PSI – Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

V.2.0

Índice

A **Política de Segurança da Informação (PSI)** é o documento que estabelece as diretrizes corporativas do Instituto Municipal de Seguridade Social do Servidor de Blumenau (ISSBLU) para a proteção dos ativos de informação, garantindo conformidade legal e segurança para todos os usuários e colaboradores. Esta PSI aplica-se a todas as áreas do Instituto e deve ser cumprida por todos os colaboradores, prestadores de serviço e parceiros.

Esta versão da PSI foi atualizada com base nas melhores práticas de segurança da informação, conforme recomendadas pela **ABNT NBR ISO/IEC 27002:2022**, que trata de controles de segurança da informação, cibersegurança e proteção da privacidade, além de seguir as exigências legais estabelecidas pela **Lei Geral de Proteção de Dados (LGPD)** - Lei n.º 13.709/2018

OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores e parceiros do ISSBLU seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades e de proteção legal do Instituto e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

O objetivo desta PSI é:

- Estabelecer diretrizes para garantir a **proteção, confidencialidade, integridade e disponibilidade** das informações do ISSBLU.
- Orientar a definição de normas, procedimentos e controles de segurança da informação em conformidade com a legislação vigente e normas internacionais.
- Garantir que todos os colaboradores, prestadores de serviços e parceiros sigam padrões comportamentais que minimizem riscos à segurança da informação.

APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes do Instituto poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação do colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DA PSI

A segurança da informação no ISSBLU baseia-se nos seguintes princípios fundamentais:

- **Confidencialidade**: Garantia de que o acesso às informações seja permitido apenas a indivíduos autorizados, protegendo os dados de acessos indevidos.
- **Integridade**: Assegura que as informações permaneçam corretas e completas, protegidas contra alterações não autorizadas, acidentais ou intencionais.
- **Disponibilidade**: Assegura que as informações e recursos de TI estejam disponíveis aos usuários autorizados sempre que necessário para a execução de suas atividades.
- **Legalidade e Conformidade**: O ISSBLU compromete-se a cumprir as legislações aplicáveis, incluindo a **Lei Geral de Proteção de Dados (LGPD)**, e as normas de segurança da informação, como as da **ABNT NBR ISO/IEC 27002:2022**.
- **Responsabilidade**: Todos os colaboradores, prestadores de serviços e parceiros do ISSBLU são responsáveis pela proteção das informações às quais têm acesso, devendo cumprir esta PSI e as normas relacionadas.
- **Responsabilidade Compartilhada**: No uso de serviços em nuvem e outras tecnologias, a segurança é uma responsabilidade compartilhada entre o ISSBLU e os provedores de serviço.
- **Minimização de Riscos**: O ISSBLU adota uma abordagem proativa para identificar, avaliar e mitigar riscos de segurança da informação, com foco na prevenção de incidentes.

REQUISITOS DA PSI

1. Comunicação e Treinamento

- A PSI será amplamente comunicada a todos os colaboradores, prestadores de serviço e parceiros do ISSBLU.
- Todos os colaboradores devem receber treinamento periódico sobre segurança da informação, incluindo atualizações em conformidade com a LGPD e as normas internacionais, como a ISO/IEC 27002:2022.

2. Revisão e Atualização

- A PSI e as normas de segurança relacionadas deverão ser revisadas e atualizadas periodicamente, ou sempre que houver alterações significativas nas regulamentações aplicáveis ou no ambiente tecnológico do ISSBLU.
- Revisões serão conduzidas pelo Comitê de Segurança da Informação, que incluirá representantes da área de TI, jurídica, e gestores de negócios.

3. Classificação e Controle de Acesso à Informação

- Todos os acessos aos ativos de informação devem ser feitos de forma controlada, utilizando autenticação.
- O acesso a informações sensíveis ou confidenciais será concedido apenas a colaboradores que necessitem dessas informações para a execução de suas funções, sendo obrigatória a adoção de controles de acesso rigorosos, com gestão de identidades.

4. Proteção dos Dados Pessoais e Conformidade com a LGPD

- O tratamento de dados pessoais deve estar em conformidade com a LGPD, respeitando os direitos dos titulares dos dados e garantindo a segurança no armazenamento, processamento e descarte de dados pessoais.
- Devem ser implementadas medidas técnicas e administrativas adequadas para proteger dados pessoais contra acessos não autorizados, perdas acidentais ou qualquer forma de uso inadequado.

5. Gestão de Incidentes de Segurança

- Incidentes de segurança da informação, como acessos não autorizados, vazamento de dados ou falhas nos sistemas, devem ser imediatamente comunicados à Área de TI.
- Um Plano de Resposta a Incidentes será mantido, documentando as ações a serem tomadas, incluindo a notificação de autoridades competentes e dos titulares dos dados, conforme a LGPD.

6. Segurança em Ambientes de Nuvem

- Serviços em nuvem devem ser utilizados conforme os controles descritos na norma ABNT NBR ISO/IEC 27017, com a aplicação de criptografia para proteger os dados em repouso e em trânsito.
- O provedor de serviços em nuvem deve ser avaliado quanto à sua conformidade com normas de segurança, como a ISO/IEC 27018, que trata da proteção de dados pessoais em ambientes de nuvem.

7. Backup e Recuperação de Dados

- Todos os dados críticos do ISSBLU deverão ser incluídos em uma política de backup regular, com os backups sendo armazenados em local seguro.
- Testes de restauração (restore) serão realizados periodicamente para garantir que os dados possam ser recuperados de maneira eficaz em caso de incidente.

8. Auditoria e Monitoramento

- O ambiente de TI do ISSBLU será monitorado continuamente para identificar e prevenir acessos não autorizados ou atividades suspeitas.
- Logs detalhados de acessos e atividades serão mantidos, com revisões periódicas para detecção de falhas ou vulnerabilidades.

DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Colaboradores em Geral

- Todos os colaboradores, sejam contratados diretamente ou prestadores de serviço, têm a responsabilidade de proteger as informações às quais têm acesso, cumprindo integralmente esta PSI e as normas de segurança associadas.
- Treinamento Regular: Devem participar de treinamentos periódicos em segurança da informação, cibersegurança e proteção de dados pessoais, para garantir conformidade com a LGPD e as normas internas.
- Uso Adequado de Recursos: Devem utilizar os recursos tecnológicos do ISSBLU exclusivamente para fins profissionais, observando as políticas de uso de internet, correio eletrônico e outros sistemas institucionais, evitando qualquer tipo de atividade ilícita ou que exponha a instituição a riscos.
- Proteção de Credenciais: Devem proteger suas credenciais de acesso (login e senha) e jamais compartilhar com terceiros.

2 - Dos Colaboradores em Regime de Exceção (Temporários)

- Colaboradores temporários devem seguir rigorosamente as diretrizes desta PSI e receberão acesso restrito aos sistemas e informações necessários para suas atividades específicas.
- Restrições de Acesso: O acesso de temporários será concedido apenas após avaliação de risco e poderá ser revogado a qualquer momento, se os riscos superarem os benefícios operacionais.

3 - Dos Gestores de Pessoas e/ou Processos

- Gestores são responsáveis por garantir que todos os colaboradores sob sua supervisão conheçam e sigam a PSI, além de fornecer a infraestrutura necessária para a segurança da informação.
- Modelo de Conduta: Devem adotar postura exemplar no cumprimento das normas de segurança, servindo de modelo para seus colaboradores.
- Responsabilidade Contratual: Antes de conceder acesso a sistemas ou informações institucionais, os gestores devem assegurar que os contratos de trabalho ou prestação de serviço contenham cláusulas de confidencialidade e sigilo, mesmo após o desligamento do colaborador.

4 - Dos Custodiantes da Informação

4.1 - Da Área de Tecnologia da Informação (TI)

- **Proteção de Sistemas:** A área de TI é responsável por implantar e manter controles de segurança para todos os sistemas e dispositivos sob sua gestão, garantindo que estejam em conformidade com as melhores práticas descritas nas normas ISO/IEC 27002:2022 e ISO/IEC 27017.
- **Gestão de Incidentes:** Deve monitorar o ambiente de TI continuamente, detectando e respondendo a incidentes de segurança. Incidentes graves devem ser reportados à alta administração e, quando envolverem dados pessoais, à Autoridade Nacional de Proteção de Dados (ANPD), conforme a LGPD.
- **Gerenciamento de Acesso:** A área de TI deve garantir que todos os acessos aos sistemas do ISSBLU sejam devidamente auditados, e que o controle de acesso a informações confidenciais siga o princípio do menor privilégio, com autenticação multifator (MFA) implementada para funções críticas.

4.2 Gestão de Infraestrutura e Dados

- **Segurança Física e Lógica:** A área de TI deve implementar controles rigorosos para proteger a infraestrutura física e lógica do ISSBLU, incluindo o datacenter e outros locais onde informações sensíveis são armazenadas ou processadas.
- **Backup e Recuperação:** Deve assegurar que todos os backups de dados críticos estejam devidamente armazenados e protegidos, seguindo os padrões estabelecidos e com testes periódicos de recuperação.

4.3 Monitoramento e Auditoria

- Monitoramento Contínuo: A área de TI deve realizar o monitoramento contínuo dos sistemas e redes do ISSBLU, garantindo que atividades suspeitas ou não autorizadas sejam detectadas em tempo real.
- Auditoria Regular: A equipe de TI deve conduzir auditorias periódicas nos sistemas críticos, verificando o cumprimento das políticas de segurança, e gerar relatórios que sejam auditáveis e revisáveis pela alta administração.

5 Da Área de Segurança da Informação

- **Planejamento e Coordenação:** A Área de Segurança da Informação é responsável por definir as metodologias e coordenar a implementação dos processos de segurança, incluindo a classificação de informações e a avaliação de riscos.
- **Conscientização e Treinamento:** Promover campanhas de conscientização sobre a importância da segurança da informação, além de coordenar programas de treinamento contínuos para todos os colaboradores.
- **Política de Privacidade e Proteção de Dados:** Coordenar a implementação das práticas de conformidade com a LGPD, garantindo que a coleta, o processamento e o armazenamento de dados pessoais sigam as diretrizes legais e internas.

6 - Do Comitê de Segurança da Informação

- **Revisão e Atualização da PSI**: O Comitê será responsável por revisar e atualizar a PSI periodicamente, ou sempre que houver alterações nas leis ou normas que possam impactar as diretrizes de segurança.
- **Acompanhamento de Incidentes:** Analisar criticamente os incidentes de segurança reportados, propondo melhorias nos controles e processos de resposta.

7 - Do Monitoramento e da Auditoria do Ambiente

O ISSBLU deve adotar medidas para garantir que todas as atividades nos sistemas e redes sejam monitoradas e auditadas, conforme os seguintes princípios:

- **Monitoramento Contínuo**: Sistemas de monitoramento devem ser implantados em todas as estações de trabalho, servidores, dispositivos móveis e conexões à internet. Esses sistemas devem coletar logs detalhados, que serão usados para identificar e rastrear acessos, atividades e materiais manipulados.
- **Auditoria Periódica**: Devem ser realizadas auditorias periódicas nas configurações técnicas e no ambiente de rede, com especial atenção para sistemas críticos e dados pessoais. Relatórios dessas auditorias devem ser apresentados à alta administração e utilizados para identificar e mitigar vulnerabilidades.
- **Notificação de Incidentes**: Caso seja detectado um incidente de segurança, como violação de dados pessoais, a **Área de TI** deve notificar imediatamente a **Área de Segurança da Informação**, que avaliará a necessidade de comunicar a **Autoridade Nacional de Proteção de Dados (ANPD)**, conforme determina a LGPD.

CORREIO ELETRÔNICO

O uso do correio eletrônico corporativo do ISSBLU deve seguir estritamente os seguintes controles de segurança:

1. Uso Adequado

- O correio eletrônico corporativo deve ser utilizado exclusivamente para fins profissionais, relacionados às atividades do ISSBLU. O uso pessoal deve ser limitado e não comprometer o desempenho da rede ou a produtividade.

2. Atividades Proibidas

É proibido aos colaboradores:

- Enviar mensagens não solicitadas (SPAM) para múltiplos destinatários, exceto quando autorizadas pela gerência.
- Utilizar endereços de correio eletrônico de terceiros ou disfarçar a identidade do remetente.
- Transmitir informações confidenciais ou sensíveis sem a devida autorização e sem medidas de proteção, como criptografia.
- Enviar arquivos executáveis (.exe, .bat, etc.) sem justificativa clara e aprovada pela Área de TI.

3. Assinaturas de E-mail

Todas as mensagens de correio eletrônico corporativo devem incluir uma assinatura padrão contendo:

- Nome do colaborador
- Departamento
- Nome da empresa

4. Proteção e Monitoramento

- Mensagens de correio eletrônico estarão sujeitas a monitoramento para identificar possíveis violações de segurança.
- O ISSBLU reserva-se o direito de analisar o conteúdo das comunicações eletrônicas para garantir conformidade com as políticas de segurança e, se necessário, adotar medidas legais cabíveis.

INTERNET

A utilização dos recursos de internet disponibilizados pelo ISSBLU deve ser segura e conforme as diretrizes abaixo:

1. Uso Aceitável

- A internet disponibilizada pelo ISSBLU é destinada exclusivamente ao uso profissional. O uso pessoal, como a navegação em sites de notícias ou serviços de interesse geral, será permitido desde que não comprometa o desempenho da rede nem conflite com as atividades profissionais.

2. Atividades Proibidas

É estritamente proibido:

- Acessar conteúdos ilegais, obscenos ou que contrariem as diretrizes institucionais, como sites de pirataria, pornografia, ou que promovam discurso de ódio.
- Usar serviços de proxy ou VPNs não autorizadas para burlar controles de segurança da rede.
- Fazer download ou upload de arquivos que não sejam diretamente relacionados às atividades profissionais sem autorização da TI.

3. Monitoramento

- Todo o tráfego de internet será monitorado pela Área de TI para garantir a segurança dos ativos e o cumprimento das normas. Logs de acessos serão armazenados por um período definido pela política interna e auditados regularmente.

4. Restrições de Acesso

- Sites de alto risco, como serviços de compartilhamento de arquivos peer-to-peer (P2P) e redes sociais, serão bloqueados automaticamente. Exceções podem ser solicitadas formalmente pelo gestor e autorizadas pela Área de TI.

IDENTIFICAÇÃO E AUTENTICAÇÃO

1. Uso de Dispositivos de Identificação

- Todos os colaboradores devem utilizar dispositivos de identificação individual (login e senha, crachás, tokens, certificados digitais, etc.) para acessar os sistemas e instalações do ISSBLU.
- Autenticação Multifator (MFA) é obrigatória para acessos a sistemas críticos e deve ser configurada pela Área de TI.

2. Proteção das Senhas

- Senhas devem ser criadas de acordo com as políticas estabelecidas, contendo no mínimo 8 caracteres com combinações de letras maiúsculas, minúsculas, números e símbolos.
- As senhas devem ser alteradas periodicamente (a cada 45 dias para usuários comuns e a cada 30 dias para usuários com privilégios administrativos). Não podem ser reutilizadas as últimas 5 senhas.
- O compartilhamento de senhas é proibido. Caso seja detectado uso compartilhado, todos os usuários envolvidos serão responsabilizados.

3. Bloqueio de Acesso

- Após 3 tentativas malsucedidas de login, a conta do usuário será bloqueada automaticamente. O desbloqueio só poderá ser feito mediante solicitação formal à Área de TI.
- A Área de TI deve ser imediatamente notificada em casos de desligamento de

colaboradores para que suas contas de acesso sejam desativadas e os recursos, revogados.

DISPOSITIVOS MÓVEIS

1. Uso de Dispositivos Móveis Corporativos

- Dispositivos móveis fornecidos pelo ISSBLU (notebooks, smartphones, tablets) devem ser utilizados exclusivamente para fins profissionais.
- Todos os dispositivos móveis devem ter senhas de bloqueio e, quando disponível, criptografia para proteger os dados armazenados.

2. Uso de Dispositivos Pessoais (BYOD)

- O uso de dispositivos pessoais para acessar os sistemas ou redes do ISSBLU só será permitido após avaliação de risco e aprovação da Área de TI.
- Dispositivos pessoais usados para acessar informações corporativas devem ter software de segurança instalado (antivírus, firewall) e estarem configurados para criptografar os dados sensíveis.

3. Política de Segurança de Dispositivos Móveis

- Senhas de bloqueio automático devem ser habilitadas em todos os dispositivos móveis. O colaborador é responsável por garantir que seus dispositivos estejam protegidos contra acessos não autorizados.
- Proibição de Root ou Jailbreak: Modificar o sistema operacional de dispositivos móveis fornecidos pelo ISSBLU (como fazer root ou jailbreak) é estritamente proibido, pois isso compromete a segurança do dispositivo.

4. Em Caso de Roubo ou Perda

- Em caso de furto ou perda de dispositivos móveis, o colaborador deve notificar imediatamente a Área de TI e seu gestor direto, além de registrar um boletim de ocorrência junto às autoridades competentes.

5. Acesso Remoto e Redes Públicas

- O acesso remoto a sistemas corporativos deve ser feito exclusivamente por VPNs seguras fornecidas pelo ISSBLU.
- O uso de redes públicas de Wi-Fi para acessar informações do ISSBLU é proibido, a menos que esteja configurada uma VPN segura.

DATACENTER

1. Controle de Acesso ao Datacenter

- O acesso ao datacenter do ISSBLU será estritamente controlado, sendo permitido apenas a colaboradores autorizados pela Área de TI.
- Visitantes e terceiros só poderão acessar o datacenter com acompanhamento de um colaborador autorizado.

2. Segurança Física

- O datacenter deve ser protegido contra ameaças físicas, como incêndios e inundações, utilizando sistemas de combate a incêndios, controle de temperatura e umidade, e sistemas de segurança contra intrusões.
- O acessos as salas possuem portas magneticas, permitndo apenas acessos de colaboradores do instituto ou terceiros acompanhados ou com acesso autorizado.
- Sala Datacenter possui tranca com chave, onde apenas o setor de informatica possui acesso. Em caso de manutenção na sala deve haver um acompanhante do setor.
- Câmeras de segurança e sistemas de monitoramento instalados em áreas estratégicas do datacenter e demais salas para garantir que todos os acessos sejam monitorados e registrados.

3. Segregação de Ambientes

- O ambiente de produção do datacenter deve ser segregado dos ambientes de desenvolvimento e homologação, garantindo que alterações ou testes não comprometam a integridade dos sistemas em produção.

4. Procedimentos para Movimentação de Equipamentos

- A movimentação de qualquer equipamento dentro do datacenter, ou a retirada de equipamentos, deve ser formalmente registrada e autorizada pelo gestor do datacenter, seguindo as normas internas de controle de inventário.

5. Desligamento de Colaboradores

- Quando um colaborador com acesso ao datacenter for desligado, seu acesso deve ser imediatamente revogado, garantindo que ele não tenha mais qualquer privilégio de acesso aos sistemas e infraestrutura do ISSBLU.

BACKUP

1. Política de Backup

- Todos os dados críticos e sensíveis do ISSBLU devem ser incluídos em uma política de backup regular, que assegure a integridade, disponibilidade e recuperação dos dados em caso de incidentes.
- Backups automatizados devem ser realizados fora do horário comercial, nas chamadas "janelas de backup", para minimizar o impacto no desempenho dos sistemas.

2. Armazenamento Seguro

- As mídias de backup (físicas) devem ser armazenadas em locais seguros, com controle de acesso, de preferência em cofres corta-fogo e separados fisicamente do datacenter principal.

3. Gestão e Ciclo de Vida das Mídias

- As mídias de backup (físicas ou virtuais) devem ter seu ciclo de vida monitorado, garantindo que mídias desgastadas sejam substituídas para evitar falhas na recuperação de dados.

- O tempo de retenção das mídias de backup deve ser definido conforme os requisitos legais e normativos, como a LGPD, que exige que os dados pessoais sejam mantidos apenas pelo tempo necessário ao seu processamento.

4. Testes de Recuperação

- Testes periódicos de restauração (restore) devem ser realizados a cada 30 ou 60 dias, dependendo da criticidade dos dados e sistemas envolvidos.
- O processo de restauração deve ser documentado e os testes devem ocorrer em ambientes de teste separados, para evitar impactos nos sistemas de produção.

5. Planos de Recuperação de Desastres (DRP)

- Um Plano de Recuperação de Desastres (DRP) deve estar formalmente documentado e ser testado regularmente, garantindo que os sistemas críticos possam ser restaurados rapidamente em caso de incidentes severos (ex: ciberataques, desastres naturais).

DAS DISPOSIÇÕES FINAIS

1. Conformidade e Revisões

- Esta PSI deverá ser revisada periodicamente, pelo menos uma vez por ano, ou sempre que houver mudanças significativas na legislação ou no ambiente tecnológico que possam impactar a segurança da informação.
- **Auditorias internas e externas** devem ser realizadas periodicamente para garantir que os controles de segurança estão sendo cumpridos e que o ISSBLU está em conformidade com a **LGPD** e outras regulamentações aplicáveis.

2. Consequências pelo Não Cumprimento

- O não cumprimento desta PSI e das Normas de Segurança da Informação acarretará medidas administrativas e legais contra os responsáveis, conforme previsto nas políticas internas do ISSBLU e na legislação vigente.

3. Política de Conscientização

- A segurança da informação é parte essencial da cultura do ISSBLU, sendo de responsabilidade de todos os colaboradores, gestores e prestadores de serviço.
- O ISSBLU promoverá **campanhas regulares de conscientização** e **treinamentos contínuos** sobre segurança da informação, cibersegurança e proteção de dados pessoais, para garantir que todos estejam cientes das suas responsabilidades.

4. Plano de Continuidade de Negócios (PCN)

- Um **Plano de Continuidade de Negócios (PCN)** deve estar formalizado e testado regularmente, garantindo que os processos essenciais do ISSBLU possam continuar

operando mesmo em situações de crise, como desastres naturais ou ataques cibernéticos.

- O PCN deve incluir planos para a recuperação de dados e sistemas críticos, comunicação de crises e retorno às operações normais.