADE PELOS ATIVOS

Cada ativo informático deve ter um único Proprietário.

Cada ativo deve ter uma única identificação (nome de ativo) que se usará para sua classificação e proteção.

Os ativos informáticos serão atribuídos aos usuários com propósitos exclusivos do negócio.

Com o propósito de facilitar a administração sobre a propriedade dos ativos, a Área de Sistemas e Organização assumirá esta responsabilidade em primeira instância, até tanto se estabeleça e designe formalmente o proprietário de cada ativo de informação.

INVENTÁRIO DE ATIVOS DE INFORMAÇÃO

Os proprietários com a colaboração das áreas envoltas com o ativo devem classificar os ativos de informação quanto a sensibilidade e criticidade.

Define-se **sensibilidade** da informação como o grau de confidencialidade que esta tem em função do impacto negativo para o Banco que causaria seu indevido acesso e/ou perda de integridade.

Define-se **criticidade** como o grau de disponibilidade que a informação tem que ter para cumprir com as expectativas de negócio do Banco.

CLASSIFICAÇÃO DA INFORMAÇÃO

Os procedimentos de classificação devem contemplar a avaliação da confidencialidade, integridade e disponibilidade da mesma.

A área responsável pela classificação dos ativos de informação deve colaborar com os proprietários dos mesmos para a aplicação da metodologia aprovada para tal fim.

Todos os ativos informáticos do Banco devem estar sujeitos aos níveis de classificação estabelecidos.

A incorporação de ativos de informação deve contemplar a correspondente classificação e incorporação ao inventário a efeitos de manter atualizado o mesmo.

Deve-se contemplar um processo de atualização da classificação dos ativos de informação dado que esta pode variar durante o ciclo de vida dos mesmos.

Os processos de eliminação e/ou desafetação de ativos de informação devem ser refletidos no inventário e informados às áreas correspondentes a efeitos de proceder em consequência.

ROTULAGEM DA INFORMAÇÃO

Devem-se definir procedimentos para a rotulagem e o manuseio de informação, de acordo ao esquema de classificação definido. Os mesmos contemplarão os recursos de informação tanto em formatos físicos como eletrônicos.

SEGURANÇA DO PESSOAL

OBJETIVO

Estabelecer os esboços de segurança que se devem cumprir nas etapas de ingresso ou contratação de pessoal, desempenho de atividades e finalização da relação trabalhista com o Banco e de terceiros que desempenhem atividades em qualquer âmbito do mesmo.

ALCANCE

Esta Política será de aplicação para todos os empregados, contratados, fornecedores e consultores com atividade autorizada em todos os âmbitos do Banco.

POLÍTICA

INCORPORAÇÃO DE PESSOAL À INSTITUIÇÃO

INCORPORAÇÃO DE PESSOAL

A área do RRHH deve efetuar a verificação de antecedentes de todos os candidatos a emprego conforme às leis e regulamentos vigentes na Entidade.

FUNÇÕES E RESPONSABILIDADES DO EMPREGADO

As funções e responsabilidades de segurança dos usuários devem definir-se em concordância com a Política de Segurança da Informação do Banco.

As responsabilidades em matéria de Segurança dos Sistemas e as Tecnologias de Informação devem ser explicitadas ao momento do ingresso da pessoa à Organização.

TÉRMINOS E CONDIÇÕES PARA A INCORPORAÇÃO Ou CONTRATAÇÃO

Ao momento da incorporação ou contratação, o pessoal deve ser informado das políticas, términos e condições de bom uso dos Ativos de Informação.

O pessoal deve assinar, ao momento de receber sua identificação de usuário, um acordo de confidencialidade e bom uso dos recursos informáticos do Banco como parte de seus términos e condições de emprego.

O pessoal se compromete a preservar a segurança de seu meio de identificação assim como de sua senha ou meio de autenticação e aceita a responsabilidade das atividades desenvolvidas com os mesmos.

Os usuários devem cumprir os términos e condições de uso dos ativos informáticos.

DURANTE O EMPREGO

CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO E RESPONSABILIDADES DE USUÁRIOS

A área de Segurança Informática deve promover a capacitação periódica dos usuários do Banco em matéria de Políticas, Normas e Procedimentos de segurança.

devem-se dispor dos recursos necessários para capacitar aos usuários em relação às necessidades de segurança dos sistemas e as tecnologias de informação, para que os mesmos possam respaldar o marco normativo vigente no transcurso de suas tarefas normais.

PROCESSO DISCIPLINADOR

O pessoal que viole as políticas e procedimentos de segurança, poderá ser submetido ao processo disciplinador que a área de Recursos humanos considere adequado detrás ser informado do sucesso e o nível de gravidade do mesmo.

AFASTAMENTO DO EMPREGO OU MUDANÇA DE POSTO DE TRABALHO

RESPONSABILIDADES DO AFASTAMENTO OU MUDANÇA

A área de Recursos humanos deve informar à área de Segurança Informática a suspensão ou desvinculação do pessoal.

Os responsáveis por área devem informar ao responsável por gestão de usuários que corresponda as mudanças de posto ou afastamento de atividades, temporário ou permanente, do pessoal de terceiros que desempenhem atividades baixo sua responsabilidade.

As permissões de acesso do usuário aos ativos informáticos devem ser retiradas à terminação de seu emprego, contrato ou acordo ou devem ser reajustados de acordo com a mudança.

DEVOLUÇÃO DE ATIVOS

Toda a informação contida nas equipes informáticas é propriedade do Banco.

Todos os usuários devem devolver todos os ativos informáticos que o Banco tenha posto ao seu dispor à terminação de seu emprego, contrato ou acordo.

SEGURANÇA FÍSICA E AMBIENTAL

OBJETIVO

Implantar as medidas de segurança física e ambiental nas dependências do Banco onde se processe e/ou armazene informação, para minimizar os riscos e obter um adequado nível de proteção dos ativos de informação.

ALCANCE

Esta norma deve ser aplicada em todas as áreas do Banco na qual se identifique equipamento relacionado em forma direta ou indireta com o processamento ou armazenamento de informação e pelo pessoal que utilize equipamento do Banco fora do âmbito do mesmo.

POLÍTICA

SEGURANÇA FÍSICA E AMBIENTAL

devem-se identificar quais são as áreas a proteger de acordo com o nível de criticidad dos ativos de informação envoltos, os parâmetros de segurança requeridos e as permissões de acesso do pessoal a sortes áreas.

CONTROLE DE ACESSO

Devem existir procedimentos de controle de acesso específicos ao centro de processamento de dados e áreas relacionadas.

Segurança Bancária deve definir as características dos dispositivos e controles de segurança para as áreas definidas como críticas e implementar os mesmos.

O pessoal deve saber da existência de áreas consideradas como críticas e as tarefas que ali se realizam sozinho quando existir uma necessidade imposta por sua atividade ou rol no Banco.

Ao pessoal que deva acessar fisicamente às áreas consideradas como críticas só lhes deve autorizar o acesso às áreas que sejam estritamente necessárias e se deve levar um registro detalhado de acessos. Quando se encontrarem vacantes de pessoal se devem fechar fisicamente e controladas periodicamente.

A área de Segurança Bancária deve delimitar o acesso do pessoal externo às áreas protegidas.

A área de Segurança da Informação deve revisar periodicamente os direitos de acesso às áreas críticas.

deve-se impedir o ingresso a áreas críticas de equipes de computação móvel, fotográficos, de vídeo, áudio ou qualquer outro tipo de equipamento que registre informação, a menos que tenham sido formalmente autorizadas por Segurança da Informação e/ou Segurança Bancária, conforme corresponda e o responsável da o área envolta.

O acesso às áreas onde se processa ou resguarda informação se sensível deve ser restringida somente a pessoal autorizado implementado um controle de acesso adequado.

Todos os empregados, contratados, estagiários e externos devem utilizar algum tipo de identificação visível e devem notificar imediatamente a Segurança Bancária se encontrarem a alguém que não possua uma e/ou que não esteja escoltado.

devem-se controlar os pontos de acesso como as áreas de entrega e carga e outros pontos por onde pessoas no-autorizadas possam ingressar nas instalações e devem isolar-se dos meios de processamento de informação para evitar o acesso não autorizado.

A detecção de acessos forçados ou não autorizados a qualquer das áreas sensíveis deve originar uma alerta a Segurança Bancária.

CONTROLE AMBIENTAL E ANTE DESASTRES

devem-se implementar dispositivos de controle ambiental a efeitos de manter em condições adequadas acordes com as especificações e recomendações dos fornecedores de equipamento.

devem-se atribuir e aplicar proteção física contra desastres (fogo, inundações, tormentas elétricas, etc.), intencionais ou acidentais.

O desenho dos espaços de trabalho deve ter em conta as disposições de Segurança e Higiene no Trabalho e as regulações pertinentes.

SEGURANÇA DO EQUIPAMENTO

PROTEÇÃO FÍSICA DAS EQUIPES

deve-se determinar quais são os níveis adequados de segurança física dos ativos informáticos, tendo em conta as especificações dos fornecedores do hardware e a criticidad da informação segundo a definição de seus Proprietários.

A instalación/desinstalación de computadores pessoais e componentes informáticos, já seja em rede ou não, deve ser realizada por pessoal de Sistemas e Organização ou fornecedores autorizados por sorte área.

As equipes críticas devem estar se localizados ou protegidos de modo de reduzir as ameaças, perigos ambientais e oportunidades para acesso não autorizado.

devem-se definir as características ambientais dos meios de armazenamento para que se conservem em um ambiente que concorde com as especificações dos fabricantes.

O equipamento do Banco deve estar protegido com respeito às possíveis falha no fornecimento de energia ou outras anomalias elétricas, em função de seu criticidad.

O cableado de energia elétrica e de comunicações que transporta dados ou brinda apoio aos serviços de informação deve estar protegido contra intercepción ou dano.

Todo o tendido da rede de dados deve estar acorde às normas e especificações de cableado estruturado.

A manutenção das equipes dever ser levado a cabo por pessoal capacitado, devidamente autorizado e de acordo com as recomendações do fabricante.

As falhas, reais ou supostos, e a manutenção, preventivo ou corretivo, das equipes devem ser registrados e informados ao Proprietário correspondente.

O ingresso às instalações do Banco de equipamento, informação ou software alheio ao Banco deve contar com a autorização prévia de Sistemas e Organização e de Segurança da Informação.

PROTEÇÃO POR PARTE DO PESSOAL

Os responsáveis por setor devem velar pela segurança das equipes informáticas que tenham sido designados ao pessoal a seu cargo.

Os usuários, quando terminarem seu horário trabalhista e se retirem de seu lugar de trabalho, devem deixar toda a informação que estiveram utilizando em um lugar seguro.

O retiro de equipamento, informação ou software das instalações do Banco deve requerer a autorização prévia do Proprietário correspondente.

deve-se eliminar a informação confidencial que contenha qualquer equipamento que seja necessário retirar, realizando-se previamente as respectivas cópias de resguardo que se considerem necessárias.

Os meios de armazenamento do equipamento baixado do inventário do Banco devem ser fisicamente destruídos ou sobrescritos em forma segura, em lugar de utilizar as funções de apagado padrão, conforme corresponda.

Em caso de fechamento de sucursal, deverão tomar-se medidas ao momento da desocupação de maneira que não se possa continuar acessando à rede do Banco através da sucursal desocupada.

POLÍTICA DE ESCRITÓRIOS LIMPOS E TELAS PODAS

Todo o pessoal do Banco deve manter, em todo momento, seus escritórios ou mesas de trabalho livres de documentação à vista e os postos de trabalho bloqueados a fim de reduzir o risco e

acautelar acessos não autorizados, perdida e dano da informação durante ou por fora do horário trabalhista.

devem-se brindar facilidades aos empregados para resguardar de forma segura a documentação frente a incidentes tais como incêndios, goteiras, filtrações e outros possíveis riscos que possam acontecer.

PROTEÇÃO FÍSICA DAS EQUIPES FORA DO ÂMBITO DO BANCO

O uso de equipamento destinado ao processamento de informação, fora do âmbito do Banco, deve ser autorizado por Sistemas e Organização. No caso de que no mesmo se armazene informação classificada, deve ser aprovado além pelo Proprietário da mesma.

A segurança física do equipamento deve ser equivalente à brindada dentro do âmbito do Banco e deve prevê-la contratação de seguros quando o considerar necessário.

Segurança da Informação deve informar aos usuários de equipes móveis em relação às recomendações de segurança do equipamento durante seu transporte e uso fora do âmbito do Banco.

GESTÃO DE COMUNICAÇÕES E OPERAÇÕES

OBJETIVO

Estabelecer os esboços para assegurar a integridade, confidencialidade e disponibilidade dos serviços e as comunicações para garantir um correto processamento da informação, resguardando a segurança da mesma.

ALCANCE

Todos os empregados, contratados, fornecedores e consultores com atividade autorizada em todos os âmbitos do banco.

CONTEÚDO

PROCEDIMENTOS E RESPONSABILIDADES OPERATIVAS

Todos os procedimentos de operação devem ser documentados, mantidos e postos a disposição de todo usuário que por sua função o mereça.

Os procedimentos devem incluir uma lista de pessoal chave ante dificuldades operativas que inclua os dados pertinentes para o contato em caso de ser necessário.

Deve definir um procedimento de gestão para o tratamento de incidentes de segurança que possam afetar as operações. Estes incidentes devem ser reportados a segurança informática.

As mudanças na organização, os processos de negócio, nos sistemas e instalações de processamento de informação devem realizar-se mediante um estrito procedimento de controle de mudanças que inclua como mínimo:

- Identificação e registro de alterações;
- As responsabilidades atribuídas e autorizações pertinentes para cada caso;
- Planejamento e teste de tais mudanças;
- Avaliação do potencial, incluindo segurança da informação, de tais mudanças;
- Procedimentos formais de aprovação para mudanças propostas;
- Verificação do atendimento aos requisitos da Área de Segurança da Informação;
- Comunicar os detalhes da mudança a todas as pessoas relevantes;
- Procedimentos de recuperação, incluindo procedimentos e responsabilidades atribuídas para abortos ou recuperação de mudanças malsucedidas e eventos imprevistos;
- A provisão de um processo de mudança de emergência para habilitar.

As funções de cada área ou pessoa devem ser atribuídas de modo tal que se reduzam as oportunidades de modificações não autorizadas ou uso indevido da informação ou os serviços. Nos casos nos que exista risco de conivência, devem-se desenhar os controles necessários para poder levar a cabo um seguimento adequado.

Os ambientes de desenvolvimento, prova e produção devem estar separados entre si, impedindo a comunicação desde qualquer deles para o outro, a fim de reduzir os riscos de acessos não autorizados ou modificações no ambiente operacional.

A transferência de software ao ambiente de produção deve realizar-se baixo um estrito controle de mudanças.

Os compiladores, editores e outros utilitários do sistema não devem ser acessíveis dos sistemas no ambiente de produção.

Em situações de emergência geradas por enganos no ambiente de produção poderão utilizar-se, conforme se considere necessário, as contas de usuários especiais ou contas de usuário de emergência autorizadas por segurança informática mediante um procedimento disposto para tal fim. A atividade realizada com estas contas deve ser registrada e informada ao proprietário correspondente.

Sistemas e Organização devem garantir os níveis de serviço acordados com as distintas áreas do Banco.

GESTÃO DE SERVIÇOS DE TERCEIROS

deve-se assegurar que os controles de segurança e níveis do serviço definidos no acordo de nível do serviço com terceiros sejam implementados, operem e sejam mantidos conforme o estabelecido no mesmo.

Os serviços providos por terceiros devem ser monitorados e revisados a intervalos periódicos. Esta situação deve ser estabelecida em todos os contratos de serviços tercerizados.

Nos contratos de serviços de processamento externo de dados deve-se considerar que o terceiro em questão possui procedimentos de controles lógicos e físicos para restringir o acesso dos usuários autorizados às informações sensíveis relacionadas ao Banco, planos de contingência que assegurem a disponibilidade dos serviços tercerizados e medidas de segurança física a aplicar ao equipamento terceirizado que prestam serviços ao Banco.

Se a terceira parte não contemplar algum destes pontos, deve tomar os requerimentos definidos pelo Banco ou caso contrário ser aprovado pelo comitê de Segurança da Informação.

PLANEJAMENTO E APROVAÇÃO DE SISTEMAS

PLANEJAMENTO DA CAPACIDADE

A área de Tecnologia e Processamento deve realizar o monitoro do uso dos recursos e projetar as demandas de capacidade para assegurar o poder de processamento e armazenamento.

APROVAÇÃO DO SISTEMA

A área de Sistemas e Organização junto com a área de Segurança Informática definirão critérios de aprovação para novos sistemas de informação, atualizações e novas versões, solicitando a realização das provas necessárias antes de sua aprovação definitiva.

Todo projeto e/ou desenvolvimento e/ou implementação deve cumprir os requerimentos de segurança definidos pela área de Segurança Informática.

AMPARO CONTRA SOFTWARE MALICIOSO E ATAQUE INFORMÁTICOS

Devem existir controles de prevenção e detecção contra o "software malicioso", proveniente tanto da rede externa como a interna.

Devem existir controles de prevenção e detecção contra ataques informáticos, entendidos estes como acessos não autorizados por parte de usuários tão válidos como não validos, denegação de serviço, intentos de execução de ferramentas não permitidas, roubo de informação e roubo de identidade de usuários, entre outros.

Deve aplicar o conceito de defesa em profundidade a efeitos de ter distintas etapas de detecção antes de chegar ao ponto final de infecção e reduzir ao máximo possível a concreção do ataque.

Os usuários não devem ter acesso à instalação de programas e aplicações nos computadores atribuídos pelo Banco.

Segurança Informática deve definir as categorias ou tipos de software que não podem ser executados baixo nenhuma circunstância dentro da Organização.

Devem desenvolver-se procedimentos para evitar riscos relacionados com a obtenção de arquivos ou aplicações desde ou através de redes externas ou qualquer outro meio.

CÓPIAS DE SEGURANÇA

O proprietário da informação deve assegurar-se que toda a informação de sua propriedade seja armazenada de acordo com as definições pelo estabelecidas acorde com as pressente normas.

O Proprietário da Informação, juntamente com os responsáveis pela proteção, deve assegurar que todas as informações armazenadas possam ser recuperadas em caso de emergência.

As cópias de segurança da informação essencial para o negócio e do software, devem ser realizadas e provadas regularmente segundo procedimentos padrão definidos pela Organização.

Deve definir um esquema de identificação para a adequada identificação das cópias de segurança.

deve-se manter um registro do acesso do pessoal às cópias de segurança da informação do Banco e os registros de atividade destes usuários serão verificados periodicamente.

Os arquivos pessoais não devem ser armazenados nos servidores da rede.

Devem ser desenvolvidos procedimentos especiais para o tratamento dos backups dos servidores da sucursal de forma a preservar a integridade física do meio e dos dados suportados, de acordo com as recomendações do fabricante e da Segurança de informação.

ADMINISTRAÇÃO DE REDES

Deve-se garantir a segurança dos dados e os serviços conectados nas redes do Banco, evitando o acesso não autorizado às mesmas.

Devem-se estabelecer procedimento para a administração do equipamento em forma remota inclusive para o equipamento das áreas dos usuários.

Os links de comunicação que transmitem informações consideradas sensíveis pelo Banco devem ser criptografados de acordo com as boas práticas de segurança informática.

ADMINISTRAÇÃO DE SEGURANÇA DOS MEIOS DE ARMAZENAMENTO

MEIOS DE ARMAZENAMENTO REMOVÍVEIS

Consideram-se meios de armazenamento removíveis a todos aqueles dispositivos que permitam armazenar informação e possam ser retirados pelo usuário sem necessidade de afetar o normal funcionamento da equipe ou contar com pessoal ou elementos adicionais para realizá-lo.

Deve limitar-se ao máximo possível o uso dos meios removíveis de armazenamento e seu uso deve estar avalizado por uma necessidade concreta de negócio. Qualquer empregado que requeira o uso de um meio removível deve possuir expressa autorização para seu uso.

Segurança da Informação deve levar um registro da atribuição dos meios removíveis assim como daqueles que se descontinue seu uso com o fim de manter um registro de auditoria. Além disso deverá monitorar a transferência de dados para os mesmos.

Sistemas e o Banco devem estabelecer as diretrizes para a atribuição das mídias removíveis de armazenamento.

A criticidade dos meios de armazenamento removíveis está dada pelos níveis de sensibilidade e criticidade da informação armazenada.

Devem-se determinar os controles que deverão levar-se a cabo para a utilização de meios de armazenamento removíveis que possam ser utilizados para copiar e transportar informação.

Quando se requerer resguardar dados críticos nos meios removíveis devem utilizar-se técnicas de encriptado para proteger os mesmos.

Todos os meios removíveis adquiridos pelo Banco para seu uso devem proteger-se em um entorno seguro até o momento de sua atribuição em concordância com as especificações dos fabricantes.

Deve-se ter em conta que a qualidade do meio removível se degrada no tempo, por isso se deverá transferir os dados a um meio novo antes de que os mesmos se voltem ilegíveis.

Devem estabelecer-se procedimento para a destruição física ou lógica, conforme corresponda, dos meios de armazenamento removíveis, tal que a informação contida no mesmo não se possa recuperar

Segurança informática deve informar aos usuários em relação aos riscos associados com a utilização de meios de armazenamento removíveis nas estações de trabalho e servidores do banco.

INFORMAÇÕES IMPRESSAS

As diretrizes para o tratamento das informações impressas devem ser definidas de acordo com seu nível de classificação.

Todas as informações críticas ou sensíveis ao negócio do Banco que se encontrem em suporte impresso devem ser guardadas em local seguro ou destruídas por método que impeça a recuperação. As diretrizes de destruição devem ser definidas com base em sua classificação.

O uso de impressoras ou copiadoras (fotocopiadoras, scanners ou similares) deve ser autorizado. Além disso, o uso excessivo dessas tecnologias deve ser evitado.

Impressoras ou copiadoras devem ser acessadas pelos usuários usando um fator de autenticação. A sessão deve ter uma duração limitada.

Cópias de documentos contendo informações confidenciais devem ser imediatamente removidas das impressoras ou copiadoras.

PROCEDIMENTOS PARA O TRATAMENTO DE INFORMAÇÃO

A informação deve ser tratada de acordo com os níveis de classificação atribuídos.

Devem-se estabelecer os esboços para o tratamento de informação classificada independentemente do meio no que este suportada (dados, voz, vídeo, impressa, etc.).

Deve-se restringir o acesso à informação classificada sozinho ao pessoal devidamente identificado.

Deve-se manter um registro formal dos receptores autorizados de dados.

Devem-se proteger os dados em espera ou caudas de processamento.

Todos os arquivos pessoais de um funcionário desvinculado que permaneçam na rede ou no disco rígido do computador pessoal devem ser eliminados de maneira segura antes de ser atribuído a outro funcionário, a não ser que o responsável pela área ao qual pertencia o usuário solicite formalmente o contrário.

SEGURANÇA DA DOCUMENTAÇÃO DOS SISTEMAS

A documentação dos sistemas, projetos de infraestrutura tecnológica e edificações dos centros de processamento deve ser armazenada com segurança.

O acesso a essas informações deve ser restrito apenas ao pessoal devidamente autorizado pelo Proprietário das mesmas.

Todas as informações relativas aos projetos de sistemas, tecnologia e / ou infraestrutura predial dos centros de processamento somente poderão ser publicadas ou transferidas a terceiros com a autorização do Proprietário. A segurança informática deve analisar previamente se não está a ser gerada uma declaração de segurança com a referida publicação ou transferência a terceiros.

SEGURANÇA DE MEIOS DE ARMAZENAMENTO EM TRÂNSITO

Devem ser estabelecidas diretrizes para a segurança dos meios de armazenamento de informações em trânsito.

INTERCÂMBIO DE INFORMAÇÃO E SOFTWARE

O intercâmbio de informação com outras organizações deve realizar-se dentro do marco de um acordo de confidencialidade definido conforme corresponda.

A informação do Banco só deve ser transportada pelos meios autorizados.

A publicação de informação do Banco deve ser passada por seu Proprietário.

O uso de comunicações de voz, fax ou vídeo deve estar controlado para evitar sua interrupção, alteração ou divulgação.

Toda informação confiada por terceiros para ser armazenada, transmitida ou processada pelo Banco deve ser tratada e protegida como o especifico o contrato correspondente, ou em seu defeito deve ser considerada como informação confidencial própria do Banco.

Toda transferência de informação a um terceiro deve ser previamente aprovada pelo Proprietário da Informação.

USO DOS SISTEMAS OPERACIONAIS E APLICAÇÕES

Todos os sistemas operacionais e aplicações devem gerar registros de auditoria. O tratamento destes registros deve estar acorde com o nível da classificação dos recursos e as regulações vigentes.

Sistemas e Organização é a responsável por realizar as implementações com os padrões de segurança definidos por Segurança Informática.

Segurança Informática controlará periodicamente que o software instalado nas equipes dos usuários cumpra com os requerimentos de segurança definidos.

BANCA ELETRÔNICA POR DIVERSOS MEIOS

As informações envolvidas nas transações online devem ser protegidas para evitar transmissão incompleta, roteamento incorreto, alteração, divulgação, duplicação ou repetição não autorizada da mensagem.

A integridade das informações disponibilizadas em um sistema de acesso público deve ser protegida para evitar modificações não autorizadas.

Devem ser usados controles criptográficos de robustez reconhecida internacionalmente.

Devem ser considerados todos os regulamentos existentes sobre o controle e operação do ATM, POS, Internet Banking (Home Banking), Telefone Banking (Phone Banking) e outros canais alternativos.

SUPERVISÃO

Devem-se monitorar os sistemas, manter pistas de auditoria de operação e registrar e reportar os enguiços para assegurar que se identifiquem os problemas nos sistemas de informação.

Deve-se utilizar o monitoramento do sistema para revisar a efetividade dos controles adotados e para verificar a conformidade com os requerimentos de segurança da informação.

Devem-se proteger os meios de registro das pistas de auditoria e a informação do registro para evitar a alteração e o acesso não autorizado.

A informação de monitoramento deve ser armazenada por um período não menor ao definido pelos requerimentos legais vigentes.

Toda informação monitorada poderá ser utilizada como evidência para a investigação de um incidente de segurança como assim também para tomar ações legais contra empregados envoltos.

Devem-se registrar todas as atividades dos administradores e operadores do sistema.

Os eventos a ser monitorados devem incluir como mínimo: nome de usuário, hora do sistema, atividade realizada, equipe ao que está conectado, tempo de conexão e execução de comandos críticos.

Os relógios de todos os sistemas de processamento de informação relevantes dentro da organização devem estar sincronizados com uma fonte que proporcione a hora exata acordada.

CONTROLE DE ACESSO

OBJETIVO

Estabelecer as diretrizes necessárias para a implementação de controles de segurança que permitam:

- Impedir o acesso não autorizado a sistemas de informação, bases de dados e serviços de informação.
- Implementar segurança no acesso do usuário por meio de técnicas de autenticação e autorização.
- Controlar a segurança na conexão da rede da Agência com outras redes públicas ou privadas.
- Registrar e revisar eventos e atividades críticas realizadas por usuários nos sistemas.
- Conscientize os usuários de sua responsabilidade com relação ao uso de senhas e equipamentos.
- Garanta a segurança das informações ao usar computação móvel e instalações de trabalho remotas.

ALCANCE

Esta Norma se aplica a todas as formas de acesso de quem possui permissão nos sistemas de informação, bases de dados ou serviços de informação do Banco, independentemente da função que desempenhe no Banco.

POLÍTICA

ACORDOS DE CONFIDENCIALIDADE

Os usuários que não assinaram um contrato de confidencialidade somente terão acesso às informações classificadas como de uso público.

Os usuários devem respeitar a classificação das informações acessadas no âmbito do contrato de confidencialidade devidamente estabelecido.

REQUERIMENTOS PARA O CONTROLE DE ACESSO

Todos os ativos de informação devem ter um sistema de controle de acesso autorizado pela Segurança da Informação e devem estar de acordo com a classificação das informações relacionadas.

Todos os sistemas de controle de acesso devem ser gerenciados e / ou controlados pela Segurança da Informação.

ADMINISTRAÇÃO DE ACESSOS

A solicitação de acesso à informação para um usuário deve ser autorizada pelo responsável do setor a que pertence.

O acesso aos ativos de Informação que não tenham sido classificados pelo seu Titular deve ser autorizado pelo responsável da área da qual depende.

A área de Sistemas deve atribuir os privilégios de cada ambiente de acordo com as necessidades de conhecimento e evento a evento de acordo com a definição do Proprietário do Ativo de Informação.

A área de Sistemas é responsável por conceder acesso aos usuários de acordo com o que for definido pelo Proprietário do Ativo de Informação.

A área de Sistemas deve identificar os privilégios ou atributos especiais de cada ambiente.

A área de Sistemas deve cadastrar e informar aos responsáveis da área as permissões concedidas aos usuários sobre sua responsabilidade.

Os Recursos Humanos são responsáveis por comunicar à Sistemas os funcionários que tenham saído do Banco para que possam ser retirados de todos os sistemas correspondentes.

Os responsáveis da Área devem informar a Sistemas sobre qualquer alteração de funções ou transferências de pessoal sob sua responsabilidade, a fim de eliminar os acessos correspondentes.

As identificações de usuários inativos devem ser desabilitadas e eliminadas pela área de Sistemas de acordo com os procedimentos fornecidos.

As senhas devem ser fornecidas aos usuários atendendo aos requisitos de segurança definidos pela área de Segurança da Informação.

RESPONSABILIDADES DOS USUÁRIOS

Os usuários são responsáveis por toda atividade realizada nos sistemas de informação com sua identificação de usuário.

As senhas devem ser consideradas de uso pessoal e privado com o qual não devem ser divulgadas nem compartilhadas e devem ser consideradas informação confidencial.

Os usuários devem adequar e atualizar suas senhas de acordo com os critérios estabelecidos pela Segurança da Informação.

Os usuários devem respeitar os padrões e procedimentos relacionados com o controle de acesso aos ativos de Informação definidos pela Segurança da Informação.

CONTROLE DE ACESSO À REDE

Os usuários devem ter acesso só aos serviços para os quais tenham sido especificamente autorizados.

Os equipamentos que se conectem à rede do Banco devem ser previamente homologados por Sistemas e pelo Banco.

Os equipamentos que acessem à rede ou serviços de rede do Banco devem estar configurados acorde com os padrões definidos pela Segurança da Informação.

A separação de redes para os grupos de serviços de informação, usuários e sistemas de informação deve estar aprovada pela Segurança da Informação.

Todas as vias de acesso aos sistemas e serviços de informação do Banco devem ser aprovadas pela Segurança da Informação.

As conexões da rede do Banco de / para redes externas devem ser aprovadas por Sistemas e o Banco e autorizadas pela Segurança da Informação.

Todos os Sistemas de Informação da rede do Banco devem ser capazes de gerar e manter um registro das atividades neles.

INTERNET, CORREIO ELETRÔNICO E OUTROS SERVIÇOS RELACIONADOS

Estes serviços são providos pelo Banco para ser utilizados com objetivos relacionados com o negócio do mesmo.

A utilização destes serviços deve estar regulada por procedimentos que definam o bom uso dos mesmos.

Deve-se registrar toda a atividade de uso e a mesma poderá ser verificada de acordo com as necessidades do Banco.

CONEXÕES REMOTAS E EQUIPAMENTOS PORTÁTEIS

Os níveis de segurança requeridos para as conexões remotas devem ser definidos por Segurança da Informação.

Segurança da Informação deve notificar em forma confiável a quão usuários tenham a carrego equipamento portátil e/ou conexões remotas em relação às boas práticas em matéria de segurança da informação associadas aos mesmos.

USO DE CONTAS DE PRIVILÉGIO OU DE EMERGÊNCIA

O acesso privilegiado de um usuário só deve ser concedido de forma restrita à necessidade de trabalho, ter autorização por escrito do responsável da área a que pertence o usuário e a aprovação do Proprietário do ativo de informação relacionado.

A Segurança da Informação deve notificar de forma confiável os usuários com acesso privilegiado sobre as responsabilidades e boas práticas relacionadas ao seu uso.

As contas privilegiadas ou de emergência devem estar sob a custódia da Segurança da Informação e deve haver procedimentos formais para usá-las.

Todas as atividades realizadas por contas privilegiadas ou de emergência devem ser monitoradas e controladas.

IDENTIFICAÇÃO DOS RISCOS RELACIONADOS COM OS GRUPOS EXTERNOS

A área de Segurança da Informação estabelecerá os seguintes controles de acesso de terceiros aos ativos de TI ou instalações do Banco, considerando que:

- Deve haver acordo de confidencialidade entre o contratado e o Banco.
- Deve haver notificação confiável a terceiros usuários sobre a confidencialidade das informações e o uso adequado dos ativos de Informação do Banco.
- O acesso deve ser limitado às áreas estabelecidas para a realização de suas tarefas.
- Os requisitos de segurança para acesso de terceiros aos ativos de Informação do Banco serão detalhados nos respectivos contratos.
- As identificações dos usuários serão habilitadas por tempo de acordo com o período de contratação.

A qualquer pessoa externa ao Banco que necessite de acesso aos ativos de Informação deve ser atribuído um responsável permanente do Banco, que se encarrega de administrar e justificar os acessos, bem como supervisionar as atividades que esta realize.

AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

OBJETIVO

Garantir que o desenvolvimento, manutenção e / ou aquisição dos sistemas de informação do Banco incluam controles de segurança quanto à confidencialidade, integridade, disponibilidade e auditabilidade da informação, de forma a prevenir perdas, modificações ou uso indevido dos dados e / ou dos sistemas de informação do Banco ao longo de seu ciclo de vida e na infraestrutura básica em que são apoiados.

ALCANCE

Esta Norma se aplica a todos os sistemas informáticos, tanto desenvolvimentos próprios ou de terceiros, e a todos os Sistemas operacionais e/ou Software de Base e/ou infraestrutura envolta que integrem qualquer dos ambientes gerenciados.

POLÍTICA

GENERALIDADES

Todos os sistemas de informação do Banco e os ativos que os suportam devem contar com a homologação de Sistemas e o Banco e a aprovação da Segurança da Informação.

Todos os requerimentos de segurança, incluindo a necessidade de planos de contingência, devem ser identificados na fase de requerimentos de um projeto e justificados, aprovados e documentados como uma parte da totalidade do caso de negócio de um sistema de informação.

REQUERIMENTOS DE SEGURANÇA DOS SISTEMAS

A Segurança da Informação, em conjunto com os Proprietários dos ativos de Informação, deve definir os requisitos de segurança para novos sistemas de informação ou melhorias nos existentes.

Os requisitos de segurança definidos devem ser apoiados por uma avaliação de risco prévia.

Os Proprietários da Plataforma e da Segurança da Informação devem definir, para cada plataforma tecnológica, o conjunto de softwares básicos e produtos de segurança que a compõem.

As cláusulas para aquisição de software de terceiros devem incluir aquelas correspondentes a suporte, manutenção e atualizações de segurança, conforme o caso.

SEGURANÇA NOS SISTEMAS DE APLICAÇÃO

Os controles devem ser projetados nos aplicativos para garantir o processamento correto. Esses controles devem incluir validação de dados de entrada, processamento interno e dados de saída.

Boas práticas de segurança aprovadas pela Segurança da Informação devem ser utilizadas para o projeto e desenvolvimento de sistemas aplicativos. O design das aplicações deve incluir controles que garantam a integridade e confidencialidade das informações que processam.

Se o desenho da aplicação requer transferência eletrônica de informação, protocolos de comunicação e técnicas de autenticações/criptografias devem ser utilizadas de acordo com os níveis de segurança estabelecidos para este tipo de troca.

Devem ser realizados testes de segurança para garantir o correto funcionamento dos controles estabelecidos.

CONTROLE CRIPTOGRÁFICOS

A área de Segurança da Informação deve definir os mecanismos criptográficos de proteção da informação.

Devem ser desenvolvidos procedimentos para gerenciamento de chaves, recuperação de informações criptografadas em caso de perda, comprometimento ou dano de chaves e para substituição de chaves de criptografia.

Os controles criptográficos devem ser aplicados de acordo com a confidencialidade das informações envolvidas definida no processo de Classificação de Ativos de Informação.

SEGURANÇA DOS ARQUIVOS DO SISTEMA

A atualização das bibliotecas do programa de produção (código-fonte ou código executável) deve ser realizada sob estrito controle de alterações.

O lançamento de novos aplicativos ou atualizações de aplicativos existentes deve requerer a autorização prévia do Proprietário correspondente de acordo com o processo de gerenciamento de mudanças em curso.

Em acordos com fornecedores de software, a responsabilidade por sua manutenção e conformidade com os padrões de segurança deve ser especificada.

No caso de software aplicativo adquirido de terceiro, sobre o qual o Banco não detém qualquer direito sobre o código-fonte, o mesmo deve ser mantido sob custódia de terceiro, em acordo com o provedor.

O acesso e a utilização dos sistemas e tecnologias de informação do Banco pelos fornecedores devem ser autorizados pelo Proprietário da Informação e subsequentemente monitorados e controlados.

Devem ser estabelecidos workflows específicos para a cópia das informações do ambiente de produção para o ambiente de teste, devem ser aprovados pelo Proprietário da Informação e sua proteção deve ser garantida em condições semelhantes às do ambiente de produção. Além disso, se a cópia incluir informações de caráter pessoal, os dados que revelem a identidade devem ser apagados.

As informações dos sistemas em produção usados em sistemas de teste devem ser excluídas quando seu período de uso terminar.

A área de Segurança da Informação deve realizar o controle de acesso aos ambientes de produção, teste e desenvolvimento.

O Proprietário da Informação deve designar o pessoal autorizado a realizar a atualização das bibliotecas de programas em produção.

SEGURANÇA DOS PROCESSOS DE DESENVOLVIMENTO E SUPORTE

A área de Sistemas e Organização, com a participação da Segurança da Informação, deve planejar e coordenar as alterações de hardware e software básico com os responsáveis pelos sistemas aplicativos. Essas alterações devem ser comunicadas aos respectivos proprietários.

No caso de uma atualização ou alteração nos sistemas operacionais, você deve garantir que os sistemas de aplicativos sejam revisados e testados para garantir que tal alteração não tenha um impacto adverso nas operações ou na segurança.

Caso sejam necessárias alterações nos pacotes de software fornecidos pelos fornecedores, a área de Segurança da Informação deve autorizá-las e definir os controles de segurança que devem ser levados em consideração para sua aplicação.

A segurança do computador deve definir os requisitos de segurança relevantes antes de comprar software desenvolvido por terceiros.

GESTÃO DE VULNERABILIDADES

Devem ser definidos procedimentos e / ou mecanismos para a aplicação de patches de segurança nos sistemas de informação do Banco.

A área de Segurança da Informação deve realizar um gerenciamento de vulnerabilidade nos sistemas de informação em uso para reduzir a exposição ao risco por falhas ou configurações inadequadas.

GESTÃO DE INCIDENTES

OBJETIVO

Estabelecer diretrizes para garantir que os incidentes e fragilidades de segurança associados aos ativos de informação sejam gerenciados com uma abordagem coerente e eficaz, permitindo que ações corretivas sejam tomadas em tempo hábil, minimizando sua possibilidade de ocorrência no futuro e reduzindo ao máximo o impacto para o Banco. Também inclui aspectos relacionados à comunicação de eventos e pontos fracos de segurança.

ALCANCE

Esta Norma é de aplicação para todos os incidentes de segurança relacionados aos ativos de informação e funcionários do Banco e/ou terceiros relacionados.

POLÍTICA

RESPONSABILIDADES E PROCEDIMENTOS

Responsabilidades e procedimentos devem ser definidos para garantir uma resposta rápida, eficaz e metódica aos incidentes de Segurança da Informação.

A gestão de responsabilidades deve assegurar que os seguintes procedimentos sejam desenvolvidos e comunicados de forma adequada dentro do Banco:

- Procedimentos de resposta e preparação de respostas a Incidentes.
- Procedimentos de monitoramento, detecção, análise e reporte de eventos e incidentes de Segurança da Informação.
- Procedimentos para registrar ações relacionadas ao gerenciamento de incidentes.
- Procedimentos para lidar com evidências forenses.
- Procedimentos de avaliação e decisão sobre eventos de Segurança da Informação e avaliação de fragilidades da Segurança da Informação.
- Procedimentos de resposta que incluem mecanismos de escalonamento, recuperação controlada de um incidente e comunicação interna ou externa.

Os procedimentos estabelecidos devem garantir que:

- Somente pessoal competente lida com problemas relacionados a incidentes de Segurança da Informação por meio do Banco.
- Um único ponto de contato é implementado para o relato de Incidentes de Segurança.
- Contatos apropriados são mantidos com autoridades, grupos de interesse externos e fóruns que tratam de assuntos relacionados a Incidentes de Segurança.

Os procedimentos de relatório devem incluir:

- A preparação de formulários para o Reporte de eventos de Segurança da Informação para apoiar as ações de denúncia e para ajudar quem realiza uma ação de denúncia a lembrar todas as ações necessárias a serem tomadas em caso de ocorrência de um evento.
- O procedimento que será realizado no caso de um evento de Segurança da Informação.
- Referências ao estabelecimento de um processo disciplinar formal para gerenciar o relacionamento com os funcionários que cometem ou estão envolvidos em uma violação de segurança.
- Processos de resposta apropriados que garantem que aqueles que relatam eventos de segurança da informação sejam notificados nos resultados após o evento ter sido controlado e fechado.

Os objetivos do gerenciamento de incidentes de segurança devem ser consistentes com o gerenciamento de TI e devem garantir que aqueles com responsabilidades pelo gerenciamento de incidentes de segurança, entenda as prioridades do Banco para o tratamento de informações sobre eventos de Segurança.

Os incidentes de segurança da informação podem transcender as fronteiras do Banco e do país. Para responder a esses incidentes, há uma necessidade crescente de coordenar a resposta e o compartilhamento de informações sobre eles com organizações externas, sempre que apropriado.

REPORTES DE INCIDENTES DE SEGURANÇA

Os eventos de segurança da informação devem ser relatados por meio dos canais administrativos apropriados o mais rápido possível.

A segurança da informação deve estabelecer um procedimento formal para relatar eventos de segurança da informação.

Todos os usuários do Banco, fornecedores e terceiros devem estar cientes de suas responsabilidades de relatar eventos de Segurança da Informação o mais rápido possível.

Todos os usuários do Banco, fornecedores e terceiros devem estar cientes dos procedimentos para relatar incidentes e fragilidades de segurança que possam impactar a segurança dos ativos da Organização. Os usuários não devem realizar nenhuma ação por conta própria e, sob nenhuma circunstância, devem provar uma vulnerabilidade suspeita.

Os seguintes eventos de Segurança da Informação devem ser relatados, no mínimo:

- Ineficácia dos controles de segurança.,
- Falhas na integridade, confidencialidade e disponibilidade esperada das informações.
- Erros humanos.
- Violação de políticas ou padrões de segurança da informação.
- Falhas na segurança física.
- Mudanças não controladas nos sistemas.
- Mau funcionamento de peças de software ou hardware.
- Violações no acesso físico ou lógico.

Mau funcionamento ou qualquer outro comportamento anômalo de um sistema pode ser um indicador de um ataque de segurança ou uma violação de segurança e deve sempre ser relatado como um evento de segurança da informação.

REPORTES DE VULNERABILIDADES DE SEGURANÇA

Todos os utilizadores do Banco, fornecedores e terceiros que utilizem os sistemas e serviços de informação do Baco devem comunicar qualquer observação ou suspeita de vulnerabilidades de Segurança da Informação nos sistemas ou serviços.

Essas questões devem ser relatadas ao ponto de contato o mais rápido possível, a fim de evitar incidentes de Segurança da Informação. O mecanismo de relatório deve ser o mais fácil, acessível e disponível possível.

Nenhum usuário do Banco, provedor ou terceiro deve tentar testar uma vulnerabilidade de segurança nos sistemas. As vulnerabilidades de teste podem ser interpretadas como um potencial

uso indevido do sistema e também pode causar danos ao sistema de informações ou serviço e resultar em responsabilidade legal para o indivíduo que realiza o teste.

AVALIAÇÃO E CLASSIFICAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

A área de Segurança da Informação deve avaliar os eventos e decidir se eles são classificados como incidentes de Segurança.

O ponto de contato deve avaliar as informações disponíveis sobre um evento de segurança e, usando a escala de classificação de incidente de segurança desenvolvida anteriormente, deve decidir se classifica tal evento como um incidente de Segurança da Informação.

Deve haver uma Equipe de Resposta a Incidentes de Segurança (CSIRT - Equipe de Resposta a Incidentes de Segurança em Computadores) que deve confirmar ou reavaliar o evento de Segurança.

Os resultados da avaliação e a decisão tomada devem ser registrados em detalhes para fins de referência ou verificação futura.

RESPOSTA A INCIDENTES DE SEGURANÇA

Procedimentos metódicos devem ser estabelecidos para garantir respostas rápidas e eficazes.

- O gerenciamento de um incidente de segurança deve incluir, no mínimo: A coleta de evidências o mais rápido possível após a ocorrência do evento.
- Realização de análises forenses de Segurança da Informação, quando necessário.
- Escalonamento de incidentes, quando necessário.
- Certifique-se de que todas as atividades de resposta envolvidas sejam registradas de forma apropriada para análise posterior.
- Comunicar a existência de um Incidente de Segurança da Informação ou qualquer detalhe relevante a outras pessoas ou organizações que devam notificar.
- Tratar as vulnerabilidades da Segurança da Informação que causaram ou contribuíram para causar o incidente de Segurança da Informação.
- Uma vez que o incidente tenha sido tratado com sucesso, ele deve ser formalmente encerrado e registrado.

Todos os incidentes de segurança relatados devem ser validados para serem analisados e encaminhados à área responsável pela sua resolução.

Os resultados devem ser relatados após o incidente ter sido tratado para aqueles que o relataram.

Deve ser mantido um registro e analisados os incidentes, ameaças, falhas de segurança dos sistemas ou serviços de informação do Banco e elaborados relatórios periódicos de revisão e acompanhamento.

Devem ser implementados mecanismos para quantificar e monitorar os tipos e volumes de incidentes.

Sistemas e o Banco devem colaborar na detecção e investigação de incidentes de segurança e implementar as contramedidas necessárias para conter um incidente em curso, bem como aquelas necessárias para evitar uma recorrência no futuro.

GESTÃO DE INCIDENTES DE SEGURANÇA

A Segurança da Informação deve possuir um procedimento de Gerenciamento de Incidentes que contemple os requisitos de ação necessários para a identificação, classificação, priorização, medição, registro e responsabilidades pela resolução de incidentes de segurança.

A área designada para a resolução de um incidente de segurança deve reportar à Segurança da Informação as ações tomadas para resolvê-lo.

A área de Segurança da Informação deve monitorar e controlar a resolução dos incidentes de segurança relatados.

Sistemas e o Banco devem colaborar com a Segurança Informática na detecção e investigação de incidentes de segurança e implementar as medidas necessárias para conter um incidente em curso, bem como as necessárias para evitar que se repitam no futuro.

Quando houver suspeita ou conhecimento de que os computadores ou outros equipamentos fornecidos pelo Banco estão ou podem estar envolvidos em um incidente de segurança, o pessoal de Tecnologia da Informação e / ou Sistemas e Segurança da Organização está autorizado a aplicar os procedimentos para examinar o seu conteúdo, incluindo arquivos e / ou programas de caráter pessoal.

Convém que as informações obtidas na avaliação de incidentes de segurança sejam utilizadas para identificar, prevenir e resolver incidentes recorrentes ou de alto impacto.

Um mecanismo deve ser implementado para permitir que os tipos, volumes e custos dos incidentes de Segurança da Informação sejam quantificados e monitorados. Convém que as informações obtidas na avaliação de incidentes de segurança da informação sejam usadas para identificar incidentes recorrentes ou de alto impacto.

A avaliação de incidentes de Segurança da Informação pode indicar a necessidade de controles aprimorados ou adicionais para limitar a frequência, danos e custo de ocorrências futuras, ou para levá-los em consideração no processo de revisão das políticas de Segurança da Informação.

COLETA DE EVIDÊNCIAS

SE O INCIDENTE ENVOLVER UMA AÇÃO JURÍDICA CONTRA UM FUNCIONÁRIO, O BANCO OU OUTRA ORGANIZAÇÃO, A PROVA DEVERÁ SER COLETADA E CUSTÓDIA DE ACORDO COM OS PROCEDIMENTOS EXIGIDOS PARA QUE SEJA VÁLIDA NAS INSTÂNCIAS DO TRIBUNAL.

Os procedimentos de identificação, coleta, aquisição e preservação de evidências devem ser desenvolvidos e executados de acordo com os diferentes tipos de mídia, dispositivos e estados dos dispositivos. Os procedimentos devem considerar: A cadeia de custódia, o cuidado com as evidências, a segurança do pessoal, as funções e responsabilidades do pessoal, as competências do pessoal envolvido, a documentação de todas as ações e as instruções aplicadas.

Ferramentas qualificadas devem estar disponíveis para consolidar o valor das evidências coletadas.

Nos casos em que as provas envolvidas transcendam os limites jurisdicionais do Banco, deve-se assegurar que o Banco tenha autorização para coletar as informações exigidas como prova pericial. Além disso, os requisitos de diferentes jurisdições devem ser levados em consideração para maximizar a probabilidade de admissão através das jurisdições relevantes.

Quando um evento de segurança da informação é detectado pela primeira vez, pode não ser identificado se levar a um processo judicial. Portanto, haverá o risco de que as provas necessárias sejam destruídas intencionalmente ou acidentalmente antes que a gravidade do incidente se torne aparente. A participação antecipada deve ser dada à área Jurídica e Jurídica em qualquer ação judicial contemplada. Deve aconselhar sobre as evidências exigidas.

Glossário:

- Identificação é o processo que envolve a busca, reconhecimento e documentação de evidências potenciais.
- Coleta é o processo de coleta de itens físicos que podem conter evidências potenciais.
- Aquisição é o processo de criação de uma cópia dos dados em um conjunto específico de dados.
- Preservação é o processo para manter e salvaguardar a integridade e a condição original de possíveis evidências.

CONTINUIDADE DE NEGÓCIO

OBJETIVO

Estabelecer orientações gerais para o desenvolvimento e manutenção de procedimentos que garantam a continuidade operacional dos processos críticos de negócio em condições aceitáveis dos sistemas de informação que os suportam.

ALCANCE

Esta Norma é aplicável a todos os processos de negócios classificados como críticos.

POLÍTICA

GENERALIDADES

Entende-se por plano de continuidade de negócios o conjunto de procedimentos estrategicamente desenvolvidos para garantir a continuidade operacional de processos críticos para que possam continuar a ser executados independentemente do evento que os afetou, em condições aceitáveis para o Banco.

Por plano de contingência entende-se o conjunto de procedimentos desenvolvidos para garantir a continuidade operacional da infraestrutura tecnológica de suporte aos processos críticos de negócio, em condições aceitáveis para o Banco.

A gestão da continuidade do negócio é um processo que deve envolver todos os níveis do Banco.

O desenvolvimento e implementação de planos de contingência é uma ferramenta básica para garantir que as atividades da Agência possam ser restauradas nos prazos exigidos.

Tais planos devem ser mantidos atualizados e fazerem parte integrante dos demais processos de administração e gestão, devendo necessariamente incluir controles que visem identificar e reduzir riscos, mitigar as consequências de eventuais interrupções nas atividades da organização e garantir a retomada atempada das atividades operações essenciais.

REQUERIMENTOS PARA A GESTÃO DA CONTINUIDADE DO NEGÓCIO

A Unidade Organizacional responsável pelo plano de continuidade de negócios, juntamente com os Proprietários das Informações, os Proprietários da Plataforma e a Segurança da informação, deve projetar os Planos de Contingência e Recuperação de Desastres e controlar se eles são atualizados em tempo hábil.

As condições e procedimentos de recuperação dos processos devem basear-se numa Análise de Impacto no Negócio a partir da qual se identifiquem os incidentes que podem causar interrupções nos processos, bem como a probabilidade e o impacto dessas interrupções e as suas consequências para o negócio do Banco. Os níveis e tempos de recuperação dos processos de negócio devem ser definidos de acordo com o resultado dessa análise.

Os responsáveis pelas Plataformas devem incluir nos projetos de infraestruturas tecnológicas os componentes necessários para garantir a continuidade operacional dos serviços.

Os planos de contingência devem incluir controles para conter as consequências dos incidentes e garantir a disponibilidade de informações sobre os processos críticos de negócios.

O plano de continuidade de negócios e planos de contingência devem ser distribuídas de forma que estejam disponíveis para o pessoal responsável envolvido, independentemente do evento que os originou.

Uma orientação geral será mantida para o plano de continuidade de negócios e planos de contingência, a fim de garantir que todos os planos sejam completos e consistentes com os requisitos de segurança da informação e necessidades de recuperação estabelecidas.

Os planos de continuidade de negócios e planos de contingência devem ser testados e atualizados para garantir que sejam eficazes. A revisão e o teste dos planos devem ser periódicos e realizados por meio de procedimentos específicos.

Um plano de treinamento formal deve ser estabelecido para o pessoal-chave envolvido com relação aos planos de continuidade e contingência.

Os serviços prestados por terceiros devem ter planos de contingência que devem ser comunicados formalmente à área responsável pela contratação. Esses planos de contingência devem ser considerados no plano de continuidade de negócios do Banco.

CUMPRIMENTO LEGAL E NORMATIVO

OBJETIVO

Cumprir as disposições legais, regulamentares e contratuais de forma a evitar danos de natureza jurídica ou administrativa ao Banco e/ou aos seus colaboradores, garantindo que os sistemas informáticos e a utilização das tecnologias associadas cumpram a Política, Norma, Normas e Procedimentos da Segurança do Banco.

ALCANCE

Esta Norma é de aplicação para todos os funcionários do Banco, pessoal contratado, fornecedores e consultores que desempenhem atividades em qualquer área do Banco.

POLÍTICA

CUMPRIMENTO DE REQUISITOS LEGAIS E NORMATIVOS

IDENTIFICAÇÃO DA LEGISLAÇÃO E REGULAÇÕES APLICÁVEIS

O Proprietário dos Ativos de Informação, em conjunto com a Segurança da Informação, Assessoria Jurídica e Sistemas e o Banco, deve definir os controles específicos e as responsabilidades individuais para cumprir os correspondentes requisitos legais e regulamentares.

Todos os requisitos legislativos, regulamentares e de certificação aplicáveis ao Banco devem ser explicitamente definidos, documentados e atualizados.

A proteção e privacidade dos dados pessoais deve ser garantida conforme exigido pela legislação, regulamentos e, se aplicável, pelas cláusulas contratuais pertinentes.

DIREITOS DE PROPRIEDADE INTELECTUAL

Todas as cópias do software utilizado pelo Banco devem ter suas respectivas licenças e cumprir os requisitos legais correspondentes.

Sistemas e o Banco devem controlar o cumprimento das normas legais correspondentes à propriedade intelectual com relação ao uso do software.

No momento da aquisição, implementação, transferência ou eliminação do software licenciado, devem ser seguidos os procedimentos definidos pelo Banco para o efeito.

Sistemas e o Banco devem manter um registro de evidências e evidências de propriedade de licenças, discos principais, manuais, etc.

É expressamente proibida a instalação, utilização ou cópia do software adquirido pelo Banco em computador diferente daquele para o qual está licenciado.

O software adquirido pelo Banco deve ser utilizado estritamente para o fim para o qual foi licenciado.

Todos os programas e utilitários de uso livre devem ser licenciados e cumprir estritamente as leis de direitos autorais, bem como as restrições detalhadas pelo fabricante.

Os controles necessários devem ser realizados de forma a não ultrapassar o número máximo de usuários permitidos pelo fornecedor do software.

PROTEÇÃO DOS REGISTROS DO ORGANISMO

Os documentos que suportam as atividades essenciais do Banco, bem como os necessários ao cumprimento de requisitos legais ou regulamentares, devem ser protegidos dos riscos de perda, destruição e falsificação de acordo com a classificação definida pelos seus Titulares.

Os meios de armazenamento dos documentos que suportam as atividades essenciais do Banco devem ser reservados e protegidos de acordo com as recomendações do fabricante, devendo ser considerada a possibilidade de degradação dos meios utilizados para o armazenamento dos documentos.

O sistema de armazenamento e manuseio deve garantir uma identificação clara dos registros e seu período de retenção legal ou regulamentar. Da mesma forma, será permitida a destruição adequada dos registros uma vez transcorrido esse prazo, caso não sejam mais necessários para o Banco.

A utilização de meios de armazenamento eletrônico deve incluir procedimentos que garantam a capacidade de acesso aos dados (formato e legibilidade dos suportes) durante todo o período de retenção, de forma a protegê-los de eventuais perdas causadas por futuras alterações tecnológicas.

A Segurança da Informação deve assegurar o uso adequado dos ativos informáticos do Banco, a fim de verificar o cumprimento do quadro regulamentar.

O software desenvolvido pelo Banco ou para o Banco é propriedade do Banco e não pode ser fornecido a terceiros sem a autorização do respectivo Proprietário.

Softwares desenvolvidos interna e / ou externamente devem ser registrados em nome do Banco. No caso de Sistemas e Organização considerar necessário, a Assessoria Jurídica deve intervir no acordo escrito entre as partes onde a titularidade do direito de propriedade intelectual é acordada.

PREVENÇÃO DO USO INADEQUADO DOS RECURSOS DE PROCESSAMENTO DE INFORMAÇÃO

Deve-se garantir que os sistemas de informação cumpram os regulamentos e padrões ou códigos de prática relacionados à produção de evidências válidas.

REGULAÇÃO DE CONTROLES PARA O USO DE CRIPTOGRAFIA

Os controles criptográficos a serem utilizados devem ser aqueles definidos pelo Banco de acordo com as leis e regulamentos específicos.

COLETA DE EVIDÊNCIA

Devem ser definidos os procedimentos necessários à recolha e guarda das provas digitais, respeitando o disposto na regulamentação processual, considerando as boas práticas para garantir a sua validade.

REVISÕES INTERNAS DE SEGURANÇA E COMPATIBILIDADE TÉCNICA

A Segurança da Informação deve revisar periodicamente a segurança dos ativos de Informação e sua conformidade com os padrões definidos, auxiliada pelos Proprietários das Informações e Proprietários da Plataforma.

Os Proprietários das Informações e Proprietários da Plataforma devem garantir a conformidade com a Política e Padrões de Segurança da Informação e a aplicação dos procedimentos e padrões de segurança dentro de sua área de responsabilidade.

REVISÕES EXTERNAS DE SEGURANÇA

A Segurança da Informação deve planejar e pactuar as atividades que envolvam verificações de terceiros dos sistemas operacionais, de forma a minimizar o risco de descontinuidade das tarefas do Banco.

As ferramentas utilizadas durante as auditorias devem ser revisadas e aprovadas pela Segurança da Informação antes de serem utilizadas nos sistemas do Banco para evitar qualquer possível uso indevido ou transgressão.

Os contratos de revisões externas de conformidade com as Políticas de Segurança devem incluir um acordo de confidencialidade atemporal com a empresa e seus funcionários designados para realizar a tarefa em relação às informações envolvidas no processo.

PENALIDADES POR NÃO CUMPRIMENTO

O descumprimento da Política e Normas de segurança deve ser sancionado administrativamente de acordo com as normas estatutárias, escalonarias e convencionais que regem para o pessoal do Banco.

POLÍTICA DE SEGURANÇA CIBERNÉTICA

RESUMO

Esta Política aborda as diretrizes, atribuições e responsabilidades no processo de Segurança Cibernética do Banco de La Nación Argentina no Brasil.

INTRODUÇÃO

A Política de Segurança Cibernética é o documento que orienta sobre as responsabilidades da Filial do Brasil do Banco de La Nación Argentina, doravante denominado neste documento como BNA Brasil, para cumprimento dos requisitos da Resolução 4.658 do Banco Central do Brasil.

OBJETIVO

O objetivo desta política é orientar os funcionários e definir os procedimentos e controles do BNA Brasil em relação à segurança cibernética, os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, estando em conformidade com a legislação vigente.

Destaca-se que além dos fornecedores de nuvem, os fornecedores de tecnologia da informação relevantes devem estar em conformidade com esta Política.

PÚBLICO ALVO

Esta Política Corporativa, submete-se a todas as áreas do BNA Brasil, ao seu cumprimento.

Aplicam-se a todos os administradores e demais funcionários do BNA Brasil, com a recomendação de que todos sejam diligentes no cumprimento das diretrizes definidas referente ao processo de contratação de serviços de fornecedores.

DEFINIÇÕES INTERNAS

É de extrema importância a disseminação da cultura de segurança cibernética para garantir a integridade, confiabilidade e disponibilidade das informações. Para garantir o cumprimento dos princípios dispostos acima, o BNA Brasil utiliza diversos meios como as políticas internas, instruções normativas, comunicados corporativos e a realização de treinamentos periódicos (quando necessários) de segurança da informação e compliance.

CONTROLES INTERNO

O BNA Brasil possui diversos controles e procedimentos internos para garantir a segurança das informações sensíveis, conforme descrito nos tópicos abaixo:

- **Controle de Acesso e Gerenciamento**
- **Gerenciamento de Riscos**
- **Segurança de Rede**
- **Segurança e gerenciamento**

- **Gestão de TI (Ameaças e Vulnerabilidades)**
- **Dispositivos e Controles de Mídia**
- **Segurança Física**

REGISTRO E ANÁLISE DE INCIDENTES RELEVANTES E VULNERABILIDADES

O registro, análise dos efeitos de incidentes relevantes são atividades cruciais para minimizar impactos negativos para o BNA Brasil, a nível operacional e reputacional.

DIRETRIZES GERAIS

- **Teste de Continuidade de Negócios**
- **Prestadores de Serviços de Tecnologia**
- **Classificações da criticidade dos Incidentes**

TREINAMENTO DE SEGURANÇA NO BNA BRASIL

O BNA Brasil incentiva e promove uma cultura de segurança dentro da instituição, visando proteger os objetivos citados nesta política, e principalmente proteger a informação.

INFORMAÇÕES NO BNA BRASIL

O BNA Brasil buscando sempre atuar com transparência e objetivando a melhoria dos seus procedimentos relacionados à Segurança Cibernética, tem o compromisso de compartilhar com o BACEN todos incidentes relevantes, tempestivamente, sempre que solicitado.

CONTRATAÇÃO DE SERVIÇOS (LOCAL OU EM NUVEM)

Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem seguem aderentes com as diretrizes indicadas na Resolução 4.658 do BACEN.

PROCESSO DE SEGURANÇA CIBERNÉTICA

O monitoramento da segurança cibernética é realizado pela nossa Área de Sistemas Exterior e a Área de Segurança da Informação ambas de nossa Casa Central na Argentina, frente a um incidente o mesmo é comunicado para a Área de Sistemas e a Diretoria do Banco e após a solução do problema o mesmo fica registrado na ata de comitê de Sistemas.

RELATÓRIO ANUAL

De acordo com a Resolução 4.658 do BACEN, anualmente, até o dia 31 de março, o Banco deverá emitir um relatório sobre a implementação do plano de ação de respostas a incidentes, com data base de 31 de dezembro do ano anterior ao relatório, contendo:

- A efetividade da implementação das ações a serem desenvolvidas pela instituição para adequar suas estruturas aos princípios e às diretrizes da política de Segurança Cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes ocorridos no período;
- Resultado dos testes de continuidade de negócios.

DOCUMENTAÇÃO MÍNIMA A SERARQUIVADA ECORRENTE DA RESOLUÇÃO 4.658

Devem ficar à disposição do Banco Central do Brasil pelo prazo de 05 (cinco) anos:

- A presente Política;
- Ata do Comitê de Sistemas que consta a aprovação da Política;
- Documento relativo ao plano de ação e de resposta a incidentes (caso ocorra incidentes);
- Relatório anual;
- Documentação sobre os procedimentos;
- Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle que visam assegurar a implementação e a efetividade da política se Segurança Cibernética.

AVALIAÇÃO

O processo e a Política de Segurança Cibernética estão sujeitos à avaliação no Comitê de Sistemas.

RESPONSÁVEL PERANTE O BANCO CENTRAL DO BRASIL

O Diretor de Riscos é o responsável pela Política de Segurança Cibernética e, encontra-se cadastrado no sistema do BACEN.

POLÍTICA, NORMATIVOS E MANUAIS RELACIONADOS

- Política de Segurança da Informação
- Normativos internos do BNA Brasil
- Segurança da Área de Sistemas
- Gestão da Área de Sistemas
- Procedimentos dos Sistemas Informáticos
- Plano de Contingência
- Avaliação e Administração de Risco de TI

APROVAÇÃO/REVISÃO

APROVAÇÃO

Informo que essa Política de Segurança Cibernética foi aprovada e consta na ata de Comitê de Sistemas do mês de maio/2020.