MANUAL DE NORMAS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO - CONTROLE DE ACESSO NORMAS DE BACKUP E RECUPERAÇÃO DE DADOS

DITEC

HISTÓRICO DE REVISÃO

Data	Versão	Principais Alterações (Itens)
22/09/2025	2	• Capitulo I - GESTÃO E CONTROLE DE ACESSO - item 6.2.21 • Capítulo II - BACKUP E RECUPERAÇÃO DE DADOS - item 11. BACKUP DE E-MAILS CORPORATIVOS
07/04/2025	1.1	• Capitulo I - GESTÃO E CONTROLE DE ACESSO - Item 6.2– subitem I (inclusão); • Capitulo I - GESTÃO E CONTROLE DE ACESSO - item 6.2.18.1 – subitem VI; • Capitulo I - GESTÃO E CONTROLE DE ACESSO - item 6.2.18.1 – subitem IX
24/02/2025	1	• 1ª Publicação

SUMÁRIO

APRESENTAÇÃO

Este Manual de Normas e Procedimentos institucionaliza, define as diretrizes do processo, papéis e responsabilidades, estabelece fluxos de trabalho e outros atributos necessários para o processo de segurança da informação nos aspectos de controle e manutenção do acesso e normatização quanto a backup e recuperação de dados.

CAPÍTULO I – GESTÃO E CONTROLE DE ACESSO

1. OBJETIVO

Formalizar e tornar institucional o Manual de Normas e Procedimentos de Segurança da Informação, referente aos processos de controle e manutenção de acesso e seus respectivos indicadores.

2. UNIDADE GESTORA

Caberá ao Subnúcleo de Segurança da Informação e Proteção de Dados Pessoais atuar como gestor na criação/alteração de normas e procedimentos a serem aplicados nas unidades do Banpará com relação ao processo gerenciamento de segurança da informação regido por este normativo, e caberá às demais unidades do Banco, a observância das normas e procedimentos contidos neste documento.

3. ESCOPO DO PROCESSO

Processo de gestão e controle de acesso à rede, e-mails, internet, VPN, servidor de arquivo, sistemas corporativos e ambiente de tecnologia abordando requisitos de segurança voltados ao Privilégio mínimo.

3.1. CONTROLE E MANUTENÇÃO DE ACESSO:

- Acesso à rede corporativa;
- Acesso à internet;
- Acesso de correio eletrônico;
- Acesso de usuários temporários;
- Acesso à VPN;
- Acesso a servidores de arquivos;
- Acesso a ambientes de tecnologia da informação;
- Acesso a sistemas corporativos;
- Acesso e auditoria nos sistemas corporativos;

4. RETORNO E BENEFÍCIOS DO PROCESSO

Benefícios ao processo de gerenciamento de acesso:

- Controle de privilégio mínimo minimizando o potencial de abuso ou erro humano;
- Prevenção de acessos não autorizados;
- Atendimento a regulamentações e a auditorias;
- Registros de atividades possibilitando a rastreabilidade a prestação de contas;
- Facilidade na administração, simplificando a administração e permitindo uma visão consolidada e o gerenciamento eficiente;

- Redução de riscos internos de fraude pela limitação de acesso a informações somente a pessoas autorizadas;
- Detecção de atividades suspeitas por meio de monitoramento contínuo;
- Mitigação de ameaças externas ajudando a controlar, proteger acessos a sistemas e dados críticos;
- Controle sobre acesso a informações sensíveis.

5. PAPÉIS E RESPONSABILIDADES NO PROCESSO

Abaixo estão definidos os papéis, seus executores e suas respectivas responsabilidades que serão referenciados no detalhamento do processo e matriz RACI a seguir.

Tabela 1 – Papeis e responsabilidades

PAPEL	RESPONSABILIDADES	RESPONSÁVEL
DONO DO PROCESSO	• Estabelecer políticas, Normas e Procedimentos de forma clara e diretrizes para o acesso a sistemas e dados sensíveis. • Categorizar usuários de acordo com suas funções e responsabilidades para atribuir os níveis apropriados de acesso. • Garantir que os privilégios concedidos se alinhem com as funções e responsabilidades dos usuários. • Realizar revisões regulares de acessos para garantir que os privilégios de usuário permaneçam apropriados. • Implementar sistemas de monitoramento para identificar atividades suspeitas ou acessos não autorizados. • Realizar auditorias periódicas para garantir conformidade com políticas e regulamentos. • Fornecer treinamento aos usuários sobre as políticas de acesso e as práticas de segurança. • Garantir que os usuários estejam cientes das implicações de segurança e conformidade relacionadas ao acesso a sistemas. • Fornecer instruções básico aos usuários sobre boas práticas de segurança, políticas de acesso e uso adequado de credenciais. • Desenvolver procedimentos para lidar com violações de segurança e responder a incidentes relacionados a acessos não autorizados. • Colaborar com outros processos de gerenciamento, como o gerenciamento de identidade, para garantir uma abordagem holística para o controle de acesso. • Manter-se atualizado sobre as melhores práticas de segurança e regulamentações relevantes para ajustar as políticas de acesso conforme necessário.	Chefe e Analistas do Subnúcleo de Segurança da Informação e Proteção de Dados Pessoais – SSI

	• Garantir que as ferramentas e sistemas utilizados para a gestão de acesso estejam atualizadas e funcionando corretamente.	
OPERADOR DO PROCESSO	• Criar contas de usuário conforme as solicitações, garantindo que sigam as políticas de segurança e as atribuições de funções adequadas. • Modificar os níveis de acesso conforme as mudanças nas responsabilidades dos usuários ou conforme solicitado pelo responsável pela gestão de acesso. • Remover ou ajustar acessos quando as funções dos usuários mudam ou quando há uma mudança nas políticas de segurança. • Colaborar com equipes de segurança cibernética e resposta a incidentes conforme necessário. • Desativar contas de usuários quando necessário, como quando um funcionário deixa a empresa ou muda de função. • Responder e processar solicitações de acesso de usuários de acordo com os procedimentos estabelecidos. • Auxiliar em auditorias regulares de acessos para garantir a conformidade com as políticas de segurança. • Manter registros precisos de todas as atividades relacionadas à gestão de acesso, incluindo criação, modificação e desativação de contas. • Colaborar com o responsável pela gestão de acesso na implementação de políticas e na resolução de problemas relacionados ao controle de acesso. • Reportar imediatamente quaisquer incidentes de segurança, violações ou atividades suspeitas ao responsável pela gestão de acesso. • Colaborar na implementação de mudanças nos processos de gestão de acesso conforme necessário.	Gerencia da Central de Serviços de TI Gerencia de Suporte e Infraestrutura Avançado Gerencia de Telecomunicações
GESTOR DE SISTEMA	• Determinar quem tem acesso a quais recursos com base nas necessidades de trabalho e na política de segurança da organização. • Atualizar essas classificações conforme as mudanças nas funções dos usuários. • Comunicar imediatamente qualquer violação de normas de segurança deste manual. • Revisar anualmente os perfis dos sistemas. • Revisar anualmente os usuários dos perfis.	Gestor do contrato relacionado ao sistema escopo.

5.1. MATRIZ DE RESPONSABILIDADE DO PROCESSO (RACI)

A matriz RACI abaixo documenta a relação existente entre as atividades e os papéis do processo:

Tabela 2 – Matriz de responsabilidades

	Dono do Processo (NUSIF)	Gestor do Processo (SSI)	Analista de Segurança	Operação Suporte Avançado	Operação Central de Serviços	Operação Telecomunicações	Gestor do Sistema	Todas as unidades do Banco	Recursos Humanos	auditoria	Departamento pessoal	Operação de monitoramento	Operação de Sistemas
ATIVIDADES DE CONTROLES DO PROCESSO													
Categorizar usuários de acordo com suas funções e responsabilidades para atribuir os níveis apropriados de acesso.		R	R										
Realizar revisões regulares de acessos para garantir que os privilégios de usuário permaneçam apropriados.		R	R				C						
Remover ou ajustar acessos quando as funções dos usuários mudam ou quando há uma mudança nas políticas de segurança.		R	R				I						
Implementar sistemas de monitoramento para identificar atividades suspeitas ou acessos não autorizados.		R	R	I	I	I							
Fornecer treinamento aos usuários sobre as políticas de acesso e as práticas de segurança.	A	R	R										
Avaliar, periodicamente e de acordo com o seu planejamento de trabalho, a adequação e efetividade dos mecanismos de acompanhamento, controle e mitigação de riscos implementados, visando a observância e cumprimento das disposições contidas neste manual										R			
Garantir que os usuários estejam cientes das implicações de segurança e conformidade relacionadas ao acesso a sistemas.		R	R										
SISTEMAS CORPORATIVOS													
Verificar a conformidade dos sistemas corporativos aos requisitos de segurança contidos neste manual, e necessidade de integração com o SGA ou validação do módulo de controle de acesso do legado e ao sistema de identidade humanas e não humanas.		R	R										

cadastro de perfis e atribuição de perfis administrativos.		A	A		R	R	R						
Criar/modificar contas de usuário conforme as solicitações, garantindo que sigam as políticas de segurança e as atribuições de funções adequadas.				R	R	R							
Participar dos procedimentos de homologação dos sistemas voltados a requisitos de Segurança da Informação		R	R				C						
Revisão periódica de usuários genéricos de sistemas							R						
gestão das credenciais de usuários GENÉRICOS de aplicação/sistemas		R	R										
Manter registros precisos de todas as atividades relacionadas à gestão de acesso, incluindo criação, modificação e desativação de contas.		C	C	R	R	R							
ACESSO FÍSICO AOS AMBIENTES DE TI													
Realizar o cadastro, análise e gerenciamento dos acessos.		R	R										
Controle periódico do sistema de biometria através de emissão de relatórios		R	R										
REDE CORPORATIVA													
Geração de relatórios do Active Diretory				R									
Revisão dos acessos periódicos				R									
Responsável por revisar todos os usuários de rede com perfil de administrador local, funcionário, menor aprendiz e estagiário desligado, a partir do relatório gerado pela área de Operação de Suporte, para renovação ou revogação dos referidos perfis.		R	R	C	C	C							
Liberação de acesso à internet para usuários				R									
Inclusão do usuário no grupo correspondente				R									
Inclusão e/ou exclusão de um funcionário na rotina de retenção caixa de correio do Office 365				R					C				
Criação de conta de e-mail e realizar a revisão das contas periodicamente				R									
Gestor dos servidores de arquivos do Banpará				R									
Incluir as pastas e definir a limitação de espaço das pastas				R									
Restrições necessárias na permissão de acesso a cada pasta.				R				C					
Controlar acesso lógico ao ambiente de produção, desenvolvimento e homologação;				R									
Responsável pela criação dos ambientes				R									

Gestor dos Servidores de arquivos				R									
Gestor dos Datacenters				R									
Armazenamento, exclusão e da identificação das fitas no site principal e do armazenamento no site Backup.				R									
Revisão dos acessos dos usuários de banco de dados periodicamente.				R									
Solicita a criação dos usuários de rede dos estagiários/Menor aprendiz				R					R				
Solicita a criação dos usuários de rede dos empregados ou sua transferência									R				
Informar a todas as unidades, por e-mail, em caso de desligamento de funcionário.									R				
Envio das mensagens internas de caráter geral ou circulação institucional											R		
Manter a relação de funcionários que terão suas caixas postais na rotina de retenção sempre atualizada										R			
Adição do usuário no grupo local de acesso remoto					R								
Garantir que os mecanismos de controle de acesso à rede estejam configurados para permitir a conexão apenas de dispositivos autorizados				R									
Analisar e deliberar sobre as exceções de acesso de dispositivos externos a rede corporativa, mantendo registros e justificativas documentadas				R									
Comunicar obrigatoriamente e com antecedência à área de Segurança da Informação qualquer situação que envolva o uso de dispositivos externos ou não patrimonializados								I					
REDE PRIVADA VIRTUAL - VPN													
Configuração da VPN no firewall do Banpará e seu modelos - site to site ou client to site		R	R			R							
Adição/Remoção de permissões do usuário ao grupo de VPN no AD		I	I	R									
Autorização de acesso remoto ao ambiente de produção		R	R										
BASE DE DADOS													
Envio da solicitação de acesso.				R									R
Autorização do acesso a base de dados				R			R						R
Criação de Logins				R									
Solicitação de Consulta a base de dados													R
Solicitação de acesso a base dos sistemas de aplicação				R			A						

ATIVIDADES GERENCIAIS DO PROCESSO													
Execução dos procedimentos normativos a serem aplicados nas unidades do Banpará									R				
Estabelecer políticas, Normas e Procedimentos de forma clara e diretrizes para o acesso a sistemas e dados sensíveis.	A	R	R	C	C	C	I						
Realizar auditorias periódicas para garantir conformidade com políticas e regulamentos.		R	R	C	C	C							
Desenvolver procedimentos para lidar com violações de segurança e responder a incidentes relacionados a acessos não autorizados.		R	R	C	C	C							
Colaborar com equipes de segurança cibernética e resposta a incidentes conforme necessário.		R	R	C	C	C							
Colaborar com outros processos de gerenciamento, como o gerenciamento de identidade, para garantir uma abordagem holística para o controle de acesso.		R	R										
Manter-se atualizado sobre as melhores práticas de segurança e regulamentações relevantes para ajustar as políticas de acesso conforme necessário.	R	R	R										
Atuar como gestora responsável pelo planejamento, elaboração e manutenção das diretivas e procedimentos disponíveis neste normativo		R	R	C	C	C							
Gestão de hardwares e softwares relacionados a área de segurança da informação.		R	R										
Auxiliar em auditorias regulares de acessos para garantir a conformidade com as políticas de segurança.		R	R	R	R	R				I			
Fornecer instruções básico aos usuários sobre boas práticas de segurança, políticas de acesso e uso adequado de credenciais.			R	R	R	R							
Colaborar com o responsável pela gestão de acesso na implementação de políticas e na resolução de problemas relacionados ao controle de acesso.				R	R	R		I					
Reportar imediatamente quaisquer incidentes de segurança, violações ou atividades suspeitas ao responsável pela gestão de acesso.				R	R	R							
Garantir que as ferramentas e sistemas utilizados para a gestão de acesso estejam atualizadas e funcionando corretamente.		R	R	C	C	C							

Colaborar na implementação de mudanças nos processos de gestão de acesso conforme necessário.				R	R	R							
Determinar quem tem acesso a quais recursos com base nas necessidades de trabalho e na política de segurança da organização.							R		R				

6. NORMAS GERAIS

6.1. PRINCÍPIOS FUNDAMENTAIS

6.1.1. Princípio do Menor Privilégio

Conceder apenas os privilégios necessários para que os usuários executem suas funções.

6.1.2. Segregação de Funções

Evitar que uma única pessoa tenha controle completo sobre qualquer processo crítico.

6.1.3. Necessidade de Saber

Acesso concedido com base na necessidade operacional ou funcional do usuário.

6.2. NORMAS GERAIS DE CONTROLE DE ACESSO

I. A área de Segurança da Informação, conforme suas responsabilidades, é encarregada da gestão, administração e armazenamento das credenciais de administradores, atendendo as boas práticas de Segurança da Informação e de frameworks reconhecidos internacionalmente, como: ISO/IEC 27001, NIST SP 800-53, COBIT, LGPD e GDPR.

II. Toda solicitação de acesso inicial deve vir com autorização do superior imediato.

III. O preenchimento do Formulário de Solicitação será necessário para todas as solicitações referentes a acessos, após seu preenchimento deverá ser anexado em formato .PDF no chamado realizado no ITSM. O formulário está disponível no ícone Formulários na url https://intrabanpis/menu/nucleos/seguran%C3%A7a-da-informa%C3%A7%C3%A3o,-preven%C3%A7%C3%A3o-%C3%A0-fraude-e-prote%C3%A7%C3%A3o-de-dados.aspx .

IV. O acesso somente será concedido caso exista perfil para a função do usuário que necessita acesso.

V. É vedado a inclusão de usuários a um grupo que não correspondam a sua lotação e função.

VI. Os perfis de acesso serão criados conforme Controle de Acesso Baseado em Funções (RBAC).

VII. Somente o gestor de sistema poderá solicitar a criação de um perfil novo, lista de gestores de sistemas que pode ser consultada através do sistema Risk Management.

VIII. Os acessos deverão ser concedidos somente com uma requisição de serviços na ferramenta de ITSM – BMC HELIX ou Cherwell.

IX. A equipe de Operação de Central de Serviços deverá enviar mensalmente relatórios de concessão de acesso para os sistemas críticos da instituição demonstrando o aprovador, o usuário que necessita acesso, sistema, registro de data/hora e responsável pelo atendimento de concessão de acesso.

X. Em caso de mudança de departamento, é papel do gestor da unidade onde o funcionário foi transferido solicitar a remoção de acesso aos perfis.

XI. Para cumprimento de normas de revogação de acesso, é obrigatório que sistemas pertencentes ao escopo de auditoria externa e sistemas críticos um dos quesitos abaixo:

XII. Integração do sistema novo ao SGA (sistema de gerenciamento de acesso).

XIII. Integração do sistema novo ao SSO (Sistema de Sigle Sing-On)

6.2.1. Normas de acesso para usuários a redes corporativas

I. Toda solicitação de acesso para usuários a rede corporativa deve ser realizada exclusivamente por meio da abertura de um chamado na Central de Serviços, com o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf.

II. A conta de usuário de rede deverá ser utilizada exclusivamente para assuntos de interesse do Banpará;

III. É vedado que usuários de rede sejam administradores locais. A concessão de perfil de administrador local das estações deve ser restrita aos funcionários da Supervisão de Atendimento ao Usuário da operação de suporte avançado, que exerçam atividades de analistas de atendimento ao usuário. Casos excepcionais deverão ser encaminhados à segurança da informação para análise e possível aprovação.

IV. A senha da conta de usuário é pessoal e intransferível, devendo ser mantido sigilo absoluto, pois o uso indevido dela será de inteira responsabilidade do colaborador, podendo acarretar sanções administrativas;

V. A troca de senha de rede de todos os funcionários, estagiários e fornecedores deve ser efetuada, obrigatoriamente, a cada 90 (noventa) dias e/ou após o retorno do período férias;

VI. A senha de usuário de rede deverá ser composta, no mínimo, por 8 (oito) dígitos, sendo obrigatória a combinação de números, letras maiúsculas, letras minúsculas e caracteres especiais;

VII. A nova senha, alterada nos prazos e período estabelecidos no item V, deverá ser diferente das três últimas senhas cadastradas pelo usuário de rede;

VIII. Após 03 (três) tentativas de login inválidas a conta será automaticamente bloqueada, sendo necessária a solicitação de desbloqueio junto à Operação de Central de Serviços do Banpará;

IX. Para o desbloqueio do usuário, o superior imediato deverá solicitar via ITSM a Operação de Central de Serviços;

X. O acesso de usuários a rede corporativa é controlado através do sistema de RH, assim determinando o horário permitido para acesso.

XI. Na criação de usuário de rede para Fornecedores e Prestadores de Serviços é obrigatório que o e-mail do usuário seja fornecido e cadastrado em sua conta no Active Directory.

XII. A criação de contas de usuários temporários se dará através de prévia análise pela Segurança da Informação.

XIII. Na criação de usuários genéricos será utilizado o TERMO DE RESPONSABILIDADE PARA USO DE USUÁRIO GENÉRICO disponibilizado em https://intrabanpis/menu/nucleos/seguran%C3%A7a-da-

informa%C3%A7%C3%A3o,-preven%C3%A7%C3%A3o-%C3%A0-fraude-e-prote%C3%A7%C3%A3o-de-dados.aspx . O termo terá que ser assinado e anexado ao chamado.

XIV. Novos usuários genéricos obrigatoriamente deverão ser embarcados no cofre de senhas.

XV. A criação do usuário será realizada pela área de Operação de Suporte Avançado e sua senha pela área de segurança da informação.

XVI. O responsável pela custodia das credenciais embarcadas no cofre de senhas será a área de segurança da informação.

6.2.2. Normas para utilização de correio eletrônico

I. Toda solicitação para utilização de correio eletrônico deve ser realizada exclusivamente por meio da abertura de um chamado na Central de Serviços, com o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf.

II. Deve ser utilizado exclusivamente para assuntos de interesse do Banco.

III. Aplicam-se as mesmas normas legais e de acesso às informações sigilosas que se aplicam a correspondências escritas do Banco.

IV. Devem ser observados os seguintes critérios na elaboração da mensagem:

V. Redação clara

VI. Objetividade

VII. Ética

VIII. Linguagem não ofensiva

IX. Centrada nos objetivos do Banco

X. Toda mensagem eletrônica enviada pelo cliente a qualquer funcionário do Banco para os endereços @banparanet.com.br é considerado documento oficial de comunicação, merecendo a mesma atenção e formalidade de atendimento do documento impresso.

XI. Menor Aprendiz não terá direito a caixa de correio eletrônico.

XII. A composição de grupos de e-mails deve ser responsabilidade do gestor da unidade. Exemplos: gecti@banparanet.com.br e getel@banparanet.com.br

XIII. As caixas compartilhadas devem ser de responsabilidade do gestor da unidade. Exemplos: sorteiodeingressos@banparanet.com.br e sac@banparanet.com.br

XIV. A opção de enviar e-mail de caixa compartilhada, sem identificação é de competência do gestor da unidade solicitante podendo designar outro funcionário para o envio, mas somente um usuário poderá estar responsável pelo envio dos e-mails desta caixa compartilhada.

XV. As caixas compartilhadas sem identificação do remetente, por padrão terão apenas um responsável pelo envio fica a critério do gestor da unidade.

XVI. A opção de enviar e-mail de caixa compartilhada com identificação do remetente é permitida.

6.2.2.1. Criação e uso das contas de correio eletrônico

I. O padrão de conta do usuário será: login_do_usuário@banparanet.com.br

II. A senha utilizada pelos usuários na conta de e-mail corporativo representa a sua assinatura digital, sendo de caráter pessoal e intransferível.

6.2.2.2. Conta de correio eletrônico de estagiário/menor aprendiz

Por padrão, estagiários/menores aprendizes não possuem conta de e-mail corporativo, em virtude do curto período que transitam pela empresa e por não possuírem vínculo empregatício com a Instituição.

6.2.2.3. Conta de correio eletrônico de prestador de serviços

Por padrão, os prestadores de serviços não possuem conta de e-mail corporativo, em virtude do curto período que transitam pela empresa e por não possuírem vínculo empregatício com a Instituição, contudo, caso necessário, o e-mail será criado com o nome da empresa e não conta individual.

6.2.2.4. Conta de correio de funcionários cedidos

Por padrão, funcionários cedidos não possuem conta de e-mail corporativo, em virtude de não possuírem vínculo empregatício com a Instituição.

6.2.2.5. Envio de e-mail internamente

I. Na comunicação interna, admite-se a utilização de uma linguagem menos formal na redação, privilegiando-se a objetividade e concisão das informações.

II. Mensagens internas, de caráter geral ou circulação institucional, devem ser enviadas ao Departamento Pessoal para divulgação.

III. Os grupos de Agência da Capital, Agência de Interior, Postos de atendimentos, Unidades da Matriz, e outras similares só devem ser utilizados se o assunto for do interesse de toda UNIDADE. Caso contrário procurar direcionar apenas para as chefias de cada unidade.

IV. Fica determinado que por padrão cada usuário só poderá enviar e-mails a 20 (vinte) destinatários simultaneamente.

6.2.3. Normas para uso da rede privada virtual (VPN) do Banpara

I.Toda solicitação de para uso da rede privada virtual (VPN) deve ser realizada exclusivamente por meio da abertura de um chamado na Central de Serviços, com o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf.

II. O login e senha dos usuários de vpn cliente-to-site de funcionários são os mesmos usuários e senhas de rede.

III. O acesso a VPN será condicionado a utilização da aplicação de Múltiplo fator de autenticação (MFA).

IV. O acesso será desabilitado automaticamente ao término do período concedido. Caso exista necessidade de prorrogação do acesso, o solicitante deverá fazer novo pedido via Operação de Central de Serviços cumprindo os mesmos requisitos obrigatórios presente no formulário.

V. A solicitação de acesso VPN de Usuários Externos (fornecedor ou prestador de serviço), por meio da Operação de Central de Serviços, deverá conter o e-mail com a autorização do superior imediato do solicitante do banco e/ou do gestor do sistema/servidor, anexando-o ao chamado;

VI. A Segurança da Informação irá avaliar a solicitação, podendo incorrer nas seguintes situações:

a) Deverá ser informado o formato de acesso, podendo ser solicitado “Client-to-site” ou “site-to-site”. Caso a Segurança da Informação decida pelo tipo site to site, o firewall do usuário externo deverá ter suporte ao protocolo IPSec (Internet Protocol Security).

b) Caso o pedido seja indeferido, a Segurança da Informação fechará o chamado, justificando o motivo da negativa.

VII. Se não houver acesso por um período ininterrupto de 1 (um) ano, o acesso será revogado.

VIII. No caso de VPN (Site-to-Site) deve ser encaminhada também via Operação de Central de Serviços à Segurança da Informação, o Formulário de criação de VPN Site-to-Site disponibilizado no ícone Formulários no link abaixo juntamente com o Formulário de solicitação em formato .pdf:

IX. https://intrabanpis/menu/nucleos/seguran%C3%A7a-da-informa%C3%A7%C3%A3o,-preven%C3%A7%C3%A3o-%C3%A0-fraude-e-prote%C3%A7%C3%A3o-de-dados.aspx.

X. O prazo de validade do acesso à VPN Client-to-Site está segregado da seguinte forma:

XI. Para funcionários Banpará solicitar via abertura do chamado na Operação de Central de Serviços incluindo como anexo a autorização da diretoria/assessoria responsável pela unidade, caso não esteja descrito o prazo na autorização ficará até que a Segurança da Informação, o funcionário ou seu chefe imediato solicite a revogação.

XII. Para Usuários Externos (Fornecedores e Prestadores de Serviços) será concedido o prazo máximo de 180 dias (6 meses) a contar da data de abertura do chamado na Operação de Central de Serviços.

XIII. O prazo de validade do acesso à VPN (Site-to-Site) deverá obedecer ao contrato vigente com o fornecedor/terceirizado, devendo ao fim do contrato/relacionamento, ser desfeito o túnel de comunicação criado.

6.2.4. Normas para utilização dos servidores de arquivos

I. Todas as pastas terão uma limitação de espaço a ser definido pela área gestora (Operação de Suporte Avançado) após análise da capacidade de armazenamento disponível, devendo-se preferencialmente realizar a divisão igualitária entre cada superintendência ou núcleo.

II. Com o objetivo de manter a confidencialidade dos documentos gravados nos servidores de arquivos, fica proibida a gravação de qualquer documento que não seja de interesse do Banco.

III. Fica proibida a gravação de arquivos como: MP3, AVI, MPG, MPEG e similares, bem como jogos e outros arquivos e aplicativos que não sejam de interesse do Banco.

IV. Fica proibida, em qualquer servidor, a gravação de arquivos do tipo PST de pastas particulares de outlook.

V. Fica proibida, em qualquer servidor, a gravação de arquivos de qualquer extensão que contenham assuntos alheios ao Banco, ficando autorizado a área gestora a remover tais arquivos.

VI. A fim de atender os itens I e II e manter o controle sobre os arquivos armazenados nos servidores de arquivos, estes deverão ser gerenciados por sistema operacional

que permita a configuração de cota de armazenamento por pasta compartilhada e/ou grupo do Active Directory, além da restrição de armazenamento por tipo de arquivo.

6.2.5. Pastas públicas

I. Os funcionários de cada área terão acesso total às subpastas da unidade em que estão lotados, enquanto nas demais, o acesso será somente de leitura.

II. Os documentos gravados em pastas públicas especiais, resguardadas por criptografia, para áreas que precisem compartilhar arquivos entre si de forma constante, ficarão por tempo determinado, de acordo com a necessidade da publicação.

III. Os documentos serão removidos diariamente as 23hrs, sem comunicação prévia à unidade responsável pela pasta. A manutenção mensal será entre o primeiro e o terceiro dia útil cada mês. Entenda-se por manutenção o ato de liberar espaço nos discos dos servidores de arquivos.

IV. As pastas públicas, em hipótese nenhuma, farão parte da rotina de backup.

6.2.6. Das pastas restritas a cada superintendência ou núcleo

I. Apenas os funcionários de cada área terão acesso total às subpastas da unidade em que estão lotados, enquanto nas demais, não será concedido o acesso.

II. Os documentos gravados nas pastas restritas a cada Superintendência ou Núcleo ficarão por tempo indeterminado.

III. Não poderão ser removidos os documentos contidos nestas pastas, sem comunicação e anuência prévia do respectivo Superintendentes ou Chefes de Núcleo responsável pela pasta, com exceção para arquivos que forem detectados como maliciosos pelas ferramentas de segurança do banco.

IV. A manutenção semestral nas pastas restritas será entre o primeiro e o terceiro dia útil do semestre, neste caso o responsável pela pasta poderá solicitar a área gestora que seja feito backup das pastas consideradas importantes onde o conteúdo será gravado em mídia e entregue ao responsável. Entenda-se por manutenção o ato de liberar espaço nas pastas dos servidores de arquivos.

V. As planilhas eletrônicas e documentos com informações de interesse restrito deverão ser usadas somente nas pastas restritas a cada Superintendência ou Núcleo. Os Gestores devem solicitar à Operação de Suporte Avançado as restrições necessárias na permissão de acesso a cada pasta.

6.2.7. Das cópias de segurança (backup´s)

I. Os arquivos contidos nas pastas restritas a cada Superintendência ou Núcleo poderão ser contemplados pela política de backup a pedido da Segurança da Informação ou superintendente da área gestora da pasta, enquanto os contidos nas pastas públicas não.

II. No caso de pastas que sofrem apenas backup parcial de seu conteúdo, a cada alteração, inclusão ou remoção de subpastas, deverá ser informado a área gestora a retirada ou inclusão das mesmas na política de backup, se for o caso.

III. Os arquivos contemplados ficarão guardados em local seguro e definido pelo órgão gestor por um período de 90 dias a contar da data do último backup.

IV. A restauração dos arquivos antigos só poderá ser feita mediante prévia solicitação ao órgão gestor.

V. A inclusão de uma pasta, na rotina de backup deverá ser expressamente solicitada para a Operação de Suporte Avançado via Operação de Central de Serviços pelos Gestores, excetuando as pastas públicas.

6.2.8. Segurança

I. O funcionário que utilizar pastas públicas fica totalmente responsável pelo conteúdo dela.

II. Todos os acessos e gravações de arquivos em todas as pastas efetuadas por funcionários poderão ser auditadas pela Segurança da Informação, a fim de assegurar que a utilização deste meio de armazenamento seja utilizada exclusivamente para interesse do Banco.

6.2.9. Normas para o acesso de pessoas aos ambientes de tecnologia da informação

6.2.9.1. Ambientes de tecnologia da informação com acesso controlado via sistema biométrico

I. Salas da Gerência de Suporte Técnico e Produção – GEINS e Gerência de Telecomunicações – GETEL (Rua Municipalidade, n.º 1036).

II. Data Center Principal – Sala dos Servidores (Rua Municipalidade, n.º 1036).

III. Data Center Principal – Sala de teleprocessamento (Rua Municipalidade, n.º 1036).

IV. Data Center Secundário – Sala dos Servidores (Av. Presidente Vargas, n.º 251).

V. Data Center Secundário – Sala de teleprocessamento (Av. Presidente Vargas, n.º 251).

VI. Fitoteca - (Rua Municipalidade, n.º 1036).

VII. Salas da Gerência Da Central de Serviços de TI – GESER e Gerência de Monitoramento - GEMON (Rua Municipalidade, n.º 1036).

VIII. Porta principal de acesso ao prédio da TI para as dependências das superintendências SUSIS, SUPRO e SUGOT (Rua Municipalidade, n.º 1036).

6.2.9.2. Toda solicitação de acesso de pessoas aos ambientes de tecnologia da informação deve ser realizada exclusivamente por meio da abertura de um chamado na Central de Serviços, com o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf.

6.2.9.3. Estas normas aplicam-se a todos os funcionários, prestadores de serviço, visitantes e outras partes interessadas que necessitem acessar os ambientes de TI.

6.2.9.4. O acesso aos ambientes de TI será permitido apenas a pessoas autorizadas.

6.2.9.5. As permissões de acesso serão concedidas pela Segurança da Informação com anuência do gestor das áreas a serem acessadas.

6.2.9.6. Todo acesso deve ser registrado identificado com o nome e o horário de entrada.

6.2.9.7. Necessidades de acesso aos Data Centers

Tabela 3 – Necessidade de aceso aos data centers

ÁREA	NECESSIDADE	PERIODICIDADE
GEINS	Gestão dos servidores.	Regularmente

GETEL	Gestão dos equipamentos de Telecom.	Regularmente
SSI	Gestão dos equipamentos de Segurança da Informação.	Regularmente
GEENG	Gestão da manutenção elétrica.	Periodicamente ou acionamento
GEMAN	Gestão dos equipamentos de ar-condicionado.	Periodicamente ou acionamento
GESAT	Gestão dos extintores de incêndio instalados no ambiente.	Periodicamente ou acionamento

6.2.9.8. Colaboradores e visitantes deverão portar crachás de identificação visíveis.

6.2.9.9. Colaboradores e visitantes somente poderão acessar áreas restritas acompanhados por um responsável autorizado.

6.2.9.10. A Segurança da Informação é responsável pela administração das fechaduras biométricas.

6.2.9.11. Caberá à Segurança da Informação a emissão de relatórios periódicos referentes aos sistemas de biometria de todos os ambientes.

6.2.9.12. No relatório de registros de entrada de fechaduras biométricas terá os acessos a áreas restritas, oferecendo detalhes essenciais para segurança. Estruturado da seguinte forma:

I. **Informações Gerais**: Período de monitoramento, local, responsável e data do relatório.

II. **Resumo de Acessos**: Total de acessos, acessos permitidos e negados.

III. **Detalhamento dos Registros de Acesso**: Listagem de data, hora, usuário, status (permitido, negado), matrícula e local.

6.2.9.13. O controle e revisão de acesso automático com fechadura biométrica usa autenticação biométrica (impressão digital) para garantir a segurança física e automatizar a gestão de permissões de acesso a áreas restritas.

6.2.9.14. As permissões são atribuídas com base na função do usuário e revisadas periodicamente.

6.2.9.15. Serão realizadas revisões anuais de acesso em fechaduras biométricas para a verificação de permissões e auditorias dos logs.

6.2.9.16. A padronização do procedimento de cadastro de usuários em fechaduras biométricas envolve as seguintes etapas:

6.2.9.17. Solicitação e Aprovação: Receber através da central de chamados e a área de segurança da informação aprovará solicitações de acesso, com base na função e áreas necessárias.

I. Captura de Dados Biométricos: Registrar as características biométricas do usuário (impressão digital).

II. Atribuição de Permissões: A segurança da informação defini e configura permissões de acesso de acordo com o cargo e as necessidades do usuário.

III. Integração ao Sistema: A segurança da informação registra o usuário no sistema de gestão de acesso e configurar seu perfil de acesso.

IV. Validação e Testes: O usuário realiza um teste para verificar que o sistema reconheça corretamente o usuário e permita os acessos necessários.

V. Treinamento: A segurança da informação orienta o usuário sobre o uso das fechaduras biométricas e as políticas de segurança.

VI. Monitoramento e Auditoria: A segurança da informação realiza auditorias periódicas para garantir que os acessos sejam válidos e seguros.

VII. Desativação: A segurança da informação remove ou ajusta acessos quando o usuário não for mais autorizado.

6.2.10. Normas de acesso aos sistemas corporativos.

I. Toda solicitação de acesso aos sistemas Corporativos deve ser realizada exclusivamente por meio da abertura de um chamado na Central de Serviços, com o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf.

II. A solicitação para acesso deverá ser de acordo com cargo/função exercida pelo funcionário.

III. A solicitação para acesso inicial ou substituição eventual/emergencial de funcionários, aos Sistemas, deverá obedecer aos critérios de subordinação a seguir:

IV. NÃO serão atendidas solicitações em desacordo com os CRITÉRIOS DE HIERARQUIA estabelecidos no ITEM II

Tabela 4 – Critérios de hierarquia

SOLICITANTE	USUÁRIO
Gerente Geral de Agência ou Coordenador de PAB	Subordinados
Gerente Geral de Agência em que o Posto está subordinado	Coordenadores de Postos de Serviço
SUNEG	Gerentes Gerais ou Gerentes Regionais das agências
Superintendente/Chefe de Núcleo	Subordinados
Gerentes/Chefe de Subnúcleo/ Coordenador de serviço	Funcionários lotados na respectiva gerência ou subnúcleo ou coordenadoria

V. Para solicitação de acesso de substituição eventual/emergencial de funcionários, aos Sistemas, o próprio usuário designado poderá fazer essa solicitação desde que no termo de função haja a assinatura do superior hierárquico.

VI. Somente o usuário poderá solicitar o reset/desbloqueio de sua senha.

VII. Em casos de substituição, caso o funcionário solicite acesso a perfis incompatíveis com a função substituída não será concedido o acesso.

VIII. Após a expiração do prazo de validade do termo de função, caso o funcionário necessite renovar o termo deverá ser aberto novo chamado, cujo prazo de permanência na base, será vinculado ao novo termo de substituição/emergencial.

IX. Os CRITÉRIOS DE HIERARQUIA estabelecidos no ITEM II também é responsável pela solicitação de revisão de acesso de seus subordinados com periodicidade de pelo menos uma vez a cada 365 dias.

X. O gestor do sistema deverá revisar os perfis do sistema que gere pelo menos uma vez a cada 365 dias, sendo essa revisão através do mapeamento permissão x perfil ou através do relatório permissão x perfil do sistema, assim como revisar os usuários ativos anualmente.

XI. A criação/revisão de perfis seguirá a diretriz: Para matriz conforme organograma: SUPERINTENDENCIA – GERENCIA – FUNCAO/CARGO ou NÚCLEO – SUBNUCLEO – FUNCAO/CARGO. Para agência: AGÊNCIA – FUNÇÃO/CARGO. Sendo que os perfis precisam estar em consonância com as atividades do MNP de Organização da Matriz e MNP de Organização das Agências, além disso eles devem ser distintos e possuir controle de alçada, ou seja, estar em conformidade com Manual de Cargos e Funções para que seja implementado as distinções e segregações entre as atividades tanto das funções como dos cargos listados nesse normativo interno.

XII. O acesso será norteado pelo conjunto: unidade/subunidade + cargo/função; que o funcionário está cadastrado no Sistema de RH.

XIII. Para os casos em que o funcionário esteja "Adido" deve-se anexar no chamado o "Termo de Adição" emitido pelo RH e/ou e-mail emitido por esta área para a abertura de chamado.

XIV. No caso de MODIFICAÇÃO ou PERDA DE FUNÇÃO exercida pelos funcionários, caberá ao chefe da unidade onde o funcionário está lotado, solicitar por meio do Sistema da Operação de Central de Serviços o CANCELAMENTO/SUSPENSÃO do acesso do subordinado evitando a utilização indevida de perfil privilegiado aos sistemas.

XV. Os termos de função de "Trainee", quando da solicitação de alteração de perfil terão prazo de validade de 90 dias. Após a expiração do termo, o prazo de permanência poderá ser prorrogado, a pedido do Gerente Geral, Gerente de Área ou Superior imediato ou Chefia da unidade.

XVI. Todos os acessos dos sistemas corporativos utilizados por funcionários/terceiros poderão ser revisados pela Segurança da Informação, a fim de assegurar que a utilização deste esteja de acordo com função dos mesmos. Caso seja encontrado algum acesso em desconformidade esse será ajustado e/ou mesmo retirado, se for o caso.

XVII. Quando o RH informar o desligamento de funcionário/estagiário/menor aprendiz os acessos das pessoas indicadas serão retirados após a data informada de forma automática ou manual.

XVIII. Por padrão, terceiro que presta serviço para o Banpará não deve ter acesso aos sistemas corporativos em ambiente de produção, com exceção da a terceiros da Central de Serviços.

6.2.11. Normas de Acesso aos sistemas: DE DEMANDA, ADMLOG, CBRSEG, SGBCMF, SGBFND, SGBSWP, SGBSRC, MULTISERV, MYTHUS, OTP, PD CRED, PD COMPE, SISARC, PD DESENV, PD DESENVWEB, PD FINESP, PD INSS, PD POUPANÇA, PD POUPWEB, PD REDE PD SIPAE, PWA, SEGURANÇA INTRANET, SISBACEN, SPB/SPAWEB, TOTVS (CADASTRO, CONTA CORRENTE WEB, SIAFEM, CONTABILIDADE, CDB GOV, CARTÕES E MÓDULO GESTOR CONTA CORRENTE) E demais sistemas utilizados que não estão listados acima.

I. A solicitação de DESBLOQUEIO DE SENHA nos Sistemas Corporativos deverá ser feita por meio do Operação de Central de Serviços exclusivamente pelo próprio usuário interessado.

II. A listagem de permissões de perfis de sistemas para funcionários de agência está mapeada a seguir:

Tabela 5 – Permissões de perfis

SISTEMA	CARGO / FUNÇÃO	PERFIL
PD_CRED	Agente de Área	Nenhum
	Caixa	Ag - Caixa
		Ag - Private Agencias
	Coordenador de Posto	Ag - Private Agencias
		Ag - Coordenador De Posto
	Coordenador Retaguarda Tesou	Ag- Coordenador De Tesouraria
		Ag - Private Agencias
	Coordenadoria de Cobrança	Nenhum
	Estagiário/C.I.E.E.	Nenhum
	Gerente de Atendimento (GEAT)	Ag - Gerente De Atendimento
		Ag - Private Agencias
	Gerente de Negócios	Ag - Gerente De Negocio
		Ag - Private Agencias
	Gerente de Serviços Internos	Ag - Gerente De Serviços Internos
		Ag - Private Agencias
	Gerente Geral	Ag - Gerente Geral
		Ag - Private Agencias
	Técnico Bancário Nível Médio	Ag - Técnico Bancário
		Ag - Private Agencias
PD_DESENV	Agente de Área	Agente De Área/Agencia
	Caixa	Caixa/Agencia
	Coordenador de Posto	Coordenador De Posto/Agencia
	Coordenador Retaguarda Tesou	Nenhum
	Coordenadoria de Cobrança	Nenhum
	Estagiário/C.I.E.E.	Estagiário/Agencia
	Gerente de Atendimento (GEAT)	Gerente De Atendimento/Agencia
	Gerente de Negócios	Gerente De Negócio/Agencia
	Gerente de Serviços Internos	Gerente De Serviços Internos/Agencia
	Gerente Geral	Gerente Geral/Agencia
	Técnico Bancário Nível Médio	Operativo/Agencia
PD_POUP	Agente de Área	Nenhum
	Caixa	Nenhum
	Coordenador de Posto	Nenhum
	Coordenador Retaguarda Tesou	Nenhum
	Coordenadoria de Cobrança	Nenhum
	Estagiário/C.I.E.E.	Nenhum
	Gerente de Atendimento (GEAT)	Nenhum
	Gerente de Negócios	Nenhum
	Gerente de Serviços Internos	Nenhum
	Gerente Geral	Nenhum
	Técnico Bancário Nível Médio	Nenhum
PD_POUPWEB	Agente de Área	Nenhum
	Caixa	Operativo
	Coordenador de Posto	Gerente

	Coordenador Retaguarda Tesou	Gerente
	Coordenadoria de Cobrança	Nenhum
	Estagiário/C.I.E.E.	Nenhum
	Gerente de Atendimento (GEAT)	Gerente
	Gerente de Negócios	Gerente
	Gerente de Serviços Internos	Gerente
	Gerente Geral	Gerente
	Técnico Bancário Nível Médio	Operativo
SGBSRC	Agente de Área	Cr Web
	Caixa	Cr Web
	Coordenador de Posto	Cr Web
	Coordenador Retaguarda Tesou	Cr Web
	Coordenadoria de Cobrança	Cr Web
	Estagiário/C.I.E.E.	Nenhum
	Gerente de Atendimento (GEAT)	Cr Web
	Gerente de Negócios	Cr Web
	Gerente de Serviços Internos	Cr Web
	Gerente Geral	Cr Web
	Técnico Bancário Nível Médio	Cr Web
Aplicações Financeiras (SGBFND, SGBCMF, SGBSWP)	Agente de Área	Nenhum
	Caixa	Nenhum
	Coordenador de Posto	Agencia
	Coordenador Retaguarda Tesou	Agencia
	Coordenadoria de Cobrança	Nenhum
	Estagiário/C.I.E.E.	Nenhum
	Gerente de Atendimento (GEAT)	Agencia
	Gerente de Negócios	Agencia
	Gerente de Serviços Internos	Agencia
	Gerente Geral	Agencia
	Técnico Bancário Nível Médio	Agencia
TOTVS	Agente de Área	Nenhum
	Caixa	Ag_Caixa
	Coordenador de Posto	Ag_Coordpab
	Coordenador de Retaguarda de Serviço	Ag_Coordretserv
	Coordenador Retaguarda Tesou	Ag_Tesoureiro
	Coordenadoria de Cobrança	Nenhum
	Estagiário/C.I.E.E.	Nenhum
	Gerente de Atendimento (GEAT)	Ag_Geate
	Gerente de Negócios	Ag_Geneg
	Gerente de Serviços Internos	Ag_Gesin
	Gerente Geral	Ag_Gergeral
	Técnico Bancário Nivel Médio	Ag_Tecban

PerfilxFuncionalidade_WHITELIST												
DEFINIÇÃO Funcionalidades X Perfis de Acesso												
Funcionalidades		AGENCIA							GPFRA			
		1	2	3	4	5	6	7	8	9	10	11
		G Geral	Geate	Geneg	Coord Tesouraria	Tesoureiro	Coord. Caixa	Coord. Retaguarda	Coord. Pab	Gerente	Analista	Técnico Bancário
1	Gerenciar White List	S	S	S	S	S	S	S	S	S	S	N
2	Emitir Relatório de White List	S	S	S	S	S	S	S	S	S	S	S
3	Gerenciamento de Motivo White List	N	N	N	N	N	N	N	N	S	N	N
	S	Possui permissão										
	N	Não possui permissão										

Figura 1 – Perfis x Funcionalidades

III. Para Sistemas não listados acima ou que não possuem aviso circular próprio de permissão de perfil ou controle de acesso deverá ser consultado a Segurança da Informação antes do atendimento da solicitação.

IV. Para os Sistemas integrados ao Sistema de Gestão de Acesso-SGA os usuários deverão estar nos grupos conforme organograma do banco, ou seja:

V. Para agência: Agencia – Caixa, Agencia - Coordenador de Caixa, AGENCIA - Coordenador de Cobrança, Agencia - Coordenador de Posto, Agencia - Coordenador de Retaguarda, Agencia - Coordenador de Retaguarda de Tesouraria, Agencia - Coordenador de Tesouraria, Agencia - Gerente de Atendimento, Agencia - Gerente de Negócio, Agencia - Gerente de Serviços Internos, Agencia - Gerente Geral, Agencia - Técnico Bancário, Agencia - Tesoureiro - Coord. de Retaguarda de Tesouraria, Agencia - Tesoureiro - Coord. de Tesouraria.

VI. Para os usuários de agência sempre deverá ser verificado se o mesmo se encontra vinculado a agência o qual está lotado no RH ou conforme o termo de função anexado no chamado da Operação de Central de Serviços.

VII. Para matriz conforme organograma: Superintendência – Gerencia – Função/Cargo Ou Núcleo – Subnúcleo – Função/Cargo.

VIII. VIII. Para cadastramento de usuário com Private Agência do PD_CRED somente deverá ser incluído no mesmo as funções conforme a Nota 3, do item 4 , do Capítulo I do MNP de Crédito Comercial Pessoa Física.

6.2.12. Normas De Acesso Ao Internet Banking Prefeitura

I. O Gerente da Agência será responsável por verificar a autenticidade e checar as informações, antes de enviá-las via sistema de Operação de Central de Serviços. Ficando sobre sua inteira responsabilidade o conteúdo do procedimento solicitado.

6.2.13. Normas De Acesso Ao Sistema De Transmissão Web

I. A solicitação de acesso no Sistema de Transmissão Web deverá ser feita por meio do sistema Operação de Central de Serviços, pela Gepac (Gerência de Folha de Pagamento e Controle de Pessoal e do Siafem).

6.2.14. Normas Para Controle De Acesso A Internet

I. Toda solicitação de acesso a internet deve ser realizada exclusivamente por meio da abertura de um chamado na Central de Serviços, com o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf.

II. Com base em levantamento realizado nas unidades do Banco, foram criados grupos de Internet com permissão de acesso somente aos sites necessários para execução das suas respectivas atividades.

III. No momento da criação do usuário de rede, ele já deverá automaticamente ser vinculado a um dos grupos da tabela abaixo de acordo com a Unidade de Lotação e Função relacionada.

Tabela 6 – Grupo unidade x função

UNIDADE DE LOTAÇÃO	FUNÇÃO	GRUPO NO ACTIVE DIRECTORY
Presidência e Diretores	Todas	INTERNET_DIRETORIA
Gabinete da Diretoria	Todas	INTERNET_GABINETE
AUDIN	Todas	INTERNET_AUDIN
NUSIF	Todas	INTERNET_NUSIF
SUPRO	Todas	INTERNET_SUPRO
Fornecedores	Todas	INTERNET_FORNECEDOR
Agências e Postos	Gerentes e Coordenadores	INTERNET_AGENCIAS
Agências e Postos	Demais Funcionários	INTERNET_AGENCIAS_ATENDIMENTO
Todas as Unidades do Banco	Estagiários	INTERNET_ESTAGIARIOS

IV. Toda solicitação deverá ser feita por meio da abertura de chamado na Operação de Central de Serviços pelo chefe da unidade ou chefe da unidade gestora do contrato onde o funcionário ou fornecedor/temporário, respectivamente, estiver lotado. Não serão aceitas solicitações por outros meios de comunicação.

V. É expressamente proibido o uso da Internet nos seguintes casos:

VI. Fins comerciais ou cessão a terceiros, independente da finalidade;

VII. Propósitos ilegais, que logre êxito ou não;

VIII. Propagação de vírus de computador, programas de invasão ou outros similares;

IX. Instalação de programas de computador auto-replicastes ou não, que causem danos permanentes ou temporários nos equipamentos do destinatário;

X. Transmissão de tipos ou quantidades de dados que causem falhas em serviços ou equipamentos na Internet;

XI. Violar a privacidade de outros usuários;

XII. Forjar endereços de máquinas da rede na tentativa de ocultar a identidade ou autoria ou de responsabilizar terceiros;

XIII. Violar copyright ou direito autoral alheio reproduzindo material sem prévia autorização;

XIV. Transmitir ou divulgar ameaças, pornografia infantil, material racista ou qualquer outro que viole a legislação em vigor;

XV. Acessar conteúdo que não seja de interesse do Banco;

XVI. Acessar sites com conteúdo pornográficos, jogos, música e similares.

XVII. Todo acesso à Internet será auditado a fim de garantir o cumprimento do MNP de Segurança da Informação e resguardar os interesses da instituição.

6.2.15. Liberações De Acesso À Internet Para Usuários

I. Toda solicitação de liberação de acesso a internet para usuários deve ser realizada exclusivamente por meio da abertura de um chamado na Central de Serviços, com o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf.

6.2.16. Liberações De Acesso A Novos Sites

I. Toda solicitação de acesso a novos sites deve ser realizada exclusivamente por meio da abertura de um chamado na Central de Serviços, com o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf.

II. Toda liberação de acesso a novos sites somente poderá ser providenciada após análise e autorização da Segurança da Informação.

III. Quando se tratar de cursos, o usuário deve solicitar a autorização de acesso a Universidade do Banpará (UNIBANP).

6.2.17. Solicitação De Acesso À Base De Dados De Produção

I. A solicitação de acesso à base de dados deve ser solicitada levando em consideração a necessidade de um “sistema A” obter informações e/ou atualização no “Sistema B”. A permissão deve ser necessária e suficiente para o bom andamento do negócio do Banco.

II. A permissão de Db_owner deve ser única por sistema, ou seja, somente um usuário por sistema poderá ter a permissão de Db_owner em um Banco de Dados.

III. A responsabilidade sobre a solicitação do acesso é do Prestador de Serviço, que deve garantir que os acessos sejam sempre necessários e suficientes para o atendimento a sua aplicação.

IV. A solicitação de Acesso só deve ser enviada para ambiente de produção por solicitação expressa da superintendência de sistemas, da superintendência de infraestrutura ou quando o Prestador de Serviço identificar a necessidade de envio do mesmo para atender uma necessidade do Banco. Em ambos os casos, a Gerência responsável da superintendência de sistemas ou da superintendência de infraestrutura deve ser formalmente informada do procedimento.

V. A responsabilidade sobre a execução integral da permissão de acesso em ambiente de produção é do Banco.

6.2.17.1. O envio de uma solicitação de acesso para produção deve ser através do preenchimento do Formulário de Solicitação em formato .pdf o qual deve conter as seguintes informações:

I. Objetivo: Motivo da solicitação de acesso;

II. Informações técnicas: Informações de onde a solicitação de acesso deve ser aplicada, como por exemplo, sistema, servidor, banco de dados, objetos e níveis de permissão;

III. Data e hora da execução: Informar a data e hora que a solicitação deverá ser efetuada;

IV. Motivo da solicitação: descrever o motivo da solicitação de Acesso;

V. Impactos: Sistemas e Funcionalidades que serão afetados após a concessão da permissão de acessos;

VI. Plano de retorno: O que deve ou pode ser feito caso ocorra algum problema.

6.2.17.2. Caso a solicitação de acesso seja para correção de um problema técnico do sistema, o fato deve ser explicitado no Formulário de Solicitação.

6.2.17.3. A definição do responsável pela autorização da solicitação do acesso ficará a cargo da superintendência de sistemas ou da superintendência de infraestrutura, sendo os possíveis responsáveis: a superintendência de sistemas ou a superintendência de infraestrutura ou os gestores de sistemas.

6.2.17.4. Após o envio da solicitação de acesso para produção, o Prestador de Serviço deve aguardar o documento atualizado com o resultado que será sempre: Permissão concedida com Sucesso ou permissão não foi concedida e qual o motivo.

6.2.18. Criação De Logins E Acesso À Base De Dados De Produção

6.2.18.1. Normas para a criação de logins:

I. Cada Sistema deverá possuir seu próprio login que deverá ser vinculado ao banco de dados da aplicação;

II. Os logins de aplicação deverão começar pela palavra “gen_” seguindo do nome do sistema;

III. Os logins dos usuários deverão ser seu próprio login de rede. Caso o usuário não possua um login de rede, ele deverá começar pelo nome da sua empresa ou abreviação e o primeiro nome do usuário + sobrenome, conforme exemplos abaixo:

- Exemplo-01: <nome da empresa / instituição>_ + <inicial(is) do primeiro nome> + <sobrenome>.
- Exemplo-02: vibe_ jsouza;

IV. As senhas de logins deverão ser fortes, com 08 ou mais caracteres, contendo letras maiúsculas e minúsculas, números e caracteres especiais;

V. A parametrização de senha de usuários novos de banco de dados:

- Usuário de sistema utilizar a parametrização a seguir:

Tabela 7 – Parametrização de senhas

Proposta Auditoria Externa	Parâmetros de senha de usuário de banco de dados ATUAL
Número mínimo de caracteres da senha: 8	Número mínimo de caracteres da senha: 8
Manter histórico das últimas 12 senhas	Manter histórico da última senha
Habilitar senhas complexas	Habilitar senhas complexas
Bloquear após três tentativas incorretas de acesso; e	Bloquear após 5 tentativas incorretas de acesso; e

Destravamento da conta apenas pelo administrador do sistema.	Está ativo o desbloqueio ou reset de senha somente com usuário administrador de SGBD.

- Caso o sistema esteja integrado ao cofre de senha será habilitado idade máxima da senha também.

- Usuário de banco de dados que não são de sistema utilizar parametrização a seguir:

Tabela 8 – Parametrização de senhas de banco de dados

Proposta Auditoria Externa	Parâmetros de senha de usuário de banco de dados ATUAL
Idade máxima da senha: 30 a 45 dias	90 dias
Número mínimo de caracteres da senha: 8	Número mínimo de caracteres da senha: 8
Manter histórico das últimas 12 senhas	Manter histórico da última senha
Habilitar senhas complexas	Habilitar senhas complexas
Bloquear após três tentativas incorretas de acesso; e	Bloquear após 3 tentativas incorretas de acesso; e
Destravamento da conta apenas pelo administrador do sistema.	Está ativo o desbloqueio ou reset de senha somente com usuário administrador de SGBD.

- Os usuários antigos que não são de sistemas serão ativadas parametrizações do item anterior.

VI. Os logins e suas respectivas senhas criadas antes de novembro de 2021, deverão ser exportados periodicamente pelos DBA's e armazenadas em local seguro, para que possam ser aplicadas em outros ambientes ou em futuras migrações, ressaltando que as senhas exportadas estarão criptografadas;

VII. Os logins e suas respectivas senhas deverão ser embarcadas na solução de cofre de senhas utilizada pelo Banco, conforme Normativo de Desenvolvimento Seguro, para isto após a criação de um usuário os DBA's entrarão em contato com a segurança da informação para a inserção da senha no SGBD e posterior embarque no cofre de senhas.

VIII. Não existe a possibilidade de a senha ser quebrada por DBA's administradores do SGBD ou quaisquer softwares que se tenha conhecimento até hoje;

IX. A criação de logins contida no Formulário de Solicitação, juntamente com as suas respectivas autorizações, deverão ser armazenadas pela Segurança da Informação, ficando disponível para auditoria caso seja solicitado;

X. A criação de logins e a execução de solicitação de acesso à base de dados deverão ser executadas exclusivamente pelos DBA's utilizando acesso individual, não sendo permitida a utilização do usuário administrador "SA". No processo de criação de login e execução de quaisquer permissões de acesso será disparado um trigger contendo o login do usuário que executou a ação assim como a data e hora da execução, e as

demais instruções de permissão de acesso, ficando também disponível para auditoria caso seja solicitado;

XI. A responsabilidade sobre a criação de logins e da permissão de acesso em ambiente de produção é do Banco.

6.2.18.2. Criação de login de usuário comum:

I. A solicitação de criação de login de usuário comum deverá ser solicitada pelo próprio usuário e/ou fornecedor, juntamente com a autorização de seu respectivo gerente, via operação de Central de Serviço através de um chamado que deverá conter o Formulário de Solicitação devidamente preenchido e anexado em formato .pdf;

II. O login criado na base de dados deverá ser igual ao de rede.

III. O usuário solicitante deverá informar a senha in-loco ou via Teams com concessão de controle de acesso durante o processo de criação de login pelo DBA's;

IV. A senha informada pelo usuário tem caráter sigiloso e o sigilo da senha é de inteira responsabilidade do usuário;

V. As senhas devem ter a propriedade de expirarem a cada 03 meses.

6.2.18.3. Solicitação de consulta a base de produção:

I. A solicitação de consulta a base de produção deverá ser solicitada pelo funcionário da superintendência de sistemas via Operação Central de Serviço através de um chamado específico por usuário que deverá conter o Formulário de Solicitação anexado em formato .pdf;

II. O login de rede do funcionário será mapeado para um usuário da base(s) de dado(s) a qual foi autorizado a acessar;

III. As permissões serão a nível campos, a objetos (tabelas, views) do banco dados de acordo com o autorizado pelo superior descrito Formulário de Solicitação;

IV. Os funcionários poderão acessar as bases de dados de produção pela ferramenta ConsultaBD, utilizando suas prerrogativas de acessos já autorizada pelo funcionário competente.

6.2.18.4. Acessos remotos ao ambiente de produção:

I. Será vetado qualquer acesso remoto à base de dados de produção por usuários e por fornecedores;

II. Somente a equipe de DBA's poderá ter acesso remoto à bases de dados da produção, com autorização e com recursos disponíveis pela segurança da informação.

6.2.19. Permissões De Acesso A Base Dos Sistemas De Aplicação

I. A solicitação de acesso as bases dos sistemas de aplicações deverá ser solicitada pelo fornecedor requerente via Operação de Central de Serviço, através de um chamado especifico por usuário e banco que deverá conter Formulário de Solicitação anexado em formato .pdf;

II. O gestor do sistema deve autorizar permissões somente a sistemas que estejam sobre suas responsabilidades;

III. O gestor do sistema deve analisar a solicitação do fornecedor para verificar se ela é estritamente necessária para o bom desempenho da aplicação e avaliar o nível de acesso solicitado através do Formulário de Solicitação, levando em consideração para

a autorização sempre o mínimo de privilégios necessários para que a aplicação possa desempenhar com plenitude suas funcionalidades. Caso a solicitação seja referente a um sistema que não esteja sobre a sua responsabilidade, o mesmo deve solicitar o de acordo do funcionário responsável que deve também atender os requisitos.

6.2.20. Permissões De Acesso A Base De Dados Em Desenvolvimento

I. A solicitação de acesso as bases dos sistemas de aplicações deverá ser solicitada via Operação de Central de Serviço, através de um chamado especifico para solicitação de acesso, que deverá conter Formulário de Solicitação anexado em formato .pdf;

II. O gestor do sistema deve autorizar permissões somente a sistemas que estejam sobre suas responsabilidades;

III. A área gestora do sistema deve analisar a solicitação do fornecedor para verificar se a mesma é estritamente necessária para o bom desempenho da aplicação e avaliar o nível de acesso solicitado através do Formulário de Solicitação, levando em consideração para a autorização sempre o mínimo de privilégios necessários para que a aplicação possa desempenhar com plenitude suas funcionalidades. Caso a solicitação seja referente a um sistema que não esteja sobre a sua responsabilidade, o mesmo deve solicitar o de acordo do funcionário responsável que deve também atender os requisitos.

6.2.21. Controle de Acesso de dispositivos a Rede Corporativa

I. Esta norma se aplica a todos os colaboradores, terceirizados, prestadores de serviço e quaisquer outros usuários que necessitem acesso à rede do BANPARÁ, em qualquer uma das unidades.

II. Somente dispositivos devidamente registrados no sistema de patrimônio do BANPARÁ estão autorizados a se conectar logicamente à rede corporativa, seja por meio de conexão cabeada, sem fio (Wi-Fi), VPN ou qualquer outra forma de acesso.

III. Qualquer necessidade de conexão de dispositivos não vinculados ao patrimônio do BANPARÁ (por exemplo, equipamentos de visitantes, parceiros, ou equipamentos próprios temporários) deverá ser previamente analisada, aprovada e registrada pela equipe de Segurança da Informação.

7. FLUXOS DE TRABALHO DO PROCESSO

7.1. FLUXO PARA CONCESSÃO DE ACESSO.

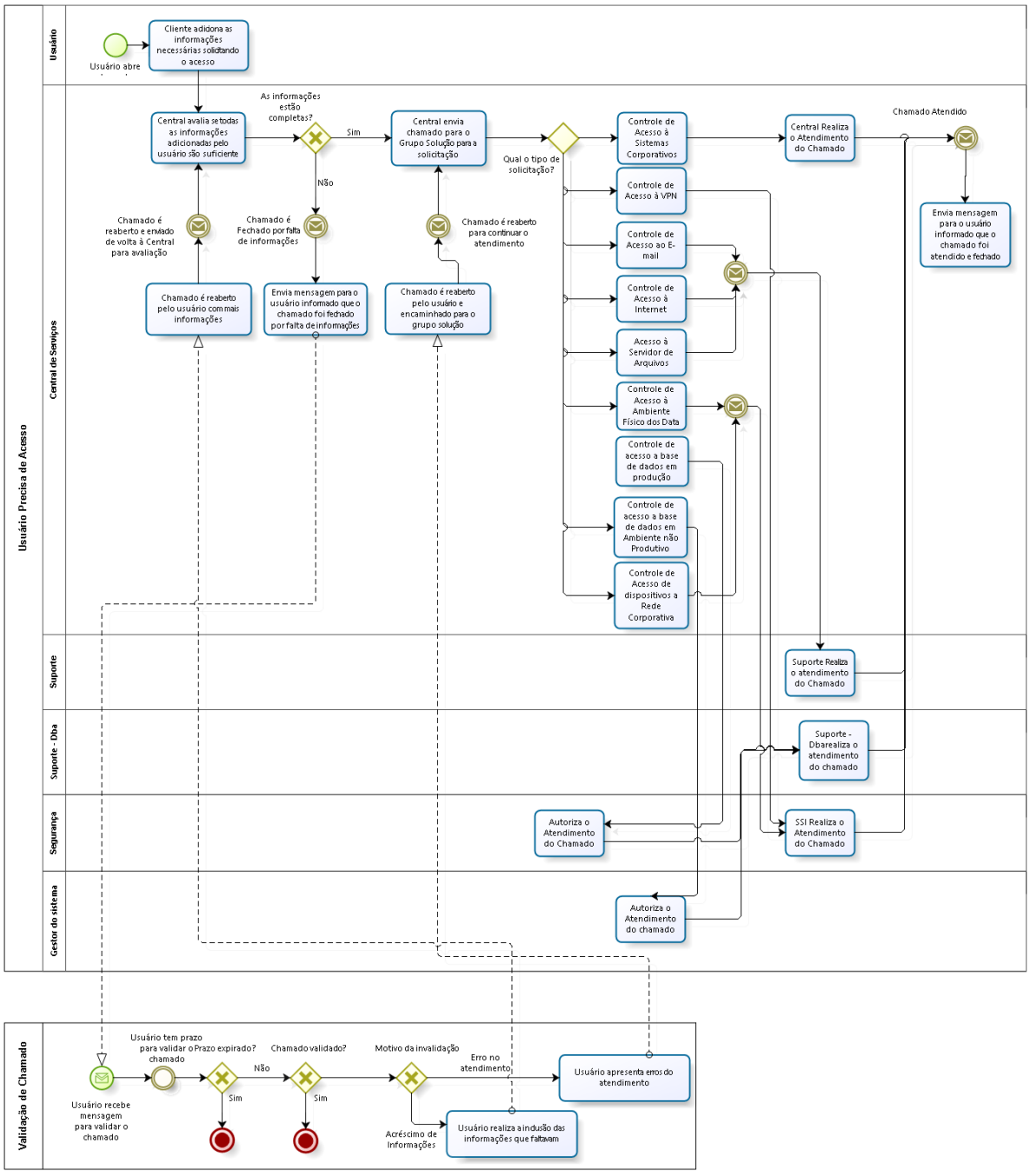

Figura 2 – Fluxo para concessão de acesso

7.1.1. Gatilhos para iniciar o processo

Tabela 9 - Controle de acessos a sistemas corporativos

ENTRADA	Solicitação de cadastro de usuário, acesso, alteração ou cancelamento/exclusão
DESCRIÇÃO	A Operação de Central de Serviços irá avaliar as informações contidas no Formulário de Acesso
RESPONSÁVEL	Operação de Central de Serviços
PARTICIPANTE (S)	Área solicitante e Operação de Central de Serviços
PROCEDIMENTO	1 – Avaliar Formulário de Acesso 2 – Conceder o acesso, alteração ou cancelamento/exclusão
SAÍDA	Usuário cadastrado, alterado ou cancelado/excluído Adição no relatório de concessão de acesso, em caso de Sistema crítico

Tabela 10 - Controle de acessos a VPN

ENTRADA	Solicitação de acesso a VPN
DESCRIÇÃO	A Operação de Central de Serviços irá avaliar as informações contidas no Formulário de Acesso e encaminhar para Segurança da Informação
RESPONSÁVEL	Operação de Central de Serviços Segurança da Informação
PARTICIPANTE (S)	Área solicitante Operação de Central de Serviços Segurança da Informação
PROCEDIMENTO	1 – Avaliar Formulário de Acesso 2 – Conceder o acesso
SAÍDA	Usuário com acesso a VPN

Tabela 11 - Controle de acessos ao e-mail

ENTRADA	Solicitação de acesso ao e-mail
DESCRIÇÃO	A Operação de Central de Serviços irá avaliar as informações contidas no Formulário de Acesso e encaminhar para Operação de Suporte Avançado
RESPONSÁVEL	Operação de Central de Serviços Operação de Suporte Avançado
PARTICIPANTE (S)	Área solicitante

	Operação de Central de Serviços Operação de Suporte Avançado
PROCEDIMENTO	1 – Avaliar Formulário de Acesso 2 – Conceder ou não o acesso
SAÍDA	Usuário com acesso ao e-mail ou não

Tabela 12 - Controle de acessos a internet

ENTRADA	Solicitação de acesso à internet Solicitação de acesso à internet por mudança de função Solicitação de acesso a novos sites
DESCRIÇÃO	A Operação de Central de Serviços irá avaliar as informações contidas no Formulário de Acesso e encaminhar para Operação de Suporte Avançado e Segurança da Informação.
RESPONSÁVEL	Operação de Central de Serviços Operação de Suporte Avançado Segurança da Informação UNIBANP
PARTICIPANTE (S)	Área solicitante Operação de Central de Serviços Operação de Suporte Avançado Segurança da Informação UNIBANP
PROCEDIMENTO	1 – Avaliar Formulário de Acesso 2 – Verificar autorização da Segurança da Informação 3 – Conceder o acesso
SAÍDA	Usuário com acesso a internet Usuário com acesso a site

Tabela 13 - Controle de acessos a ambientes físicos e datacenters

ENTRADA	Solicitação de acesso ao Site Principal, Site Backup e Sala de Teleprocessamento Solicitação de acesso a Fitoteca Solicitação de acesso as demais áreas restritas de TI
DESCRIÇÃO	A Operação de Central de Serviços irá avaliar as informações contidas no Formulário de Acesso e encaminhar para Segurança da informação

RESPONSÁVEL	Operação de Central de Serviços Segurança da informação
PARTICIPANTE (S)	Área solicitante Operação de Central de Serviços Operação de Suporte Avançado Segurança da Informação Áreas da Matriz
PROCEDIMENTO	1 – Avaliar Formulário de Acesso 2 – Verificar autorização da Segurança da Informação 3 – Conceder o ou não acesso
SAÍDA	Usuário com acesso ou não ao ambiente solicitado

Tabela 14 - Controle de acessos a base de dados em produção

ENTRADA	Solicitação de acesso a base de dados em produção Solicitação de criação de login Solicitação de consulta a base em produção
DESCRIÇÃO	A Operação de Central de Serviços irá avaliar as informações contidas no Formulário de Acesso e encaminhar para Segurança da informação que irá analisar e encaminhar para a área de operação de suporte avançado - Dba
RESPONSÁVEL	Operação de Central de Serviços Segurança da informação Operação de Suporte avançado - Dba
PARTICIPANTE (S)	Área solicitante Operação de Central de Serviços Operação de Suporte Avançado -Dba Segurança da Informação
PROCEDIMENTO	1 – Avaliar Formulário de Acesso 2 – Verificar autorização da Segurança da Informação 3 – Conceder o ou não acesso
SAÍDA	Acesso ou não a base solicitada

Tabela 15 - Controle de acessos a base de dados em ambiente não produtivo

ENTRADA	Solicitação de acesso a base de dados em Ambiente não Produtivo

	Solicitação de criação de login Solicitação de consulta a base em desenvolvimento
DESCRIÇÃO	A Operação de Central de Serviços irá avaliar as informações contidas no Formulário de Acesso e encaminhar para Gestor do Sistema que irá analisar e encaminhar para a área de operação de suporte avançado - Dba
RESPONSÁVEL	Operação de Central de Serviços Gestor do sistema Operação de Suporte avançado - Dba
PARTICIPANTE (S)	Área solicitante Operação de Central de Serviços Operação de Suporte Avançado - DBa Gestor do Sistemas
PROCEDIMENTO	1 – Avaliar Formulário de Acesso 2 – Verificar autorização do Gestor do sistema 3 – Conceder o ou não acesso
SAÍDA	Acesso ou não a base solicitada

Tabela 16 - Controle de acesso de dispositivos a rede corporativa

ENTRADA	Solicitação de Acesso de dispositivos a Rede Corporativa
DESCRIÇÃO	A Operação de Central de Serviços irá avaliar as informações contidas no Formulário de Acesso e encaminhar para a SSI.
RESPONSÁVEL	Operação de Central de Serviços Segurança da Informação
PARTICIPANTE (S)	Área solicitante Operação de Central de Serviços Segurança da informação
PROCEDIMENTO	1 – Avaliar Formulário de Acesso 2 – Analisar a demanda 3 – Conceder o ou não acesso
SAÍDA	Acesso ou não do dispositivo solicita a rede

CAPÍTULO II: BACKUP E RECUPERAÇÃO DE DADOS

1. OBJETIVO

O objetivo de uma normatização de backup é garantir a integridade, disponibilidade e recuperação eficiente dos dados em caso de perda, corrupção ou falha do sistema. Isso envolve a definição de políticas, procedimentos e melhores práticas para a realização de cópias de segurança.

1.1. LEGISLAÇÃO VIGENTE

No Brasil, a legislação que trata sobre os backups em instituições financeiras está principalmente contida nas normas do Banco Central do Brasil (Bacen) e nas resoluções do Conselho Monetário Nacional (CMN). Essas normas visam garantir a segurança, integridade e disponibilidade dos dados em instituições financeiras.

Todas as áreas do Banpará devem atentar para essas normas com o objetivo de implementá-las, garantindo a conformidade. As principais legislações e regulamentações no que diz respeito ao armazenamento dos dados são:

- Resolução CMN 4.658/2018: A Resolução CMN 4.658 estabelece requisitos para a política de segurança cibernética e a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem para as instituições financeiras.
- Política de Segurança Cibernética: As instituições devem definir e implementar uma política de segurança cibernética que inclua a proteção dos dados, incluindo os dados em backup.
- Plano de Recuperação de Desastres: Devem elaborar e manter atualizados planos de continuidade de negócios e de recuperação de desastres, assegurando a integridade, a confidencialidade e a disponibilidade dos dados e sistemas.
- Monitoramento e Gestão de Riscos: Devem monitorar e gerenciar os riscos associados ao uso de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo os relacionados aos backups.
- Circular Bacen 3.909/2018: A Circular Bacen 3.909 complementa a Resolução CMN 4.658, detalhando os requisitos para a implementação da política de segurança cibernética.
- Requisitos Mínimos: Define requisitos mínimos para a política de segurança cibernética, incluindo a gestão de incidentes de segurança e a necessidade de manutenção de backups seguros.
- Plano de Resposta a Incidentes: Reforça a necessidade de um plano de resposta a incidentes que contemple a recuperação de dados a partir de backups em caso de incidentes cibernéticos.
- Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/2018: Embora a LGPD não trate especificamente de backups, ela impõe requisitos rigorosos sobre a proteção de dados pessoais, que impactam diretamente como os backups devem ser gerenciados.
- Segurança de Dados: A LGPD exige que as instituições tomem medidas técnicas e administrativas para proteger os dados pessoais contra acesso não autorizado, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

- Retenção e Exclusão de Dados: Assegura que os dados pessoais não sejam mantidos por um período mais longo do que o necessário para cumprir as finalidades para as quais foram coletados, o que afeta as políticas de retenção de backups.

- Resolução CMN 4.893/2021: A Resolução CMN 4.893 altera dispositivos da Resolução CMN 4.658/2018, reforçando aspectos relacionados à segurança cibernética e à gestão de riscos em serviços de processamento e armazenamento de dados, incluindo computação em nuvem.

- ISO 27001: Instituições financeiras também seguem requisitos internos e auditorias baseadas em padrões internacionais de segurança da informação, como ISO/IEC 27001, que impactam diretamente a gestão de backups.

2. OBJETIVO ESPECÍFICO

Este documento define as normas de Backup as serem seguidas pelo Banpará, tendo como principais objetivos:

- **Recuperação de Desastres:** Em caso de desastres naturais, falhas de hardware, incêndios ou outros eventos catastróficos, as rotinas de backup permitem que o banco recupere rapidamente seus dados e restabeleça suas operações.

- **Proteção contra Perda de Dados:** Erros humanos, falhas de software ou ataques cibernéticos podem resultar em perda de dados. Com backups regulares, o banco pode restaurar informações perdidas ou comprometidas.

- **Continuidade de Negócios:** Garantir que os serviços bancários permaneçam operacionais é crucial. Backups permitem que o banco mantenha suas operações mesmo após interrupções significativas, minimizando o impacto sobre os clientes e a reputação da instituição.

- **Conformidade Regulamentar:** Muitos regulamentos financeiros exigem que os bancos mantenham backups regulares de dados para garantir a integridade e disponibilidade de informações. Cumprir essas exigências ajuda o banco a evitar penalidades e sanções.

- **Proteção contra *Ransomware* e Outros Ataques Cibernéticos:** Em caso de um ataque de *ransomware*, onde os dados são criptografados e um resgate é exigido, ter backups recentes e seguros permite que o banco restaure seus sistemas sem pagar aos atacantes.

- **Integridade e Segurança de Dados:** Manter backups ajuda a garantir que os dados críticos estejam seguros e intactos, protegendo contra corrupção de dados e outras ameaças que podem comprometer a precisão e confiabilidade das informações.

- **Retenção Histórica de Dados:** Para fins de auditoria e análise, é importante ter cópias históricas dos dados. Isso pode ser útil para revisões financeiras, auditorias regulatórias e análises de tendências ao longo do tempo.

- **Facilidade de Atualização e Migração de Sistemas:** Durante a atualização ou migração de sistemas, os backups garantem que os dados possam ser restaurados em caso de falhas ou problemas inesperados durante o processo.

3. UNIDADE GESTORA

Caberá a área de segurança da informação e proteção de dados pessoais atuar como gestor na criação/alteração de normas e procedimentos a serem aplicados nas unidades do Banpará com relação ao processo de Backup dos dados dos sistemas utilizados no Banpará. Além disso, caberá às demais unidades do Banco, a observância das normas e procedimentos contidos neste documento.

4. NORMAS GERAIS

Deverão ser realizadas cópias de segurança das bases de dados e de todos os Sistemas pertencentes ao BANPARÁ e/ou os quais o BANPARÁ possui suas licenças de uso:

I. Servidores de arquivos;

II. Versões e fontes dos Sistemas desenvolvidos por fornecedores;

III. Base de dados da Ferramenta de Backup;

IV. Dados de voz;

V. Máquinas virtuais do ambiente de produção;

VI. Banco de dados do ambiente de produção;

VII. Outros que se fizerem necessários.

Deverão ser realizadas atualizações e acompanhamento das rotinas de acesso físico aos seguintes locais e respectivos responsáveis:

I. Datacenters (responsáveis: Segurança da Informação e Operação de Suporte Avançado);

II. Sala cofre das mídias – (responsável: Operação de Suporte Avançado).

Deverão ser inventariadas as mídias em uso via software específico, cuja a responsabilidade pela referida tarefa será dos DBA's.

5. OPERACIONALIZAÇÃO DOS BACKUPS DA BASE DE DADOS

I. As rotinas de backup do banco de dados deverão funcionar 24 horas por dia, 7 dias por semana e 365 dias por ano, através de job's programados previamente pelos DBA's de acordo com as necessidades do BANPARÁ.

II. Caberá aos operadores de produção, que serão divididos em turnos, a monitoração diária dos backup's que impactam no processamento dos bancos de dados e que serão executados no servidor de Backup.

III. O operador, em caso de dúvida na monitoração dos job's deverá consultar o "manual de operacionalização de backup vigente", o qual orienta passo a passo como o operador deverá proceder. Caso a dúvida persista, deverá entrar em contato com o DBA que estiver à disposição na ocasião do fato. O "manual de operacionalização de backup vigente" ficará arquivado na Operação de Suporte Avançado.

IV. Em caso de falha em algum job do backup, o operador de produção deverá entrar em contato com o DBA que estiver à disposição na ocasião do acontecimento.

V. Os DBAs deverão duplicar as fitas de backup, de acordo com a recomendação de documento específico, através de espelhamento do job de backup do site principal para o site backup ou vice e versa.

VI. Caberá diariamente a equipe de DBA's, checar a situação das rotinas de backup, tomando providências se necessário.

6. PERIODICIDADE DOS BACKUPS

6.1. AS ROTINAS DE BACKUP DEVERÃO OBEDECER ÀS PERIODICIDADES ABAIXO RELACIONADAS

6.1.1. File system

I. Os backups dos arquivos dos servidores de interfaces e dos servidores de aplicação, relacionados ao sistema conta corrente, são feitos de terça-feira à sábado, sendo backups incrementais de terça-feira a sexta-feira e um backup full no sábado. Estes backups são feitos no pool de fitas Ccor, e a cópia no pool de fitas Ccor_Seguranca, com retenção permanente. Fazem parte do backup os seguintes servidores: ccorapp, ccorweb-01, ccorweb-02, soure, srvapp01, srvapp02 e srvinterfaces;

II. Os backups da base de dados interna do Data Protector são feitos todos os dias às 11:00 assim como uma cópia de segurança, com retenção de 10 dias;

III. Os backups dos arquivos das câmeras de segurança da SUPRO/SUSIS, existentes no servidor camsutec, são feitos todos os sábados, ao meio dia, sendo um backup full a cada seis semanas e backups incrementais no restante. Estes backups são feitos no pool de fitas FileSystem_Diario e a cópia no pool de fita Copia_Diaria_FileSystem, com retenção de 90 dias;

IV. Os backups do diretório de fotos, existente nos servidores das agências virtualizadas, assim com a cópia de segurança são feitos todo dia 10 de cada mês com retenção permanente;

V. O restante de todos os arquivos e diretórios são feitos semanalmente de terça-feira a sexta-feira, sendo um backup full na sexta-feira às 22:00 e backups incrementais as 00:00h no restante dos dias com retenção de 90 dias.

6.1.2. Banco de Dados

I. A periodicidade padrão do backup das bases de dados de produção é diária de segunda-feira a sexta-feira.

II. As bases de desenvolvimento e homologação são backups semanais durante o final de semana.

III. Todas as bases de dados são inseridas nesta periodicidade, com algumas exceções que são mencionadas posteriormente. Algumas bases de dados de produção possuem backups mais de uma vez ao dia. São elas: pd_cred e bases relacionadas, multiserv, cdi_admlog e bases relacionadas, e tb_dispon. Estes backups ocorrem de acordo com a tabela abaixo:

Tabela 17 - Periodicidade

Bases de Dados	Periodicidade
Pd_azd, pd_azdemp, pd_base, pd_cred, pd_credito_contratacao, pd_credito_linha, pd_credito_politica,	De segunda-feira a sexta-feira. Um backup full as 07:00h e um às 14:00h. Um backup diferencial as 14:00h e um às 20:00h.

pd_credito_portal, pd_extcons, pd_mcc, pd_rede e pd_risk.	Um backup transacional a cada 30 minutos, quando não estiver em execução um dos backups anteriores.
Cdi_acesso, cdi_admacesso, cdi_admcombustivel, cdi_admlog, cdi_admmoradia, cdi_admvale, cdi_ccf, cdi_dep_judicial, cdi_multicid, cdi_seguranca, cdi_seig, multiserv.	De segunda-feira a sexta-feira. Um backup full as 14:00h e um às 03:15h.
Tb_dispon	De segunda-feira a sexta-feira. Um backup full as 22:00h. Um backup diferencial iniciado manualmente pelo operador da produção, no intervalo do processamento do sistema conta corrente, aproximadamente as 1:30h. Um backup full iniciado manualmente pelo operador da produção no final do processamento do sistema conta corrente, aproximadamente as 6:00h.

6.1.3. Máquinas virtuais

I. Será detalhado no item 8, que é referente às máquinas virtuais.

6.1.4. Servidor de correio eletrônico

I. É realizado diariamente às 00:00 sendo segunda, quarta e sexta-feira um full e nos demais dias incremental no mesmo horário.

6.1.5. Caixa postal de correio eletrônico

I. Deverá ser realizado backup full todo sábado e incremental de segunda a sexta feira de todo mês às 00:05 para as funções obrigatórias: Conselheiro, Presidente, Diretor, Assessor de Diretoria, Superintendente e Chefe de Núcleo.

6.1.6. Banco de dados da base do conta corrente

I. Deverá ser realizado backup full de segunda a sexta, às 22h e outro backup full após o processamento noturno. Deverá ser realizado backup incremental após a importação das interfaces durante o processamento noturno.

7. PERIODICIDADE DAS CÓPIAS DOS BACKUPS

As rotinas de cópias de dados deverão obedecer às periodicidades abaixo relacionadas e deverão ter proteção permanente:

I. Banco de dados da base do conta corrente – deverá ser executada todo domingo para fita de pool CCOR e CCOR_SEGURANÇA;

II. Fotos da fita cash dos servidores das agências virtualizadas – deverá ser executada todo dia 11 do mês Cópia mensal de file system (servidor de correio eletrônico, base interna do software de backup, ftpserver e arquivos do servidor de interfaces) – deverá ser executada todo dia 03 do mês para o site principal e para o site backup;

III. Cópia mensal de file server (servidores de arquivos em geral) – deverá ser executada mensalmente, no primeiro sábado no site principal e site backup.

IV. Banco de dados excetuando a base do conta corrente – deverá ser executada após ao último processamento do mês com as informações referentes aos dados das mesmas antes do último processamento mensal para O site principal e site backup.

8. BACKUPS DE MÁQUINAS VIRTUAIS

I. As máquinas virtuais são gerenciadas pela plataforma centralizada Vcenter. Atualmente existe dois Vcenters chamados srvvcenter6 e srvvcenter que gerenciam todas as máquinas virtuais, agrupados em dois dataCenters: Municipalidade e PVargas com máquinas do ambiente de desenvolvimento e homologação e VPLEX com máquina de produção:

II. Os backups das máquinas foram agrupados por data center conforme distribuição e schedules abaixo. Para os data center que agrupam as máquinas virtuais de desenvolvimento e homologação são agendados backup full para serem executados uma vez por mês, aos finais de semana Já o ambiente de produção é agendado o backup full periodicamente aos sábados.

III. É realizado backup de todos os discos da máquina exceto aqueles que estão marcados como independentes no vcenter. Para estes deverá ser configurado backup de fileSystem, onde a área demandante responsável deverá demandar formalmente via central de serviço chamado solicitando para que seja agendada rotina de backup para o arquivo necessário caso este ainda não seja contemplado na politica de backup de file system existente.

IV. O agendamento dos Jobs ocorre conforme abaixo:

Tabela 18 – Agendamento dos jobs

Job	Máquinas	Retenção	Destino	Periodicidade	Tipo de Backup
bkp_Vplex	VMs de Produção	4 Semanas	Data Domain	Sábado 07:30	Full
SrVcenter02_Desenv	Data Center Pvargas - Desenvolvimento	30 dias	Data Domain	1 vez por mês às 08:00	Full
SrVcenter02_Homol	Data Center Pvargas - Homologação	30 dias	Data Domain	1 vez por mês às 14:00	Full
SrVcenter_Agencias	Vplex - Máquinas de agência	45 dias	Data Domain	Domingo 20:15	Full
Srvvcenter_Desenv	Data Center Municipalidade - Desenvolvimento	30 dias	Data Domain	à cada 28 dias às 10:00	Full

9. BACKUP DE BANCO DE DADOS

I. As bases de dados estão distribuídas em ambientes de produção, homologação e desenvolvimento. É feito backup de todas as bases de produção e desenvolvimento. Em homologação é feito backup apenas da base de dados do SPB e de bases na mesma instância que está relacionada com o SPB, por exemplo: CBR_SEG, SGB e SPB_HIST. O tipo de backup utilizado para estes backups é o full.

II. A adição das bases de dados na política de backup é feita pelos DBA's logo após a criação da base. Durante a criação de uma base de dados, o requisitante pode informar uma periodicidade para a base em questão, porém, caso esta informação não seja dada, o DBA define a periodicidade padrão para o ambiente em que a base foi armazenada.

III. A periodicidade padrão do backup das bases de dados de produção e homologação é diária, de segunda-feira a sexta-feira, e das bases de desenvolvimento é semanal,

durante o final de semana. Todas as bases de dados são inseridas nesta periodicidade, com algumas exceções, conforme o item IV.

IV. Algumas bases de dados de produção possuem backups mais de uma vez ao dia. São elas: pd_cred e bases relacionadas, multiserv, cdi_admlog e bases relacionadas, e tb_dispon. Estes backups ocorrem da seguinte forma:

Tabela 19 – Periodicidade dos backups

Bases de Dados	Periodicidade
Pd_azd, pd_azdemp, pd_base, pd_cred, pd_credito_contratacao, pd_credito_linha, pd_credito_politica, pd_credito_portal, pd_extcons, pd_mcc, pd_rede e pd_risk.	De segunda-feira a sexta-feira. Um backup full as 06:00h e um as 14:00h. Um backup diferencial as 14:00h e um as 20:00h. Um backup transacional a cada 30 minutos, quando não estiver em execução um dos backups anteriores.
Cdi_acesso, cdi_admacesso, cdi_admcombustivel, cdi_admlog, cdi_admmoradia, cdi_admvale, cdi_ccf, cdi_dep_judicial, cdi_multicid, cdi_seguranca, cdi_seig, multiserv.	De segunda-feira a sexta-feira. Um backup full as 14:00h e um as 03:15h.
Tb_dispon	De segunda-feira a sexta-feira. Um backup full as 22:30h. Um backup diferencial iniciado manualmente pelo operador da produção, no intervalo do processamento do sistema conta corrente, aproximadamente as 1:30h. Um backup full iniciado manualmente pelo operador da produção no final do processamento do sistema conta corrente, aproximadamente as 6:00h.

V. Os backups de produção e homologação são gravados simultaneamente no site principal e a cópia no site PVargas já as bases de dados de desenvolvimento não possuem cópia de segurança sendo gravado somente no site principal. A retenção dos backups das bases de dados de produção e homologação é de 90 dias e das bases de dados de desenvolvimento é de 45 dias.

VI. Os backups das bases de dados do servidor de histórico também fazem parte dos backups do ambiente de produção, porém possuem uma periodicidade e uma retenção diferenciadas. O backup destas bases é feito uma vez na semana durante o final de semana de forma incremental e uma vez por mês executa um full. Possuem retenção permanente. - Um dia após o último dia útil do mês é feita a cópia mensal dos backups das bases de dados de produção e homologação para fita mensal. Desta forma, os backups destas bases de dados anterior ao processamento do último dia útil do mês são salvos em fitas mensais. Estas cópias possuem retenção permanente.

10. BACKUP DE ARQUIVOS DE DIRETÓRIOS

I. São inseridos na rotina de backup apenas os arquivos ou diretórios que são requisitados pelas áreas responsáveis, pois os DBAs não possuem gerência sobre os arquivos ou diretórios existentes. As pastas públicas dos servidores não entrarão na rotina de backup, ainda que solicitado.

II. Os backups dos arquivos dos servidores de interfaces e dos servidores de aplicação, relacionados ao sistema conta corrente, são feitos de segunda-feira a sexta-feira, sendo backups incrementais de segunda-feira a quinta-feira e um backup

full na sexta-feira. Possuem retenção permanente. Fazem parte do backup os seguintes servidores: ccorapp, ccorweb-01, ccorweb-02, soure, srvapp01, srvapp02 e srvinterfaces.

III. Os backups da base de dados interna do Data Protector são feitos todos os dias às 11:00, com retenção de 10 dias.

IV. Os backups dos arquivos das câmeras de segurança das áreas de infraestruturas de TI, existentes no servidor camsutec, são feitos todos os sábados, ao meio dia, sendo um backup full a cada seis semanas e backups incrementais no restante. Estes backups são feitos no pool de fitas FileSystem_Diario e a cópia no pool de fita Copia_Diaria_FileSystem, com retenção de 90 dias.

V. Os backups do diretório de fotos, existente nos servidores das agências virtualizadas e servidor de mídia, \\arqserver\fotocash, são feitos todo dia 10 de cada mês, para o pool de fitas Copia_Mensal_1 e a cópia para o pool de fitas Copia_Mensal_2, com retenção permanente.

VI. O restante de todos os arquivos e diretórios são feitos semanalmente de terça-feira a sexta-feira, sendo um backup full na sexta às 22:00 e backups incrementais as 00:00h no restante dos dias. Estes backups possuem retenção de 90 dias.

VII. Um dia útil após o primeiro sábado do mês é feita a cópia mensal dos backups dos arquivos e diretórios. Esta cópia é feita para fita mensal no pool Copia_Mensal_1 e Copia_Mensal_2, com retenção permanente.

11. BACKUP DE E-MAILS CORPORATIVOS

I. Aplica-se a todos os usuários, sistemas e serviços de e-mail corporativo, incluindo:

- Servidores de e-mail locais (on-premise)
- Plataformas em nuvem (ex.: Microsoft 365, Google Workspace)
- Dispositivos corporativos que sincronizam e-mails

II. Backup diário automático de todas as caixas postais.

III. Retenção padrão:

- E-mails operacionais: 5 anos
- E-mails críticos/legais: 10 anos ou conforme legislação específica

IV. E-mails antigos devem ser movidos para solução de arquivamento que permita busca e auditoria.

V. Backups devem ser criptografados com algoritmo mínimo AES-256.

VI. Armazenamento em local físico distinto ou provedor de nuvem certificado (ISO 27001, SOC 2, etc.).

VII. Controle de acesso restrito apenas a administradores autorizados.

VIII. Registro de logs de acesso aos backups por mínimo de 12 meses.

IX. Equipe de TI: execução, monitoramento e manutenção dos backups.

X. Segurança da Informação: auditoria, revisão de conformidade e análise de incidentes.

XI. Usuários finais: uso correto do e-mail corporativo e reporte imediato de incidentes.

12. NORMAS PARA ARMAZENAMENTO DAS MÍDIAS DE BACKUP

I. As fitas (principal e cópia) serão armazenadas em um ambiente restrito dentro dos CPDs (Site principal e site backup) em racks.

II. Caberá à Operação de Suporte Avançado a responsabilidade do armazenamento e da identificação das fitas no site principal e do armazenamento no site Backup.

III. É proibida a permanência de fitas que não estiverem em uso fora dos locais definidos previamente.

IV. Os locais deverão estar protegidos contra acessos de pessoas não autorizadas. - Caberá à Segurança da Informação e à área de Infraestrutura de TI o controle de acesso aos locais de armazenamento. Quando não for mais necessário, o conteúdo das mídias deve ser apagado e a mesma reaproveitada para as rotinas de backup. - No caso da mídia ser retirada definitivamente do BANPARA, seu conteúdo deverá ser totalmente excluído. Ação de responsabilidade da Operação de Suporte Avançado.

13. NORMAS PARA TEMPORALIDADE E RODÍZIO DAS MÍDIAS

I. Caberá aos coordenadores responsáveis por cada sistema levantar e definir em conjunto com os fornecedores e gestores a temporalidade dos dados, a qual deverá ser enquadrada nas políticas já existentes na política de backup e ser entregue via documento escrito e devidamente assinado pelos mesmos. Caso a necessidade seja diferente das mesmas, os coordenadores responsáveis deverão encaminhar uma solicitação via central de serviço descrevendo uma nova política de retenção e justificando-a, e caberá à Segurança da Informação aprovar ou não tal solicitação. Caso seja aprovada, a mesma deverá ser encaminhada aos DBAs para sua operacionalização.

II. Existem 05 grupos de rodízios de fitas, segue abaixo:

- Fitas Diárias de ficarão retidas por 90 dias, findo esse prazo serão reutilizadas;

13.1.1. Fitas do CCOR:

I. Arquivos: de terça-feira a sábado. Ficarão retidas por período indeterminado;

II. SQL: de segunda a quinta ficarão retidas por período de 90 dias. Às sextas e aos sábados, ficarão retidos por tempo indeterminado.

13.1.2. Fitas de cópia mensal: retêm-se estas fitas por tempo indeterminado;

13.1.3. Fitas de caixa postal de correio eletrônico: ficarão retidas por tempo indeterminado;

13.1.4. Fitas de final de Mês: retêm-se estas fitas por tempo indeterminado;

13.1.5. Cópias de segurança: todos os jobs de backup deverão ser realizados simultaneamente na library do site principal e na library do site backup.

14. NORMAS PARA TESTES DAS MÍDIAS DE BACKUP

I. Caberá aos DBA's a realização de testes periódicos de verificação dos backup's através de restores aleatórios de arquivos e base de dados, para que possa garantir a integridade das mídias.

II. Deverá ser redigido um roteiro com os procedimentos da realização dos testes. Esses procedimentos deverão ser devidamente salvos em pasta para posterior pesquisa.

15. NORMAS PARA TRANSPORTE DAS MÍDIAS DE BACKUP

I. O transporte físico de mídias que contém dados aos limites da organização é um potencial ponto de risco à segurança da informação, visto que as torna vulneráveis a acessos não autorizados, danos ou adulterações, principalmente quando realizado por terceiros, assim, os seguintes procedimentos devem ser adotados:

- Quando não realizado pelo próprio DBA, deve ser utilizado transporte ou serviço de mensageiro confiável.
- Enviar a mídia via mensageiro identificado e seguro ou outro método de entrega que pode ser monitorado com precisão.
- Adotar controles especiais, para proteger informações críticas, tais como: recipientes lacrados, entrega em mãos, lacres específicos de pacotes (que revele qualquer tentativa de acesso).

16. NORMAS PARA DESCARTE DAS MÍDIAS DE BACKUP

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas pela equipe de DBA's, levando em consideração os seguintes itens:

I. Identificar e registrar as mídias descartadas.

II. Efetuar a contingência para os dados presentes na mídia, garantindo que os mesmos não sejam perdidos.

III. Inutilizar a mídia, triturando, incinerando ou utilizando qualquer outro método em que os dados não possam ser recuperados.

17. OPERACIONALIZAÇÃO DOS RESTORES

I. A solicitação de restore na base de dados de produção deverá ser solicitada via RDM através do preenchimento do Formulário de Solicitação de Restore anexado em formato .pdf, existente no Sistema de Gerenciamento de Serviços TI devidamente autorizado pelo gerente da área, seguida da autorização do Gerente da Operação de Suporte Avançado.

II. Na falta do Gerente da Operação de Suporte Avançado, chefia de hierarquia superior à que estiver vinculado o solicitante poderá conceder a autorização do item anterior.

III. A operacionalização do restore deverá ser executada exclusivamente pelos DBA's.

IV. O DBA deverá informar todos os envolvidos, através do canal utilizado (email, service desk, etc), do término do restore, para que sejam tomadas as devidas providências de continuidade do Sistema.

V. O procedimento de restore solicitado de bases de dados contendo em suas respectivas tabelas informações de clientes (como: nome, CPF e endereço) devem passar pelo processo descaracterização de dados.

18. AUTORIZAÇÃO PARA EXECUÇÃO DE RESTORE

I. Caso o objetivo do restore seja solicitado em ambiente de desenvolvimento ou homologação, a análise e/ou correção de um problema técnico, a execução do mesmo

será feita pela equipe de DBAs, havendo necessidade de autorização de um funcionário da área de sistemas ou Infraestrutura de TI, integrante da equipe responsável pelo sistema/projeto. Caso o restore seja solicitado por alguém de uma equipe que não seja a responsável pelo sistema, o mesmo deverá ser autorizado pelo responsável. Após a aprovação, o mesmo deve ser encaminhado à equipe de DBAs para execução, obedecendo aos itens constantes dos procedimentos para a "execução de restores".

II. A autorização da execução do restore em ambiente produção, será de alçada exclusiva dos Superintendentes da diretoria de tecnologia ou Gerentes da área de sistemas ou da área de infraestrutura com aval da área de Segurança da Informação.

III. Nos casos de serviços urgentes em ambiente de desenvolvimento e homologação, assim entendidos aqueles onde não seja possível seguir todo o fluxo de documentação e autorização, a solicitação deverá ser registrada formalmente através do e-mail corporativo e a equipe de DBAs fica autorizada a executar o restore, sendo o solicitante o total responsável pelas informações para a execução dele, bem como suas consequências.

19. EXECUÇÃO DE RESTORE

I. A execução de restores em ambiente de produção somente deve ser realizada em casos em que nenhuma outra solução não atenda às necessidades do Banco sendo caracterizado assim como desastre. Vale ressaltar somente devem ser executados em último caso, pois aumentam significativamente a probabilidade de perda de dados.

II. O Prestador de Serviço deve sempre informar ao funcionário responsável do Banco da possibilidade de desenvolvimento de um novo tratamento de erros no sistema – a ser executada pelos coordenadores – que poderá substituir a execução do restore, em qualquer ambiente.

III. A responsabilidade sobre a solicitação do restore é do Prestador de Serviço, ou seja, o Banco não se responsabiliza pela substituição de bases no destino. Dessa forma, o Prestador deve garantir que o restore não tenha consequências divergentes das definidas no escopo da solicitação dele. Para tal, o Banco sugere que o Prestador realize um procedimento de dupla validação do restore antes de sua solicitação.

IV. Os restores só devem ser enviados por solicitação expressa da área de sistemas ou da área de infraestrutura ou quando o Prestador de Serviço identificar a necessidade de envio do mesmo para atender uma necessidade do Banco. Em ambos os casos, a área de Infraestrutura e Sistemas deve ser formalmente informada do procedimento.

V. A responsabilidade sobre a operacionalização integral do restore é do Banco.

VI. Fica terminantemente proibida, a disponibilização de arquivos de backup de Base de Dados, conforme norma de segurança vigente.

VII. O envio de um novo restore deve ser feito através de uma nova RDM pela Central de Serviços (serão desconsideradas solicitações via tarefa, incidentes e requisição) e sempre com o preenchimento completo da aba de solicitação de restore disponibilizada no Sistema de Gerenciamento de Serviços TI, o qual deve conter as seguintes informações:

- Objetivo: Motivo do restore que está sendo solicitado;

- Informações técnicas: Informações do nome e em que servidor a base de destino encontra-se e qual o nome da base de destino e em que servidor e instância o restore será efetuado. Caso a nova base necessite de alguma(s) permissão(ões) além e/ou diferentes da base de origem, especificá-la(s) detalhadamente. Caso o restore seja de arquivo, informar o local de origem, datas e o máximo possível de informações sobre os arquivos desejados, tais como nome, extensão, etc., bem como o local em que os mesmos poderão ser disponibilizados;
- Motivo: Descrever por qual motivo o restore está sendo solicitado;
- Responsável Solicitante: Descrever nome completo e dados de contato (e-mail, fone, etc.) de quem está solicitando o restore.
- Período de Permanência: O período máximo de disponibilidade da base restaurada será de 30 dias a contar da data do restore, podendo ser;
- Impactos: Sistemas e Funcionalidades que serão analisadas após a execução do restore;
- Autorizador: Quem concedeu a autorização para execução do restore, sua respectiva função e setor.
- Plano de Retorno: Em caso de algum problema, a quem deve-se avisar e o que deve ser feito a nível técnico para que se retorne à situação/cenário anterior a execução do restore.

VIII. Caso o objetivo do restore destina-se a ambiente de desenvolvimento ou homologação e seja para análise e/ou correção de um problema técnico do sistema, o fato deve ser explicitado no campo Objetivo do referido documento;

IX. O item “b” do documento será atualizado pelo funcionário da área de Infraestrutura e área de Sistemas que procedeu com a solicitação do restore ;

X. O resultado do restore deve ser informado pelo executor através do chamado que originou a solicitação.

XI. Fluxo de solicitação de restore de base:

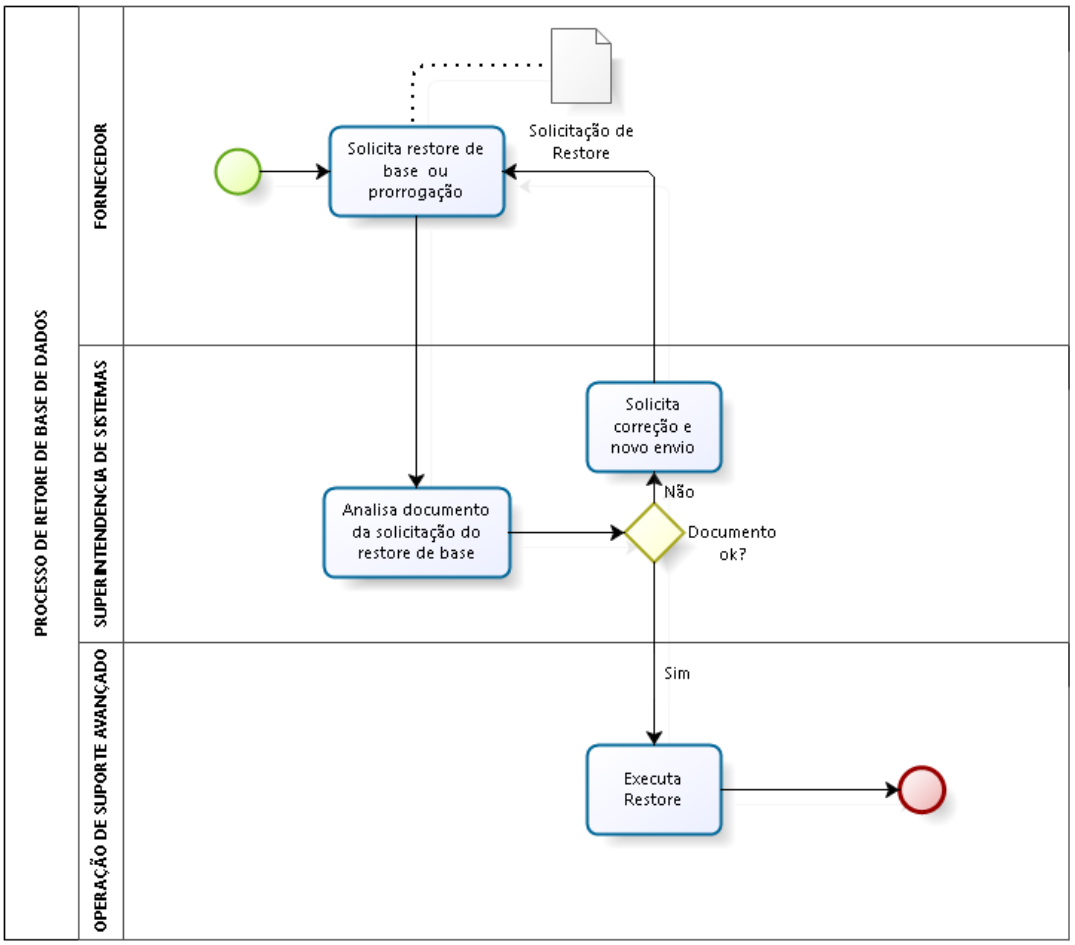

Figura 3 – Fluxo de solicitação de restore de base.

20. SOLICITAÇÃO DE EXECUÇÃO DE SCRIPT

I. O script é uma sequência de comandos que são executados visando a manipulação do ativo de dados dos sistemas legados, para atendimento das diversas solicitações das áreas gestoras, e da manutenção do ambiente de banco de dados, por esse motivo, a definição de regras que direcionem essa atividade é de fundamental importância, fazendo com que seja realizada sem prejuízos aos ativos de dados da instituição.

II. Os scripts podem ser classificados como:

- Script de manutenção e monitoração do ambiente de banco de dados;
- Script de manutenção das bases de dados;
- Script criação de bases de dados (DDL– linguagem de definição de dados);
- Script de criação de objetos de banco de dados (DDL - linguagem de definição de dados);
- Script de consultas (DQL - linguagem de consulta de dados);

- Script de manipulação de bases de dados (DML – linguagem de manipulação de dados);

- Script de criação de usuários e permissão de usuários (DCL – linguagem de controle de dados)

III. A execução de scripts em ambiente de produção somente deve ser realizada em casos em que outra solução não atenda às necessidades do Banco, ou seja, os scripts em produção, somente devem ser executados em último caso.

IV. Sempre que um script for executado de forma recorrente, é obrigação do analista de sistemas (coordenador) verificar a possibilidade da criação de uma funcionalidade no sistema junto ao fornecedor, informando ao gestor (área de negócios) de tal possibilidade, e se for o caso, abrir uma demanda para que a solução definitiva seja implementada.

V. A solicitação da execução de script, preferencialmente deve ser solicitada pela área gestora (área de negócios), por meio de chamados para os analistas de sistemas (coordenadores), que avaliará o pedido e, se for o caso, será solicitado ao fornecedor a criação de um script para resolução do problema. O resultado dessa demanda, sempre deve ser comunicado aos gestores envolvidos, de maneira que os mesmos saibam os impactos gerados.

VI. A solicitação da execução de script pode ser feita pelos coordenadores de sistemas, sempre que eles observarem a necessidade de resolução de algum problema, ficando o mesmo responsável por encaminhar a demanda para o fornecedor realizar a criação do script, bem como avisar a área gestora (Negócios), sobre o procedimento realizado e os impactos causados.

VII. A solicitação da execução de script pode ser feita pelos fornecedores, sempre que eles observarem a necessidade de resolução de algum problema, ficando o mesmo responsável por informar o problema para os analistas de sistemas (coordenadores)e/ou gerente de projetos, e após análise e aprovação do mesmo, o script deverá ser encaminhado para a equipe de DBAs, devidamente autorizado pelos coordenadores ou gerencias imediatas.

VIII. O Prestador de Serviço deve sempre informar ao Gestor do Banco da possibilidade de desenvolvimento de uma nova transação no sistema – a ser executada pelos gestores – que poderá substituir a execução do script em ambiente de produção.

IX. A responsabilidade sobre a qualidade do script é do Prestador de Serviço, ou seja, o Banco não se responsabiliza pelos comandos existentes no mesmo. Dessa forma, o Prestador deve garantir que o script não tenha consequências divergentes das definidas no escopo da solicitação dele. Para tal, o Banco sugere que o Prestador realize um procedimento de dupla validação do script antes de sua execução em produção.

X. Os scripts só devem ser enviados para ambiente de produção por solicitação expressa da superintendência de infraestrutura e/ou da superintendência de sistemas ou quando o Prestador de Serviço identificar a necessidade de envio do mesmo para atender uma necessidade do Banco. No caso da superintendência de infraestrutura e/ou superintendência de sistemas, o analista de sistemas (coordenador)/Gerente de projetos, se responsabiliza por solicitar o script junto ao fornecedor, para posterior envio para execução em Produção, já na hipótese que diz respeito ao prestador de serviço, o mesmo precisa solicitar o envio, para o analista de sistemas (coordenador)/Gerente de projetos responsável ou pela Gerencia responsável da

superintendência de infraestrutura e/ou superintendência de sistemas, que irá avaliar e, se julgar necessário, autorizar a execução.

XI. A responsabilidade sobre a execução integral do script em ambiente de produção é do Banco.

XII. O envio de um novo script para produção deve sempre acompanhar um documento formal de solicitação Formulário de Solicitação anexado em formato .pdf, o qual deve conter as seguintes informações:

- Objetivo: Motivo do script está sendo enviado;
- Resultado esperado: Qual o resultado esperado no sistema após a execução do script, como por exemplo, quantidade de linhas afetadas, estado final de objetos de sistemas e etc.;
- Informações técnicas: Informações de onde o script será executado, como por exemplo, sistema, banco de dados e etc.;
- Script: Comandos do script;
- Resultado da execução do script; será atualizado pelo funcionário da superintendência de infraestrutura e/ou superintendência de sistemas que procedeu com a execução do script em produção;
- Impactos: Sistemas e Funcionalidades que serão impactadas durante a execução do script;
- Tempo estimado para execução do script (com base em ambiente de testes): considerar somente as seguintes opções; até 15 minutos, até 30 minutos, até 1 hora, mais de 1 hora;
- Plano de retorno: O que deve ou pode ser feito caso ocorra algum problema.

XIII. Cada script precisa vir acompanhado de um documento de execução, scripts sem o devido documento serão devolvidos.

XIV. Caso o objetivo do script seja para correção de um problema técnico do sistema, o fato deve ser explicitado no objetivo do Formulário de Solicitação;

XV. A definição do responsável pela autorização do escopo do script ficará a cargo da superintendência de infraestrutura ou da superintendência de sistemas, sendo os possíveis responsáveis, a própria superintendência de infraestrutura, a superintendência de sistemas ou os gestores de sistemas;

XVI. O resultado do script deve ser formatado contendo no mínimo as seguintes informações:

- Servidor de banco de dados que está sendo executado o script;
- Base de dados que será executado o script;
- Nome do criador do script;
- Data/hora da execução do script;
- Número de linhas afetadas;
- Tempo de execução do script.

20.1. Após o envio do script para produção, os solicitantes (analista de sistemas (coordenador) /gerente de projetos e o fornecedor) devem aguardar o documento atualizado com o resultado do mesmo, que será enviado após a execução do script,

tendo o cuidado de observar se o resultado gerado após a execução era de fato o resultado esperado.

XVII. No cabeçalho do script deverá conter o número do chamado na Central de Serviço, como no exemplo abaixo:

```
set serveroutput on;
declare var_host_name varchar2(50);
 var_machine varchar2(50);
 var_osuser varchar2(50);
 var_schema varchar2(50);
begin
select host_name into var_host_name FROM v$instance;
select machine, osuser, username into var_machine, var_osuser, var_schema from v$session where AUDSID = USERENV('SESSIONID');
dbms_output.put_line('-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-');
dbms_output.put_line('Data e Hora Inicial de Atualização: ' || to_char(sysdate,'DD-MM-YYYY HH24:MI:SS') );
dbms_output.put_line('Server: ' || var_host_name);
dbms_output.put_line('Hostname: ' || var_machine);
dbms_output.put_line('User: ' || var_osuser);
dbms_output.put_line(' Schema: ' || var_schema);
dbms_output.put_line('Criador do Script: [Nome do Criador do Script]');
dbms_output.put_line('Sistema de Gerenciamento de Serviços TI: 999999');
dbms_output.put_line('-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-');
end;
/
---------- inserir script ----------
begin
dbms_output.put_line('-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-');
dbms_output.put_line('Data e Hora Final de Atualização: ' || to_char(sysdate,'DD-MM-YYYY HH24:MI:SS') );
dbms_output.put_line('-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-');
end;
```

21. AUTORIZAÇÃO PARA EXECUÇÃO DE SCRIPT

I. Caso o objetivo do script seja a correção de um problema técnico no ambiente de banco de dados, a execução dele será feita pela equipe de DBAs, havendo a necessidade de autorização da Gerência imediata do responsável pelo respectivo sistema dentro do Banco. Caso o procedimento de execução de scripts traga algum tipo de indisponibilidade nos sistemas do Banco, a equipe de DBA's ficará responsável por comunicar as demais gerências e os gestores afetados (Negócio), sobre a medida adotada e os seus respectivos impactos.

II. Caso o objetivo do script envolva regras de negócio do Banco, a superintendência de infraestrutura ou superintendência de sistemas deverá entrar em contato com o gestor do sistema (área de negócios) e solicitar o de acordo formal do escopo do script dele. Após a aprovação, o script deverá ser encaminhado à equipe de DBA's para execução em produção, havendo a necessidade de autorização de um funcionário da equipe responsável pelo sistema no Banco.

III. Caso o script em questão seja um script de DDL, o mesmo deverá ser disponibilizado via SVN para que os DBAs possam executá-lo. Sendo o caminho informado na abertura da RDM.

IV. Caso o script faça parte de uma atualização de versão, a execução do mesmo em produção deve seguir as regras hoje vigentes para atualização de versão.

V. Todas as solicitações deverão ser registradas na Central de Serviços, sendo que serão desconsideradas todas as solicitações efetuadas através de e-mail, ligação telefônica, solicitações verbais ou qualquer outro meio.

VI. Nos casos de serviços urgentes em ambiente de produção, como rotinas que envolvam o processamento noturno ou aqueles onde não seja possível seguir todo o fluxo de documentação e de autorização, a solicitação deverá ser registrada formalmente através do e-mail corporativo enviado pelo funcionário responsável para a equipe de DBA's e mesma fica autorizada a executar o script, sendo o solicitante o total responsável pelas informações necessárias à execução do script, bem como suas consequências. Sendo obrigatório o envio das documentações com as suas respectivas autorizações no dia útil seguinte a execução dele.

VII. Todos os scripts, exceto os que vão impactar no processamento ou na atualização de versões, devem ser encaminhados até as 19:00h, tendo em vista que a partir desse horário, os analistas de sistemas (coordenadores), gerente de projetos, gerentes e superintendentes, na grande maioria das vezes, não estão mais nas dependências da Diretoria de Tecnologia para avaliar e autorizar se for o caso a referida execução.

VIII. Os chamados para execução de scripts, devem ser encaminhados para o grupo de DBAs, ou seja, as solicitações endereçadas a um DBA específico serão devolvidas, devido o problema de controle causado por tal situação.

IX. Caso o chamado tenha mais de 5 scripts, os mesmos devem ser compactados em um único arquivo, tal medida é necessária para agilizar o atendimento e melhorar o controle dos arquivos envidados;

X. Cada chamado deve conter scripts para serem executados em apenas uma base, os chamados que vierem com scripts para execução em bases diferentes serão devolvidos para devida adequação;

XI. Os scripts devem ser numerados, caso não seja possível, os mesmos devem ser encaminhados com nomes diferenciados, visando um melhor controle dos arquivos

encaminhados, sendo assim, scripts enviados com o mesmo nome, serão devolvidos para alteração do nome;

XII. Para realização de consultas simples de dados no ambiente de produção, os fornecedores e os analistas de sistemas (coordenadores) contam com a ferramenta CONSULTABD, tal ferramenta permite que os dados sejam acessados diretamente, sem prévio aviso, para verificação de problemas pontuais, vale destacar que não é possível alterar ou apagar os dados através da ferramenta.

22. NORMAS PARA O PLANO DE CONTINGÊNCIA

I. Caberá ao suporte disponibilizar imagem de todos os servidores físicos de produção.

II. Deverá ser realizado backup de pasta que contém as imagens semanalmente.

III. Deverão ser disponibilizado recursos mínimos para as implementações de testes de disaster recovery, os quais deverão estar disponibilizados em ambiente distante do CPD.

IV. Os coordenadores dos Sistemas deverão elaborar plano de contingência com procedimentos para casos de disaster recovery, os quais deverão ser testados periodicamente.

23. OPERACIONALIZAÇÃO DOS BACKUPS DE AGÊNCIAS E POSTOS

I. Com objetivo de proporcionar maior segurança e preservar os dados gravados nos servidores de Agências e Postos de Serviço, foi implementada uma rotina de backup que visa oferecer uma fonte de contingência.

II. Os jobs do SQL SERVER serão executados diariamente para realização do backup diário três vezes ao dia conforme descrito a seguir:

- 07h00 da manhã após o recebimento das cargas diárias e saída do FEP;
- 19h30 após ida para o FEP;
- 23h30 após o corte da automação (virada de data)

III. Os backups terão retenção de 15 dias.

IV. Para as demais agências ou postos deverá ser adotado as providências a seguir:

- Definir uma estação de trabalho (LS) onde será gravada a cópia de segurança;
- Para obter o nome da estação selecionada deve-se acessar o SPA e verificar no rodapé do monitor o referido número que aparecerá no formato “Terminal: XX”
- Informar para o Atendimento de 1° Nível, através de e-mail endereçado a gerência de serviços, o nome da estação;
- Manter a estação selecionada, obrigatoriamente ligada, por 24 horas, visto que a cópia de segurança será gravada na madrugada;
- A estação poderá ser usada normalmente pelos funcionários durante o expediente;
- No final do expediente o usuário do terminal deverá fazer logoff e desligar somente o monitor.

- Comunicar imediatamente a Atendimento de 1° Nível, através de email, em caso de defeito na estação, para que seja procedida a recuperação do equipamento. Caso o equipamento não seja recuperado em tempo hábil, a Administração da Unidade deverá indicar uma outra estação.

24. ETAPAS DO PROCESSO DE BACKUP

I. Gestor do Sistema solicita que os dados de seu sistema tenham backup para a Operação de Suporte Avançado;

II. Operação de Suporte Avançado realiza avaliação do sistema para identificar qual será a periodicidade dos backups para esse sistema, de acordo com o risco do sistema e a disponibilidade de recursos no Banco;

III. Operação de Suporte Avançado informa a Segurança da Informação da solicitação feita pelo gestor do Sistema para a realização do backup e a periodicidade que será adotada;

IV. Segurança da Informação emite ciência do procedimento;

V. Operação de Suporte Avançado realiza os procedimentos de backup dos dados que foram solicitados pelo Gestor do sistema;

VI. Segurança da Informação deverá solicitar relatórios periódicos a Operação de Suporte Avançado com as evidências de que os Backups estão sendo realizados conforme informado inicialmente, além de demonstrar a integridade dos dados. Por fim, demonstrar que os backups estão prontos para serem restaurados caso ocorra algum tipo de problema dos dados em produção.

25. PAPÉIS E RESPONSABILIDADE DO PROCESSO DE BACKUP

Papéis e responsabilidades relacionados ao processo de solicitação de Backup dos dados dos Sistemas Internos do Banco.

Tabela 203 - Resumo do processo

PAPEL	RESPONSABILIDADES	RESPONSÁVEL
GESTOR DO SISTEMA	• Solicitar o Backup dos dados do seu sistema • Informar quais dados devem ser armazenados em Backup • Solicitar as evidências de que os backups estão sendo feitos regularmente • Solicitar regularmente os resultados de testes de integridades • Solicitar o Restore dos dados, caso seja necessário • Possuir todos os registros dos backups e resultados de testes que diz respeito aos dados de seu sistema	Cada sistema terá um ou mais responsável diferentes. Deverá ser avaliado individualmente
ANALISTA DE SEGURANÇA	• Definir as políticas de *Backup* e *Restore* dos dados dos sistemas internos • Solicitar as evidências de que os backups estão sendo feitos regularmente	NUSIF – SSI – Analista

	• Solicitar regularmente os resultados de testes de integridades dos dados • Solicitar evidências de que tanto os servidores de produção quanto os servidores de backup estão com as demais políticas de segurança sendo seguidas	
SUPERINTENDENCIA DE SISTEMAS	• Receber a solicitação do Gestor e orquestrar a realização dos backups contactando as áreas responsáveis conforme Matriz RACI • Informar a relação técnica dos dados que devem ter os Backups realizados • Acompanhar os procedimentos de *Backup*, *Rollback* e *Restore* para identificação de possíveis erros • Solicitar regularmente os resultados de testes de integridades dos dados	SUSIS
SUPORTE AVANÇADO - DBA	• Receber a solicitação do Gestor e do Gerente de Projetos • Preparar os Scripts que farão o *Backup* dos dados • Realizar os procedimentos de *Backup*, *Rollback* e *Restore* para identificação de possíveis erros • Realizar regularmente os resultados de testes de integridades dos dados	SUPRO – GEINS – Administradores de Banco de Dados
SUPORTE AVANÇADO - SERVIDORES	• Alocar os recursos necessários para receber os Backups • Acompanhar os procedimentos de *Backup*, *Rollback* e *Restore* para identificação de possíveis erros • Disponibilizar os dados em Backup para eventual Restore	SUPRO – GEINS – Analista de Sistemas
AUDITORIA	• Ser informado quando o Gestor solicitar *Backup* ou *Restore* dos dados • Solicitar as evidências de que os backups estão sendo feitos regularmente • Solicitar regularmente os resultados de testes de integridades dos dados	AUDIN
MONITORAMENTO	• Acompanhar os procedimentos de *Backup*, *Rollback* e *Restore* para identificação de possíveis erros • Monitorar os Servidores de Produção e os Servidores de Backup para garantir a máxima disponibilidade	SUPRO – GEMON – Técnicos de Atendimento de TI

Tabela 21 - Matriz de responsabilidade do processo (RACI)

	Gestor Do Sistema	*Analista De Segurança*	*Superintendência de Sistemas*	*Suporte Avançado - DBA*	*Suporte Avançado - Servidores*	*Auditoria*	*Monitoramento*	*Atendimento 1º Nível*
ATIVIDADES								
Solicitação de Backup dos Dados do Sistema	***R***	***C***	***C***	***C***		***I***		
Avaliação do Sistema e dos Dados	***I***		***R***	***I***				
Preparação dos dados que serão feitos o backup e *Script*	***I***			***R***				
Alocação dos Recursos para receber o Backup	***I***				***R***			
Execução procedimento de Backup	***I***		***I***	***R***	***C***		***C***	
Rollback em caso de erro	***I***		***C***	***R***	***C***		***C***	
Teste de integridade periódicos dos dados em Backup	***I***		***I***	***R***		***I***		
Solicitação de *Restore* em caso de falha nos dados em produção	***R***	***C***	***C***			***I***		
Execução de *Restore*	***I***	***A***	***I***	***R***		***I***		
Aprovação da execução do restore em ambiente de produção	R	R						

26. FLUXO DO PROCESSO DE BACKUP

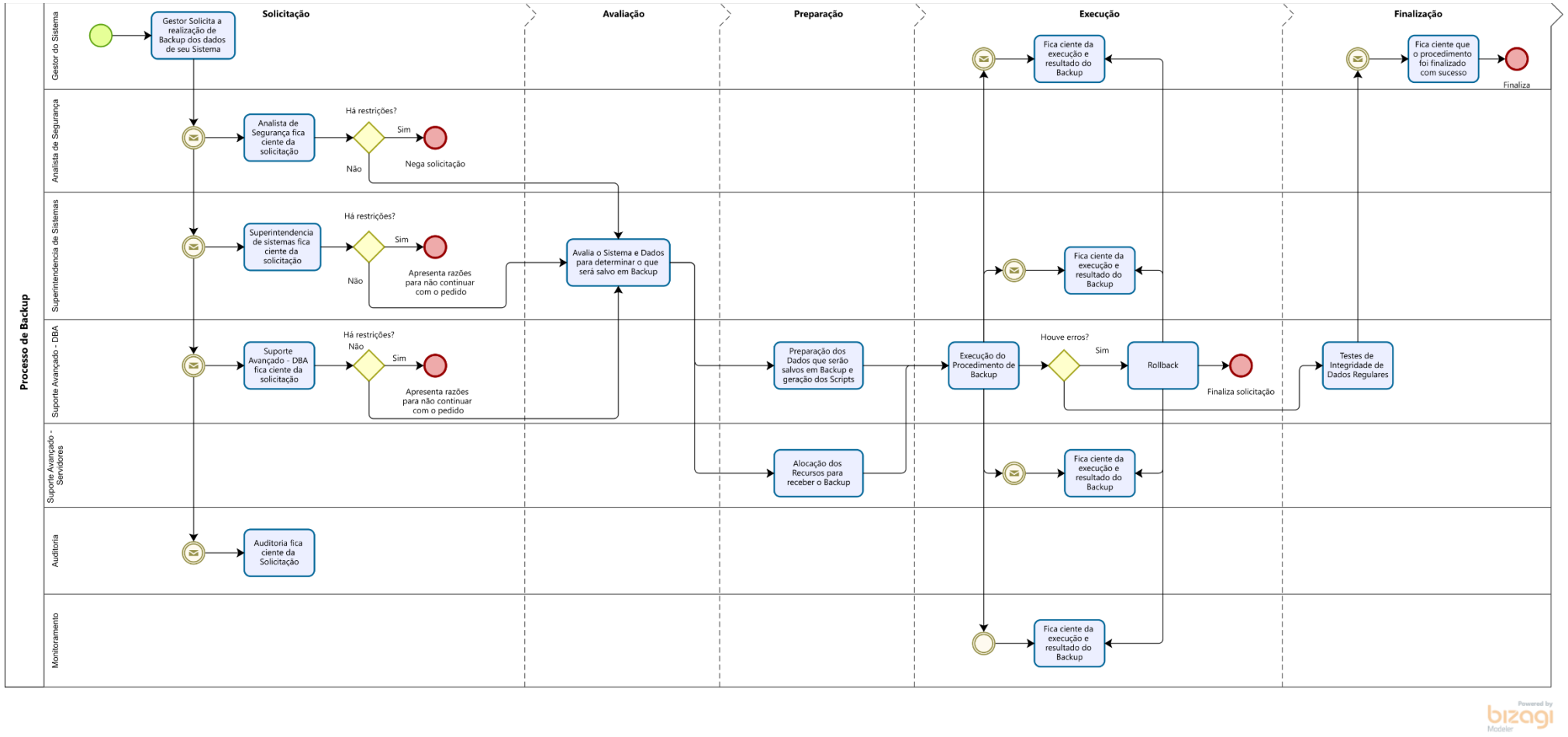

Figura 4 – Fluxo do processo de backup

27. FLUXO DO PROCESSO DE RESTORE

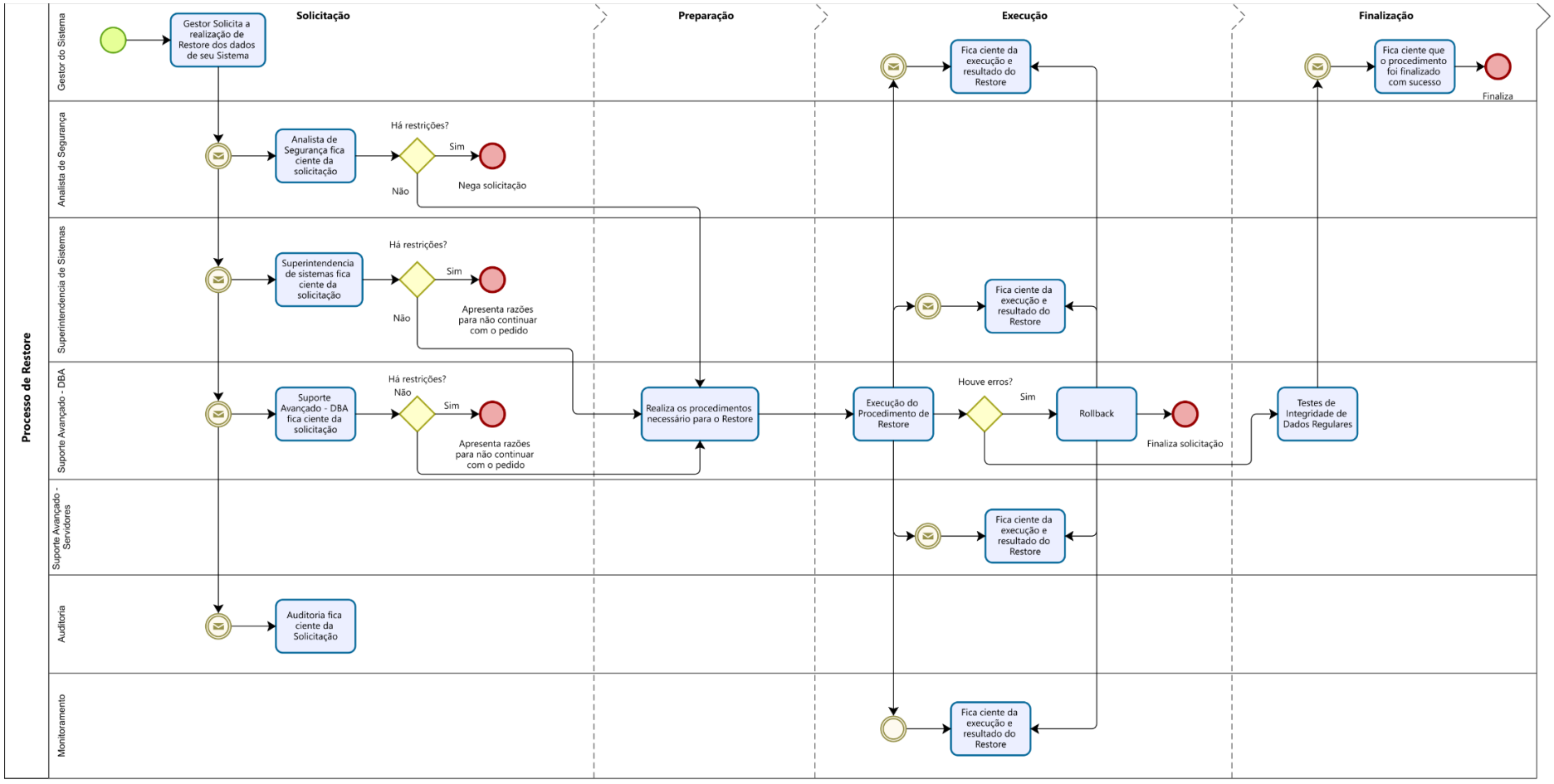

Figura 5 – Fluxo do processo de restore

28. GATILHOS PARA INICIAR O PROCESSO

Tabela 22 - Backup

ENTRADA	Solicitação de Backup de dados
DESCRIÇÃO	A segurança da informação, a superintendência de sistemas e a operação de suporte avançado - DBA irão analisar a solicitação e será atendido pelo suporte avançado - DBA
RESPONSÁVEL	Operação de Suporte Avançado – DBA Segurança da informação
PARTICIPANTE (S)	Superintendência de sistemas Auditoria
PROCEDIMENTO	1 – Avaliar solicitação 2 – Autorizar ou não o backup 3 – Realizar o procedimento para o backup
SAÍDA	Rotina de Backup cadastrado ou não Informação repassada a auditoria.

Tabela 23 - Restore

ENTRADA	Solicitação de Restore de dados
DESCRIÇÃO	A segurança da informação, a superintendência de sistemas e a operação de suporte avançado - DBA irão analisar a solicitação e será atendido pelo suporte avançado - DBA
RESPONSÁVEL	Operação de Suporte Avançado – DBA Segurança da informação
PARTICIPANTE (S)	Superintendência de sistemas Auditoria
PROCEDIMENTO	1 – Avaliar solicitação 2 – Autorizar ou não o restore 3 – Realizar o procedimento para o restore
SAÍDA	Restore realizado ou não Informação repassada a auditoria.

29. METODOLOGIA PARA TESTES DE BACKUP DE BANCO DE DADOS

29.1. NORMAS GERAIS

I. Realizar testes de backup de base de dados regularmente.

II. Garantir que mudanças no banco ou na infraestrutura não afetem os backups.

III. Atualizar a metodologia conforme o banco de dados ou ferramentas sejam modificados.

29.2. PLANEJAMENTO

29.2.1. Definir os objetivos do teste

I. Garantir a integridade e consistência dos dados restaurados.

II. Avaliar o Tempo necessário para recuperação (RTO).

III. Assegurar que o backup atenda ao Ponto Objetivo de Recuperação (RPO).

29.2.2. Determinar o escopo do teste

I. Identificar quais base de dados serão testados.

II. Especificar os tipos de backup a serem testados:

- Backup completo (full).
- Incremental ou diferencial.
- Backup de logs de transações.

29.2.3. Identificar o ambiente de teste

I. Decidir se o teste será realizado em um ambiente de desenvolvimento, homologação ou em um ambiente isolado.

29.2.4. Estabelecer os critérios de sucesso

I. Recuperação completa e funcional da base.

II. Validação de integridade dos dados e consistência transacional.

29.3. PREPARAÇÃO

29.3.1. Inventário de backups:

I. Verificar a periodicidade dos backups disponíveis.

II. Confirmar a existência de backups recentes e sua localização.

29.3.2. Ambiente de teste:

I. Configurar um ambiente seguro e isolado.

II. Garantir que o ambiente simule a configuração de produção, se possível.

29.3.3. Ferramentas necessárias:

I. Confirmar o uso de ferramentas adequadas para backup e restauração (por exemplo, utilitários nativos do banco de dados, como mysqldump, pg_dump, ou soluções de terceiros).

29.3.4. Configurar permissões:

I. Garantir que a equipe de testes tenha acesso apropriado para realizar operações de backup e restauração.

29.4. EXECUÇÃO

29.4.1. Simulação de cenários

I. Excluir dados ou tabelas específicas.

II. Corromper dados deliberadamente.

III. Simular falhas de hardware ou perda de conectividade.

29.4.2. Realizar restauração

I.Restaurar o backup completo.

II. Validar o processo de recuperação incremental ou dos logs de transação, se aplicável.

29.4.3. Validar os dados restaurados

29.4.3.1. **Consistência**

I.Verificar a consistência referencial (chaves estrangeiras, índices, etc.).

29.4.3.2. **Integridade**

I.Comparar amostras de dados restaurados com os originais.

29.4.3.3. **Operacionalidade**

I.Testar consultas e transações no banco restaurado.

29.4.4. Medição de tempos

I.Registrar o tempo de recuperação e compará-lo ao RTO.

29.5. DOCUMENTAÇÃO

29.5.1. Registrar resultados

I.Dados restaurados.

II. Erros encontrados.

III.Logs do processo de backup e restauração.

29.5.2. Elaborar relatório

I.Incluir métricas como tempos de recuperação, tamanho dos backups e eficiência do processo.

29.5.3. Identificar falhas

I.Documentar problemas e propor soluções para melhorar os processos de backup e restauração.

29.6. REVISÃO

29.6.1. Análise da equipe

I.Realizar uma reunião para discutir os resultados e revisar o desempenho.

29.6.2. Comunicação com stakeholders:

I.Compartilhar um resumo dos resultados e recomendações.

29.6.3. Ajustar os procedimentos:

I.Incorporar melhorias com base nos resultados obtidos.

29.7. PERIODICIDADE

29.7.1. Testes Semanais

I.Objetivo: Garantir a legibilidade das fitas de backup e a capacidade de restaurar os dados com sucesso.

II. Aplicação: Realiza-se frequentemente a verificação de uma amostra das fitas de backup, especialmente para sistemas críticos, para assegurar que o processo de recuperação esteja funcionando corretamente.

29.7.2. Testes Mensais

I.Objetivo: Validar a integridade dos backups completos e a eficácia do processo de backup.

II. Aplicação: Realiza-se a recuperação completa de dados de uma fita de backup a cada mês, com o intuito de garantir que a política de retenção está sendo seguida corretamente e que os backups são confiáveis.

29.7.3. Testes Semestrais

I.Objetivo: Executar uma restauração completa em um ambiente de teste, simulando uma recuperação em caso de desastre.

II. Aplicação: Realiza-se uma verificação detalhada do processo de backup e recuperação para identificar possíveis falhas que podem não ser detectadas durante os testes semanais ou mensais.

29.7.4. Testes Anuais

I.Objetivo: Realizar uma auditoria completa dos processos de backup e recuperação.

II. Aplicação: Inclui testes de recuperação de backups arquivados de longo prazo, com o objetivo de validar a integridade dos dados armazenados em fitas ao longo do tempo.

30. ETAPAS DO PROCEDIMENTO DE TESTE DE INTEGRIDADE DE DADOS

I. Após a realização dos procedimentos de Backup, se faz necessária a realização constante de testes integridade desses dados. Esse procedimento visa manter a operação normal do banco em uma eventual necessidade de Restore das bases de dados.

II. As etapas de execução desses testes de integridade são:

- Gerente da Operação de Suporte Avançado monta um cronograma mensal dos dados que precisam ser testados;
- Um dos analistas da Operação de Suporte Avançado realiza o Restore em um ambiente controlado para a realização dos testes de integridade;
- O resultado desse teste é enviado ao Gerente da Operação de Suporte Avançado, ao Gestor do sistema que os dados e a Segurança da Informação;
- Caso algum erro seja encontrado, deverá ser feito imediatamente um novo Backup dos dados de produção para gerar uma cópia integra.

GLOSSÁRIO

Active Directory (AD): fornece um serviço centralizado que liga todas essas máquinas e permite que os usuários possam se logar e acessar qualquer coisa que eles tenham permissão. Os usuários devem receber permissão de acesso para que possam acessar arquivos compartilhados, banco de dados ou mesmo caixas de e-mail.

E-mail: correio eletrônico; recurso que torna possível o envio e recebimento de mensagens pela Internet:

ITSM - IT Service Management (em português, Gerenciamento de Serviços de TI). É um conjunto de práticas, processos e ferramentas usadas para projetar, fornecer, gerenciar e suportar os serviços de Tecnologia da Informação (TI) dentro de uma organização.

LOG (log de dados): é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

Sistema biométrico: sistema que ao invés de usar uma chave (login e senha), é usado o reconhecimento biométrico para ter acesso.

VPN Client-to-Site: permite o acesso a uma rede interna da empresa, com uso seja por terceiro ou funcionário trabalhando em casa usando um software específico.

VPN (Rede Virtual Privada): rede virtual privada que funciona criando uma rede de comunicações entre computadores e outros dispositivos que têm acesso restrito a qum tem as credenciais necessárias.

VPN Site-to-Site: VPN Site a Site também é chamada de VPN Roteador a Roteador e é usada principalmente entre corporações.

RBAC - Role-Based Access Control (ou Controle de Acesso Baseado em Funções, em português). É um modelo de controle de acesso em que os direitos e permissões de acesso a sistemas, dados e recursos são atribuídos com base em funções dentro de uma organização, e não a indivíduos específicos.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2013.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2013.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO IEC 27007 - Diretrizes para auditoria de sistemas de gestão da segurança da informação. ABNT, 2012.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27007 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2012.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 3100 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2018.

BRASIL. Resolução Nº 4.658, 26 de abril de 2018, Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, 30 abr. 2018. Seção 1, p. 26-28.