POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

V2 2024

PREVINIL

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE NILÓPOLIS

A PSI visa a estabelecer um conjunto de normas e práticas que orientem a gestão de riscos relacionados à segurança da informação

previnil@previnil.rj.gov.br

www.previnil,rj.gov.br

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE NILÓPOLIS – PREVINIL

DEPARTAMENTO DE INFORMÁTICA

VERSÃO 2.0
Nilópolis, agosto 2024

PREVINIL
INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE NILÓPOLIS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICIPIO DE NILÓPOLIS – PREVINIL

Rodrigo Serpa Florêncio
Presidente

DEPARTAMENTO DE INFORMÁTICA

Saulo Fernandes Dantas
Chefe do departamento

ENCARREGADO DE DADOS

Saulo Fernandes Dantas

TÉCNICO DE ELABORAÇÃO

Saulo Fernandes Dantas

VERSÃO 2.0
Nilópolis, agosto 2024

Histórico de Versões

Data	Versão	Descrição	Autor
26/07/2021	1.0	Criação da PSI do PREVINIL	Paulo Sergio cardoso
09/08/2024	2.0	Extingue a versão anterior e cria a nova PSI visando à adequação do documento segundo modelos da Secretaria de Governo Digital – Ministério Da Gestão e Da Inovação Em Serviços Públicos, assim como a novas legislações, normas nacionais e internacionais e adequação às novas realidades do instituto	Saulo Fernandes Dantas

Sumário

1. Introdução

A segurança da informação é fundamental para garantir a integridade, confidencialidade e disponibilidade dos dados manejados pelo Instituto de Previdência dos Servidores do município de Nilópolis (PREVINIL). Esta política tem como objetivo principal estabelecer diretrizes que assegurem a proteção de todos os ativos de informação, em conformidade com as legislações vigentes e as melhores práticas de segurança.

1.1. Contexto e Importância

No cenário atual, as ameaças à segurança da informação têm se tornado mais frequentes e sofisticadas, podendo causar danos significativos à operação do PREVINIL e à privacidade dos dados dos segurados, servidores e colaboradores. Por isso, a implementação de uma PSI robusta é essencial para mitigar riscos e assegurar a continuidade das operações da instituição.

2. Termos e Definições

Nesta seção, são apresentados os principais termos utilizados nesta PSI, com o objetivo de garantir a clareza e compreensão de todos os envolvidos:

- **Ativo de Informação**: Qualquer dado ou recurso que tenha valor para o Instituto, incluindo documentos, sistemas, e hardware.
- **Confidencialidade**: Garantia de que a informação seja acessada apenas por pessoas autorizadas.
- **Integridade**: Garantia de que a informação seja mantida em seu estado original, protegida contra alterações indevidas, intencionais ou acidentais.
- **Disponibilidade**: Garantia de que a informação esteja disponível para os usuários autorizados sempre que necessário.
- **TI**: Tecnologia da informação.
- **Incidentes De Segurança:** Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais. (ANPD)
- **Níveis de Acesso**: Diferentes níveis de acesso são atribuídos a informações com base na necessidade de saber. Somente indivíduos autorizados, com base na função e responsabilidades, podem acessar certos tipos de dados.
- **Gestão de Informação**: É crucial que as organizações tenham políticas e processos claros para a classificação, proteção e desclassificação de informações, garantindo que os dados sejam geridos de forma segura e em conformidade com a legislação.

3. Objetivo da Política

I. A PSI visa a estabelecer um conjunto de normas e práticas que orientem a gestão de riscos relacionados à segurança da informação no Instituto. Especificamente, busca-se:

- **Proteção da Informação**: Assegurar que todas as informações do Instituto sejam protegidas contra acessos não autorizados, perda, destruição, ou qualquer forma de comprometimento.
- **Conformidade Legal**: Garantir que todas as atividades de tratamento de dados estejam em conformidade com a legislação aplicável, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Continuidade dos Negócios**: Minimizar interrupções nas operações do PREVINIL em caso de incidentes de segurança, através da implementação de planos de continuidade de negócios e recuperação de desastres.
- **Responsabilidade, Consciência e Padronização**: Promover uma cultura de segurança da informação entre todos os colaboradores, prestadores de serviço e demais partes interessadas. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Estabelecer diretrizes que permitam aos colaboradores e fornecedores do PREVINIL seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Autarquia e do indivíduo

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

III. Preservar as informações do Instituto quanto à:

- **Integridade:** Garantia de que a informação seja mantida em seu estado original, protegida contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

4. Escopo

Esta política se aplica a todos os colaboradores, prestadores de serviços, fornecedores, e qualquer outro agente que tenha acesso a informações ou sistemas de TI do PREVINIL. O escopo abrange:

- **Sistemas de Informação**: Todos os sistemas utilizados para armazenar, processar e transmitir dados.
- **Dispositivos Físicos e Virtuais**: Incluindo servidores, estações de trabalho, dispositivos móveis, e outros equipamentos de TI.
- **Informações em Todos os Formatos**: Abrangendo dados digitais e em papel, bem como quaisquer outros meios de armazenamento de informações.

É obrigação de cada servidor manter-se atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do gestor ou da área de TI sempre que necessário.

5. Diretrizes Gerais de Segurança

As diretrizes gerais de segurança estabelecem os princípios básicos que devem ser seguidos por todos os membros do Instituto:

- **Segregação de Funções**: As responsabilidades e privilégios de acesso devem ser definidos de forma a evitar conflitos de interesse e reduzir o risco de erros ou fraudes.
- **Gestão de Incidentes**: Todos os incidentes de segurança devem ser reportados imediatamente e tratados conforme os procedimentos estabelecidos.
- **Auditorias e Monitoramento**: A implementação de mecanismos de auditoria e monitoramento contínuo é essencial para detectar e responder a eventuais vulnerabilidades ou incidentes.

5.1. Ameaças e Riscos

As ameaças e riscos mais comuns observados em nossas estruturas incluem:

- **Ameaças Internas**: Acessos indevidos por parte de colaboradores seja por erro ou má intenção.
- **Ameaças Externas**: Ataques cibernéticos, como phishing, ransomware, e tentativas de invasão por hackers.
- **Riscos de Conformidade**: Falta de aderência às legislações e regulamentações podem resultar em multas, penalidades legais, e danos à reputação.
- **Falhas físicas**: Problemas técnicos ou falhas de hardware.
- **Perda de dados**: Devido a falhas de backup ou desastres.

- **Vulnerabilidades em sistemas**: Exploração de falhas em software desatualizado.
- **Falhas de Sistemas**: Problemas técnicos ou falhas em sistemas de TI que podem levar à perda de dados ou interrupção de serviços.
- **Desastres naturais:** Incidentes como incêndios, inundações e terremotos que podem danificar a infraestrutura de TI.
- **Erros Humanos:** Incluindo a má configuração de sistemas, falhas no seguimento de procedimentos de segurança e o manuseio inadequado de informações sensíveis.
- **Vazamento de Dados:** A exposição não autorizada de informações sensíveis ou confidenciais, seja por meio de ataques cibernéticos, falhas de segurança, erro humano ou proposital.

6. Controle de Acesso

O controle de acesso é fundamental para garantir que apenas pessoas autorizadas tenham acesso às informações e sistemas do Instituto. Os principais tipos de controle de acesso incluem:

- **Controle de Acesso Lógico:**
  - **Níveis de Acesso e Setorização:** Garantem que cada usuário tenha acesso apenas às informações e sistemas necessários para suas funções. Definição de privilégios de acesso baseados em funções e necessidades específicas dos usuários, garantindo que eles só possam acessar as informações necessárias para suas funções, reduzindo o risco de acesso indevido.
  - **Autenticação e Autorização:** Processos de verificação de identidade e permissão que asseguram que apenas usuários autorizados possam acessar recursos específicos. Utilização de métodos como senhas fortes, autenticação multifator (MFA), e biometria para verificar a identidade dos usuários.
  - **Controle de Entrada e Saída de Informações via Firewall:** Monitora e regula o tráfego de rede para proteger contra acessos não autorizados e ataques cibernéticos.
  - **Monitoramento de Acesso**: Implementação de logs e auditorias para registrar e revisar atividades de acesso, permitindo a detecção precoce de acessos não autorizados

- **Controle de Acesso Físico:**
  - **Segurança Física de Instalações:** Inclui o controle de acesso a salas de servidores e áreas de TI, utilizando métodos como cartões de acesso, biometria, trancas analógicas e vigilância por câmeras.
  - **Controle de Equipamentos:** Garantir que dispositivos de TI sejam protegidos contra roubo, dano ou uso não autorizado.

A importância desses controles reside na prevenção de acessos indevidos e no reforço da segurança da informação, garantindo que os dados críticos sejam acessados apenas por pessoas qualificadas e com necessidade legítima, minimizando o risco de vazamentos ou acessos indevidos.

7. Treinamento e Conscientização

Para garantir a eficácia da PSI, é fundamental que todos os colaboradores do PREVINIL estejam bem informados e treinados sobre as práticas de segurança da informação:

- **Capacitação Técnica:** Prover treinamento contínuo para a equipe técnica do departamento de informática através de certificações, seminários, cursos dentre outras formas de agregação de conhecimento.
- **Treinamentos Regulares**: Realização de workshops, seminários, e cursos online para capacitar os colaboradores em segurança da informação.
- **Campanhas de Conscientização**: Implementação de campanhas periódicas para reforçar boas práticas, como evitar phishing, criar senhas seguras, e reconhecer sinais de ameaças.
- **Simulações de Incidentes**: Execução de exercícios simulados para testar a prontidão dos colaboradores em situações de risco, como ataques de phishing ou violações de segurança.
- **Envio de memorandos**: Com atualizações e lembretes sobre políticas de segurança.
- **Simulações de phishing**: Para educar os funcionários sobre como identificar e evitar ataques de phishing.
- **Boletins Informativos e Newsletters:** Enviar regularmente boletins informativos com dicas de segurança, atualizações sobre políticas e alertas sobre novas ameaças.

Essas iniciativas ajudam a criar uma cultura de segurança dentro da organização, onde todos compreendem a importância da segurança da informação e sabem como agir para protegê-las.

8. Gestão de Riscos e Resposta a Incidentes

A gestão de riscos é uma prática contínua que envolve a identificação, avaliação e mitigação de riscos relacionados à segurança da informação. As etapas incluem:

- **Identificação de Riscos**: Mapeamento de todos os potenciais riscos que podem afetar a segurança das informações.
- **Avaliação de Riscos**: Análise da probabilidade e impacto de cada risco identificado, priorizando os mais críticos.
- **Mitigação de Riscos**: Implementação de controles e procedimentos para minimizar a probabilidade e o impacto dos riscos.
- **Revisão e Monitoramento**: Revisão periódica dos riscos e dos controles implementados para garantir que permanecem eficazes.

Em caso de incidentes de segurança, deve ser adotado o Plano de Contingência para assegurar a continuidade dos negócios.

A resposta a incidentes de segurança é um aspecto crucial da PSI, garantindo que quaisquer violações ou ameaças sejam tratadas de forma rápida e eficaz para minimizar os danos. A abordagem do PREVINIL inclui:

- **Detecção**: Implementação de sistemas de monitoramento contínuo para identificar atividades suspeitas e possíveis incidentes em tempo real.
- **Comunicação**: Estabelecimento de canais claros para que os colaboradores possam reportar incidentes de segurança de forma imediata.
- **Investigação**: Adoção de procedimentos formais para investigar a causa raiz de incidentes de segurança, com a finalidade de prevenir futuras ocorrências.
- **Mitigação**: Implementação de ações corretivas para mitigar os efeitos do incidente, incluindo a contenção e a eliminação da ameaça.
- **Recuperação**: Garantir a rápida restauração dos sistemas e dados afetados, com o mínimo de interrupção para as operações do PREVINIL.
- **Relato e Aprendizado**: Documentar todos os incidentes, analisar as lições aprendidas e ajustar as políticas e procedimentos de segurança, se necessário.

9. Continuidade de Serviços e Recuperação de Desastres

Para assegurar que o PREVINIL continue a operar em situações de emergência, a política inclui:

- **Planejamento de Continuidade de Negócios**: Desenvolvimento de planos detalhados que descrevam como as operações críticas serão mantidas em caso de incidentes graves.
- **Recuperação de Desastres**: Estabelecimento de procedimentos específicos para a restauração de sistemas e dados após desastres naturais, falhas técnicas graves ou ataques cibernéticos.
- **Testes e Revisões Regulares**: Realização de testes periódicos dos planos de continuidade e recuperação para garantir que sejam eficazes e atualizados.

10. Gestão de Ativos

A gestão eficaz dos ativos de informação é essencial para proteger os recursos do PREVINIL. A política define que:

- **Inventário de Ativos**: Todos os ativos de informação, incluindo hardware, software, dados e documentos, devem ser identificados e catalogados.
- **Classificação de Ativos**: Os ativos devem ser classificados com base em sua importância e sensibilidade, para determinar os níveis apropriados de proteção.
- **Controle de Acesso a Ativos**: O acesso a ativos críticos deve ser restrito a pessoas autorizadas, e todos os acessos devem ser monitorados.

11. Gestão de Dados

A política aborda a gestão de dados, assegurando que:

- **Classificação de Dados**: Dados devem ser classificados de acordo com sua sensibilidade e importância, o que guiará as práticas de armazenamento e proteção.
- **Armazenamento Seguro**: Dados confidenciais devem ser armazenados em ambientes seguros, com criptografia aplicada quando necessário.
- **Retenção e Descarte de Dados**: Dados devem ser mantidos apenas pelo tempo necessário e descartados de forma segura e irreversível quando não forem mais necessários.

12. Monitoramento e Revisão

Para garantir que a PSI permaneça relevante e eficaz:

- **Revisões Regulares**: A política de segurança da informação deve ser revisada periodicamente para refletir mudanças nas operações, tecnologia, ou ameaças.

13. Classificação da Informação

Níveis de classificação:

Público

- **Definição**: Informações classificadas como públicas são aquelas que podem ser acessadas por qualquer pessoa, sem restrições. São informações transparentes que, em conformidade com a Lei de Acesso à Informação (LAI), devem ser disponibilizadas ao público, promovendo a transparência e o controle social.
- **Exemplos**: Relatórios de atividades públicas, estatísticas, dados abertos, etc.

Interno

- **Definição**: Informações classificadas como internas são destinadas exclusivamente ao uso dentro da organização e não devem ser divulgadas externamente, exceto para parceiros específicos ou mediante autorização. Este nível de classificação é utilizado para controlar o fluxo de informações que, embora não sejam sigilosas, são relevantes para a operação interna e devem ser protegidas de acessos indevidos.
- **Exemplos**: Políticas internas, manuais operacionais, comunicações administrativas internas, etc.

Confidencial

- **Definição**: Esse nível pode ser utilizado para informações que, embora não sejam sigilosas nos termos das classificações mais altas (Ultrassecreto, Secreto e Reservado), ainda assim exigem proteção devido à sua sensibilidade ou impacto potencial caso sejam divulgadas fora dos limites autorizados.
- **Exemplos**: Informações de clientes, contratos comerciais, planos de negócios, etc.

Restrito

- **Definição**: Embora não seja um nível oficial no contexto governamental de classificação de dados sigilosos, o termo "restrito" é frequentemente utilizado em diversas organizações para designar informações que devem ser acessadas apenas por determinadas pessoas ou grupos dentro da organização.
- **Exemplos**: Informações relacionadas a projetos em desenvolvimento, dados pessoais de funcionários, etc.

14. Segurança em Dispositivos Móveis e Trabalhos Remotos

Medidas de segurança:

- Utilização de VPN para acesso remoto.
- Instalação de software de segurança móvel.
- Procedimentos de reporte e bloqueio em caso de perda ou roubo de dispositivos.

15. Backup e Recuperação de Dados

Objetivo:

O objetivo deste tópico é estabelecer diretrizes para garantir que todos os dados críticos e relevantes do Instituto de Previdência dos Servidores do município de Nilópolis (PREVINIL) sejam regularmente copiados, protegidos e, em caso de falha ou perda de dados, possam ser recuperados de forma eficiente e segura.

Diretrizes Gerais:

- **Frequência de Backup:** Todos os dados essenciais devem ser submetidos a backups regulares, sendo recomendável a realização de backups diários para os dados mais críticos e semanais para dados menos sensíveis. A frequência exata

deverá ser determinada com base na importância dos dados e na capacidade operacional do PREVINIL.

- **Armazenamento de Backups:** Os backups devem ser armazenados em locais fisicamente separados da localização dos dados originais para evitar a perda total de informações em caso de desastre no local principal. Recomenda-se a utilização de um ambiente de armazenamento seguro em nuvem e/ou mídias físicas externas, como discos rígidos criptografados.
- **Segurança dos Backups:** Todos os backups devem ser protegidos por criptografia forte para prevenir acessos não autorizados. A chave de criptografia deve ser gerenciada com segurança e apenas pessoal autorizado deve ter acesso a ela.
- **Verificação de Integridade:** Realizar verificações periódicas de integridade dos dados armazenados nos backups para garantir que as cópias não estejam corrompidas ou danificadas.
- **Política de Retenção:** Estabelecer uma política clara de retenção de backups, especificando por quanto tempo cada tipo de dado deve ser mantido. Após o período de retenção, os backups devem ser destruídos de forma segura e irrecuperável.
- **Testes de Recuperação:** Realizar testes regulares de recuperação de dados para garantir que os processos funcionem conforme esperado. Estes testes devem ser documentados, e quaisquer problemas identificados devem ser resolvidos prontamente.
- **Responsabilidades:** A responsabilidade pela execução dos backups e pela recuperação de dados em caso de falhas deve ser claramente atribuída a membros específicos da equipe de TI, que devem ser devidamente treinados.

Exemplos de Implementação:

- **Exemplo 1:** Um servidor crítico que hospeda o sistema de gestão de aposentadorias realiza backups incrementais diariamente, com um backup completo semanal armazenado em uma nuvem segura.
- **Exemplo 2:** Os backups são criptografados com AES-256 e armazenados em uma unidade de armazenamento offsite, acessível apenas pelos administradores de sistema autorizados.

16. Política de Uso Aceitável

Objetivo:

A Política de Uso Aceitável visa definir o uso permitido e proibido dos recursos de TI do PREVINIL, incluindo computadores, redes, e-mail, internet e outros dispositivos. O

objetivo é garantir que esses recursos sejam utilizados de forma que proteja a integridade, segurança e confidencialidade das informações do instituto.

Diretrizes Gerais:

- **Uso Adequado dos Recursos:** Todos os recursos de TI devem ser utilizados estritamente para fins relacionados ao trabalho e aos objetivos do PREVINIL. O uso pessoal é permitido apenas de forma limitada e desde que não interfira no desempenho das atividades profissionais.
- **Acesso à Internet:** O acesso à internet deve ser utilizado de forma responsável e ética. É proibido o acesso a sites que contenham conteúdo ilícito, ofensivo ou que possam comprometer a segurança da rede.
- **Uso de E-mails:** E-mails corporativos devem ser utilizados exclusivamente para comunicações relacionadas ao trabalho. É proibido o envio de informações confidenciais sem a devida autorização ou medidas de segurança, como criptografia.
- **Instalação de Software:** A instalação de qualquer software ou aplicativo nos dispositivos do PREVINIL deve ser previamente autorizada pelo departamento de TI. Softwares não licenciados ou não verificados são estritamente proibidos.
- **Armazenamento de Dados:** Todos os dados devem ser armazenados de acordo com as políticas de segurança e backup. É proibido o armazenamento de dados confidenciais em dispositivos pessoais ou mídias externas não autorizadas.
- **Proteção de Credenciais:** Os usuários são responsáveis por proteger suas credenciais de acesso. É proibido compartilhar senhas ou permitir que outros usem suas contas de usuário.
- **Monitoramento e Auditoria:** O uso dos recursos de TI pode ser monitorado para garantir a conformidade com esta política. O PREVINIL reserva-se o direito de realizar auditorias periódicas e de aplicar medidas disciplinares em caso de violação.

DIRETRIZES DE SEGURANÇA PARA EMPRESAS PRESTADORAS DE SERVIÇOS TERCEIRIZADAS

17. Conformidade com Normas e Leis

- **LGPD:** Cumprir com todas as disposições da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).
- **Outras Leis e Regulamentações:** Conformidade com a Lei de Acesso à Informação (Lei nº 12.527/2011), Marco Civil da Internet (Lei nº 12.965/2014), Lei do Software (Lei nº 9.609/1998) e outras regulamentações aplicáveis.

18. Políticas e Procedimentos de Segurança

- **Política de Segurança da Informação:** Adotar e implementar uma Política de Segurança da Informação alinhada com a do PREVINIL.
- **Planos de Continuidade e Recuperação:** Desenvolver e manter planos de continuidade de negócios e recuperação de desastres.

19. Gestão de Acesso

- **Controle de Acesso:** Implementar controles de acesso rígidos para garantir que apenas pessoal autorizado tenha acesso a informações e sistemas sensíveis.
- **Autenticação Multifatorial:** Utilizar autenticação multifatorial para acesso a sistemas críticos.

20. Treinamento e Conscientização

- **Capacitação Contínua:** Prover treinamento contínuo e conscientização sobre segurança da informação para todos os colaboradores que terão acesso às informações do PREVINIL.
- **Testes de Simulação:** Realizar simulações periódicas de ciberataques para avaliar a preparação e resposta dos colaboradores.

21. Proteção de Dados

- **Criptografia:** Usar criptografia para proteger dados em trânsito e em repouso.
- **Backup Seguro:** Realizar backups regulares e garantir que estes sejam armazenados de forma segura e de acordo com as melhores práticas.

22. Monitoramento e Auditoria

- **Monitoramento Contínuo:** Implementar sistemas de monitoramento contínuo para detectar e responder a incidentes de segurança.
- **Auditorias Regulares:** Realizar auditorias periódicas para garantir a conformidade com as políticas de segurança e identificar possíveis vulnerabilidades.

23. Gestão de Riscos

- **Avaliação de Riscos:** Realizar avaliações regulares de riscos de segurança da informação e implementar medidas para mitigar os riscos identificados.
- **Relatório de Incidentes:** Reportar imediatamente qualquer incidente de segurança ao PREVINIL, incluindo detalhes sobre a natureza do incidente, impacto e medidas de mitigação adotadas.

24. Segurança Física

- **Proteção de Infraestrutura:** Implementar medidas de segurança física para proteger a infraestrutura que hospeda informações e sistemas críticos do PREVINIL.
- **Controle de Acesso Físico:** Garantir que o acesso físico a instalações sensíveis seja restrito e monitorado.

25. Contrato de Confidencialidade

- **Acordos de Confidencialidade:** Assinar acordos de confidencialidade para garantir que todas as informações acessadas ou processadas pela empresa terceirizada sejam tratadas com o mais alto grau de confidencialidade.

26. Responsabilidade e Sanções

- **Responsabilidade:** Estabelecer claramente a responsabilidade da empresa terceirizada em caso de violação das diretrizes de segurança.
- **Sanções:** Definir sanções e penalidades aplicáveis em caso de não conformidade com as diretrizes estabelecidas.

- **Incluir as Diretrizes no Contrato:** Certificar-se de que todas as diretrizes de segurança sejam incluídas nos contratos com as empresas terceirizadas.
- **Avaliação de Conformidade:** Realizar avaliações regulares de conformidade para garantir que a empresa terceirizada esteja seguindo as diretrizes.
- **Comunicação Contínua:** Manter uma comunicação contínua com a empresa terceirizada para discutir questões de segurança e melhorias.

As diretrizes específicas para empresas prestadoras de serviço e serviços terceirizados não retira a necessidade do cumprimento de quaisquer outros tópicos abordados nesta PSI.

27. Considerações Finais

A segurança da informação é uma responsabilidade compartilhada por todos os membros do RPPS. Esta PSI serve como um guia para proteger os dados e sistemas da instituição, e sua eficácia depende do comprometimento contínuo de todos os colaboradores, fornecedores e prestadores de serviço.

SAULO FERNANDES DANTAS
Chefe Do Departamento de Informática

Nilópolis, 09 de agosto de 2024

REFERÊNCIAS BIBLIOGRÁFICAS

Legislações Nacionais

1. **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)**
   Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
2. **Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI)**
   Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12527.htm
3. **Lei nº 12.965/2014 (Marco Civil da Internet)**
   Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
4. **Lei nº 9.609/1998 (Lei do Software)**
   Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm
5. **Decreto nº 7.579/2011**
   Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/decreto/d7579.htm
6. **Instrução Normativa SGD nº 94/2022**
   Disponível em: https://www.in.gov.br/web/dou/-/instrucao-normativa-sgd/me-n-94-de-23-de-dezembro-de-2022-452050586
7. **Portaria SGD/MGI nº 852/2023**
   Disponível em: https://www.in.gov.br/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473095253

Normas e Padrões

8. **ISO/IEC 27001:2013 (Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos)**
   Disponível em: https://www.iso.org/isoiec-27001-information-security.html
9. **ISO/IEC 27002:2013 (Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação)**
   Disponível em: https://www.iso.org/standard/54533.html
10. **ISO/IEC 20000-1:2018 (Sistemas de Gestão de Serviços de TI - Requisitos)**
    Disponível em: https://www.iso.org/standard/70636.html
11. **ISO/IEC 17799:2005 (Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Gestão da Segurança da Informação)**
    Disponível em: https://www.iso.org/standard/39612.html
12. **COBIT 5 (Control Objectives for Information and Related Technologies)**
    Disponível em: https://www.isaca.org/resources/cobit
13. **ITIL 4 (Information Technology Infrastructure Library)**
    Disponível em: https://www.axelos.com/best-practice-solutions/itil

Documentos de Referência e Guias

14. **Guia de Política de Segurança da Informação - Governo Federal do Brasil**
Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf
15. **Guia de Governança em Privacidade e Proteção de Dados - Governo Federal do Brasil**
Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf
16. **Guia de Continuidade de Negócios - ITI**
Disponível em: https://www.iti.gov.br/seguranca/guia-de-continuidade-de-negocios
17. **Modelo de Política de Segurança da Informação - Governo Federal**
Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos
18. **Manual de Segurança da Informação para Órgãos Públicos**
Disponível em: https://www.gov.br/governodigital/pt-br/seguranca/manual-seguranca-informacao.pdf
19. Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação. Disponível em: : https://www.in.gov.br/en/web/dou/-/portaria-n93-de-26-de-setembro-de-2019-%20219115663 . Acesso em: 04 set. 2020
20. COMITÊ ESTRATÉGICO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS - MINISTÉRIO DA ECONOMIA - Resolução CEPPDP/ME Nº 7. Fevereiro de 2022. Política de Proteção de Dados Pessoais no Ministério da Economia. Disponível em: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-eprogramas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-dedados-pessoais-ceppdp/documentos-ceppdp/resolucoes-ceppdp/resolucao-no-7-ceppdp-22-02-22 Acesso em: 11 set 2023

Outros Links Importantes

21. **Marco Civil da Internet: Princípios e Aplicações**
Disponível em: https://www.cgi.br/marcocivil/principios/
22. **Regulamento Geral sobre a Proteção de Dados (RGPD)**
Disponível em: https://gdpr.eu/

Os links com acesso omitidos foram acessados entre Junho e agosto de 2024.

APROVAÇÃO DIRETORIA EXECUTIVA	
NOME	ASSINATURA
RODRIGO SERPA FLORÊNCIO	
ALBERTO ZAMPAGLIONE	
ISABEL CRISTINA DE OLIVEIRA DOS SANTOS	
SOLANGE DUTRA	
APROVAÇÃO CONSELHO DE ADMINISTRAÇÃO	
NOME	ASSINATURA
CARLOS RAFAEL DRUMMOND ALVAREZ	
RODRIGO SERPA FLORENCIO	
JAIME HERCULANO DA SILVA FILHO	
MAGNA ALVARENGA DALLIA ROSA	
MARCELO NEVES MONTEIRO	
MARCOS ANTONIO DA SILVA SANTOS	