1 OBJETIVO

Estabelecer diretrizes e procedimentos para o controle de acesso de fornecedores, prestadores de serviços, consultores e demais terceiros aos recursos físicos e lógicos, sistemas e informações da organização, garantindo que o acesso seja limitado estritamente ao necessário para a execução de suas atividades, minimizando riscos de segurança da informação e assegurando auditabilidade completa.

2 APLICAÇÃO

Sistema: SGI – NBR ISO 9001: 2015 / NBR ISO 14001:2015 / NBR ISO 27001:2022 / NBR ISO 45001:2024
LQN - NBR ISO/IEC 17025

Site: ☒ Betim / MG ☒ Manaus / AM ☒ Outro / BR

3 HISTÓRICO DE REVISÃO

Rev.	Data emissão	Válido a partir de	Descrição	Revisado por
01.000	22/01/2026	26/01/2026	Publicação inicial	Saulo Lima / 11618

4 DEFINIÇÕES / REFERÊNCIAS

Siglas:

- **PoLP**: Princípio do Menor Privilégio;
- **SoD:** *Separation of Duties* (Separação de Funções);
- **MFA:** *Multi-Factor Authentication* (Autenticação Multifatorial);
- **NDA:** *Non-Disclosure Agreement* (Acordo de Confidencialidade);
- **SLA:** *Service Level Agreement* (Acordo de Nível de Serviço);
- **VPN:** *Virtual Private Network* (Rede Privada Virtual);
- **GLPI**: *Gestionnaire Libre de Parc Informatique* (Sistema para Gestão de Ativos de T.I. [Inventário] e Service Desk [Help Desk]);
- **DPO:** *Data Protection Officer* (Encarregado de Proteção de Dados).

Termos:

- **Fornecedor/Terceiro:** Qualquer pessoa física ou jurídica externa à organização que necessite acesso aos recursos, sistemas ou informações para executar serviços contratados.
- **Acesso Temporário:** Permissão de acesso com prazo definido de validade, automaticamente revogada ao término do período ou conclusão do serviço.
- **Acesso Supervisionado:** Acesso que requer acompanhamento presencial de um colaborador interno durante toda a execução das atividades.

- **Segregação de Rede:** Isolamento lógico de fornecedores em rede separada da rede corporativa, com controles específicos de segurança.
- **Conta Nominativa:** Conta de acesso individual e não compartilhada, vinculada a um usuário específico identificável.
- **Patrocinador Interno:** Colaborador responsável pela solicitação, aprovação e acompanhamento do acesso de terceiros.

Referências:

- **ISO/IEC 27001:2022** - Sistema de Gestão de Segurança da Informação;
- **ISO/IEC 27002** - Código de Prática para Controles de Segurança da Informação;
- **LGPD** - Lei nº 13.709/2018 - Lei Geral de Proteção de Dados;
- **ITIL v4** - Framework de Gerenciamento de Serviços de TI;
- **NIST SP 800-53** - Controles de Segurança para Sistemas de Informação;
- **Política de Controle de Acesso** - Documento base da organização.

5 DESCRIÇÃO/TEXTO NORMATIVO

5.1 Princípios Fundamentais:

5.1.1 Princípio do Menor Privilégio (PoLP)

Fornecedores e terceiros devem receber apenas as permissões mínimas necessárias para executar as tarefas específicas contratadas, sem acesso a recursos ou informações não relacionadas ao escopo do serviço.

5.1.2 Princípio da Necessidade de Saber

O acesso a dados e sistemas deve ser concedido exclusivamente com base na necessidade de conhecer informações específicas relacionadas ao trabalho contratado.

5.1.3 Princípio de Segregação

Fornecedores devem operar em ambientes segregados sempre que possível, isolados da rede corporativa principal e de sistemas críticos não relacionados ao seu escopo.

5.1.4 Princípio de Rastreabilidade

Todas as atividades de fornecedores devem ser rastreáveis através de logs, contas nominativas e registros de auditoria.

5.1.5 Princípio de Temporalidade

Todo acesso de terceiros é, por natureza, temporário e deve ter prazo de validade definido, com revogação automática ao término.

5.2 Classificação de Fornecedores e Terceiros

5.2.1 Nível 1 - Crítico

Características:

- Acesso a dados sensíveis ou confidenciais;
- Acesso a sistemas críticos de negócio;
- Manipulação de dados pessoais (LGPD);
- Acesso a infraestrutura de TI.

Exemplos: Desenvolvedores, DBAs terceirizados, consultores de segurança e auditores.

5.2.2 Nível 2 - Moderado

Características:

- Acesso limitado a sistemas não críticos;
- Manipulação de dados não sensíveis;
- Serviços de suporte técnico;
- Acesso supervisionado a áreas restritas.

Exemplos: Suporte de software, técnicos de manutenção e consultores de processos.

5.2.3 Nível 3 - Básico

Características:

- Acesso apenas a áreas públicas ou recursos não sensíveis;
- Sem manipulação de dados corporativos;
- Acesso físico limitado a áreas comuns.

Exemplos: Prestadores de serviços gerais, fornecedores de insumos e visitantes técnicos.

5.3 Processo de Solicitação e Aprovação de Acesso

5.3.1 Responsabilidades na Solicitação

Patrocinador Interno (Solicitante):

- Gestor da área contratante do serviço;
- Responsável por solicitar o acesso via chamado GLPI;
- Justificar a necessidade de acesso;
- Definir escopo e prazo do acesso;
- Acompanhar execução do serviço;
- Validar conclusão e solicitar revogação;

Informações Obrigatórias na Solicitação:

- Nome completo do fornecedor/terceiro;
- CPF/CNPJ;
- Empresa representada;

- Contato (e-mail corporativo e telefone);
- Escopo detalhado do serviço;
- Justificativa técnica para cada acesso solicitado;
- Sistemas e recursos necessários;
- Tipo de acesso (leitura, escrita, administrativo);
- Prazo inicial e final do acesso;
- Nível de classificação (1, 2 ou 3);
- Necessidade de acesso remoto (VPN);
- Necessidade de acesso físico.

5.3.2 Prazo para Solicitação

Nível 1 (Crítico): Mínimo 10 dias úteis de antecedência;

Nível 2 (Moderado): Mínimo 5 dias úteis de antecedência;

Nível 3 (Básico) Mínimo 3 dias úteis de antecedência.

5.3.3 Fluxo de Aprovação

Etapa 1 - Análise pelo CSTI:

- Validação técnica da solicitação;
- Verificação de viabilidade;
- Análise de riscos de segurança;
- Estimativa de tempo para provisionamento.

Etapa 2 - Aprovação Hierárquica

Nível 1: Aprovação obrigatória do Gestor de Segurança da Informação + Diretor da área;

Nível 2: Aprovação do Gestor da área solicitante;

Nível 3: Aprovação automática via CSTI.

Etapa 3 - Documentação Legal

- Assinatura de NDA (Acordo de Confidencialidade);
- Termo de Responsabilidade Digital;
- Aceite de Políticas de Segurança da Informação;
- Termo de LGPD (quando aplicável).

Etapa 4 - Provisionamento

- Criação de conta nominativa;
- Configuração de permissões mínimas;
- Ativação de MFA (quando aplicável);
- Segregação de rede;

- Registro em sistema de auditoria;

5.4 Tipos de Acesso e Controles

5.4.1 Acesso Lógico

Controle de Acesso a Sistemas:

- Contas nominativas obrigatórias (proibido compartilhamento);
- Senhas robustas conforme política corporativa;
- MFA obrigatório para acessos Nível 1;
- Expiração automática de credenciais ao fim do prazo;
- Desativação automática após 30 dias de inatividade.

Acesso Remoto (VPN)

- Segregação obrigatória em VLAN específica para terceiros;
- Acesso restrito apenas aos recursos autorizados;
- Proibição de acesso à rede corporativa interna;
- Monitoramento em tempo real de conexões;
- Logs detalhados de todas as atividades.

Acesso a Dados

- Princípio do menor privilégio estritamente aplicado;
- Acesso somente leitura quando suficiente;
- Proibição de download de dados sem autorização específica;
- Criptografia obrigatória para dados sensíveis;
- DLP (Data Loss Prevention) ativado.

5.4.2 Acesso Físico

Áreas Comuns:

- Crachá de visitante claramente identificado;
- Acompanhamento opcional;
- Acesso durante horário comercial.

Áreas Restritas

- Crachá temporário com permissões específicas;
- Acompanhamento obrigatório por patrocinador interno;
- Registro de entrada e saída;
- Acesso apenas durante período autorizado.

Áreas Críticas (Datacenter, CPD, Sala de Servidores)

- Autorização prévia da Gestão de TI;
- Acompanhamento obrigatório por equipe de TI;
- Biometria + crachá + autorização eletrônica;
- Vídeo monitoramento obrigatório;
- Proibição de dispositivos eletrônicos pessoais;
- Registro detalhado de atividades executadas.

5.4.3 Acesso a Dispositivos

Equipamentos Corporativos:

- Proibido uso de equipamentos pessoais;
- Equipamentos fornecidos pela organização com controles de segurança;
- Monitoramento de atividades;
- Bloqueio de USB e dispositivos removíveis;
- Antivírus e políticas de segurança aplicadas.

Dispositivos Pessoais (BYOD)

Proibido para acessos Nível 1:

- Permitido apenas para Nível 2 e 3 com aprovação específica;
- Conformidade com política de BYOD corporativa;
- MDM (Mobile Device Management) obrigatório;
- Segregação de dados corporativos.

5.5 Controles de Segurança Específicos

5.5.1 Autenticação e Autorização

Métodos de Autenticação por Nível:

Nível 1: MFA obrigatório (senha + token/SMS/app autenticador);

Nível 2: Senha forte + possibilidade de MFA;

Nível 3: Senha forte.

Política de Senhas para Terceiros:

- Mínimo 12 caracteres;
- Combinação de letras, números e caracteres especiais;
- Proibição de senhas triviais ou sequenciais;
- Troca obrigatória a cada 60 dias para acessos prolongados;
- Proibição de reutilização das últimas 5 senhas.

5.5.2 Segregação de Ambientes

Ambientes Separados

- Rede segregada para terceiros (VLAN específica);
- Acesso direto à internet separado da rede corporativa;
- Ambientes de desenvolvimento/homologação isolados de produção;
- Proibição de acesso simultâneo a múltiplos ambientes.

Princípio de Isolamento

- Terceiros não podem visualizar recursos de outros terceiros;
- Acesso somente aos sistemas específicos do contrato;
- Firewall com regras específicas por fornecedor.

5.5.3 Proteção de Dados Sensíveis

Classificação de Dados

Dados Públicos: Acesso permitido com autorização básica;

Dados Internos: Acesso mediante NDA e justificativa;

Dados Confidenciais: Acesso restrito com aprovação executiva;

Dados Restritos/Críticos: Acesso excepcional com controles rigorosos.

Controles de Proteção

- Criptografia em trânsito (TLS 1.3+);
- Criptografia em repouso para dados sensíveis;
- Mascaramento de dados em ambientes de teste;
- Proibição de cópia para dispositivos pessoais;
- *Watermarking* em documentos confidenciais.

5.5.4 Controle de Dispositivos Removíveis

USB e Mídias Externas

Bloqueio total para acessos Nível 1 a sistemas críticos

- Autorização específica e registrada para uso;
- Scanning obrigatório de antivírus;
- Criptografia obrigatória de dados;
- Log de todas as transferências.

5.6 Monitoramento e Auditoria

5.6.1 Monitoramento Contínuo

Atividades Monitoradas

- Todas as conexões e desconexões de VPN;
- Acessos a sistemas e aplicações;

- Tentativas de acesso negadas;
- Transferência de arquivos;
- Modificações em dados ou configurações;
- Comandos executados em servidores;
- Acesso a áreas físicas restritas.

Alertas Automáticos

- Tentativa de acesso fora do horário autorizado;
- Acesso a recursos não autorizados;
- Download de volume anormal de dados;
- Múltiplas tentativas de login falhadas;
- Atividades suspeitas ou anomalias comportamentais;
- Acesso de localizações geográficas não esperadas.

5.6.2 Logs e Registros

Retenção de Logs

- **Logs de acesso:** 12 meses mínimo;
- **Logs de modificações críticas:** 24 meses;
- **Registros de auditoria:** 5 anos (conformidade regulatória).

Informações Registradas

- Data e hora de acesso;
- Identificação do usuário (conta nominativa);
- IP de origem e localização;
- Recursos acessados;
- Ações executadas;
- Duração da sessão;
- Patrocinador interno responsável.

5.6.3 Auditoria Regular

Frequência de Auditoria

Nível 1: Auditoria mensal obrigatória;

Nível 2: Auditoria trimestral;

Nível 3: Auditoria semestral.

Escopo da Auditoria

- Revisão de todos os acessos ativos;
- Validação de conformidade com escopo contratado;

- Verificação de acessos não utilizados;
- Análise de logs de atividades;
- Identificação de anomalias ou violações;
- Verificação de documentação (NDA, termos).

Responsável pela Auditoria

- Equipe de Segurança da Informação;
- Auditoria Interna;
- Gestor da área contratante (validação).

5.7 Gestão do Ciclo de Vida do Acesso

5.7.1 Renovação de Acesso

Processo de Renovação

- Solicitação via chamado CSTI 10 dias antes do vencimento;
- Justificativa atualizada da necessidade;
- Revisão e aprovação pelos mesmos níveis hierárquicos;
- Auditoria de atividades do período anterior;
- Renovação de documentação legal (NDA, termos).

Prazo Máximo de Acesso

Nível 1: Máximo 6 meses (renovação obrigatória após);

Nível 2: Máximo 12 meses;

Nível 3: Conforme contrato de serviço.

5.7.2 Modificação de Acesso

Expansão de Permissões

- Nova solicitação via chamado CSTI;
- Justificativa técnica detalhada;
- Aprovação conforme nível de classificação;
- Auditoria de necessidade real.

Redução de Permissões

- Aplicação imediata quando identificada permissão excessiva;
- Notificação ao patrocinador e fornecedor;
- Registro no sistema de auditoria.

5.7.3 Revogação de Acesso

Revogação Programada

- Desativação automática ao término do prazo;
- Notificação prévia 5 dias antes (ao patrocinador e fornecedor);
- Backup de dados críticos (se aplicável);
- Validação de conclusão de atividades.

Revogação Imediata

Deve ocorrer imediatamente nos seguintes casos:

- Término antecipado de contrato;
- Violação de políticas de segurança;
- Tentativa de acesso não autorizado;
- Comportamento suspeito ou fraudulento;
- Rescisão de vínculo do fornecedor com empresa prestadora;
- Solicitação do patrocinador interno;
- Determinação de auditoria ou segurança.

Procedimento de Revogação

1. Bloqueio imediato de credenciais;
2. Desativação de VPN e acessos remotos;
3. Revogação de permissões em sistemas;
4. Bloqueio de crachá de acesso físico;
5. Notificação ao patrocinador e fornecedor;
6. Registro detalhado no sistema;
7. Auditoria final de atividades;
8. Arquivamento de logs.

5.8 Gestão de Acessos Emergenciais

5.8.1 Definição de Emergência

Situações que caracterizam acesso emergencial:

- Incidentes críticos de segurança ou disponibilidade;
- Falhas em sistemas críticos de negócio;
- Desastres ou situações de contingência;
- Necessidade de resposta imediata (< 4 horas).

5.8.2 Processo Emergencial

Solicitação

- Via chamado CSTI marcado como "EMERGENCIAL";
- Contato telefônico com gestor de TI;
- Justificativa detalhada da emergência.

Aprovação Acelerada

- Aprovação verbal do Diretor de TI;
- Documentação formal em até 24 horas;
- Registro obrigatório da justificativa.

Controles Reforçados

- Monitoramento em tempo real obrigatório;
- Acompanhamento presencial quando possível;
- Gravação de sessão (quando tecnicamente viável);
- Log detalhado de todas as ações;
- Auditoria imediata pós-resolução.

Prazo Máximo

- 72 horas para acesso emergencial;
- Conversão para acesso regular se necessário continuar.

5.9 Controles Contratuais

5.9.1 Cláusulas Obrigatórias em Contratos

Todo contrato com fornecedores/terceiros que necessitem acesso deve incluir:

- Segurança da Informação;
- Conformidade com políticas de segurança da organização;
- Responsabilização por violações de segurança;
- Obrigação de confidencialidade (NDA);
- Direito de auditoria pela organização;
- Penalidades por não conformidade.

Proteção de Dados (LGPD/GDPR)

- Papel do fornecedor (operador/controlador);
- Obrigações de proteção de dados pessoais;
- Notificação obrigatória de incidentes;
- Exclusão de dados ao término do contrato;
- Conformidade com legislação aplicável.

Gestão de Acessos

- Uso exclusivo de contas nominativas;
- Proibição de compartilhamento de credenciais;
- Obrigação de notificar mudanças na equipe;
- Aceite de monitoramento de atividades;

- Revogação imediata em caso de violação.

5.9.2 Acordo de Nível de Serviço (SLA)

Para fornecedores críticos (Nível 1):

- Tempo máximo de resposta a incidentes;
- Disponibilidade esperada dos serviços;
- Horários de atendimento;
- Canais de comunicação;
- Procedimentos de escalação.

5.10 Capacitação e Conscientização

5.10.1 Treinamento Obrigatório

Antes da Concessão de Acesso

Todo fornecedor/terceiro deve participar de treinamento sobre:

- Políticas de Segurança da Informação da organização;
- Boas práticas de segurança digital;
- Responsabilidades e obrigações;
- Procedimentos de reporte de incidentes;
- Consequências de violações.

5.10.2 Conscientização Contínua

Ações Periódicas:

- Comunicados sobre ameaças e vulnerabilidades;
- Lembretes sobre políticas de segurança;
- Campanhas de conscientização;
- Simulações de phishing (para Nível 1).

5.11 Gestão de Incidentes Envolvendo Terceiros

5.11.1 Tipos de Incidentes

Incidentes de Segurança

- Tentativa de acesso não autorizado;
- Vazamento ou exposição de dados;
- Violação de políticas de segurança;
- Instalação de malware ou software não autorizado;
- Ataques ou tentativas de sabotagem.

Incidentes de Conformidade

- Descumprimento de NDA;
- Violação de LGPD/GDPR;
- Não conformidade com políticas corporativas;
- Compartilhamento indevido de credenciais.

5.11.2 Procedimento de Resposta

Detecção e Classificação:

1. Identificação do incidente;
2. Classificação de severidade (baixa, média, alta, crítica);
3. Isolamento imediato se necessário;
4. Notificação ao patrocinador e gestor de segurança.

Contenção:

1. Bloqueio imediato de acesso do terceiro envolvido;
2. Preservação de evidências (logs, registros);
3. Análise de impacto e extensão;
4. Contenção de propagação.

Investigação:

1. Análise detalhada de logs e evidências;
2. Identificação de causa raiz;
3. Avaliação de danos e comprometimento;
4. Documentação completa do incidente.

Recuperação e Remediação:

1. Correção de vulnerabilidades exploradas;
2. Restauração de sistemas afetados;
3. Reforço de controles de segurança;
4. Decisão sobre continuidade do acesso.

Comunicação:

- Notificação ao DPO (se envolver dados pessoais);
- Comunicação à ANPD (se aplicável LGPD);
- Notificação à alta direção;
- Comunicação ao fornecedor (empresa contratada);
- Possível ação legal.

Lições Aprendidas:

- Análise pós-incidente;
- Identificação de melhorias;
- Atualização de políticas e procedimentos;
- Treinamento adicional.

5.12 Responsabilidades

5.12.1 Patrocinador Interno (Gestor Solicitante)

- Solicitar acesso via CSTI com antecedência adequada;
- Justificar necessidade e escopo do acesso;
- Validar documentação legal do terceiro;
- Acompanhar execução dos serviços;
- Reportar desvios ou problemas;
- Solicitar revogação ao término.

5.12.2 Centro de Serviços de TI (GLPI)

- Receber e validar solicitações;
- Provisionar acessos conforme aprovado;
- Configurar controles de segurança;
- Monitorar atividades de terceiros;
- Gerar relatórios de auditoria;
- Executar revogações.

5.12.3 Segurança da Informação

- Aprovar acessos Nível 1 (críticos);
- Definir controles de segurança necessários;
- Realizar auditorias regulares;
- Investigar incidentes de segurança;
- Monitorar conformidade com políticas;
- Revisar e atualizar a política.

5.12.4 Gestor de Contratos

- Garantir cláusulas de segurança em contratos;
- Validar conformidade contratual;
- Gerenciar SLAs com fornecedores;
- Coordenar renovações e rescisões.

5.12.5 DPO (*Data Protection Officer*)

- Validar conformidade LGPD;
- Aprovar acesso a dados pessoais;
- Avaliar riscos de privacidade;
- Gerenciar incidentes com dados pessoais;
- Manter registro de operadores de dados.

5.12.6 Fornecedor/Terceiro

- Cumprir todas as políticas de segurança da organização;
- Proteger credenciais de acesso;
- Usar apenas recursos autorizados;
- Reportar incidentes imediatamente;
- Participar de treinamentos obrigatórios;
- Cooperar em auditorias e investigações;
- Notificar mudanças na equipe de trabalho.

5.12.7 Controle de Acesso Físico

- **Acesso Físico a Áreas Sensíveis**: As áreas físicas onde sistemas sensíveis estão localizados (como servidores, centros de dados) devem ter controles de acesso rigorosos, como biometria, cartões de acesso, e registros de entrada e saída.
- **Política de Acesso a Dispositivos**: O acesso a dispositivos como computadores, impressoras e dispositivos móveis deve ser restrito a usuários autorizados, com senhas, bloqueios automáticos e criptografia de dados sempre que possível.
- **Restrição de acesso USB, especialmente em máquinas coletivas:** É vedado o uso de USB nos computadores e notebooks da organização. Essa ação está configurada no antivírus.
- **Restrição de uso de email pessoal:** É vedado o uso de e-mail pessoal nos computadores e notebooks da organização. Essa ação está configurada no antivírus.

INFORMAÇÃO DOCUMENTADA RETIDA

Formulário	Identificação	Processo / Área	Armazenamento	Recuperação	Proteção	Retenção Tempo	Disposição
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

7 ANEXOS

Não aplicável.