www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

Classificação: Público

Política de Segurança da Informação

POL.TEC-INF.IN.001

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

Título	Política de Segurança da Informação
Identificador	POL.TEC-INF.IN.001
Versão	00
Sigla e nome da unidade elaboradora	GTI – Gerência de Tecnologia e Inovação
Sigla e nome da unidade aprovadora	COD – Conselho Deliberativo
Processo vinculado	Tecnologia da Informação
Distribuição	Postalis, Prestadores de Serviços e terceiros
Relação com outras normas	Estatuto do Postalis; Código de Ética do Postalis; Normas e Procedimentos de Segurança da Informação: Termo de Responsabilidade e Confidencialidade.
Regulamentação utilizada	NBR ISO/IEC 27001:2013 – Sistemas de Gestão da Segurança da Informação – Requisitos; NBR ISO/IEC 27002:2013 – Técnicas de segurança - Código de Prática para controles de Segurança da Informação; NBR ISO/IEC 27005:2011 – Técnicas de segurança - Gestão de Riscos de Segurança da Informação.
Início da vigência / data de aprovação	03 de junho de 2019 / DEC-INT/2019-0016.
Revisão da vigência	Até 24 meses ou nova versão
Ato revogado	Política de Segurança da Informação (anterior)
Alteração em relação à edição anterior	Alterações Gerais – Recomendamos a leitura integral do Normativo.

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

Sumário

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

1. Objetivo

Estabelecer os princípios da Segurança da Informação, visando preservar a disponibilidade, integridade, confidencialidade e autenticidade das informações sob a gestão do Postalis nos aspectos físicos, lógicos e comportamentais.

2. Definições

As definições do presente normativo estão descritas no Glossário anexo.

3. Descrição

3.1. Princípios Fundamentais

i. Todos os dados e informações produzidas para e pelo Postalis, totais ou parciais, físicas ou lógicas, são de propriedade do Postalis, assim como os equipamentos fornecidos para o armazenamento, acesso e o controle.

ii. Todos os recursos baseados em Tecnologia da Informação ou produzidos por estes, estão sujeitos ao monitoramento e rastreabilidade, possibilitando a pronta resposta a incidentes de segurança.

iii. O Postalis, como responsável pelos dados e informações de participantes, assistidos, beneficiários, ex-participantes, patrocinadora e parceiros, os declara sigilosos, logo devem ser tratados assim pelos seus empregados e terceiros.

iv. O acesso de empregados e terceiros aos ambientes lógicos e físicos é restrito e controlado. O acesso inicial considerará o princípio do menor privilégio, que estabelece os recursos mínimos de trabalho, podendo ser alterado conforme as atividades definidas pelo processo, alçada, cargo ou função. O preenchimento do Termo de Confidencialidade e Responsabilidade é condição inegociável para a concessão de chaves de acesso e senhas aos ambientes lógicos.

v. Todos os usuários devem estar atentos e comprometidos com a Política Controles Internos e *Compliance*, auxiliando na identificação dos tipos de exposição,

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

avaliação das probabilidades de incidência e impactos dos riscos, baseados nos processos de negócio do Postalis, que devem estar mapeados e documentados.

vi. Os dados e informações, independente do seu formato, devem ser classificados quanto a sua confidencialidade, conforme sua importância estratégica para o Instituto. A classificação definirá a forma como as informações serão: armazenadas, copiadas, transmitidas, manuseadas, descartadas ou destruídas. As informações ainda não classificadas são declaradas sigilosas.

vii. Esta Política e as normas internas relacionadas devem integrar os contratos e acordos comerciais, definindo claramente os papéis, responsabilidades e os acordos de confidencialidade das partes envolvidas, quanto aos níveis de processamento de dados e informações, segurança, monitoramento e requisitos de contingência.

viii. Todos os usuários serão treinados e conscientizados quanto ao uso correto dos recursos que produzem ou manuseiam dados e informações.

ix. Os empregados e terceiros devem utilizar os recursos e informações, seguindo os princípios do Código de Ética e da Segurança da Informação, sem afetar ou causar prejuízo a outrem. Todas as espécies de pressões e chantagens devem ser denunciadas.

x. No que se refere às informações sob responsabilidade do POSTALIS, é vedado o manuseio sem estar expressamente previsto em normativos internos ou aprovação do gestor responsável.

xi. Todo e qualquer programa ou aplicativo a serem utilizados pelo Postalis deverão ser previamente aprovados pela Diretoria Executiva que observará a garantia da segurança das informações dos participantes, assistidos e beneficiários bem como avaliará a exposição aos riscos corporativos.

xii. Os empregados e terceiros devem seguir as diretrizes de segurança quanto ao uso de Mídias Removíveis e da porta USB.

xiii. Todos os acessos à Internet serão monitorados e registrados, podendo ser negados nos sites de conteúdo inadequado e/ou que tragam risco à segurança de TIC.

3.2. Responsabilidades

3.2.1. Da Gerência de Tecnologia e Inovação

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

- Zelar, em nível físico e lógico, pelos ativos de informações e de processamento do Postalis.
- Monitorar e reportar à Diretoria Executiva qualquer uso inadequado de dados, informações ou condutas que possam ferir esta Política ou normas internas relacionadas

3.2.2. Da Diretoria Executiva

Definir e aplicar sanções em caso de descumprimento das diretrizes previstas, conforme Código de Ética e legislação vigente.

3.2.3. Dos Funcionários e Terceiros

- Preservar a integridade e guardar sigilo das informações que fazem uso, bem como zelar e proteger os respectivos recursos usados para produzir, acessar ou armazenar os dados e informações.
- Cumprir e disseminar os princípios desta Política, sob pena de incorrer em sanções disciplinares previstas nas normas internas e legislação vigente
- Utilizar recursos, dados e informações do Postalis somente para fins corporativos.
- Responder pelo uso de recursos e informações, bem como seus efeitos.
- Comunicar, por escrito, aos órgãos que regem esta Política o conhecimento de qualquer irregularidade ou desvio.

4. Temporalidade

Responsável pela publicação	Temporalidade	Arquivo digital
GCC	Até 24 meses ou nova versão.	*SE Suite.*

O presente normativo necessariamente será revisado após a conclusão do processo de alteração do Estatuto do Postalis.

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

5. Anexos

Glossário.

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

Glossário

1. **Acesso remoto** - é uma tecnologia que permite a conexão à distância, feita com segurança de dados em ambos os lados, em que um computador consegue acessar um servidor/computador privado – normalmente de uma empresa – que não está fisicamente conectado à rede.
   a. Exemplos: VPN - Virtual Private Network (Rede Privada Virtual), Teamviewer.
2. **Administradores** – pessoas ou equipe com delegação superior para administrar um determinado ambiente de tecnologia da informação.
3. **Ataque cibernético/ciberataque** – ação praticada por hackers que consiste na transmissão de vírus (arquivos maliciosos) que infectam, danificam e roubam informações de computadores e demais bancos de dados online, por exemplo.
4. **Áreas organizacionais** – todas as gerências, coordenações, assessorias, diretorias e conselhos.
5. **Arquivamento:** procedimento de armazenar informações nos arquivos.
6. **Arquivo digital -** é um documento eletrônico caracterizado pela codificação em dígitos binários e acessado por meio de sistema computacional. Todo documento digital é eletrônico, mas nem todo documento eletrônico é digital (transformado do papel para digital).
   a. Exemplos: texto em PDF, planilha de cálculo em Microsoft Excel, áudio em MP3, filme em AVI.
7. **Arquivo eletrônico** - Um documento eletrônico é acessível e interpretável por meio de um equipamento eletrônico (filmadora, computador), podendo ser registrado e codificado em forma analógica ou em dígitos binários. Exemplos: filme em VHS, música em fita cassete.
8. **Ativos de informação -** referem-se à base de dados, contratos e acordos, documentação de sistema ou negócios, infraestrutura de tecnologia, manuais, material de treinamento, procedimentos, planos de continuidade de negócio.
9. **Ciclo de vida de acesso** – é o tempo entre o início e o fim das permissões de acesso dadas a um usuário.
10. **Ciclo de vida da informação** - etapas da informação dentro da organização a partir da criação ou obtenção, tratamento, distribuição, uso e descarte.

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

11. **Chaves de acesso / Login** – identificação/nome do usuário (*userid/username*) no ambiente informatizado.

12. **Conformidade** - é o atendimento em concordância com leis, regulamentos e cláusulas contratuais as quais os processos de negócio estão sujeitos.

13. **Correio Eletrônico Externo** (e-mail externo) – meio utilizado pelos funcionários, fornecedores, terceiros para comunicação via internet, podendo ou não estar conectado diretamente à rede do Instituto.

14. **Correio Eletrônico Interno** (e-mail Interno) – meio utilizado pelos colaboradores e terceiros via Internet, quando conectados à rede do Instituto.

15. **Direito de acesso privilegiado** - contas administrativas com direito de atribuir, permitir ou revogar os direitos de acesso de usuários.

16. **Disponibilidade** - quando a informação está acessível no momento em que for requerida pelos processos do negócio.

17. **Dispositivos de armazenamento:** são os locais onde a informação pode ser armazenada.

    a. Exemplos: HD, CD, DVD, pendrive, papel.

18. **Dispositivos móveis –** aparelhos como smartphone, *tablet*, celular que oferecem a possibilidade de acesso imediato e com o usuário em movimento.

19. **Equipamentos críticos** – equipamentos que manipulam informações críticas.

    a. Exemplos: servidores, firewall, banco de dados.

20. **Equipamentos de TI** - é por meio deles que os dados/informações são processados, armazenados, podendo ou não gerar novas informações.

    a. Exemplos: computadores, impressoras, smartphones e televisores.

21. **Equipamentos de telecomunicação** – equipamentos auxiliares (*hubs*, modems, roteadores, *switches*, etc.), dedicados à execução de tarefas específicas na rede, de acordo com os padrões tecnológicos estabelecidos.

22. **Estações compartilhadas** – computadores utilizados por mais de um usuário.

23. **Estação de trabalho** - computador conectado à rede, ou independente, utilizado pelos usuários para execução dos serviços diários, de acordo com os padrões tecnológicos estabelecidos.

24. **Falha/incidente** - qualquer evento adverso, relacionado à segurança de sistemas de computação ou de redes de computadores confirmado ou sob suspeita.

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

25. **Ferramenta de segurança** – software ou equipamento capaz de proteger e controlar os acessos às informações e ao ambiente do Instituto, de acordo com os padrões tecnológicos estabelecidos.

26. **Funcionários** – relacionamento contratual com indivíduos que possuem ocupação de caráter permanente, com salário acordado e direito(s) previsto(s) em lei.

27. **GED** – gerenciamento eletrônico de documentos.

28. **Gerente / Coordenador** – responsável pela administração do conjunto de atividades e informações pertinentes à sua área de atuação, deliberando ações necessárias que permitam o pleno funcionamento das operações do Instituto.

29. **Gestão de Capacidade** - tem o objetivo de gerenciar o armazenamento e desempenho dos ativos do ambiente de TI.

30. ***Hardware*** – é a parte física do computador, palpável, ou seja, é o conjunto de componentes eletrônicos, circuitos integrados, placas e cabos, que se comunicam através de barramentos.

31. **Incidente de Segurança** - um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à sistemas ou a própria informação, levando a perda de um ou mais princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade.

32. **Informação:** qualquer conteúdo falado, escrito, armazenado ou não, utilizado na comunicação interna ou externa pelos colaboradores, fornecedores, prestadores de serviços, terceiros ou clientes.

33. **Integridade:** é a precisão e a manutenção da totalidade da informação, bem como sua validade de acordo com os padrões estabelecidos e expectativas do negócio.

34. **Internet** - Internet é um sistema global de redes de computadores interligados que possibilita o acesso a informações sobre e em qualquer lugar do mundo.

35. **Informação crítica -** que pode causar danos ou perdas graves à organização.

36. **Incidente** – qualquer acontecimento que não faça parte do comportamento padrão que cause ou possa causar, uma interrupção ou redução da qualidade de um serviço.

37. **Identificador do usuário / *User id*** - identificação/nome do usuário no ambiente informatizado.

38. **Local seguro** – cofre, armário com tranca, sala com sistema de segurança.

39. ***Login*** – chave de acesso que identifica o usuário na rede e/ou softwares.

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

40. ***Logoff*** - terminar o uso de um sistema computacional, removendo a senha do usuário. Trata-se de um reiniciar rápido, onde todos os programas são fechados e posteriormente é possível iniciar a área de trabalho com outro usuário.

41. **Manutenção física** – conjunto de operações (revisão, inspeção e correção de falhas) que visam à conservação e proteção de um recurso em uso.

42. **Manutenção lógica** – ação efetivada mediante dispositivo ou ferramenta de diagnóstico de *software* usada em testes de varredura para verificações regulares no equipamento, objetivando prevenir e/ou corrigir falhas.

43. **Parceiros** – relacionamento contratual com indivíduos ou empresas que objetiva a realização ou desenvolvimento de projetos comuns, com funções, direitos e responsabilidades claramente definidos.

44. **Privilégio de administrador da máquina local** – privilégio concedido para instalação de aplicativos, arquivos executáveis e de alteração de configuração no computador.

45. **Proprietário de ativos de informação** - pessoa que define o nível de classificação do ativo de informação.

46. **Patches** – pacotes de correção/atualização de sistemas operacionais e aplicativos.

47. **Rede cabeada** – computadores interligados a rede via cabo.

48. **Redmine** - software livre, gerenciador de projetos baseados na web e ferramenta de gerenciamento de bugs.

49. **Recursos** – equipamentos de hardware ou *software* e outros meios, que manipulam ou armazenam, direta ou indiretamente informações do Instituto.

50. **Recursos de Tecnologia da Informação** – hardware, *software* ou pessoas que manipulam direta ou indiretamente informações, inclusive a própria informação.

51. **Reinicialização de Contas** – é a mudança da senha do usuário em caso de esquecimento.

52. **Senha** – código secreto do usuário que comprova a identidade de uma chave de acesso. Chave eletrônica que abre as portas da rede e dos sistemas.

53. **Servidores** – equipamentos que servem de repositório de *software* e/ou dados ou gerenciam recursos da rede, de acordo com os padrões tecnológicos estabelecidos pelo Instituto.

54. **Sistema de negócio** – conjunto de serviços ou responsabilidades que possam ser solicitados.

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669

55. ***Software*** – parte lógica do computador, programa adquirido ou desenvolvido pelo Instituto e que atualizam ou não informações no banco de dados do Instituto.

56. ***Software* de órgãos públicos** – sistemas distribuídos pelo Governo.

a. Exemplo: DIRF, CAGED, etc.

57. ***Software* de uso exclusivo** - aquele que não passou pela análise da GTE.

58. ***Software* crítico** - sistema onde uma falha pode resultar em impactos muito altos para o negócio.

59. ***Software* restrito, proprietário**, **não livre** – é um *software* para computadores que é licenciado com direitos exclusivos para o produtor.

60. ***Spam*** – um ou vários e-mails de conteúdo malicioso ou propaganda não autorizada, enviados para vários usuários, causando aumento no tráfego da rede interna ou externa.

61. ***Spyware*** - consiste em um programa automático de computador, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Intranet, sem o conhecimento e consentimento do usuário.

62. ***Teamview*** - Pacote de software proprietário para acesso remoto, compartilhamento de área de trabalho, conferência online e transferência de arquivos entre computadores.

63. **Terceiros** – relacionamento contratual com empresas especializadas que objetiva a transferência planejada de atividades secundárias.

64. **Trello** - aplicativo *web* de gerenciamento de projeto.

65. **Trilha de auditoria** - termo genérico para registro de uma sequência de atividades.

66. **U.R.A.** – Unidade de resposta audível.

67. **Usuários** – pessoas que utilizam os recursos de Tecnologia da Informação de propriedade ou controlados pelo Instituto.

a. Exemplos: colaboradores, parceiros e terceiros (pessoa física ou jurídica).

68. **VPN** - *Virtual Private Network* – Acesso a rede corporativa por meio de uma rede doméstica.

69. ***WiFi*** - *Wireless Fidelity* - rede sem fio para acesso a Internet.

70. **Vírus** - *software* capaz de infectar outros *softwares*, sistemas operacionais e arquivos de um computador, causando variados efeitos ao funcionamento normal do computador.

www.postalis.org.br
Setor Comercial Norte Quadra 5
Torre sul sala 401 – Brasília Shopping
Asa Norte
70715900 - Brasília – DF
(61) 40033669