PROCEDIMENTO DE GESTÃO DE ACESSOS

SUMÁRIO

SUMÁRIO 1

1. OBJETIVO 3

2. ABRANGÊNCIA 3

3. DESCRIÇÃO DOS PROCESSOS 3

3.1. IDENTIFICAÇÃO DE NECESSIDADE PELO USUÁRIO 4

3.1.1. NECESSIDADE 4

3.2. ABERTURA DE CHAMADO 7

3.2.1. ABERTURA E REGISTRO DE CHAMADO NA FERRAMENTA GLPI: 7

3.2.2. DEFINIR A CRITICIDADE DA SITUAÇÃO 8

3.3. ELEMENTOS DO PROCEDIMENTO DE ATENDIMENTO DAS DEMANDAS DE GESTÃO DE ACESSOS 8

3.4. ACESSO FÍSICO AO BANCO BARI 9

3.5. REVISÃO DE PERFIS DE ACESSOS 9

3.6. ADMINISTRAÇÃO DO AMBIENTE INFORMATIZADO 11

3.6.1. AMBIENTE DE REDE (AD) E COMPONENTES DE INFRAESTRUTURA NA NUVEM 11

3.6.1.1. CRIAÇÃO DE USUÁRIO 11

3.6.1.2. ALTERAÇÃO DE USUÁRIO 11

3.6.1.3. RESET DE SENHA DE USUÁRIO 11

3.6.1.4. BLOQUEIO DE USUÁRIO 11

3.6.1.5. LIBERAÇÃO DE ACESSO A DIRETÓRIO DE REDE 12

3.6.1.6. MANUTENÇÃO DE DIRETÓRIO 12

3.6.1.7. GERENCIAR IDS (USUÁRIOS/CONTAS) CRIADAS E USADAS POR TERCEIROS 12

3.6.2. SISTEMAS CORPORATIVOS (PROGNUM, ERSYSTEM, SICRED, LYDIANS, ADMIN, VIRTUAL, CRIVO, CARDS, ELO AQUILA E PORTAL BARIGUI) 13

3.6.2.1. CRIAÇÃO DE USUÁRIO 13

3.6.2.2. MANUTENÇÃO NOS ACESSOS DO USUÁRIO DE SISTEMA 13

3.6.2.3. RESET DE SENHA DE USUÁRIO DE SISTEMA 13

3.6.2.4. BLOQUEIO DE USUÁRIO DE SISTEMA 14

3.6.2.5. GERENCIAR IDS (USUÁRIOS/CONTAS) CRIADAS E USADAS POR TERCEIROS 14

3.7. APROVAÇÕES 14

3.7.1. LISTA DE APROVADORES POR SISTEMA 14

3.8. SLA PARA ATENDIMENTO 14

3.9. CANCELAMENTO DE DEMANDA 15

4. BASE REGULATÓRIA 15

5. CONTROLE DE ALTERAÇÕES 16

6. ANEXOS 16

6.1. ANEXO I – LISTA DE APROVADORES POR SISTEMA 16

1. OBJETIVO

O procedimento de Gestão de Acessos tem como objetivo estabelecer um método de controle para gerenciar os diferentes níveis de acessos lógicos: Ambiente de Rede, Sistemas e Bancos de Dados do Conglomerado Prudencial Bari ("Bari"). Além deste, também visa assegurar que as concessões e alterações em níveis de acessos lógicos sejam realizadas de forma controlada (avaliadas, registradas e aprovadas), reduzindo o risco e impacto nas áreas de negócio.

Empresas que compõem Conglomerado Prudencial Bari:

- Banco Bari de Investimentos e Financiamentos S/A;
- Bari Companhia Hipotecária;
- Bari Securitizadora S/A.

2. ABRANGÊNCIA

Este documento é aplicável ao Departamento de Tecnologia da Informação e às demais áreas do Bari e/ou parceiros e prestadores de serviços terceirizados que atuam em nome do Bari, que venham a solicitar, aprovar e/ou atender demandas associadas a qualquer tipo de acesso ao Ambiente de Rede e Acessos Sistêmicos (camada de aplicação e/ou banco de dados).

3. DESCRIÇÃO DOS PROCESSOS

O Processo de Gestão de Acessos deve ser realizado sempre que identificada necessidade de acesso ao Ambiente de Rede e Acessos Sistêmicos (camada de aplicação e/ou banco de dados), seja pelo Departamento de Tecnologia da Informação ou pelas áreas de negócio.

I. O escopo de Acessos ao Ambiente de rede abrange as solicitações no ambiente informatizado do Bari, considerando novas contratações, solicitação de criação de novos perfis e/ou usuários, qualquer tipo de manutenção e/ou alteração em acessos que venha a ser citada nesse procedimento, incluindo bloqueios e exclusões.

II. O escopo de Gestão de Acessos Sistêmicos (camada de aplicação e banco de dados) abrange todas as solicitações nos sistemas em utilização no

Bari, tais como: cadastro de novos usuários, manutenção de perfis e/ou usuários, revogação/inativação de usuários e/ou perfis e toda e qualquer solicitação de alteração dentro dos Sistemas utilizados pelo Bari.

Os procedimentos são apresentados abaixo:

3.1. Identificação de Necessidade pelo usuário

É necessário identificar a necessidade e em seguida definir qual será a resolução para a mesma, assim se encaminhando para a abertura de demanda.

3.1.1. Necessidade

Uma necessidade é reportada à área de atendimento de demanda, a mesma podendo ser:

a. Criação de Usuário de sistema (Ambientes de Produção, Homologação e Desenvolvimento):

Inserção de novo usuário dentro de qualquer um dos sistemas escopo. Esta solicitação em caso de contratação de novo colaborador deve ser feita diretamente pelo gestor do mesmo ou pelo departamento de recursos humanos (RH). Em caso de solicitação de novo usuário para colaborador já contratado, a mesma deve ser aberta pela área de negócio do colaborador solicitante e passar por aprovação das áreas necessárias.

O procedimento é válido para criação de usuários com acessos privilegiados, ou seja, usuários com acessos de administrador da rede ou sistemas, que possuem acessos e permissões elevadas em comparação ao usuário padrão.

Para criar um usuário deve se usar o primeiro nome seguido do último sobrenome separado por "." (ponto), por exemplo "nome.sobrenome", excluindo do último sobrenome os agnomes, como Filho, Neto, Sobrinho, Junior ou outros. Em caso de existência de usuário equivalente, deve-se avaliar a utilização do primeiro nome acompanhado de outro sobrenome. Caso ainda exista equivalência de outro usuário, deve-se avaliar demais possibilidades no momento da criação, sempre levando em consideração a fácil identificação do usuário.

Importante ressaltar que exceções às diretrizes supracitadas deverão ser consideradas quando o usuário não concordar com o *login* gerado, possuindo a aprovação de seu gestor imediato.

b. Alteração de usuário de sistema:

Esta solicitação deve ser aberta pelo usuário que sofrerá a ação, a mesma passará por aprovação do gestor imediato de sua área de negócio.

c. Criação de Usuário de rede:

Esta solicitação deve ser iniciada diretamente pelo RH no caso de contratação de um novo colaborador, via abertura de chamado na ferramenta GLPI, a solicitação visa liberar os acessos básicos, sendo eles: E-mail, Ambiente de Rede do Bari.

Os acessos em pastas de rede serão liberados conforme solicitação de acesso. Por padrão o colaborador poderá apenas acessar a pasta de sua área e sua pasta pessoal.

Para geração do *login* do usuário, deve-se seguir as diretrizes formalizadas no item 3.1.1.a.

d. Alteração em Usuário de rede:

Uma vez criado, o usuário não deve ser alterado pois as alterações poderão impactar em perfil, e-mail e demais acessos vinculados ao usuário criado.

e. Criação de Perfil:

A criação de um novo perfil deve partir da Área de Negócios, a mesma passará por revisão e/ou aprovação do gestor responsável do módulo ou sistema.

f. Alteração de Perfil já existente:

A solicitação pode partir de qualquer área do Bari, independente da área solicitante, a solicitação passará por revisão e/ou aprovação do gestor responsável do módulo ou sistema.

Importante ressaltar que, a alteração realizada no perfil é refletida para todos usuários que utilizam o mesmo perfil.

g. Revisão de Acessos:

A revisão de acessos será realizada semestralmente pela área de Gestão de Acessos, devendo ser revisados os acessos, perfis de acessos e ações de cada perfil criado nos sistemas escopo. A demanda de revisão, deverá conter a análise e aprovação de todos

gestores e/ou responsáveis por cada grupo de usuários/perfis. Maiores detalhes sobre o processo de revisão de acesso no tópico 3.5.

h. Bloqueio de acesso:

Esta solicitação deve ser feita quando ocorrer qualquer tipo de afastamento de função de um colaborador, ou outra necessidade que venha a ter como ação o bloqueio de acesso, por exemplo: férias, licença maternidade/paternidade e demais licenças, ou qualquer outra atividade que o retire de sua função previamente determinada na solicitação de acesso, como: bloqueio de acesso devido a irregularidades ou vulnerabilidades do sistema. Apenas a área de RH, Gestores da Área de Negócios e Segurança da Informação podem solicitar um bloqueio de acessos sistêmico.

i. Desbloqueio de Acesso:

O desbloqueio deve ser solicitado pela mesma área que solicitou o bloqueio, o mesmo deverá ser solicitado antes do retorno do colaborador para sua função que demande o acesso.

Em caso de bloqueio por irregularidade detectada, uma justificativa ou correção precisa ser aplicada antes que o acesso seja restabelecido.

j. Revogação de Acesso:

A revogação de acesso sistêmico pode ser solicitada apenas pela área de RH, Gestor da Área de Negócios e a área de Segurança da Informação. A solicitação passará por aprovação do respectivo aprovador do solicitante. Exemplo de necessidade de revogação: Desligamento de colaborador.

k. *Reset* de senha:

Após o bloqueio da senha, o usuário não possuirá acesso às ferramentas de gestão para realizar a solicitação de desbloqueio e/ou *reset* de sua senha. A solicitação pode ser feita por qualquer outro usuário, porém, a nova senha e/ou desbloqueio será encaminhado para o gestor do usuário que necessita do *reset* ou desbloqueio da senha.

l. Acesso a componentes de infraestrutura em produção

O acesso em algum componente de produção deverá ser realizado em caso de resolução de problema ou incidente no ambiente, devendo ser temporário e ter finalidade exclusiva relacionada ao incidente ou problema ao qual teve origem. Ao fim da atividade o acesso deverá ser revogado.

Essas atividades também poderão ser realizadas opcionalmente de forma monitorada por algum operador dos times de Cibersegurança ou Infraestrutura de Nuvem (DevSecOps), utilizando sua própria credencial.

3.2. Abertura de chamado

Demandas podem ser abertas por qualquer profissional de qualquer área do Bari, sendo analisadas e tratadas em ordem de criticidade. Demandas da mesma criticidade serão atendidas por ordem cronológica.

Independentemente do tipo de necessidade, a área de atendimento de demanda pode ser acionada pelos seguintes meios:

a) Abertura de demanda via ferramenta gerenciadora de chamados - GLPI;
b) E-mail e/ou Telefone;

Nos casos de abertura de demanda via e-mail ou telefone, a mesma deverá ser criada na ferramenta GLPI pelo atendente titular da demanda. Quando e-mail, o próprio deverá ser anexado junto à demanda (em casos emergenciais e posteriormente registrado no GLPI).

3.2.1. Abertura e registro de chamado na ferramenta GLPI:

a) O usuário solicitante deve acessar o seguinte *link* da ferramenta GLPI para a abertura de demanda:

   Acesso Interno:
   http://helpdesk-banco.barigui.lan/

b) Selecionar a opção que venha a condizer com a necessidade, exemplo: *Reset* de Senha.

c) Todos os campos deverão ser preenchidos com as informações solicitadas.

d) Se possível, incluir anexo referente ao erro, acesso ou necessidade dentro do Sistema, Ambiente de Rede, ou qualquer acesso que o escopo desse procedimento atenda.

3.2.2. Definir a criticidade da situação

Após identificar o tipo de necessidade, a área de atendimento de demanda avalia, classifica e, de acordo com a criticidade, prioriza o atendimento a ser dado. As possíveis classificações que uma necessidade pode receber são:

1. Baixa - é um tipo de necessidade que acontece usualmente, não necessitando de um tratamento urgente. Ex: Revisão de Acesso ou Perfil Sistêmico.

2. Média – solicitação corriqueira, que não possa parar o funcionamento da área de negócios. Ex: Alteração em Usuário.

3. Alta – são demandas de alta urgência, que colocam em risco a continuidade da operação ou as funções que um colaborador previamente foi determinado a realizar. Ex: Reset de Senha ou Cadastro de Novo Usuário.

3.3. Elementos do Procedimento de Atendimento das demandas de Gestão de Acessos

Os elementos do Processo de Gestão de Acessos para as criticidades supra citadas, estão formalizados abaixo:

I. Recebimento do chamado

A primeira etapa do atendimento é o recebimento do chamado, o mesmo será encaminhado automaticamente para a área responsável por seu atendimento – conforme definido na ferramenta GLPI.

II. Aprovadores

Todos os chamados que necessitem de aprovação de seus respectivos aprovadores por área, devem conter no mínimo 50% de aprovação para que venham a ser atendidos. Demandas com menos de 50% de aprovação serão finalizadas sem atendimento pelo atendente responsável pela demanda.

III. Definição de Criticidade

O atendente verifica o chamado e conforme citado acima definirá o nível de criticidade da demanda.

IV. Atendimento do chamado

Após seguir todos os passos anteriores o atendente responsável pela demanda irá seguir o fluxo de atendimento, este deverá seguir todas as informações inseridas no chamado, não ignorando nenhuma necessidade informada.

3.4. Acesso Físico ao Banco Bari

Informações sobre o procedimento de concessão e gestão de Acesso Físico ao ambiente interno e áreas controladas do Bari, encontram-se formalizadas no documento interno Procedimento de Acesso Físico.

3.5. Revisão de Perfis de Acessos

O processo de revisão de acessos ocorre semestralmente e são integrantes do escopo deste processo os seguintes sistemas:

- ErSystem;
- Prognum;
- Sicred;
- Lydians;
- Diretórios de rede (AD);
- Componentes de infraestrutura na nuvem.

A primeira revisão do ano deverá ocorrer entre os meses de Fevereiro e Março e a segunda revisão do ano, deverá acontecer entre os meses de Agosto e Setembro.

No início do período de revisão, a área de Gestão de Acessos irá solicitar a área de Sistemas (TI), a geração do relatório contendo todos os usuários e seus respectivos perfis de acessos dos sistemas ErSystem, Prognum, Sicred e Lydians. Para a área de Infraestrutura de TI, será solicitado todos os usuários de rede e seus respectivos acessos e níveis de acessos aos Diretório de Rede (AD). Para a área de Segurança Cibernética, será solicitado todos os usuários e seus respectivos níveis de acessos nos componentes de infraestrutura na nuvem.

O relatório de perfis dos quatro (4) sistemas escopo deverá listar as seguintes informações:

- Identificação do sistema.
- Identificação dos usuários (User ID e demais informações do usuário – nome, cargo, empresa, entre outros) – todos os usuários dos sistemas devem estar listados no relatório.
- Relação de perfis de acessos associados aos usuários.
- Relação detalhada de atividades que os usuários podem realizar em cada perfil (telas, transações, menus e demais informações que identifiquem as atividades que cada usuário pode realizar no sistema).

A área de Gestão de Acessos enviará, por e-mail, os relatórios de perfis de acessos aos respectivos Gestores/Responsáveis do Bari, para revisão.

Os relatórios de perfis terão, além da descrição dos perfis de acesso dos usuários, os seguintes campos para preenchimento pelos revisores:

Acesso adequado?		
Sim	Não	Observações

O revisor confirmará a adequação dos acessos, ou necessidade de ajustes nos mesmos, com base nos campos acima. Nesta análise, o revisor deve considerar se os acessos dos colaboradores de suas áreas estão adequados para a função que cada profissional desempenha. Acessos excedentes aos necessários e/ou acessos conflitantes às funções realizadas pelo profissional, devem ser sinalizados como indevidos e serem devidamente corrigidos.

Os gestores terão o prazo de 10 (dez) dias para concluir e encaminhar para a área de Gestão de Acessos a revisão realizada.

Caso o prazo de 10 (dez) dias não seja cumprido, a área de Gestão de Acessos encaminhará um e-mail aos revisores que não cumpriram o prazo, com cópia à Diretoria Financeira e ao RH, solicitando a realização e conclusão da revisão.

Após a conclusão da revisão, os revisores irão enviar por e-mail os relatórios de perfis em formato de planilha do Excel (.xlsx) ou Google Spreadsheet, revisados, à Área de Gestão de Acessos.

Os perfis e acessos de Gestores deverão ser revisados por responsável da área de Governança de TI/Segurança da Informação.

A Área de Gestão de Acessos irá ajustar os perfis de acesso conforme os resultados obtidos na revisão.

A Área de Gestão de Acessos irá registrar o processo de revisão semestral de perfis de acesso em um chamado GLPI. Este chamado irá conter como anexos os e-mails enviados pelos gestores com a planilha de perfis revisada.

3.6. Administração do Ambiente Informatizado

3.6.1. Ambiente de rede (AD) e componentes de infraestrutura na nuvem

Ambiente corporativo onde são administrados os usuários e diretórios internos da companhia. Este ambiente é administrado pela área de Infraestrutura de TI.
Ademais, para componentes de infraestrutura na nuvem, estão incluídos nessa classificação servidores, bancos de dados, aplicações e todos os demais componentes e serviços. Estes ambientes são administrados pela área de Segurança Cibernética.
Ambas as áreas oferecem dentro da ferramenta GLPI os recursos abaixo que dão suporte a operação do Bari.

3.6.1.1. Criação de Usuário

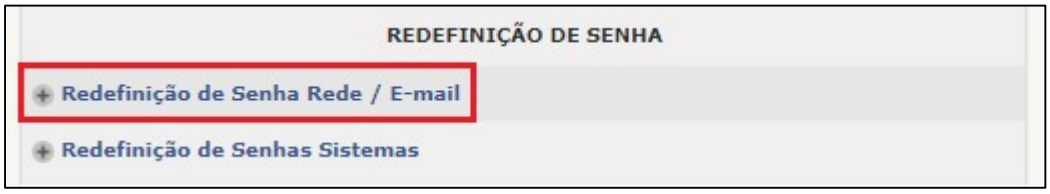
Esta solicitação deve ser iniciada diretamente pelo RH no caso de contratação de um novo colaborador, a solicitação visa liberar os acessos básicos, sendo eles: E-mail e Ambiente de Rede do Bari.

3.6.1.2. Alteração de Usuário

Uma vez criado, o usuário não pode ser alterado pois as alterações poderão impactar em perfil, e-mail e demais acessos vinculados ao usuário.

3.6.1.3. Reset de Senha de Usuário

Esta solicitação deve ser realizada quando a senha de rede do usuário expira ou é bloqueada por motivo indefinido. Esta solicitação pode ser realizada por qualquer usuário via abertura de chamado na ferramenta GLPI, selecionando a opção: Redefinição de Senha > Redefinição de Senha Rede / E-mail.



3.6.1.4. Bloqueio de Usuário

Esta solicitação deve ser feita via e-mail (controleacessos@bariguifinanceira.com.br) ou via abertura de chamado na ferramenta GLPI, quando ocorrer qualquer tipo de afastamento de função de um

colaborador, ou outra necessidade que venha a ter como ação o bloqueio de acesso. Apenas a área de RH, Gestores da Área de Negócios e Área de Segurança da Informação podem solicitar um bloqueio de acessos de rede do usuário.

3.6.1.5. Liberação de Acesso a Diretório de Rede

Esta solicitação pode ser realizada por qualquer área de negócio ou usuário via abertura de chamado na ferramenta GLPI, informando o nome e caminho completo do diretório (exemplo: V:\Governança de TI\Procedimentos de TI) e login do usuário que deseja acesso. É importante inserir no chamado de liberação, informações de nível de acesso desejado na pasta (exemplo: Somente Leitura, Acesso Total e etc.) – A solicitação de liberação é sujeita a conferência e aprovação de gestor responsável pela pasta.

3.6.1.6. Manutenção de Diretório

Esta solicitação pode ser realizada por qualquer área de negócio ou usuário via abertura de chamado na ferramenta GLPI, informando a solicitação que necessita. Exemplo: Alteração de nível de acesso de determinado usuário, atribuição de novos usuários e entre outros.

3.6.1.7. Gerenciar IDs (usuários/contas) criadas e usadas por terceiros

Usuários/Contas utilizadas por fornecedores, provedores de serviços ou parceiros de negócio para acessar, dar suporte ou manter os componentes do sistema por meio de acesso remoto deve ser realizada da seguinte forma:

- As contas deverão estar ativadas apenas durante o período necessário e desativado imediatamente quando não estiver em uso.
- As contas deverão ser monitoradas quando em uso.

3.6.2. Sistemas Corporativos (Prognum, ERSystem, Sicred, Lydians, Admin, Virtual, Crivo, Cards, ELO Aquila e Portal Barigui)

3.6.2.1. Criação de usuário

Esta solicitação pode ser realiza pelo gestor do solicitante ou o próprio usuário solicitante – quando esta última ocorrer, a solicitação deverá conter a aprovação do gestor do solicitante e do responsável pelo sistema solicitado acesso. A solicitação deve ser realizada via abertura de chamado na ferramenta GLPI, selecionando a opção: Permissão de Acessos Sistemas > Liberação de Acesso (Sistema requerido).

3.6.2.2. Manutenção nos acessos do usuário de sistema

Esta solicitação pode ser realizada por qualquer área de negócio ou usuário quando identificado a necessidade de alterações de permissões e/ou acessos no perfil. A solicitação deve ser realizada via abertura de chamado na ferramenta GLPI, selecionando a opção "Permissão de Acessos Sistemas > Liberação de Acesso (Sistema requerido) > Alteração de Perfil".

3.6.2.3. Reset de senha de usuário de sistema

Esta solicitação deve ser realizada quando a senha de sistema do usuário expira ou é bloqueada por motivo indefinido. Esta solicitação pode ser realizada por qualquer usuário via abertura de chamado na ferramenta GLPI, selecionando a opção: Redefinição de Senha > Redefinição de Senhas Sistemas.

3.6.2.4. Bloqueio de usuário de sistema

Esta solicitação deve ser feita via e-mail (controleacessos@bancobari.com.br) ou via abertura de chamado no GLPI, quando ocorrer qualquer tipo de afastamento de função de um colaborador, ou outra necessidade que venha a ter como ação o bloqueio de acesso. Apenas a área de RH, Gestores da Área de Negócios e Área de Segurança da Informação podem solicitar um bloqueio de acessos de rede do usuário.

3.6.2.5. Gerenciar IDs (usuários/contas) criadas e usadas por terceiros

A utilização de contas/usuários de fornecedores, provedores de serviços ou parceiros de negócio para acessar, dar suporte ou manter os componentes do sistema por meio de acesso remoto devem seguir as diretrizes conforme estabelecidas no item 3.6.1.7.

3.7. Aprovações

Todo chamado será encaminhado automaticamente para aprovação antes de qualquer tipo de atendimento. Essa aprovação será feita pelo devido aprovador/gestor do Sistema ou Área que o acesso foi solicitado.

Os Aprovadores das demandas são definidos pela Área de Negócios, ou caso solicitado algum perfil referente à sua área. Caso algum dos aprovadores, sendo ele da área de negócios ou do perfil solicitado, negue o chamado, o chamado será cancelado.

Exemplo: Gestor de Projetos efetuou a abertura de um chamado solicitando acesso ao sistema Prognum, dentro do Perfil Contabilidade. O aprovador/gestor da Contabilidade e o aprovador/gestor da área de negócio do solicitante deverão aprovar o chamado. Caso algum dos dois neguem, o chamado será negado.

3.7.1. Lista de Aprovadores por Sistema

Informações sobre a relação de aprovadores por sistemas do Bari, encontra-se formalizada no documento: Lista de Aprovadores por Sistema (Anexo I).

3.8. SLA para Atendimento

O SLA (*Service Level Agreement* ou Acordo de Nível de Serviço), é definido conforme o nível de criticidade da demanda, que foi definida previamente em atendimento pelo responsável da mesma.

I. **Baixa:** Este tipo de solicitação tem o prazo máximo de atendimento de 3 dias, sendo apenas contado dias úteis. Demandas abertas entre as 06:00 e as 19:00 seguirão o SLA normal, demandas abertas fora deste horário serão repassadas para o próximo horário de funcionamento, contando como primeiro dia de SLA.

II. **Média:** Este tipo de solicitação tem o prazo máximo de atendimento de 2 dias úteis. Demandas abertas entre as 06:00 e as 19:00 seguirão o SLA normal, demandas abertas fora deste horário serão repassadas para o próximo horário de funcionamento, contando como primeiro dia de SLA.

III. **Alta:** Este tipo de solicitação tem o prazo máximo de atendimento de 1 dia. Demandas abertas entre as 06:00 e as 19:00 seguirão o SLA normal, demandas abertas fora deste horário serão atendidas em primeira hora hábil de atendimento.

3.9. Cancelamento de Demanda

Uma demanda será cancelada apenas sob uma das seguintes condições:

- Não inserção de alguma informação necessária para atendimento do chamado.
- Inserção de informações incorretas.
- Solicitação divergente da escolhida previamente em menu de demandas. Exemplo: Em menu de abertura foi escolhido Sistema Prognum, mas no texto formalizado de observações foi solicitado atendimento ao Sistema Lydians.
- Solicitar mais de uma ação dentro de mesmo chamado acarretará no cancelamento do chamado, nova solicitação deverá ser aberto um novo chamado.

4. BASE REGULATÓRIA

- **Resolução nº 2.554** do Conselho Monetário Nacional, de 24.09.1998 – Dispõe sobre a implantação e implementação de sistema de controles internos;
- **Resolução nº 4.557** do Conselho Monetário Nacional, de 23.02.2017 – Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital;
- **Política de Segurança da Informação e Cibernética** – Tem o objetivo de promover as práticas de segurança para o trânsito das informações no âmbito do Bari, na forma de diretrizes e normas, para o trato de seus ativos e passivos, disseminando uma cultura de segurança das

informações entre seus colaboradores, mantendo a segurança dos sistemas, a integridade e disponibilidade dos dados, a confidencialidade das informações, a continuidade dos negócios e a aderência às leis e normas que regulamentam os serviços financeiros;

- ITIL - *Information Technology Infrastructure Library* (modelo de boas práticas para gestão de serviços de TI)
- COBIT - Control Objectives For Information and Related Technology – "Framework" de boas práticas para Governança e Gestão de TI.
- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação.
- ABNT NBR ISO/IEC 27002:2013 – Código de Prática para Gestão da Segurança da Informação.

5. CONTROLE DE ALTERAÇÕES

VERSÃO	MOTIVO	DATA
v001	Criação do Procedimento	23/12/2020
v002	Atualização – Substituição dos POPs: TI 01 - Revisão de Perfis de Acesso aos principais sistema transacionais financeiros; TI 03 - Gestão de Acessos ao Ambiente Informatizado; e TI 04 - Gerenciamento de Acessos Privilegiados e usuários não nominais	19/07/2021

6. ANEXOS

6.1. Anexo I – Lista de Aprovadores por Sistema