Tipo do Documento	Código	Página	Versão
POLÍTICA	GETEC-001	1 de 9	1.5

Título:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Este documento **CANCELA** e **SUBSTITUI** os documentos:
Política de Segurança da Informação-2014

Versão	Data	Descrição da Alteração	Elaboração	Verificação	Liberação
0.0	01/06/2014	Documento Original			
1.0	08/08/2018	Análise do documento original 2014	Flavio Fernandes	Leonardo Peixoto	
1.1	14/08/2018	Atualização do documento	Flavio Fernandes	Leonardo Peixoto	
1.2	08/10/2018	Ajustes finais	Flavio Fernandes	Leonardo Peixoto	
1.3	16/10/2018	Apresentação para DE	Flavio Fernandes	Leonardo Peixoto	
1.4	05/11/2018	Apresentação para CDE	Flavio Fernandes	Leonardo Peixoto	
1.5	10/11/2018	Ajustes conforme solicitação do CDE	Flavio Fernandes	Leonardo Peixoto	

Índice

1. INTRODUÇÃO

1.1. A informação é um recurso fundamental para o desenvolvimento das atividades do SERPROS e, como tal, necessita ser protegida. A Política de Segurança da Informação visa preservar a confidencialidade, a integridade e a disponibilidade da informação.

1.2. Este documento estabelece os princípios e diretrizes que norteiam a segurança da informação no SERPROS. É aprovado e divulgado por decisão da Diretoria Executiva e do Conselho Deliberativo, que apoiam e fomentam as iniciativas necessárias ao alcance dos objetivos de segurança estabelecidos.

2. OBJETIVO

2.1. Estabelecer princípios e orientar a definição de mecanismos de segurança que garantam o cuidado, a legalidade, a credibilidade e o prestígio do SERPROS na prestação dos seus serviços e, consequentemente, que preservem a continuidade dos seus negócios.

2.2. Definir o escopo da segurança da informação no SERPROS e suas diretrizes para gerência e administração segura dos seus ativos.

2.3. Servir de referência para auditoria, apuração e avaliação de responsabilidades.

3. DOCUMENTOS DE REFERÊNCIA

N/A

4. ABRANGÊNCIA

4.1. Esta política aplica-se aos conselheiros, diretores, empregados, gestores, contratados, temporários, fornecedores, parceiros e outras partes envolvidas com o SERPROS. Deve ser lida e conhecida por todos os usuários da informação.

4.2. A política é aplicável ao ambiente informatizado de armazenamento da Informação. Abrange todos os equipamentos e sistemas possuídos ou utilizados pelo SERPROS para estes fins.

5. GLOSSÁRIO

5.1. Ativos: Qualquer coisa que tenha valor para a organização.

5.2. **Ativos de informação**: Qualquer informação que tenha valor para a organização.

5.3. **Colaboradores**: Conselheiros, diretores, gestores, empregados, estagiários, fornecedores, terceirizados ou quaisquer outras pessoas que sejam usuários de informações.

5.4. **Confidencialidade**: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

5.5. **Integridade**: salvaguarda da exatidão, completeza da informação e dos métodos de processamento.

5.6. **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes.

5.7. **Custodiante**: pessoa ou órgão com atribuição fornecida pelo proprietário da informação de proteger adequadamente esta informação.

5.8. **Responsável pela informação**: Gestor da área onde a informação é gerada. Define o nível de classificação da informação. (recebe o nome de proprietário dos ativos ou proprietário da informação na NBR ISO/IEC 27002:2005).

5.9. **Usuário**: pessoa que acessa ou utiliza de forma legítima e autorizada as informações.

5.10. **Terceiros**: pessoas que prestam serviço e podem possuir acesso às instalações e recursos de informação do SERPROS.

5.11. **Incidente de segurança**: evento não planejado que pode acarretar prejuízos a empresa ou mesmo violar as regras de segurança.

5.12. **Áreas sensíveis**: são áreas ou setores que concentram uma quantidade considerável de informações estratégicas para o negócio.

6. CONFORMIDADE

6.1. Ao usuário de informações não é dado o direito de desconhecimento da Política de Segurança da Informação, devendo seguir rigorosamente o disposto nas regras.

6.2. Esta política deve ser comunicada para todo o pessoal envolvido e largamente divulgada, garantindo que todos a conheçam e a pratiquem.

6.3. A inobservância das políticas e normas de segurança sujeita o usuário a sanções internas e, nos casos cabíveis, às leis vigentes.

6.4. Verificações para assegurar o nível e elaborar projetos para melhoria dos índices de conformidade ou correções de não conformidade.

7. DEVERES E RESPONSABILIDADES

7.1. Dos Colaboradores

7.1.1 Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os equipamentos de informática disponibilizados para a realização do seu trabalho.

7.1.2 Cumprir as determinações desta Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis.

7.1.3 Utilizar recursos e sistemas de informações do SERPROS somente para os fins profissionais.

7.1.4 Todas as informações que forem transitadas internamente e externamente devem ser feitas através de mecanismos corporativos (e-mail da instituição) os documentos que atualmente são anexados na ferramenta de e-mail, devem ser compartilhados com a nova estrutura de serviços em Nuvem e não mais anexados ao e-mail corporativo. As informações/documentos que forem necessários transitar fora da corporação devem ter a aprovação do responsável da área.

7.1.5 Todos os contatos externos (e-mails, telefones, empresas) devem ser registrados em sistema de contato corporativo e sempre atualizados com o assunto e a origem da demanda.

7.1.6 Responder, por todo e qualquer acesso, aos recursos bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado.

7.1.7 Comunicar por escrito ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio.

7.2 **Dos Diretores e Gestores**

7.2.1. Gerenciar o cumprimento desta Política, por parte de seus supervisionados.

7.2.2. Identificar os desvios praticados e adotar as medidas corretivas apropriadas.

7.2.3. Impedir o acesso de empregados demitidos ou demissionários aos ativos, utilizando-se dos mecanismos de desligamento do empregado.

7.2.4. Zelar, em nível físico e lógico, pelos ativos de informação e de processamento do SERPROS relacionados com sua área de atuação.

7.2.5. Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações.

7.2.6. Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI (Tecnologia da Informação), que acessos e permissões devem ter os colaboradores, sob sua supervisão, à informações e sistemas.

7.2.7. Comunicar formalmente à unidade que efetua a concessão de privilégios aos usuários de TI (Tecnologia da Informação), quais os colaboradores demitidos ou transferidos, para exclusão de permissões no cadastro dos usuários.

7.2.8. Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI (Tecnologia da Informação), aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários.

7.3. **Dos Prestadores de Serviço**

7.3.1. Devem estar previstas nos contratos, cláusulas que contemplem a responsabilidade dos funcionários e prestadores de serviços no cumprimento desta Política de Segurança da Informação, suas normas e procedimentos.

8. DIRETRIZES

8.1. Toda informação gerada pelos usuários, utilizando integralmente ou parcialmente recursos do SERPROS, é de propriedade exclusiva do SERPROS.

8.2. O SERPROS, como custodiante de dados e informações de participantes e beneficiários, os considera sigilosos, logo devem ser tratados assim pelos seus colaboradores.

8.3. As ideias e métodos desenvolvidos na Entidade, devem servir exclusivamente aos interesses do SERPROS.

8.4. No que se refere às informações em custódia do SERPROS, considera-se proibido tudo aquilo que não esteja previamente autorizado por esta política e demais documentos normativos.

8.5. Devem ser prevenidas, através de controles, todas as possibilidades de vazamento de informações do SERPROS.

8.6. A divulgação de informações classificadas do SERPROS deverá ser feita por meio das áreas específicas, segundo suas atribuições e com autorização da Diretoria Executiva e/ou Conselho Deliberativo.

8.7. Os colaboradores devem utilizar os recursos da Entidade seguindo os princípios de segurança sem afetar ou causar prejuízo a outrem.

8.8. Eventual descumprimento desta Política de Segurança de Informação deve ser imediatamente comunicado ao superior imediato.

8.9. Todas as espécies de pressões e chantagens devem ser denunciadas.

8.10. Deve ser mantido um Sistema de Gestão de Segurança da Informação (SGSI), contemplando todas as áreas do SERPROS, que possa fazer a gestão dos riscos do negócio sobre o aspecto da segurança das informações, definir e melhorar seus indicadores.

8.11. Devem fazer parte do SGSI, Normas e Procedimentos que regulamentem os requisitos de segurança da informação no SERPROS.

8.12. O Gerenciamento de Riscos deve identificar por tipo de exposição, avaliar quanto à probabilidade de incidência e quanto ao impacto, todos os riscos que possam comprometer a realização dos objetivos do SERPROS. Os resultados devem ser comparáveis entre si, reproduzíveis e devem orientar as ações de gestão apropriadas para a implementação dos controles adequados.

8.13. Os sistemas de controles internos devem ser continuamente reavaliados e aprimorados, principalmente quanto ao risco de segurança das informações, com procedimentos apropriados nos processos de cada área.

8.14. Todos os processos internos devem estar mapeados e documentados. Além de serem revisados periodicamente visando elevar o nível de maturidade na sua segurança.

8.15. As informações devem ser classificadas quanto a confidencialidade e identificadas de forma a serem adequadamente armazenadas, copiadas, transmitidas, manuseadas, descartadas ou destruídas. Esta classificação deve estar coerente com a importância estratégica para o negócio do SERPROS.

8.16. As medidas de proteção aos recursos devem ser aplicadas de forma compatível com o risco e com o valor da informação para os negócios do SERPROS. Por consequência deve existir uma sistemática para classificação das informações.

8.17. Todos os ativos de informação devem ser identificados, classificados, permanentemente atualizados pelo Responsável pela informação.

8.18. No quadro de pessoal e de prestadores de serviços deve haver uma efetiva segregação de atividades e funções de forma que uma mesma pessoa não assuma simultaneamente responsabilidades das quais decorram interesses conflitantes, ainda que de forma meramente esporádica ou eventual.

8.19. A delegação de atribuições deve ser formal, com responsabilidades claramente delimitadas mediante definição de poderes, limites e alçadas, inclusive em relação a serviços de terceiros.

8.20. Deve haver um processo que visa conscientizar os usuários da necessidade da segurança das informações e aspectos previstos na Política de Segurança da Informação.

8.21. Os empregados devem estar devidamente capacitados quanto à correta e eficiente utilização dos recursos, de acordo com as normas em vigor.

8.22. A Gestão de Segurança da Informação do SERPROS deve ser feita por empregados da Entidade, devidamente capacitados para a função.

8.23. Um Plano de Continuidade do Negócio, cujo objetivo é manter em funcionamento os processos e serviços críticos, na ocorrência de desastres, atentados, falhas e intempéries, deve ser mantido atualizado, testado e documentado.

8.24. Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.

8.25. Os procedimentos de cópia de segurança (backup) e de recuperação (restore) devem ser documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações, e devem ser descritos na Instrução Normativa de Backup, Restauração e Descarte dos Dados Sensíveis.

8.26. Na concessão de quaisquer acessos aos recursos, físicos ou lógicos, deve ser observado o princípio do menor privilégio, que consiste em conceder somente os acessos e recursos estritamente necessários ao desempenho das atividades autorizadas.

8.27. Os colaboradores devem ter acesso físico e lógico liberado, somente aos recursos e informações necessários e indispensáveis ao desempenho de suas atividades e em conformidade com os interesses do SERPROS.

8.28. As autorizações devem ser concedidas de acordo com as necessidades de desempenho das funções e considerando o princípio do menor privilégio, conforme descrito na Instrução Normativa de Acesso e Uso dos Recursos da Rede.

8.29. Mecanismos de segurança baseados em sistemas de proteção de acesso devem ser utilizados para proteger as transações entre redes externas e a rede interna.

8.30. Os serviços de rede e acessos devem ser controlados e apresentados no documento de Normas de acesso do SERPROS.

8.31. As senhas, certificações digitais e outras formas de autenticação são individuais, secretas, intransferíveis e protegidas com grau de segurança compatível com a informação associada.

8.32. O acesso às áreas sensíveis deve ser resguardado, por meio do uso de dispositivos de controle de acesso e utilização de câmeras de monitoração.

8.33. O acesso de visitantes e colaboradores às dependências do SERPROS deve ser registrado através de controle de acesso de visitantes.

8.34. As câmeras de segurança devem gravar as imagens captadas para posterior análise do pessoal responsável ou através de solicitação formal.

8.35. As imagens devem ser armazenadas de forma protegida. Os procedimentos para armazenamento e restauração são definidos na Instrução Normativa de Backup, Restauração e Descarte dos Dados Sensíveis.

8.36. Devem ser guardados os registros de segurança (logs), de modo a auxiliar na identificação de desvios, falhas ou usos indevidos, além de serem periodicamente analisados para os propósitos de caráter corretivo, legal e de auditoria. O período de análise dever ser sempre o menor possível. O gestor de cada área deve indicar quais informações farão parte do registro de segurança.

8.37. Os registros (informações, arquivos, documentos, imagens) devem ser protegidos e armazenados com segurança, o período de armazenamento é definido pela área operacional, através de comunicação formal e validação dos gestores responsáveis.

8.38. Os computadores servidores, seus sistemas, switches e No-Breaks devem ser monitorados, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.

8.39. Os controles e administração de Servidores e Serviços que forem aplicados fora das dependências do SERPROS (Nuvem), devem ser feitos por profissionais da Instituição, não existindo dependências de terceiros para atividades de confiança.

8.40. Os horários das máquinas devem estar sincronizados para permitir o rastreamento de eventos.

8.41. Todas as informações do SERPROS, que forem enviadas ou divulgadas para terceiros, devem ser através de arquivos PDF e possuir a Assinatura Digital dos Gerentes e ou Diretores SERPROS.

8.42. As mídias e informações serão eliminadas de forma segura. Procedimentos formais para a eliminação segura de informações são definidos através da Instrução Normativa de Backup, Restauração e Descarte dos Dados Sensíveis.

8.43. Uma política de mesa e tela limpa deve ser implementada para reduzir o risco de acessos não autorizados ou danos a documentos/papeis, mídias e recursos de processamento de informações.

8.44. A comunicação interna e externa deve ser clara e objetiva, contemplando todas as partes interessadas, porém sem expor informações confidenciais e/ou estratégicas.

8.45. As cláusulas contratuais devem ser avaliadas criteriosamente para que haja definição clara dos papéis e responsabilidades entre as partes envolvidas, níveis de processamento necessário, segurança, monitoração e requisitos de contingência.

8.46. Acordos de confidencialidade devem ser firmados para garantir a confidencialidade das informações do SERPROS.

8.47. As informações armazenadas nos Servidores SERPROS, devem possuir Data de validada e prazo máximo de armazenamento, após o vencimento deste prazo as informações/arquivos, serão armazenados em Servidores secundários, caso seja necessário consultar estas informações/arquivos, deve enviar comunicação formal para a área de TI.

9. VIOLAÇÕES E PENALIDADES

9.1. Sanções previstas no Regulamento Disciplinar, Código de Ética e legislação vigente.

10. RESPONSABILIDADES

Cargos	Funções
Gerente de TI	Gerenciar projetos e operações de Serviços de Tecnologia da Informação.
Coordenador de TI	Orientar o trabalho de infraestrutura e suporte no desenvolvimento e aplicações de Softwares.
Analistas de TI	Responsável por Instalar, configurar e administrar redes de computadores.
Desenvolvedor	Especificar e codificar programas para área operacional e de negócio.

11. VALIDADE

Após a divulgação e disponibilização no site, considerar 12 meses de validade ou quando surgir tecnologia relevante aos processos em andamento.

12. APROVAÇÃO

Esta Política foi aprovada na Reunião Ordinária do Conselho Deliberativo em 14/12/2018, através da DL 14/2018, e vigora a partir da assinatura da deliberação.