DECLARAÇÃO DE APLICABILIDADE

Versão: 014
Data: 28/08/2025

Identificação de Controle (n°)	Descrição do Controle	Objetivo de Controle	Aplicabilidade	Implementado	Justificativa (Inclusão/Exclusão)	Documentos Associados Diretamente ao Controle (*Documentos do SGI em sua totalidade)
A.5. Controles Organizacionais						
5.1	Políticas de segurança da informação	A política de segurança da informação e as políticas específcas por tema devem ser defnidas, aprovadas pela direção, publicadas, comunicadas e reconhecidas pelo pessoal pertinente e pelas partes interessadas pertinentes, e analisadas criticamente em intervalos planejados e quando ocorrerem mudanças signifcativas.	Sim	Sim	Prover as diretrizes de segurança da informação da Alta Direção para a organização e partes intessadas, conforme apropriado.	Manual de Segurança da Informação; Política de Segurança da Informação; Atas do Comitê de Segurança da Informação; RAC; PO Gerir Auditorias do SGI; Manual do SGI; Resolução Administrativa n.º 17/2024 – Política de Segurança da Informação
5.2	Papéis e responsabilidades pela segurança da informação	Papéis e responsabilidades pela segurança da informação devem ser defnidos e alocados de acordo com as necessidades da organização.	Sim	Sim	Estabelecer, atribuir e comunicar os papéis e responsabilidades pela segurança da informação no âmbito do TCE-GO	Organograma; Manual de Segurança da Informação (item 4.0); Política de Segurança da Informação; Decritivo de Competência; Portaria 57/2023-GPRES; Resolução Administrativa Nº 11/2022
5.3	Segregação de funções	Funções confitantes e áreas de responsabilidade devem ser segregadas.	Sim	Sim	Mitigar os riscos de modificações não autorizadas nas informações da organização	Gestão de movimentação de pessoas via sistema GGP; Aplicação de Política de controle de acesso; Portaria de Designação; Registros Help Desk; Manual de Segurança da Informação (Gestão de acesso)
5.4	Responsabilidades da direção	A direção deve requerer que todo o pessoal aplique a segurança da informação de acordo com a política da segurança da informação estabelecida, com as políticas especifcas por tema e com os procedimentos da organização.	Sim	Sim	Demonstrar o comprometimento da Alta Direção com o Sistema de Gestão de Segurança da Informação incentivando o engajamento de todos os colaboradores, estagiários, aprendizes, prestadores de serviços e demais partes interessadas, conforme apropriado.	Participação ativa na aprovação de documentos vinculados ao Segurança da Informação; RAE´s e RAC´s; Termo de Responsabilidade; Termo de Referência para contratações; Canal de denuncias - Ouvidoria Manual de Integridade
5.5	Contato com autoridades	A organização deve estabelecer e manter contato com as autoridades relevantes.	Sim	Sim	Divulgar o contato de autoridades relevantes para eventuais necessidades e manter o contato ativo	Participação em grupos externos de segurança da informação; Plano de Continuidade de TI; Manual de Segurança da Informação (Comunicação Segura)
5.6	Contato com grupos de interesse especial	A organização deve estabelecer e manter contato com grupos de interesse especial ou com outros fóruns de especialistas em segurança e associações profssionais.	Sim	Sim	Manter a organização atualizada sobre os temas relacionados a segurança da informação e associações profissionais	Participação em grupos externos de segurança da informação de outras Organizações com foco em adquirir informações de boas práticas de segurança da informação, registro de informações por meio de ATA´s de Reunião.
5.7	Inteligência de ameaças	A organização deve estabelecer e manter contato com grupos de interesse especial ou com outros fóruns de especialistas em segurança e associações profssionais.	Sim	Sim	Analisar as tendências em ameaças de cibersegurança e dos impactos na organização, com o objetivo de identificar áreas de risco potencial para a organização. Adequar ferramentas/processos existentes visando a redução dos riscos.	Informativos Rotineiros ISH; Análise do ambiente interno - relatório ; Microsoft (site e aplicativo); Ata´s Reunião do Comitê de Segurança da Informação; Manual de Segurança da Informação (Ataques à sistemas e suas defesas) Política de Segurança da Informação.
5.8	Segurança da informação no gerenciamento de projetos	A segurança da informação deve ser integrada ao gerenciamento de projetos.	Sim	Sim	Assegurar que projetos passem por uma completa avaliação de potenciais riscos e impactos à segurança da informação, antes de sua implementação.	PO Gerir Vulnerabilidades; SONAR, SOC ISH (securonix), Manual de Segurança da Informação (Segurança da informação no gerenciamento de projetos)
5.9	Inventário de informações e outros ativos associados	Um inventário de informações e outros ativos associados, incluindo proprietários, deve ser desenvolvido e mantido.	Sim	Sim	Identificar e gerenciar as informações e os ativos da organização para realizar a devida proteção da informação	O PO Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos, Resolução Normativa nº. 10/2017 e seu anexo; Manual de Segurança da Informação (Gestão de Ativos)
5.10	Uso aceitável de informações e outros ativos associados	Regras para o uso aceitável e procedimentos para o manuseio de informações e outros ativos associados devem ser identifcados, documentados e implementados.	Sim	Sim	Prover as diretrizes para utilização segura das informações e dos ativos de propriedade da organização pelos colaboradores, estagiários, aprendizes, prestadores de serviços e demais partes interessadas, conforme apropriado.	O PO Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos, Resolução Normativa nº. 10/2017 e seu anexo; Manual de Segurança da Informação (Gestão de Ativos, Politica de Privacidade e Gestão de acesso virtual) Termo de Responsabilidade.
5.11	Devolução de ativos	Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação.	Sim	Sim	Garantir a proteção adequada das informações da organização após encerramento de contratação e demais acordos firmados.	Termo de Responsabilidade profissional; Termo de Patrimonio; Manual de Segurança da Informação (Gestão de Ativos, Politica de Privacidade e Gestão de acesso virtual) PO Gerir Patrimonio
5.12	Classifcação das informações	As informações devem ser classifcadas de acordo com as necessidades de segurança da informação da organização, com base na confdencialidade, integridade, disponibilidade e requisitos das partes interessadas relevantes.	Sim	Sim	Classificar as informações em formato digital ou físico, assegurando que a informação receba o nível adequado de proteção.	Manual de Segurança da Informação (5.9); PO Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos; Resolução Normativa nº 10/2017 (portaria de classificação).

5.13	Rotulagem de informações	Um conjunto adequado de procedimentos para rotulagem de informações deve ser desenvolvido e implementado de acordo com o esquema de classifcação de informações adotado pela organização.	Sim	Sim	Identificar as informaçõs de acordo com a classificação faclilitando que a informação receba o nível adequado de proteção.	Manual de Segurança da Informação (Gestão de Ativos, Transferência de Infromações); PO Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos; Resolução Normativa nº 10/2017 (portaria de classificação). Sistemas Eletronicos de gestão.
5.14	Transferência de informações	Regras, procedimentos ou acordos de transferência de informações devem ser implementados para todos os tipos de recursos de transferência dentro da organização e entre a organização e outras partes.	Sim	Sim	Garantir a proteção adequada das informações da organização durante as transferências realizadas dentro da organização e com partes interessadas externas.	Manual de Segurança da Informação (Gestão de Ativos, Transferência de Infromações); PO Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos; Resolução Normativa nº 10/2017 (portaria de classificação). Sistemas Eletronicos de gestão. Gestão e Controle de Acessos.
5.15	Controle de acesso	Regras para controlar o acesso físico e lógico às informações e a outros ativos associados devem ser estabelecidas e implementadas com base nos requisitos de segurança da informação e de negócios.	Sim	Sim	Garantir a acesso autorizado e devido as informações da organização	Manual de Segurança da Informação (Gestão de acesso virtual, Gestão e controle de acesso fisico e demais diretrizes associadas) Política de Segurança da Informação, considerando dentre as politicas e diretrizes ali traçadas a politica de controle de acessos.
5.16	Gestão de identidade	O ciclo de vida completo das identidades deve ser gerenciado.	Sim	Sim	Garantir que as etapas do ciclo de identidade de acesso às informações sejam cumpridas de acordo com as políticas da organização	Manual de Segurança da Informação (Gestão de acesso virtual, Gestão e controle de acesso fisico, Gestão da identidade e autenticação e demais diretrizes associada) Política de Segurança da Informação, considerando dentre as politicas e diretrizes ali traçadas a politica de controle de acessos. Sistema Help Desk
5.17	Informações de autenticação	A alocação e a gestão de informações de autenticação devem ser controladas por uma gestão de processo, incluindo aconselhar o pessoal sobre o manuseio adequado de informações de autenticação.	Sim	Sim	Garantir a confiabilidade dos acessos as informações a aos ativos da organização	Manual de Segurança da Informação ((Gestão de acesso virtual, Gestão e controle de acesso fisico, Gestão da identidade e autenticação e demais diretrizes associada) Política de Segurança da Informação, considerando dentre as politicas e diretrizes ali traçadas a politica de controle de acessos. Sistema Help Desk.
5.18	Direitos de acesso	Os direitos de acesso às informações e a outros ativos associados devem ser provisionados, analisados criticamente, modifcados e removidos de acordo com a política de tema específco e com as regras da organização para o controle de acesso.	Sim	Sim	Garantir que os acessos sejam definidos e autorizados de acordo com os requisitos estabelecidos pela	Manual de Segurança da Informação ((Gestão de acesso virtual, Gestão e controle de acesso fisico, Gestão da identidade e autenticação e demais diretrizes associada) Resolução Normativa nº 10/2017 (portaria de classificação). Sistemas Eletronicos de gestão. Gestão e Controle de Acessos. **Termo de Responsabilidade Profissional**
5.19	Segurança da informação nas relações com fornecedores	Processos e procedimentos devem ser defnidos e implementados para gerenciar a segurança da informação e os riscos associados com o uso dos produtos ou serviços dos fornecedores.	Sim	Sim	Garantir que a segurança da informação seja considerada nos acordos estabelecidos com os fornecedores serviços.	Manual de Segurança da Informação (Gestão de Requisitos legais, estatutários, regulamentares e contratuais); Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação; Contratos firmados, gestão de contratos e Termos de Referência contratuais.
5.20	Abordagem da segurança da informação nos contratos de fornecedores	Requisitos relevantes de segurança da informação devem ser estabelecidos e acordados com cada fornecedor, com base no tipo de relacionamento com o fornecedor	Sim	Sim	Identificar os requisitos relevantes de segurança da informação para cada fornecedor e garantir o cumprimento desses requisitos, conforme acordado com os fornecedores	Manual de Segurança da Informação (Gestão de Requisitos legais, estatutários, regulamentares e contratuais); Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação; Contratos firmados, gestão de contratos e Termos de Referência contratuais; Manual de Integridade (informações referente a DUE Dilingence item 6.2).
5.21	Gestão da segurança da informação na cadeia de fornecimento de TIC	Processos e procedimentos devem ser defnidos e implementados para gerenciar os riscos da segurança da informação associados à cadeia de fornecimento de produtos e serviços de TIC.	Sim	Sim	Identificar os requisitos relevantes de segurança da informação para cada fornecedor e garantir o cumprimento desses requisitos, conforme acordado com os fornecedores	Manual de Segurança da Informação (Gestão de Requisitos legais, estatutários, regulamentares e contratuais); Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação; Contratos firmados, gestão de contratos e Termos de Referência contratuais.
5.22	Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores	A organização deve monitorar, analisar criticamente, avaliar e gerenciar regularmente a mudança nas práticas da segurança da informação dos fornecedores e na prestação de serviços.	Sim	Sim	Monitorar e medir o nível de serviço prestado de acordo com o contratado ou a entrega do serviço adquirido.	Manual de Segurança da Informação (Gestão de Requisitos legais, estatutários, regulamentares e contratuais) RAC; RAE; Contratos firmados, Gestão de contratos; PO Gerir Atendimento de Suporte de TI; PO Gerir Melhoria Contínua; Manual do SGI item Gestão de Mudanças.
5.23	Segurança da informação para uso de serviços em nuvem	Os processos de aquisição, uso, gestão e saída de serviços em nuvem devem ser estabelecidos de acordo com os requisitos da segurança da informação da organização.	Sim	Sim	Gerenciar a segurança da informação nos serviços em nuvem, desde sua aquisição até a sua saída.	Manual de Segurança da Informação (Gestão de serviços em nuvem); Serviço de Nuvem Contratado.
5.24	Planejamento e preparação da gestão de incidentes da segurança da informação	A organização deve planejar e se preparar para gerenciar incidentes da segurança da informação, defnindo, estabelecendo e comunicando processos, papéis e responsabilidades de gestão de incidentes da segurança da informação.	Sim	Sim	Prover as diretrizes para identificação, comunicação, classificação e tratamento dos incidentes de segurança da informação.	PO Gerir Incidentes de Segurança da Informação; PO Gerir Vulnerabilidades; Registro Hel Desk; Ata Reunião do Comitê de Segurança da Informação; Contrato ISH e indicador de Getsão de incidentes; Plano de Contínuidade de TI. Manual de Segurança da Informação (comunicação segura, Gestão de Incidentes de Segurança da Informação) SOC (Centro de Operações de Segurança)

5.25	Avaliação e decisão sobre eventos da segurança da informação	A organização deve avaliar os eventos da segurança da informação e decidir se categoriza como incidentes da segurança da informação.	Sim	Sim	Prover as diretrizes para o tratamento dos incidentes de segurança da informação.	PO Gerir Incidentes de Segurança da Informação; PO Gerir Vulnerabilidades; Registro Hel Desk; Ata Reunião do Comitê de Segurança da Informação; Contrato ISH e indicador de Getsão de incidentes; Plano de Contínuidade de TI. Manual de Segurança da Informação; SOC (Centro de Operações de Segurança).
5.26	Resposta a incidentes da segurança da informação	Os incidentes da segurança da informação devem ser respondidos de acordo com os procedimentos documentados.	Sim	Sim	Garantir a agilidade na tratativa dos incidentes de segurança da informação.	PO Gerir Incidentes de Segurança da Informação; PO Gerir Vulnerabilidades; Registro Hel Desk; Ata Reunião do Comitê de Segurança da Informação; Contrato ISH e indicador de Getsão de incidentes; Plano de Contínuidade de TI. Manual de Segurança da Informação; SOC (Centro de Operações de Segurança).
5.27	Aprendizado com incidentes de segurança da informação	O conhecimento adquirido com incidentes de segurança da informação deve ser usado para fortalecer e melhorar os controles da segurança da informação.	Sim	Sim	Gerenciar os incidentes e identificar oportunidades de melhorias e/ou ações corretivas visando a redução de ocorrências.	PO Gerir Melhoria Contínua; PO Gerir Incidentes de Segurança da Informação; RegistroSGP (inicativas de melhoria); Ata Reunião do Comitê de Segurança da Informação; Contrato ISH e indicador de Getsão de incidentes; Manual de Segurança da Informação (comunicação segura, Gestão de Incidentes de Segurança da Informação); SOC
5.28	Coleta de evidências	A organização deve estabelecer e implementar procedimentos para identifcação, coleta, aquisição e preservação de evidências relacionadas a eventos da segurança da informação.	Sim	Sim	Garantir o tratamento adequado e proteção das evidências para apoiar na gestão de incidentes de segurança da informação	PO Gerir Incidentes de Segurança da Informação; PO Gerir Vulnerabilidades; Registro Hel Desk e Redimine; Ata Reunião do Comitê de Segurança da Informação; Contrato ISH e indicador de Getsão de incidentes; Plano de Contínuidade de TI. Manual de Segurança da Informação (comunicação segura, Gestão de Incidentes de Segurança da Informação); SOC (Centro de Operações de Segurança).
5.29	Segurança da informação durante a disrupção	A organização deve planejar como manter a segurança da informação em um nível apropriado durante a disrupção.	Sim	Sim	Garantir a segurança da informação dos processos críticos do Sistema de Gestão da Segurança da Informação, durante uma interrupção ou falha	PO Gerir Incidentes de Segurança da Informação; PO Gerir Vulnerabilidades; Registro Hel Desk e Redimine; Ata Reunião do Comitê de Segurança da Informação; Contrato ISH e indicador de Getsão de incidentes; Plano de Contínuidade de TI. Manual de Segurança da Informação (comunicação segura, Gestão de Incidentes de Segurança da Informação) SOC (Centro de Operações de Segurança).
5.30	Prontidão de TIC para continuidade de negócios	A prontidão de TIC deve ser planejada, implementada, mantida e testada com base nos objetivos de continuidade de negócios e nos requisitos de continuidade da TIC.	Sim	Sim	Garantir os objetivos da organização possam continuar a ser cumpridos durante a disrupção	Plano de continuidade de TI - Garantindo prontidão de TIC deve ser planejada, implementada, mantida e testada com base nos objetivos de continuidade de negócios e nos requisitos de continuidade da TIC, PO Gerir Incidentes de Segurança da Informação, PO Gerir Vulnerabilidades.
5.31	Requisitos legais, estatutários, regulamentares e contratuais	Os requisitos legais, estatutários, regulamentares e contratuais pertinentes à segurança da informação e à abordagem da organização para atender a esses requisitos devem ser identifcados, documentados e atualizados.	Sim	Sim	Garantir a conformidade legal e contratual da organização	Manual Segurança da Informação (Gestão de Requisitos legais, estatutários, regulamentares e contratuais) Quadro de Dispositivos Legais
5.32	Direitos de propriedade intelectual	A organização deve implementar procedimentos adequados para proteger os direitos de propriedade intelectual.	Sim	Sim	Garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual	Manual de Segurança da Informação (Garantia dos Direitos de Propriedade Intelectual)
5.33	Proteção de registros	Os registros devem ser protegidos contra perdas, destruição, falsifcação, acesso não autorizado e liberação não autorizada.	Sim	Sim	Garantir a proteção, disposição e retenção adequada dos registros	Controle de Registros operacionais gerenciados ao final de padrão operacional instituido; PO Gerir Processos de Trabalho. PO Gerir Backup. Sistema SGP Intranet
5.34	Privacidade e proteção de DP	A organização deve identifcar e atender aos requisitos relativos à preservação da privacidade e à proteção de DP, de acordo com as leis e os regulamentos aplicáveis e requisitos contratuais.	Sim	Sim	Garantir a conformidade legal da organização na privacidade e proteção de dados pessoais, de acordo com as legislações vigentes e regulamentos pertinentes	Politica de Privacidade e proteção de dados pessoais; Manual de Segurança da Informação (Gestão de Requisitos legais, estatutários, regulamentares e contratuais, Politica de privacidade)

5.35	Análise crítica independente da segurança da informação	A abordagem da organização para gerenciar a segurança da informação e sua implementação, incluindo pessoas, processos e tecnologias, deve ser analisada criticamente, de forma independente, a intervalos planejados ou quando ocorrerem mudanças signifcativas.	Sim	Sim	Garantir a eficácia da gestão de Segurança da Informação	PO Gerir Auditorias do SGI RAC Reunião de Analise Critica Manual do SGI (9.3)
5.36	Compliance com políticas, regras e normas para segurança da informação	O compliance da política de segurança da informação da organização, políticas, regras e normas de temas especifcos deve ser analisado criticamente a intervalos regulares.	Sim	Sim	Garantir a implementação da segurança da informação conforme as diretrizes da organização	Manual de Segurança da Informação; Atas do Comitê de Segurança da Informação; RAC; Manual do SGI; Resolução Administrativa n.º 17/2024 – Política de Segurança da Informação; Manual de Integridade.
5.37	Documentação dos procedimentos de operação	Os procedimentos de operação dos recursos de tratamento da informação devem ser documentados e disponibilizados para o pessoal que necessite deles.	Sim	Sim	Garantir a eficácia da operação dos serviços e recursos de tratamento da informação	Gestão de processos operacionais via site e via sgp, integração organizacional e reuniões de gestão. PO Gerir Processos de Trabalho. PO Gerir Melhoria Contínua Cadeia de valor. Manual do SGI. Sistema SGP.
A.6. Controles de Pessoas						
6.1	Seleção	Verificações de antecedentes de todos os candidatos a serem contratados devem ser realizadas antes de ingressarem na organização e de modo contínuo, de acordo com as leis, os regulamentos e a ética aplicáveis, e devem ser proporcionais aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.	Sim	Sim	Garantir a comprovação dos requisitos para preenchimento das quailifcações necessárias dos cargos.	PO Gerir Caotação, Alocação e Integração de Servidores; Edital de Concurso; Código de Etica, Manual do SGI (7.1.2); Manual de Função Resolução Admin Regulamentação de funções no TCE 19/2022.
6.2	Termos e condições de contratação	Os contratos trabalhistas devem declarar as responsabilidades do pessoal e da organização para a segurança da informação.	Sim	Sim	Garantir a conscientização e responsabilidade com a segurança da informação das partes envolvidas na contratação	Termo de responsibilidade profissional; Codigos de etica, Contrato de Trabalho (vide sistema eletrônico GGP); Política de Gestão de Pessoas (Roslução Administrativa 05/2024); Processos da GGP, Manual de Integridade.
6.3	Conscientização, educação e treinamento em segurança da informação	O pessoal da organização e partes interessadas relevantes devem receber treinamento, educação e conscientização em segurança da informação apropriados **e atualizações regulares da política de segurança da informação** da organização, políticas e procedimentos específicas por tema, pertinentes para as suas funções.	Sim	Sim	Garantir que os colaboradores sejam treinados sobre segurança da informação e conscientizados sobre suas respectivas responsabilidades	Manual do SGI (7.1.2, 7.1.6 e 7.2); PO Gerir Capacitação, Alocação e Integração de Servidores; PO Gerir as Ações de Capacitação; PO Planejar e Gerir o Conhecimento-Biblioteca; PO Gerir Multiplicadores e Instrutores Internos; Manual de Segurança da Informação; Lista de Presença de Integração e demais treinamentos.
6.4	Processo disciplinar	Um processo disciplinar deve ser formalizado e comunicado, para tomar ações contra pessoal e outras partes interessadas relevantes que tenham cometido uma violação da política da segurança da informação.	Sim	Sim	Definir e comunicar as consequências aplicadas em casos de violação da política de segurança da informação	Codigo de Ética; Resolução Administrativa nº. 8/2015. Manual de Integridade Política de Integridade; Processos Comissão de Ética.
6.5	Responsabilidades após encerramento ou mudança da contratação	As responsabilidades e funções de segurança da informação que permaneçam válidas após o encerramento ou a mudança da contratação devem ser defnidas, aplicadas e comunicadas ao pessoal e a outras partes interessadas pertinentes.	Sim	Sim	Garantir a proteção das informações no processo de encerramento ou mudança de contratação	Manual de Segurança da Informação (item gestão de identidade e autenticação); Politica de Controle de Acessos (ciclo de vida do usuário); PO Gerir Atendimento de Suporte de TI. Gestão de movimentação de pessoas (Portaria Presidencia, Sistema Eletronico GGP); PO Gerir Capacitação, Alocação e Integração de Servidores.
6.6	Acordos de confidencialidade ou não divulgação	Acordos de confdencialidade ou não divulgação que refitam as necessidades da organização para a proteção das informações devem ser identifcados, documentados, analisados criticamente em intervalos regulares e assinados pelo pessoal e por outras partes interessadas pertinentes.	Sim	Sim	Resguardar a confidencialidade das informações nos acordos estabelecidos	Termo de responsabilidade profissional. - Para equipe colaboradores na entrada do exercicio da função para terceiros no incio do contrato e a cada nova troca de equipe. Politica de Privacidade; Manual de Segurança da Informação; Manual de Integridade.
6.7	Trabalho remoto	Medidas de segurança devem ser implementadas quando as pessoas estiverem trabalhando remotamente para proteger as informações acessadas, tratadas ou armazenadas fora das instalações da organização.	Sim	Sim	Garantir a segurança da informação na utilização segura de acesso remoto ao ambiente tecnológico da organização	Resolução Admisnitratva nº 18/2023 considerando padrões para o trabalho remoto; Manual de Segurança da Informação (item Gestão da Segurança da Informação no Trabalho Remoto);
6.8	Relato de eventos de segurança da informação	A organização deve fornecer um mecanismo para que as pessoas relatem eventos da segurança da informação observados ou suspeitos por meio de canais apropriados em tempo hábil.	Sim	Sim	Definir e divulgar as diretrizes para notificações de eventos de segurança da informação	Help desk / Email /Grupo intermo de segurança da informação e canais diretos de comunicação. PO Gerir Atendimento de Suporte de TI. PO Gerir Incidentes de Segurança da Informação, PO Gerir Vulnerabilidades.
A.7. Controles Físicos						
7.1	Perímetros de segurança física	Perímetros de segurança devem ser defnidos e usados para proteger áreas que contenham informações e outros ativos associados.	Sim	Sim	Proteger os perímetros físicos da organização de acessos indevidos	Manual de Segurança da Informação (item Gestão e Controle de Acessos Físicos) Controle de Limites conforme padrão operacional da Assessoria Militar. Gestão de acesso via biometria; Controle de Imagens CFTV

7.2	Entrada física	As áreas seguras devem ser protegidas por controles de entrada e pontos de acesso apropriados.	Sim	Sim	Garantir acesso físico autorizado nas áreas seguras da organização	Manual de Segurança da Informação (item Gestão e Controle de Acessos Físicos) Controle de Limites conforme padrão operacional da Assessoria Militar. Gestão de acesso via biometria; Controle de Imagens CFTV
7.3	Segurança de escritórios, salas e instalações	Segurança física para escritórios, salas e instalações deve ser projetada e implementada	Sim	Sim	Garantir o acesso de pessoas autorizadas e a segurança física dos locais de tratamento de informações	Manual de Segurança da Informação (item Gestão e Controle de Acessos Físicos) Controle de Limites conforme padrão operacional da Assessoria Militar. Gestão de acesso via biometria; Controle de Imagens CFTV
7.4	Monitoramento de segurança física	As instalações devem ser monitoradas continuamente para acesso físico não autorizado	Sim	Sim	Identificar e evitar acessos físicos indevidos	Manual de Segurança da Informação (item Gestão e Controle de Acessos Físicos) Controle de Limites conforme padrão operacional da Assessoria Militar. Gestão de acesso via biometria; Controle de Imagens CFTV
7.5	Proteção contra ameaças físicas e ambientais	Proteção contra ameaças físicas e ambientais, como desastres naturais e outras ameaças físicas intencionais ou não intencionais à infraestrutura, deve ser projetada e implementada.	Sim	Sim	Proteger a organização e minimizar os efeitos de ameaças externas e ambientais	Plano de continuidade de TI; PO Responder Situações de Emergência; Manual de Abandono da Área; Manual de Práticas Seguras; Manual de Segurança da Informação PO Gerir Incidentes de Segurança da Informação; PO Gerir Vulnerabilidades. Evidência de Simulados realizados, assim como testes de sistemas. Planilha de Aspectos e Impactos Ambientais.
7.6	Trabalho em áreas seguras	Medidas de segurança para trabalhar em áreas seguras devem ser projetadas e implementadas.	Sim	Sim	Proteger as áreas seguras da organização contra acessos e atividades indevidas	Acessos controlados por meio de fechaduras eletronicas; Manual de Segurança da Informação Monitoramento eletrônico circuito de CFTV monitorado 24 horas.
7.7	Mesa limpa e tela limpa	Regras de mesa limpa para documentos impressos e mídia de armazenamento removível e regras de tela limpa para os recursos de tratamento das informações devem ser defnidas e adequadamente aplicadas.	Sim	Sim	Evitar a perda, alteração ou exfiltração de informação e ativos de informações da organização	Manual de Segurança da Informação (Item diretrizes mesa limpa e tela limpa); Termo de Responsabilidade Profissional; Treinamentos, Capacitações e conscientizações.
7.8	Localização e proteção de equipamentos	Os equipamentos devem ser posicionados com segurança e proteção.	Sim	Sim	Proteger os equipamentos que tratam informações críticas contra danos e acessos não autorizados.	Plano de continuidade de TI; PO Responder Situações de Emergência; Manual de Abandono da Área; Manual de Práticas Seguras; Manual de Segurança da Informação PO Gerir Incidentes de Segurança da Informação; PO Gerir Vulnerabilidades. Evidência de Simulados realizados, assim como testes de sistemas. Planilha de Aspectos e Impactos Ambientais. Instalações fisicas controladas e com devidos critérios de segurança adotados.
7.9	Segurança de ativos fora das instalações da organização	Os ativos fora das instalações da organização devem ser protegidos.	Sim	Sim	Garantir a proteção das informações da organização durante a realização de atividades fora das depedências da organização	PO Gerir Patrimônio; Gestão por memorando; Termo de entrega, recebimento, guada, conservação e responsabilidade. DMIP - Documento de Movimentação Interna de Patrimônio.
7.10	Mídia de armazenamento	As mídias de armazenamento devem ser gerenciadas por seu ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classifcação e com os requisitos de manuseio da organização.	Sim	Sim	Proteger informações em mídias de armazenamento utilizadas pelo Tribunal de Contas.	O controle é aplicável considerando que, embora o Tribunal de Contas não utilize pendrives, HDs externos ou fitas de backup como mídias de armazenamento regulares, há outros tipos de mídias relevantes como HDs de desktops, notebooks e servidores; Manual de Segurança da Informação; PO Gerir Atendimento de Suporte de TI; Laudo Técnico de Sanitização; PO Gerir Patrimonio; Termo de Respondabilidade; Código de Ética; Termo de Referência e cláusulas contratuais;
7.11	Serviços de infraestrutura	As instalações de tratamento de informações devem ser protegidas contra falhas de energia e outras disrupções causadas por falhas nos serviços de infraestrutura.	Sim	Sim	Proteger as áreas seguras de TI de incêndio, inundação, ventania, falhas elétricas, de telecomunicações ou demais desastres naturais ou estruturais	Plano de Continuidade do TI. PO Responder Situações de Emergência; Manual de Abandono da Área; Manual de Práticas Seguras; Manual de Segurança da Informação PO Gerir Incidentes de Segurança da Informação; PO Gerir Vulnerabilidades. Evidência de Simulados realizados, assim como testes de sistemas. Planilha de Aspectos e Impactos Ambientais.
7.12	Segurança do cabeamento	Os cabos que transportam energia ou dados, ou que sustentam serviços de informação, devem ser protegidos contra interceptação, interferência ou danos	Sim	Sim	Proteger o cabeamento de energia e dados contra danos causando o mau funcionamentos de aplicações críticas	Projeto eletrico do predio, Gestão e monioramento do manutenção predial. PO Gerir Manutenção Predial Manual de Conservação Predial do TCE. Rotinas de manutenção predial e indicadores de gestão.

7.13	Manutenção de equipamentos	Os equipamentos devem ser mantidos corretamente para assegurar a disponibilidade, integridade e confdencialidade da informação.	Sim	Sim	Proteger os equipamentos contra falhas e interrupções de serviços e indisponibilidade de informações	Atualização de sistemas Manutenção Física (Data de trocas e gestão de manutençõs por tempo de uso) Contrato de Manutenção Predial e de Equipamentos. PO Gerir Patrimonio. PO Gerir Atendimento de Suporte de TI, PO Gerir Manutenção Predial. PO Gerir Ativos
7.14	Descarte seguro ou reutilização de equipamentos	Os itens dos equipamentos que contenham mídia de armazenamento devem ser verifcados para assegurar que quaisquer dados confidenciais e software licenciado tenham sido removidos ou substituídos com segurança antes do descarte ou reutilização.	Sim	Sim	Proteger as informações da organização de acessos indevidos e garantir a adoção das medidas técnicas e organizacionais para cumprimento das ações previstas na LGPD	ITR Controle de Resíduos PO Gerir Resíduos PO Gerir Patrimonio, PO Gerir Atendimento de Suporte de TI, Laudo Técnico de Sanitização.
A.8. Controles Tecnológicos						
8.1	Dispositivos endpoint do usuário	As informações armazenadas, tratadas ou acessíveis por meio de dispositivos endpoint do usuário devem ser protegidas.	Sim	Sim	Evitar a exposição e proteger as informações da organização disponíveis nos equipamentos contra acessos indevidos levando ao seu comprometimento	Manual de Segurança da Informação (Ataques a sistemas e serviços de defesas, Gestão de identidade e autenticação, Uso de dispositivos móveis, Gestão de Acesso Virtual, Gestão da segurança da informação no trabalho remoto, Proteção contra Malware, Gestão de serviços em nuvem) Gestão da comunicação interna quanto a regras de segurança da informação. Termo Responsabilidade Profissional Informação Antivírus Firewall SOC
8.2	Direitos de acessos **privilegiad**	A atribuição e o uso de direitos de acessos privilegiados devem ser restritos e gerenciados	Sim	Sim	Proteger as informações de acessos indevidos e garantir a aplicação eficaz dos requisitos de garantia relativa a administradores de sistema / acesso privilegiado (internos e externos). Garantia do controle de acessos conforme segregação de função.	AD GPAC Git Aplicações internas e externas Politica de Controle de Acesso Manual de Segurança da Informação (Gestão de identidade e autenticação, Gestão de acesso virtual) Política de Segurança da Informação Gestão de acessos equipe DiTi. Autenticação Multifator (MFA) agente do antivírus SentinelOne e o Nessus (ferramenta que o SOC utiliza para identificar vulnerabilidades).
8.3	Restrição de acesso à informaç	O acesso às informações e a outros ativos associados deve ser restrito de acordo com a política específca por tema sobre controle de acesso.	Sim	Sim	Proteger as informações de acessos indevidos por colaboradores e terceiros	Manual de Segurança da Informação (Gestão de acesso virtual e Gestão de identidade e autenticação, Transferência da Informação, Gestão e Controle de Acesso Físico, Gerenciamento e distribuição de senhas para acesso a dados) Termo de responsabilidade profissional Política de Segurança da Informação Logs AD GPAC GIT Autenticação multifator (MFA) Políticas de senha forte Firewalls, NACs (controle de acesso à rede) Controle de pastas e arquivos com ACLs (listas de controle de acesso)
8.4	Acesso ao código-fonte	Os acessos de leitura e escrita ao código-fonte, ferramentas de desenvolvimento e bibliotecas de software devem ser adequadamente gerenciados.	Sim	Sim	Garantir a eficácia do funcionamento dos sistemas de TI e que o acesso ocorra somente por pessoas autorizadas. Item Implementado parcialmente via fornecedor externo durante o desenvolvimento e plenamente gerido internamente pela DITi na fase de manutenção e evolução.	Contrato de terceirização e termo de referencia forncedor Indra. Manual de Segurança da Informação (Gerenciamento e distribuição de senhas para acesso a dados)
8.5	Autenticação segura	Tecnologias e procedimentos de autenticação seguros devem ser implementados, com base em restrições de acesso à informação e à política específca por tema de controle de acesso.	Sim	Sim	Proteger as informações de acessos indevidos, seguindo as políticas da organização	Autenticação Multifator (MFA) Manual de Segurança da Informação (Gerenciamento e distribuição de senhas para acesso a dados, Gestão e controle de aceso físico) Política de Segurança da Informação Termo de Responsabilidade Profissional Comunicação Interna quanto a critérios de segurança da infromação.
8.6	Gestão de capacidade	O uso dos recursos deve ser monitorado e ajustado de acordo com os requisitos atuais e esperados de capacidade	Sim	Sim	Equilibrar as necessidades atuais e futuras por disponibilidade, desempenho e capacidade dos recursos para a segurança da informação (tecnologia, pessoas e instalações) com provisões técnicas e de serviços eficientes.	PDTI (Provisionamento de recursos) Zabbix SOC Reuniões internas de TI Manual de Segurança da Informação Política de Segurança da Informação Plano de Continuidade de TI

8.7	Proteção contra malware	Proteção contra malware deve ser implementada e apoiada pela conscientização adequada do usuário.	Sim	Sim	Garantir a proteção das informações da organização contra ataque de intrusos. Aplicação de ações técnicas, administrativas e comportamentais para prevenir, detectar e responder a códigos maliciosos (malware)	Sentinel One Manual de Segurança da Informação (Proteção contra Malware) Política de Segurança da Informação Deep Security Planilha de Gestão de Ativos. SOC (Monitoramento e Resposta a Incidentes) Bloqueio de Execução de Softwares não Autorizados PO Gerir Incidentes de Segurança da Informação PO Gerir Vulnerabilidades
8.8	Gestão de vulnerabilidades téc	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas; a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas	Sim	Sim	Avaliar o nível de risco geral da organização em relação à cibersegurança e elevar o nível de maturidade dos processos de segurança, minimizando os impactos no negócio, reduzindo a superfície de ataque, prevenindo explorações conhecidas e garantindo que a infraestrutura esteja protegida de falhas já documentadas.	Manual de Segurança da Informação (Atques a sistemas e suas defesas) SOC (Monitoramento e Resposta a Incidentes) PO Gerir Incidentes de Segurança da Informação PO Gerir Vulnerabilidades Microsoft Defender Redmine Ti (Avaliação de Risco da Vulnerabilidade) Firewalls internos Reuniões do Comitê de segurança da ifnormação garantindo responsabilidade e processo formalizado Tenable.io SIEM para auditoria de atividades privilegiadas PO Gerir Incidentes de Segurança da Informação, PO Gerir Vulnerabilidades
8.9	Gestão de confguração	As confgurações, incluindo confgurações de segurança, de hardware, software, serviços e redes, devem ser estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente.	Sim	Sim	Garantir a gestão e as funcionalidades dos equipamentos de acordo com as configurações determinadas. Garantir que os ativos de informação estejam configurados de maneira padronizada, segura, rastreável e auditável, evitando vulnerabilidades causadas por configurações incorretas ou inconsistentes.	PDTI (Provisionamento de recursos) Zabbix SOC Reuniões internas de TI Redmine Ti (Avaliação de Risco da Vulnerabilidade) Manual de Segurança da Informação (Gestão de Configuração) Política de Segurança da Informação Rotina de gestão de configuração Wiki Tenable.io Registros de configurações realizadas.
8.10	Exclusão de informações	As informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento devem ser excluídas quando não forem mais necessárias.	Sim	Sim	Garantir que informações armazenadas em sistemas, dispositivos ou mídias sejam excluídas de forma segura e apropriada quando não forem mais necessárias, a fim de evitar acesso não autorizado, vazamentos ou retenção indevida de dados.	Manual de segurança da informação (Gestão de Backup) Tabela de temporalidade (associada a Resolução Normativa n.º 010/2017 – Classificação das informações de acordo com grau de confidencialidade), Aplicação de Metodos seguros de exclusão; Gestão de informações via controle de registros ao final de cada processo operacional padrão. PO Gerir Backup.
8.11	Mascaramento de dados	O mascaramento de dados deve ser usado de acordo com a política específca por tema da organização sobre o controle de acesso e outros requisitos específcos por tema relacionados e requisitos de negócios, levando em consideração a legislação aplicável.	Sim	Sim	Reduzir o risco de exposição de dados sensíveis ou pessoais, especialmente em ambientes de desenvolvimento, homologação, testes, suporte ou relatórios, garantindo conformidade com a LGPD e outros requisitos legais.	Mapa de dados e Banco de Dados Política de Privacidade. Manual de Segurança da Informação (Gestão de identidade e autenticidade, gestão de acesso virtual, tranferencia de informação, controles criptograficos) Implementação de Técnicas de Mascaramento (conforme sistema) Política de Segurança da Informação Controle de acessos físicos via biometria em areas consideradas sensíveis Armario tipo cofre para arquivos sensíveis. Conformidade com a LGPD e Requisitos Legais
8.12	Prevenção de vazamento de dados	As medidas de prevenção de vazamento de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	Sim	Sim	Evitar o compartilhamento de informação sigilosa, podendo ser ou não intencional e garantir a adoção das medidas técnicas e organizacionais para cumprimento das ações previstas na LGPD	Manual de Segurança da Informação (Mesa limpa tela Limpa, Gestão de Identidade e Autenticação, Gestão de Acesso virtual, Gestão da segurança da infromação no trabalho remoto, Segurança da informação no gerenciamento de projetos, Transferência das informações) Politica de Privacidade e proteção de dados pessoais, Monitoramento por SOC e Ferramentas de Auditoria Proteção de E-mails e Compartilhamentos; Política de Segurança da Informação, Reuniões do Comitê de Segurança da Informação, PO Gerir Incidentes de Segurança da Informação, PO Gerir Vulnerabilidades. Help desk vinculado ao tema.
8.13	Backup das informações	Cópias de backup de informações, software e sistemas devem ser mantidas e testadas regularmente de acordo com a política específca por tema acordada sobre backup.	Sim	Sim	Garantir a continuidade e a disponibilidade das informações, mesmo diante de falhas, ataques ou incidentes que possam comprometer os dados originais.	Manual de Segurança da Informação (Gestão de Backup) Testes de integridade PO de Gerir Backup. Plano de Continuidade de TI. Integração com SOC para análise de incidentes de falha de backup Logs de backup e restauração

8.14	Redundância dos recursos de tratamento de informações	Os recursos de tratamento de informações devem ser implementados com redundância sufciente para atender aos requisitos de disponibilidade.	Sim	Sim	Assegurar que os recursos de processamento de informações (como servidores, rede, sistemas e armazenamento) estejam disponíveis mesmo diante de falhas técnicas, incidentes ou interrupções, por meio da implementação de mecanismos de redundância apropriados.	Uso de Ambientes em Nuvem com Alta Disponibilidade; Infraestrutura com Redundância Física e Lógica; Servidores com failover (cluster ativo-passivo ou ativo-ativo); Fontes de energia redundantes (UPS, nobreak, gerador); Redundância de links de internet (ISPs distintos); RAID em storages e servidores; Redundância em datacenters ou uso de nuvem híbrida. Plano de Continuidade de TI Zabbix (monitoramento de recursos); SOC para resposta a falhas em tempo real; Alertas automáticos para degradação de servicos.
8.15	Log	Logs que registrem atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados.	Sim	Sim	Assegurar que eventos de segurança, atividades críticas e exceções sejam registrados, protegidos e analisados, de forma a permitir: A detecção oportuna de incidentes; A rastreabilidade de ações e eventos relevantes; O apoio à investigação de falhas ou comportamentos suspeitos; O atendimento a requisitos legais, normativos ou contratuais.	Contrato ISH, Portal de chamados ISH, Habilitação de logs em sistemas, aplicações e redes Utilização de SIEM Zabbix e ferramentas de monitoramento Sincronização de data e hora (NTP) Proteção contra edição e exclusão indevida de logs Armazenamento seguro e com acesso restrito (Manual de segurança da informação e regras de gestão de acesso) Revisão periódica e análise crítica dos registros Retenção conforme requisitos legais e da política Registros do Firewall e Antivírus Gestão de Incidentes via Redmine TCE Goiás. Logs de sistemas operacionais e serviços. Manual de Segurança da Informação / Política de Segurança da informação
8.16	Atividades de monitoramento	As redes, sistemas e aplicações devem ser monitorados por comportamentos anômalos e por ações apropriadas, tomadas para avaliar possíveis incidentes de segurança da informação.	Sim	Sim	Garantir a detecção oportuna de eventos de segurança, atividades suspeitas e comportamentos anômalos, por meio do monitoramento contínuo de redes, sistemas e aplicações. Isso permite: Identificação proativa de potenciais ameaças ou incidentes de segurança; Ativação de respostas apropriadas; Suporte a análises forenses e ações corretivas; Apoio ao cumprimento de requisitos legais, normativos e contratuais.	Uso de ferramentas de SIEM (ex: Microsoft Sentinel, Splunk, QRadar) Monitoramento contínuo via Zabbix ou ferramentas similares Monitoramento de logs de sistemas operacionais, aplicações e dispositivos de rede Análise e registro de eventos de segurança relevantes Sentinel One Uso de firewall com logging e análise de tráfego SOC - ISH Antivírus Firewall Logs, PO Gerir Incidentes de Segurança da Informação, PO Gerir Vulnerabilidades. Registro Help Desk e Redmine TI Controle de acesso aos sistemas de monitoramento e aos registros gerados
8.17	Sincronização do relógio	Os relógios dos sistemas de tratamento de informações utilizados pela organização devem ser sincronizados com fontes de tempo aprovadas.	Sim	Sim	Assegurar que todos os sistemas da organização utilizem referências de tempo consistentes e precisas, garantindo a correção e integridade dos registros de logs.	Configuração de servidores internos para uso de protocolo NTP (Network Time Protocol) Sincronização de relógios dos servidores, equipamentos de rede, estações de trabalho e sistemas de segurança com fontes de tempo confiáveis PO Gerir Incidentes de Segurança da Informação, PO Gerir Vulnerabilidades.
8.18	Uso de programas utilitários privilegiados	O uso de programas utilitários que possam ser capazes de substituir os controles de sistema e as aplicações deve ser restrito e rigorosamente controlado.	Sim	Sim	Proteger os sistemas contra uso indevido ou não autorizado de programas com capacidades privilegiadas (como acesso root, administrador ou sysadmin), os quais podem modificar configurações críticas, acessar dados sensíveis, ou burlar mecanismos de segurança.	Manual de Segurança da Informação (Gestão de acesso virtual e Gestão de identidade e autenticação, Transferência da Informação, Gestão e Controle de Acesso Físico, Gerenciamento e distribuição de senhas para acesso a dados) Termo de responsabilidade profissional Política de Segurança da Informação Logs Monitoramento com SIEM MFA SOC Autenticação multifator (MFA) Políticas de senha forte Firewalls, NACs (controle de acesso à rede) Controle de pastas e arquivos com ACLs (listas de controle de acesso) Termo de responsabilidade profissional, Cofre de Senha (PAM), PO Gerir Incidentes de Segurança da Informação, PO Gerir Vulnerabilidades.

8.19	Instalação de software em sistemas operacionais	Procedimentos e medidas devem ser implementados para gerenciar com segurança a instalação de software em sistemas operacionais.	Sim	Sim	Assegurar que somente softwares autorizados, licenciados e seguros sejam instalados nos sistemas operacionais, evitando riscos como malware, vulnerabilidades técnicas, não conformidades legais e falhas de integridade do ambiente.	PO Gerir Desenvolvimento de Software Terceirizado Product Backlog Sprint Backlog Help desk Servidor WSUS Formlaizçaão de ações via Redmine Planilha de Gerir Ativos PO Gerir Ativos Política de Segurança da Informação. Manual de Segurança da Informação (Gerenciamento e distribuição de senhas para acesso a dados, Gestão de Configurações) Monitoramento de alterações em sistemas críticos (ex: por SOC, EDR ou SIEM) Auditorias periódicas nos sistemas para detectar softwares não autorizados
8.20	Segurança de redes	Redes e dispositivos de rede devem ser protegidos, gerenciados e controlados para proteger as informações em sistemas e aplicações.	Sim	Sim	Garantir a proteção das informações sobre a infraestutura de redes evitando acessos indevidos e indisponibilidade de rede	Segmentação de rede com base na criticidade e função dos ativos (ex: VLANs, DMZ); Uso de firewalls e sistemas de detecção e prevenção de intrusão (IDS/IPS); Gerenciamento seguro de dispositivos de rede (senhas, firmware atualizado, SSH); Políticas de acesso remoto seguras (VPN com autenticação forte, logs); Desabilitação de serviços e portas não utilizados em dispositivos de rede; Monitoramento contínuo de tráfego de rede (via SIEM, Zabbix, SOC); Aplicação de controles de autenticação e autorização para administradores de rede; Criptografia de tráfego sensível (TLS, IPsec, etc.); Controle de configuração de rede, com documentação e backups; Auditorias periódicas de segurança da rede e testes de vulnerabilidade; Manual de Segurança da Informação e Processos Operacionais DiTi.
8.21	Segurança dos serviços de rede	Mecanismos de segurança, níveis de serviço e requisitos de serviços de rede devem ser identifcados, implementados e monitorados.	Sim	Sim	Garantir que os serviços de rede internos e externos (incluindo internet, VPNs, DNS, serviços de diretório, entre outros) estejam adequadamente protegidos contra falhas, acessos não autorizados, vazamento de dados e interrupções, e que cumpram com os requisitos técnicos, operacionais e de segurança definidos pela organização.	Manual de Segurança da Informação (Ataques à sistemas e suas defesas) Acordos de Nível de Serviço (SLAs) com fornecedores de serviços de rede, incluindo cláusulas de segurança; Monitoramento contínuo dos serviços de rede e geração de alertas em caso de falhas ou anomalias; Documentação de arquitetura de rede e serviços contratados com níveis de segurança esperados; Controle de alterações (Change Management) para serviços de rede Utilização de SOC, Zabbix, SIEM e ferramentas de inventário e monitoramento.
8.22	Segregação de redes	Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização.	Sim	Sim	Evitar acesso não autorizado, propagação de ameaças e impactos cruzados entre diferentes áreas, serviços ou sistemas da organização, por meio da separação lógica ou física de suas redes.	Diagrama de rede, demonstrando segregação e arquitetura de redes. Cisco / Firewall, Criação de VLANs para separar redes por área (ex: RH, TI, usuários, convidados); Lista de controle de acesso (ACLs) em switches e roteadores para restringir tráfego entre segmentos; Implementação de zonas de segurança (ex: DMZ para servidores públicos, rede interna, rede de backup); Isolamento de servidores críticos (ex: AD, banco de dados, aplicações sensíveis); Monitoramento de tráfego entre segmentos com uso de SIEM e IDS/IPS; Documentação das topologias de rede e suas regras de segregação; Manual de Segurança da Infromação (Gestão de Controle de Acessos, Ataques a sistemas e suas defeas)
8.23	Filtragem da web	O acesso a sites externos deve ser gerenciado para reduzir a exposição a conteúdo malicioso.	Sim	Sim	Evitar acessos a sites não autorizados reduzindo o risco de ataques cibernéticos	Filtros de conteúdo web (Web Filtering), via firewall UTM, proxy ou soluções de segurança como: Microsoft Defender for Endpoint (com Web Protection) FortiGate Web Filtering Cisco Umbrella Bloqueio de categorias de sites considerados de risco (ex: pornografia, jogos, redes sociais, torrents); Permissão apenas a sites com reputação positiva (listas de confiabilidade); Uso de listas de bloqueio e de permissão (blacklist/whitelist); Registro e auditoria de acessos à web para análise de comportamento e incidentes; Integração com soluções de DLP e antivírus corporativo para inspeção de tráfego HTTPS; Aviso automático ao usuário sobre bloqueio e registro da tentativa. Manual de Segurança da Informação (gestão de configurações, gestão de acesso virtual) Termo de Responsabilidade Profissional.

8.24	Uso de criptografa	Regras para o uso efetivo da criptografa, incluindo o gerenciamento de chaves criptográfca devem ser defnidas e implementadas.	Sim	Sim	Assegurar a confidencialidade, integridade e, em alguns casos, a autenticidade das informações, protegendo-as durante o armazenamento ou transmissão, com uso de criptografia apropriada e gestão segura das chaves.	Manual de Segurança da Informação (Ataque a sistemas e suas defesas, Controle de Criptografias) Adoção de algoritmos criptográficos reconhecidos Uso de VPNs com criptografia robusta para comunicações remotas; Criptografia em disco e dispositivos móveis Criptografia em serviços de nuvem Gerenciamento centralizado de chaves Registro e rastreamento do uso de criptografia e chaves PO Produzir Relatório de Inteligência.
8.25	Ciclo de vida de desenvolvimer	Regras para o desenvolvimento seguro de software e sistemas devem ser estabelecidas e aplicadas.	Sim	Sim	Garantir que os softwares e sistemas desenvolvidos atendam aos requisitos de segurança da informação, evitando a introdução de vulnerabilidades ou códigos maliciosos durante seu ciclo de vida – desde o planejamento até a manutenção.	Contrato de terceirização e termo de referencia forncedor Indra Controle de Acessos ao Codigo Fonte PO Gerir Vulnerabilidades, PO Gerir Desnevolvimenot de Software Terceirizado PO Gerir Manutenção Terceirizada de Software. Manual de Segurança da Informação (Politica de privacidade, Gestão de configuração, Garantia dos Direitos de Propriedade Intelectual, Gestão de Requisitos legais, estatutários, regulamentares e contratuais, Proteção contra malware) Política de Segurança da Informação PO Gerir Contratações Gestão de Informações via Remine TI
8.26	Requisitos de segurança da aplicação	Requisitos de segurança da informação devem ser identifcados, especifcados e aprovados ao desenvolver ou adquirir aplicações.	Sim	Sim	Garantir que todas as aplicações desenvolvidas ou adquiridas considerem desde a origem os requisitos de segurança necessários para proteger informações sensíveis, infraestrutura crítica e processos da organização, reduzindo riscos de vulnerabilidades e falhas.	Contrato de terceirização e termo de referencia forncedor Indra Controle de Acessos ao Codigo Fonte PO Gerir Vulnerabilidades, PO Gerir Desnevolvimenot de Software Terceirizado PO Gerir Manutenção Terceirizada de Software. Manual de Segurança da Informação (Politica de privacidade, Gestão de configuração, Garantia dos Direitos de Propriedade Intelectual, Gestão de Requisitos legais, estatutários, regulamentares e contratuais, Proteção contra malware) Política de Segurança da Informação PO Gerir Contratações Gestão de Informações via Remine TI
8.27	Princípios de arquitetura e engenharia de sistemas seguros	Princípios de engenharia de sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados a qualquer atividade de desenvolvimento de sistemas.	Não	Não se aplica	O Tribunal não desenvolve sistemas internamente; todos os sistemas utilizados são adquiridos por meio de processos licitatórios e termos de referência, com o desenvolvimento sendo realizado por empresa terceirizada especializada (atualmente, a Indra). Após a conclusão, os sistemas são entregues à equipe de TI do Tribunal apenas para manutenção e monitoramento, sendo as responsabilidades de arquitetura e engenharia segura atribuídas contratualmente ao fornecedor.	Contrato de terceirização e termo de referencia forncedor Indra. O item 8.27 é considerado não aplicável ao contexto do Tribunal de Contas do Estado de Goiás (TCE-GO), uma vez que o desenvolvimento de sistemas e softwares não é realizado internamente. Todos os sistemas utilizados são adquiridos de fornecedores externos especializados, por meio de termos de referência (TR) e processos licitatórios formalizados. Atualmente, a empresa contratada para essa atividade é a Indra, responsável pelo desenvolvimento completo dos sistemas institucionais. Após o desenvolvimento, as soluções são entregues à Diretoria de Tecnologia da Informação (DiTI), que assume apenas a manutenção, monitoramento e operação do software já finalizado. Dessa forma, os princípios de arquitetura e engenharia segura são responsabilidade contratual da empresa desenvolvedora e são previamente especificados nos TRs que compõem os editais de licitação. Por isso, não se aplica ao TCE-GO a implementação direta das práticas previstas neste controle.
8.28	Codifcação segura	Princípios de codifcação segura devem ser aplicados ao desenvolvimento de software.	Não	Não se aplica	É considerado não aplicável ao TCE-GO porque o Tribunal não realiza desenvolvimento ou codificação interna de software. Essa atividade é executada por empresa terceirizada (atualmente, a Indra), contratada por meio de termos de referência que estabelecem requisitos de codificação segura. A responsabilidade pela aplicação dos princípios de codificação segura recai sobre a empresa contratada, conforme previsto contratualmente, sendo que o TCE-GO atua apenas no monitoramento e acompanhamento da conformidade após a entrega do software.	Contrato de terceirização e termo de referencia forncedor Indra Validação de entrega com evidência de testes de segurança no código; Monitoramento contínuo de vulnerabilidades pela DiTI após a entrega; Auditorias contratuais periódicas com base em SLAs e KPIs definidos.. O TCE-GO não realiza codificação ou desenvolvimento interno de software. Essa atividade é totalmente terceirizada, sendo executada atualmente pela empresa Indra, contratada por meio de termos de referência (TR) que estabelecem requisitos técnicos e de segurança, inclusive os princípios de codificação segura. O TR inclui cláusulas específicas relacionadas às boas práticas de desenvolvimento seguro, com base em padrões reconhecidos (como OWASP, CWE, entre outros), sendo de responsabilidade da contratada garantir a implementação de controles seguros durante o desenvolvimento do software. Após a entrega, os sistemas são monitorados e mantidos pela equipe de tecnologia do TCE-GO, que acompanha a conformidade contratual e a segurança operacional do software. Dessa forma, o controle está instituído contratualmente e aplicado via fornecedor.

8.29	Testes de segurança em desenvolvimento e aceitação	Processos de teste de segurança devem ser defnidos e implementados no ciclo de vida do desenvolvimento.	Não	Não se aplica	Considerado não aplicável ao TCE-GO, pois o Tribunal não realiza atividades de desenvolvimento interno de software. Todo o ciclo de desenvolvimento, incluindo os testes de segurança em ambiente de desenvolvimento e de aceitação, é executado por empresa contratada por meio de processo licitatório, atualmente a Indra, conforme definido em termos de referência contratuais. Cabe à contratada garantir a execução de testes de segurança adequados antes da entrega dos sistemas, incluindo testes de vulnerabilidades e validações técnicas exigidas. O TCE-GO atua na validação funcional e no monitoramento pós-entrega, sendo a responsabilidade primária deste controle atribuída ao fornecedor.	Contrato de terceirização e termo de referencia forncedor Indra Entrega da terceirizada: Execução de testes de segurança automatizados e manuais no ambiente de desenvolvimento e homologação; Entrega de relatórios de testes de segurança e validação de correções; Aplicação de frameworks como OWASP, SAST/DAST e verificações com ferramentas como Fortify, SonarQube ou similares; Revalidação técnica dos sistemas após correções de falhas; Responsabilidade da contratada por garantir que nenhuma vulnerabilidade crítica seja entregue na versão final. Análise técnica da equipe interna da DiTI com base em documentos de aceite e evidências técnicas fornecidas pela contratada; Checklist de homologação de segurança anexado ao aceite formal do sistema.
8.30	Desenvolvimento terceirizado	A organização deve dirigir, monitorar e analisar criticamente as atividades relacionadas à terceirização de desenvolvimento de sistemas.	Sim	Sim	Gerenciar o fluxo de trabalho do desenvolvimento terceirizado e garantir a conformidade com as regras da organização para desenvolvimento seguro	Contrato Indra, Termos de Referência, Log´s, Firewall, VPN, GPO´s. PO Gerir Vulnerabilidades, PO Gerir Desnevolvimenot de Software Terceirizado e PO Gerir Manutenção Terceirizada de Software. Manual de Segurança da Informação/Política de Segurança da Informação. PO Gerir Contratações. Gestão de Contrato e gestão de entregas (acordos SLA) Avaliação crítica periódica do fornecedor, com base em: Indicadores de desempenho; Histórico de incidentes; Qualidade técnica das entregas.
8.31	Separação dos ambientes de desenvolvimento, teste e produção	Ambientes de desenvolvimento, testes e produção devem ser separados e protegidos.	Sim	Sim	Garantir a proteção e funcionalidade dos sistemas/aplicações e dos dados do ambiente de produção	Cláusulas contratuais específicas exigindo ambientes distintos para desenvolvimento, Cláusulas contratuais específicas exigindo ambientes distintos para desenvolvimento, homologação e produção. Cláusulas contratuais específicas exigindo ambientes distintos para desenvolvimento, homologação e produção. Uso de dados anonimizados ou mascarados nos testes, evitando exposição de dados reais. Acompanhamento técnico pela DiTI quanto ao cumprimento das separações via documentação e auditorias. Repositórios de código com ramificações distintas para desenvolvimento e produção. Monitoramento por ferramentas como Zabbix e revisão em reuniões da área de TI e do Comitê de Segurança da Informação. Registro e rastreabilidade das mudanças de ambiente com logs e controle de versionamento. homologação e produção.Github Servidores Ambiente .gti.br – ambiente de homologação. PO Gerir Vulnerabilidades, PO Gerir Desnevolvimenot de Software Terceirizado PO Gerir Manutenção Terceirizada de Software.
8.32	Gestão de mudanças	Mudanças nos recursos de tratamento de informações e sistemas de informação devem estar sujeitas a procedimentos de gestão de mudanças.	Sim	Sim	Assegurar que mudanças no ambiente de Tecnologia da Informação, passe por uma completa avaliação de potenciais riscos e impactos, evitando danos ou ameaças à estabilidade no ambiente de produção.	Manual de Segurança da Informação (gestão de mudanças) Ata´s de Reuniões analise critica de gestão e Reuniões do Comitê, Reunião de analise estratégica Manual do SGI, Help Desk, Plano Diretor. PO Gerir Melhorias Contínua Registro Redmine TI.
8.33	Informações de teste	Informações de teste devem ser adequadamente selecionadas, protegidas e gerenciadas.	Sim	Sim	Garantir a configuração de parâmetros para proteção de dados pessoais e sensíveis	Contrato de terceirização e termo de referencia forncedor Indra, PO Gerir Vulnerabilidades, PO Gerir Desnevolvimenot de Software Terceirizado PO Gerir Manutenção Terceirizada de Software. Manual de Segurança da Informação (Ataques à sistemas e suas defesas) Política de Segurança da Informação. PO Gerir Contratações Gestão de Testes via Redine TI e ambiente controlado entre DiTi e Terceirizado Banco de dados Oracle 19c.

8.34	Proteção de sistemas de informação durante os testes de auditoria	Testes de auditoria e outras atividades de garantia envolvendo a avaliação de sistemas operacionais devem ser planejados e acordados entre o testador e a gestão apropriada.	Sim	Sim	Mitigar o impacto nos sistemas/aplicações durante os testes	Plano de Continuidade de TI testes de intrusão formalizados Auditorias de Sistemas Registro e rastreamento das atividades realizadas durante o teste de auditoria. Gestão de informação Redmine PO Gerir Vulnerabilidades, PO Gerir Desnevolvimenot de Software Terceirizado PO Gerir Manutenção Terceirizada de Software. Manual de Segurança da Informação (Ataques à sistemas e suas defesas) Política de Segurança da Informação. PO Gerir Contratações, PO Gerir Auditorias do SGI SOC