# DECLARAÇÃO DE APLICABILIDADE REGISTRA S/A

registra

| Controle | Aplicabilidade | Requisito | Objetivo do controle | Status do Controle | Justificativa |
|---|---|---|---|---|---|
| **A.5 Políticas de segurança da informação** | | | | | |
| **A.5.1 Orientação da Direção para segurança da informação** | | | | | |
| **A5.1.1** | Sim | Política de segurança da informação | Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela direção, publicado e comunicado para funcionários e partes externas relevantes. | Implementado | Conjunto de Políticas foram aplicadas para mitigação de riscos. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A5.1.2** | Sim | Análise crítica das políticas para segurança da informação | As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia | Implementado | Aplicação de análise crítica para ajustes necessários, quando pertinente. |
| **A.6 REGISTRA da segurança da informação** | | | | | |
| **A.6.1 REGISTRA interna** | | | | | |
| **A6.1.1** | Sim | Responsabilidades e papéis pela segurança da informação | Todas as responsabilidades pela segurança da informação devem ser definidas e atribuídas | Implementado | As responsabilidades e autoridades foram definidas para o SGSI. |
| **A6.1.2** | Sim | Segregação de funções | Funções conflitantes e áreas de | Implementado | Possuem um Comitê de SI e as decisões e |

| | | | | | |
|---|---|---|---|---|---|
| | | | responsabilidade devem ser segregadas para reduzir as oportunidades de modificação não autorizada ou intencional, ou uso indevido dos ativos da REGISTRA. | | responsabilidades compartilhadas. |
| **A6.1.3** | Sim | Contato com autoridades | Contatos apropriados com autoridades relevantes devem ser mantidos | Implementado | Contatos com autoridades são estabelecidos e estão disponíveis para contatar em caso de incidente na REGISTRA que envolvam os ativos críticos. |
| **A6.1.4** | Sim | Contato com grupos especiais | Contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança devem ser mantidos | Implementado | Contatos são realizados através de fóruns, grupos sobre SI com objetivo de trocas de conhecimento e aprendizados.de conhecimento e aprendizados. |
| **A6.1.5** | Sim | Segurança da informação no gerenciamento de projetos | Segurança da informação deve ser considerada no gerenciamento de projetos independentemente do tipo do projeto | Implementado | Os projetos precisam considerar os requisitos de SI para mitigar os riscos em projetos. |
| **A.6.2 Dispositivos móveis e trabalho remoto** | | | | | |
| **A6.2.1** | Sim | Política para o uso de dispositivo móvel | Uma política e medidas que apoiam a segurança da informação devem ser adotadas para gerenciar os riscos | Implementado | Segurança da informação para uso de dispositivos moveis aplicada. |

| | | | | | |
|---|---|---|---|---|---|
| | | | decorrentes do uso de dispositivos moveis | | |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A6.2.2** | Sim | Trabalho Remoto | Uma política e medidas que apoiam a segurança da informação devem ser implementadas para proteger informações acessadas, processadas ou armazenadas em locais de trabalho remoto | Implementado | O trabalho remoto possui requisitos de SI com o objetivo de não ocorrer incidentes. |
| **A.7 Segurança em recursos humanos** | | | | | |
| **A.7.1 Antes da contratação** | | | | | |
| **A7.1.1** | Sim | Seleção | Verificações do histórico devem ser realizadas para todos os candidatos a emprego de acordo com a ética e regulamentações. | Implementado | A seleção é realizada com os requisitos de SI para cargos que possuem atividades com impacto. |
| **A7.1.2** | Sim | Termos e condições de contratação | As obrigações contratuais com funcionários e partes externas devem declarar a sua responsabilidade e a da REGISTRA para a segurança da informação. | Implementado | Os contratos declaram as responsabilidades e compromisso com a SI. |
| **A.7.2 Durante a contratação** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **A7.2.1** | Sim | Responsabilidades da Direção | A direção deve requerer aos funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da REGISTRA. | Implementado | A Alta Direção requer o compromisso com a SI com o objetivo de ter o comprometimento de todos. |
| **A7.2.2** | Sim | Conscientização, educação e treinamento em segurança da informação | Todos os funcionários da REGISTRA e onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções. | Implementado | Conscientização e treinamentos sobre SI para obter o compromisso de toda a REGISTRA. |
| **A7.2.3** | Sim | Processo disciplinar | Deve existir um processo disciplinar formal implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação | Implementado | Sanções determinadas para ações que impactam a SI. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A.7.3 Encerramento e mudança da contratação** | | | | | |
| **A7.3.1** | Sim | Responsabilidades pelo encerramento ou mudança da contratação | As responsabilidades e obrigações pela segurança da informação que permaneçam validados após um encerramento ou | Implementado | Processo de encerramento e mudança de perfil determinado com o objetivo de não ter nenhum acesso |

| | | | | | |
|---|---|---|---|---|---|
| | | | mudança da contratação devem ser definidas, comunicadas aos funcionários ou partes externas cumpridas. | | indevido a informação. |
| **A.8 Gestão de ativos** | | | | | |
| **A.8.1 Responsabilidade pelos ativos** | | | | | |
| **A8.1.1** | Sim | Inventário dos ativos | Os ativos associados com informação e com os recursos e processamento da informação devem ser identificados, e um inventario destes ativos deve ser estruturado e mantido. | Implementado | Controle dos ativos de SI. |
| **A8.1.2** | Sim | Proprietário dos ativos | Os ativos no inventario devem ter um proprietário. | Implementado | Determinado os responsáveis pelos ativos, a REGISTRA efetua o controle de ativos. |
| **A8.1.3** | Sim | Uso aceitável dos ativos | Regras para o uso aceitável das informações dos ativos associados com informação e os recursos de processamento da informação devem ser identificados, documentados e implementados. | Implementado | Uso e mal uso de ativos para não ter acessos indevidos e incidentes de segurança. |
| **A8.1.4** | Sim | Devolução de ativos | Todos os funcionários e partes externas devem devolver todos os ativos da REGISTRA que estejam em sua posse após o encerramento de | Implementado | Uso e mal uso de ativos para não ter acessos indevidos e incidentes de segurança. |

| | | | | | |
|---|---|---|---|---|---|
| | | | suas atividades do contrato ou acordo. | | |
| **A.8.2 Classificação da informação** | | | | | |
| **A8.2.1** | Sim | Classificação da informação | A informação deve ser classificada em termos do seu valor, requisitos legais. Sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. | Implementado | Determinação do valor do ativo, classificando a informação. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A8.2.2** | Sim | Rótulos e tratamento da informação | Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela REGISTRA | Implementado | Rotular a informação para conhecimento de quem acessa. |
| **A8.2.3** | Sim | Tratamento dos ativos | Procedimentos para tratamento dos ativos devem ser desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela REGISTRA | Implementado | Uso e mal uso de ativos para não ter acessos indevidos e incidentes de segurança. |
| **A.8.3 Tratamento de mídias** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **A8.3.1** | Sim | Gerenciamento de mídias removíveis | Procedimentos devem ser implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela REGISTRA | Implementado | Controle sobre mídias removíveis no acesso aos ativos da REGISTRA. . |
| **A8.3.2** | Sim | Descarte de mídias | As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais | Implementado | Descartar mídias com segurança para não ter acesso indevido. |
| **A8.3.3** | Não | Transferência física de mídias | Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso improprio ou corrupção durante o transporte. | Não implementado | Controle não aplicável a REGISTRA, pois não realiza transferência de mídias. |
| **A.9 Controle de acesso** | | | | | |
| **A.9.1 Requisitos do negócio para controle de acesso** | | | | | |
| **A9.1.1** | Sim | Política de controle de acesso | Uma política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios. | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |
| **A9.1.2** | Sim | Acesso às redes e aos serviços de rede | Os usuários devem somente receber acesso as redes e aos serviços de rede que tenham sido | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |

| | | | | | |
|---|---|---|---|---|---|
| | | | especificamente autorizados a usar. | | |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A.9.2 Gerenciamento de acesso ao usuário** | | | | | |
| **A9.2.1** | Sim | Registro e cancelamento de usuário | Um processo formal de registro e cancelamento de usuário deve ser implementado para permitir atribuição dos direitos de acesso. | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |
| **A9.2.2** | Sim | Provisionamento para acesso de usuário | Um processo formal de provisionamento de acesso do usuário deve ser implementado para conceder ou revogar os direitos de acesso para todos os tipos de sistemas e serviços. | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |
| **A9.2.3** | Sim | Gerenciamento de direitos de acesso privilegiados | A concessão e uso de direitos de acesso privilegiado devem ser restritos e controlados. | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |
| **A9.2.4** | Sim | Gerenciamento da informação de autenticação secreta de usuários | A concessão de informação de autenticação secreta deve ser controlada por meio de um processo de gerenciamento formal. | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |

| | | | | | |
|---|---|---|---|---|---|
| **A9.2.5** | Sim | Análise crítica dos direitos de acesso de usuário | Os proprietários de ativos devem analisar criticamente os direitos de acesso dos usuários a intervalos regulares. | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |
| **A9.2.6** | Sim | Retirada ou ajuste dos direitos de acesso | Os direitos de acesso de todos os funcionário e partes externas as informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades. | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |
| **A.9.3 Responsabilidade dos usuários** | | | | | |
| **A9.3.1** | Sim | Uso da informação de autenticação secreta | Os usuários devem ser orientados a seguir pratica da REGISTRA quanto ao uso da informação de autenticação secreta. | Implementado | Determinar as responsabilidades dos usuários com a autenticação secreta a ativos de informação. . |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A.9.4 Controle de acesso ao sistema e à aplicação** | | | | | |
| **A9.4.1** | Sim | Restrição de acesso à informação | O acesso à informação e as funções dos sistemas de aplicações devem ser restritos de acordo com | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |

| | | | | | |
|---|---|---|---|---|---|
| | | | a política de controle de acesso. | | |
| **A9.4.2** | Sim | Procedimentos seguros de entrada no sistema (log-on) | Onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (log-on). | Implementado | Controlar acessos de usuários de acordo com uma política determinada, baseada em perfis. |
| **A9.4.3** | Sim | Sistema de gerenciamento de senha | Sistemas para gerenciamento de senhas devem ser interativos e devem assegurar senhas de qualidade. | Implementado | Determinar política de senhas seguras e de qualidade através de um processo determinado. |
| **A9.4.4** | Sim | Uso de programas utilitários privilegiados | O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado. | Implementado | Controle de programas utilitários que possam sobrepor os controles de sistemas. |
| **A9.4.5** | Sim | Controle de acesso ao código-fonte de programas | O acesso ao código fonte deve ser restrito. | Implementado | Proteção de código-fonte de programas, com devidas restrições de acesso. |
| **A.10 Criptografia** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **A.10.1 Controles criptográficos** | | | | | |
| **A10.1.1** | Sim | Política para o uso de controles criptográficos | Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação. | Implementado | Determinação de criptografia de acordo com a classificação da informação. |
| **A10.1.2** | Sim | Gerenciamento de chaves | Uma política sobre o uso, proteção e tempo de vida das chaves criptográficas deve ser desenvolvida e implementada ao longo de todo o seu ciclo de vida. | Implementado | Controlar as chaves de criptografia no seu ciclo de vida. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A.11 Segurança física e do ambiente** | | | | | |
| **A.11.1 Áreas seguras** | | | | | |
| **A11.1.1** | Sim | Perímetro de segurança física | Perímetros de segurança devem ser definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis. | Implementado | Segurança no perímetro físico controlando acessos indevidos a áreas sensíveis. |
| **A11.1.2** | Sim | Controles de entrada física | As áreas seguras devem ser protegidas por | Implementado | Segurança no perímetro físico controlando acessos |

| | | | | | |
|---|---|---|---|---|---|
| | | | controles apropriados de entrada para assegurar que somente pessoas autorizadas acesso permitido. | | indevidos a áreas sensíveis. |
| **A11.1.3** | Sim | Segurança em escritórios, salas e instalações | Deve ser projetada e aplicada a segurança física para escritórios, salas e instalações. | Implementado | Segurança no perímetro físico controlando acessos indevidos a áreas sensíveis. |
| **A11.1.4** | Sim | Proteção contra ameaças externas e do meio ambiente | Deve ser projetada e aplicada a proteção física contra desastres naturais, ataques maliciosos ou acidentes. | Implementado | Protegendo as áreas contra ameaças externas com políticas de segurança. |
| **A11.1.5** | Sim | Trabalhando em áreas seguras | Devem ser projetados e aplicados procedimentos para o trabalho em áreas seguras. | Implementado | Protegendo as áreas contra ameaças externas com políticas de segurança. |
| **A11.1.6** | Sim | Áreas de entrega e de carregamento | Pontos de acesso, como áreas de entrega e de carregamento, e outros pontos em que pessoas não autorizadas possam entrar nas instalações devem ser controlados e se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado. | Implementado | Segurança no perímetro físico controlando acessos indevidos a áreas sensíveis. |

| Controle | Aplicabilidade | Requisito | Objetivo do controle | Status do Controle | Justificativa |
|---|---|---|---|---|---|
| **A.11.2 Equipamentos** | | | | | |
| **A11.2.1** | Sim | Localização e proteção do equipamento | Os equipamentos devem ser protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado. | Implementado | Proteção de equipamentos para não ter acessos indevidos e incidentes. . |
| **A11.2.2** | Sim | Utilidades | Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades. | Implementado | Controlando e protegendo os equipamentos por falhas de elétricas. |
| **A11.2.3** | Sim | Segurança do cabeamento | O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos. | Implementado | Proteção dos cabeamentos para não ter acessos indevidos e incidentes. |
| **A11.2.4** | Sim | Manutenção dos equipamentos | Os equipamentos devem ter manutenção correta para assegurar a sua continua integridade e disponibilidade. | Implementado | Manter os equipamentos seguros com manutenções regulares. |
| **A11.2.5** | Sim | Remoção de ativos | Equipamentos, informações ou software não devem ser retirados do local sem autorização previa. | Implementado | Controle na remoção dos ativos da REGISTRA, controle de ativos. |

| | | | | | |
|---|---|---|---|---|---|
| **A11.2.6** | Sim | Segurança de equipamentos e ativos fora das dependências da REGISTRA | Devem ser tomadas medidas de segurança par ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da REGISTRA. | Implementado | Ações para proteção em equipamentos fora da REGISTRA e que não tenham acessos indevidos. . |
| **A11.2.7** | Sim | Reutilização ou descarte seguro de equipamentos | Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre gravados com segurança. | Implementado | Assegurar que os equipamentos foram descartados de forma segura para não ter acessos indevidos a informação. . |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A11.2.8** | Sim | Equipamento de usuário sem monitoração | Os usuários devem assegurar que os equipamentos não monitorados tem proteção adequada. | Implementado | Proteção de equipamentos sem monitoração evitando incidentes a ativos de informação da REGISTRA. |
| **A11.2.9** | Sim | Política de mesa limpa e tela limpa | Deve ser adotada uma política de mesa limpa para papeis e mídia de armazenamento removíveis e uma política de tela limpa para os recursos de | Implementado | Manter mesa limpa e tela limpa para evitar acessos indevidos e vazamento de informações. |

| | | | | | |
|---|---|---|---|---|---|
| | | | processamento da informação. | | |
| **A.12 Segurança nas operações** | | | | | |
| **A.12.1 Responsabilidades e procedimentos operacionais** | | | | | |
| **A12.1.1** | Sim | Documentação dos procedimentos de operação | Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que necessitam deles. | Implementado | Documentação de procedimento operacionais para obter controle eficaz das atividades. |
| **A12.1.2** | Sim | Gestão de mudanças | Mudanças na REGISTRA, nos processos do negócio, nos recursos de processamento da informação devem ser controladas. | Implementado | Controle de mudanças em ativos de processamento de informações evitando possível incidente. |
| **A12.1.3** | Sim | Gestão de capacidade | A utilização dos recursos deve ser monitorada e ajustada e as projeções devem ser feitas para necessidades de capacidades futura para garantir o desempenho requerido do sistema. | Implementado | Monitorar e controlar a capacidade de utilização dos recursos. Garantir o desempenho necessário. |
| **A12.1.4** | Sim | Separação dos ambientes de desenvolvimento, teste e produção | Ambientes de desenvolvimento, teste e produção devem ser separados par reduzir os riscos de acessos ou modificações não | Implementado | Separação de ambientes reduzindo os riscos de acessos ou modificações não autorizadas. |

| | | | | | |
|---|---|---|---|---|---|
| | | | autorizadas no ambiente de produção. | | |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A.12.2 Controles contra *malware*** | | | | | |
| **A12.2.1** | Sim | Controles contra malware | Devem ser implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário. | Implementado | Controles para detecção, prevenção e recuperação para proteção de malwares. . |
| **A.12.3 Cópias de segurança** | | | | | |
| **A12.3.1** | Sim | Cópias de segurança das informações | Copias de controle de segurança das informações, softwares e das imagens do sistema devem ser efetuadas e testadas regularmente conforme a política de geração de copias de segurança definida. | Implementado | Backups e Restore realizados, para restauração de informações de forma eficaz. |
| **A.12.4 Registros e monitoramento** | | | | | |
| **A12.4.1** | Sim | Registros de eventos | Registros de eventos (logs) das atividades do usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente a intervalos regulares. | Implementado | Controlar os eventos de Logs das atividades de usuários, controle de eventos de SI |

| | | | | | |
|---|---|---|---|---|---|
| **A12.4.2** | Sim | Proteção das Informações dos registros de eventos | As informações do registro de eventos (logs) e seus recursos devem ser protegidos contra acesso não autorizado e adulteração. | Implementado | Controlar os eventos de Logs das atividades de usuários, controle de eventos de SI. |
| **A12.4.3** | Sim | Registros de eventos de administrador e operador | As atividades dos administradores e operadores do sistema devem ser registradas e os registros (logs) devem ser protegidos e analisados criticamente a intervalos regulares. | Implementado | Controlar os eventos de Logs das atividades de operador e administrador, controle de eventos de SI. |
| **A12.4.4** | Sim | Sincronização dos relógios | Os relógios de todos os sistemas de processamento de informações relevantes, dentro da REGISTRA ou do domínio de segurança, devem ser sincronizados com uma fonte de tempo precisa. | Implementado | Obter a fonte de tempo precisa em caso de eventos e incidentes de SI. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A.12.5 Controle de *software* operacional** | | | | | |
| **A12.5.1** | Sim | Instalação de software nos sistemas operacionais | Procedimentos para controlar a instalação de software em sistemas operacionais devem ser implementados. | Implementado | Controle de instalações de softwares controlar as mudanças de software em |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | sistemas operacionais. . |
| **A.12.6 Gestão de vulnerabilidades técnicas** | | | | | |
| **A12.6.1** | Sim | Gestão de vulnerabilidades técnicas | Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser avaliadas e devem ser tomadas as medidas apropriadas para lidar com os riscos associados. | Implementado | Prevenção de exploração de vulnerabilidades técnicas. |
| **A12.6.2** | Sim | Restrições quanto à instalação de software | Regras definindo critérios para instalação de software devem ser estabelecidas e implementadas. | Implementado | Prevenção de exploração de vulnerabilidades técnicas, controle e restrições de instalações de softwares por usuários. . |
| **A.12.7 Considerações quanto à auditoria de sistemas de informação** | | | | | |
| **A12.7.1** | Sim | Controles de auditoria de sistemas de Informação | As atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar interrupção nos processos do negócio. | Implementado | Minimizar o impacto das atividades de auditoria nos sistemas operacionais. . |
| **A.13 Segurança nas comunicações** | | | | | |
| **A.13.1 Gerenciamento de segurança em redes** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **A13.1.1** | Sim | Controles de redes | As redes devem ser gerenciadas e controladas para proteger as informações nos sistemas e aplicações. | Implementado | Garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam. . |
| **A13.1.2** | Sim | Segurança dos serviços de rede | Mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados. | Implementado | Garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A13.1.3** | Sim | Segregação de redes | Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes. | Implementado | Controlar os acessos as redes dividindo-a em diferentes domínios. . |
| **A.13.2 Transferência de informação** | | | | | |
| **A13.2.1** | Sim | Políticas e procedimentos para transferência de informações | Políticas, procedimentos e controles de transferências formais devem ser estabelecidos para proteger a transferência de informações | Implementado | Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas. |
| **A13.2.2** | Sim | Acordos para transferência de informações | Devem ser estabelecidos acordos para transferência segura de | Implementado | Manter a segurança da informação transferida dentro |

| | | | | | |
|---|---|---|---|---|---|
| | | | informações do negócio entre a REGISTRA e partes externas. | | da organização e com quaisquer entidades externas. |
| **A13.2.3** | Sim | Mensagens eletrônicas | As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas. | Implementado | Controlar as informações que trafegam em mensagens eletrônicas, de acordo com a classificação das informações. |
| **A13.2.4** | Sim | Acordos de confidencialidade e não divulgação | Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da REGISTRA para a proteção da informação devem ser identificados, analisados criticamente e documentados. | Implementado | Acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação. |
| **A.14 Aquisição, desenvolvimento e manutenção de sistemas** | | | | | |
| **A.14.1 Requisitos de segurança de sistemas de informação** | | | | | |
| **A14.1.1** | Sim | Análise e especificação dos requisitos de segurança da informação | Os requisitos relacionados com segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes. | Implementado | Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. |
| **A14.1.2** | Sim | Serviços de aplicação seguros em redes públicas | As informações envolvidas nos serviços de aplicação que transitam em redes públicas devem ser | Implementado | Garantir a segurança das informações que transitam em redes públicas. |

| | | | | | |
|---|---|---|---|---|---|
| | | | protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas. | | |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A14.1.3** | Sim | Protegendo as transações nos aplicativos de serviços | Informações envolvidas em transações nos aplicativos de serviços devem ser protegidas para prevenir transmissões incompletas, erros de roteamento | Implementado | Garantir a proteção das transações nos aplicativos de serviço, prevenindo transmissões incompletas, erros, alterações não autorizadas. |
| **A.14.2 Segurança em processos de desenvolvimento e de suporte** | | | | | |
| **A14.2.1** | Sim | Política de desenvolvimento seguro | Regras para o desenvolvimento de sistemas e software devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro da REGISTRA | Implementado | Garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. |
| **A14.2.2** | Sim | Procedimentos para controle de mudanças de sistemas | Mudanças em sistemas dentro do ciclo de vida de desenvolvimento devem ser controladas utilizando procedimentos formais de controle de mudanças. | Implementado | Garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. |
| **A14.2.3** | Sim | Análise crítica técnica das aplicações após mudanças nas | Aplicações críticas de negócios devem ser analisadas criticamente e | Implementado | Analises críticas e teste para assegurar que não ocorreu nenhum impacto |

| | | | | | |
|---|---|---|---|---|---|
| | | plataformas operacionais | testadas quando plataformas operacionais são mudadas, para garantir que não haverá nenhum impacto adverso na operação da REGISTRA ou na segurança. | | adverso nas operações da organização ou na segurança. |
| **A14.2.4** | Sim | Restrições sobre mudanças em pacotes de software | Modificações em pacotes de software devem ser desencorajadas e devem estar limitadas as mudanças necessárias, e todas as mudanças devem ser estritamente controladas. | Implementado | Mudanças controladas para desencorajar e limitar a prática. |
| **A14.2.5** | Sim | Princípios para projetar sistemas seguros | Princípios para projetar sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação. | Implementado | Garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| A**14.2.6** | Sim | Ambiente seguro para desenvolvimento | As organizações devem estabelecer e proteger adequadamente os ambientes seguros de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram | Implementado | Proteção dos ambientes de desenvolvimento garantindo a segurança dos sistemas de informação. |

| | | | | | |
|---|---|---|---|---|---|
| | | | todo o ciclo de vida de desenvolvimento de sistema. | | |
| **A14.2.7** | Não | Desenvolvimento terceirizado | A REGISTRA deve supervisionar e monitorar as atividades de desenvolvimento de sistemas terceirizado. | Não implementado | A REGISTRA não possui desenvolvimento terceiro. |
| **A14.2.8** | Sim | Teste de segurança do sistema | Testes de funcionalidade de segurança devem ser realizados durante o desenvolvimento de sistemas. | Implementado | Assegurar que o sistema está de acordo com o projeto planejado e requisitos foram atendidos. |
| **A14.2.9** | Sim | Teste de aceitação de sistemas | Programas de testes de aceitação e critérios relacionados devem ser estabelecidos para novos sistemas de informação, atualizações e novas versões. | Implementado | Assegurar que o sistema está de acordo com o projeto planejado e requisitos foram atendidos. |
| **A.14.3 Dados para teste** | | | | | |
| **A14.3.1** | Sim | Proteção dos dados para teste | Os dados de teste devem ser selecionados com cuidado, protegidos e controlados. | Implementado | Assegurar a proteção dos dados usados para teste. |
| **A.15 Relacionamento na cadeia de suprimento** | | | | | |
| **A.15.1 Segurança da informação na cadeia de suprimento** | | | | | |
| **A15.1.1** | Sim | Política de segurança da informação no relacionamento com os fornecedores | Requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da REGISTRA deem ser acordados com | Implementado | Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores. |

| | | | | | |
|---|---|---|---|---|---|
| | | | o fornecedor e documentados. | | |
| **A15.1.2** | Sim | Identificando segurança da informação nos acordos com fornecedores | Todos os requisitos de segurança da informação relevantes devem ser estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da REGISTRA. | Implementado | Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores. . |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A15.1.3** | Sim | Cadeia de suprimento na tecnologia da informação e comunicação | Acordos com fornecedores devem incluir requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação. | Implementado | Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores. |
| **A15.2.1** | Sim | Monitoramento e análise crítica de serviços com fornecedores | A REGISTRA deve monitorar, analisar criticamente e auditar, a intervalos regulares, a entrega dos serviços executados pelos fornecedores. | Implementado | Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores. . |

| | | | | | |
|---|---|---|---|---|---|
| **A15.2.2** | Sim | Gerenciamento de mudanças para serviços com fornecedores | Mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas, levando- se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos e a reavaliação dos riscos. | Implementado | Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores. |
| **A.16 Gestão de incidentes de segurança da informação** | | | | | |
| **A.16.1 Gestão de incidentes de segurança da informação e melhorias** | | | | | |
| **A16.1.1** | Sim | Responsabilidades e procedimentos | Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação. | Implementado | Assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação. |
| **A16.1.2** | Sim | Notificação de eventos de segurança da informação | Os eventos de segurança da informação devem ser relatados por meios dos canais de gestão, o mais rápido possível. | Implementado | Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | segurança da informação. |
| **A16.1.3** | Sim | Notificando fragilidades de segurança da informação | Os funcionários e partes externas que usam os sistemas de informação devem ser instruídos a notificar e registrar quaisquer fragilidades de SI, observada ou suspeita, nos sistemas ou serviços. | Implementado | Prevenir incidentes de segurança da informação. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A16.1.4** | Sim | Avaliação e decisão dos eventos de segurança da informação | Os eventos de segurança da informação devem ser reavaliados, e deve ser decidido se eles são classificados como incidentes de segurança da informação. | Implementado | Avaliações para tomada de decisão. . |
| **A16.1.5** | Sim | Resposta aos incidentes de segurança da informação | Incidentes de segurança da informação devem ser reportados de acordo com procedimentos documentados. | Implementado | Voltar ao nível de segurança normal e então iniciar a recuperação necessária. |
| **A16.1.6** | Sim | Aprendendo com os incidentes de segurança da informação | Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação devem ser usados para reduzir a probabilidade ou impacto de incidentes futuros. | Implementado | Reduzir a probabilidade ou o impacto de incidentes futuros. |
| **A16.1.7** | Sim | Coleta de evidências | A REGISTRA deve definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação das | Implementado | Servir como evidências. . |

| | | | | | |
|---|---|---|---|---|---|
| | | | informações, as quais pode servir como evidencias. | | |
| **A.17 Aspectos da segurança da informação na gestão da continuidade dos negócios** | | | | | |
| **A.17.1 Continuidade da segurança da informação** | | | | | |
| **A17.1.1** | Sim | Planejando a continuidade da segurança da informação | A REGISTRA deve determinar seus requisitos para a segurança da informação e continuidade da gestão da segurança da informação em situações adversas, por exemplo, uma crise ou ataque. | Implementado | Determinar os requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas. |
| **A17.1.2** | Sim | Implementando a continuidade da segurança da informação | A REGISTRA deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa. | Implementado | Implementar os requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas. |
| **A17.1.3** | Sim | Verificação, análise crítica e avaliação da continuidade da segurança da informação | A REGISTRA deve verificar os controles de continuidade de segurança da informação estabelecidos e implementados, a intervalos regulares, para garantir que eles são validos e eficazes em situações adversas. | Implementado | Garantir que os controles de continuidade de negócio são válidos e eficazes em situações adversas. |

| Controle | Aplicabilidade | Requisito | Objetivo do controle | Status do Controle | Justificativa |
|---|---|---|---|---|---|
| **A.17.2.1 Redundâncias** | | | | | |
| **A17.2.1** | Sim | Disponibilidade dos recursos de processamento da informação | Os recursos de processamento da informação devem ser implementados com redundância suficiente para atender os requisitos de disponibilidade. | Implementado | Assegurar a disponibilidade dos recursos de processamento da informação. |
| **A.18 Conformidade** | | | | | |
| **A.18.1 Conformidade com requisitos legais e contratuais** | | | | | |
| **A18.1.1** | Sim | Identificação da legislação aplicável e de requisitos contratuais | Todos os requisitos legislativos, estatutários, regulamentares e contratuais relevantes, e enfoque da REGISTRA para atender a esses requisitos, devem ser explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da REGISTRA. | Implementado | Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas á segurança da informação e de quaisquer requisitos de segurança. |
| **A18.1.2** | Sim | Direitos de propriedade intelectual | Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados | Implementado | Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas á segurança da informação e de |

| | | | | | |
|---|---|---|---|---|---|
| | | | com os direitos de propriedade intelectual e sobre o uso de produtos de softwares proprietários. | | quaisquer requisitos de segurança. |
| **A18.1.3** | Sim | Proteção de registros | Registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio. | Implementado | Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas á segurança da informação e de quaisquer requisitos de segurança. |
| **A18.1.4** | Sim | Proteção e privacidade de informações de identificação pessoal | A privacidade e proteção das informações de identificação pessoal devem ser asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável. | Implementado | Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas á segurança da informação e de quaisquer requisitos de segurança. |
| **Controle** | **Aplicabilidade** | **Requisito** | **Objetivo do controle** | **Status do Controle** | **Justificativa** |
| **A18.1.5** | Sim | Regulamentação de controles de criptografia | Controles de criptografia devem ser usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes. | Implementado | Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas á segurança da informação e de quaisquer requisitos de segurança. |

| A.18.2 Análise crítica da segurança da informação | | | | | |
|---|---|---|---|---|---|
| **A18.2.1** | Sim | Análise crítica independente da segurança da informação | O enfoque da REGISTRA para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, controles, politicas, processos e procedimentos para a segurança da informação) deve ser analisado criticamente, de forma independente, a intervalos planejados ou quando ocorrerem mudanças significativas. | Implementado | Garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização. |
| **A18.2.2** | Sim | Conformidade com as políticas e procedimentos de segurança da informação | Os gestores devem analisar criticamente a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação. | Implementado | Garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização. |
| **A18.2.3** | Sim | Análise crítica da conformidade técnica | Os sistemas de informação devem ser analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da REGISTRA. | Implementado | Garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização. Realização de análise crítica |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | técnica nos ativos de informação.<br>. |