DECLARAÇÃO DE APLICABILIDADE

Identificação de Controle (N°)	Descrição	Objetivo de Controle	Aplicabilidade	Justificativa	Documento	Responsável
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	Resultante da análise de risco item aplicável ao escopo da organização	Manual de Segurança da Informação	DI-PLAN e Di-Ti (Considerando que sua aplicação inclui todas as áreas do TCE-GO)
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	Resultante da análise de risco item aplicável ao escopo da organização	Organograma, Manual de Segurança da Informação, Decritivo de Competência, Portaria 57/2023-GPRES e Resolução Administrativa Nº 11/2022	Áreas conforme manual de segurança da informação e GGP
5.3	Segregação de funções	Funções confitantes e áreas de responsabilidade devem ser segregadas.	Sim	Resultante da análise de risco item aplicável ao escopo da organização	Organograma, Manual de Segurança da Informação, Decritivo de Competência, Portaria 57/2023-GPRES e Resolução Administrativa Nº 11/2023	DI-PLAN, DI-TI e GGP
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 específcas por tema e com os procedimentos da organização.	Sim	Resultante da análise de risco item aplicável ao escopo da organização	Aprovação e validação do Manual de Segurança da Informação, Gestão de Processos Operacionais, RAE´s, RAC´s e Portaria 57/2023-GPRES e Resolução Administrativa Nº 11/2023	DI-TI, Di-Plan, Presidência e Comitê de Segurança da Inofrmação.
5.5	Contato com autoridades	A organização deve estabelecer e manter contato com as autoridades relevantes.	Sim	Resultante da análise de risco item aplicável ao escopo da organização	Participação em grupos externos de segurança da informação, Plano de Continuidade de TI, Portaria 57/2023-GPRES e Resolução Administrativa Nº 11/2023, Manual de Segurança da Informação.	DI-TI, DPO e Comitê de Segurança da Informação.
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	Resultante da análise de risco item aplicável ao escopo da organização	Participação em grupos externos de segurança da informação de outras Organizações com foco em adquirir informações de boas práticas de segurança da informação.	DI-TI, DPO e Comitê de Segurança da Informação.
5.7	Inteligência de ameaças	As informações relacionadas a ameaças à segurança da informação devem ser coletadas e analisadas para produzir inteligência de ameaças.	Sim	Resultante da análise de risco item aplicável ao escopo da organização	PO Gerir Acidentes e Incidentes, SONAR, SOC ISH (securonix), SGP, PO Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos, Ata´s Reunião do Comitê de Segurança da Informação, Manual de Segurança da Informação.	DI-TI e Comitê 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	Resultante da análise de risco item aplicável ao escopo da organização	PO Gerir Acidentes e Incidentes, SONAR, SOC ISH (securonix), SGP, PO Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos, Ata´s Reunião do Comitê de Segurança da Informação, Manual de Segurança da Informação.	DI-TI e Comitê de Segurança da Informação
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	Resultante da análise de risco item aplicável ao escopo da organização	O Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos, Resolução Normativa nº. 10/2017 e seu anexo.	DI-PLAN e DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização	PO Gerir Ativos de Tecnologia da Informação, Planilha de Gestão de Ativos, Resolução Normativa nº. 10/2017 e seu anexo.	DI-PLAN e DI-TI
5.11	Devolução de ativos	Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação.	Sim	Resultante da análise de risco item aplicável ao escopo da organização	Manual de Segurança da Informação, PO Gerir Riscos, PO Gerir Patrimônio, Planilha de Gestão de Ativos, Resolução Normativa nº. 10/2017 e seu anexo, Termos de Responsbailidade Aplicados.	DI-PLAN, DI-TI e SEC-ADMIN
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	Resultante da análise de risco item aplicável ao escopo da organização	Planilha de Gestão de Ativos, Resultante da análise de risco item aplicável ao escopo da organização, Resolução Normativa nº 10/2017 (portaria de classificação)	DI-PLAN e DI-TI, considerando a aplicação do requisitos vinculada a todos os colaboradores do TCE Goiás.
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	Resultante da análise de risco item aplicável ao escopo da organização	PO Gerir Riscos, Planilha de Gestão de Ativos, Manual de Segurança da Informação e Resolução Resolução Normativa nº 10/2017 (portaria de classificação).	DI-PLAN e DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização	PO Gerir Riscos, Planilha de Gestão de Ativos, Manual de Segurança da Informação e Resolução Normativa nº. 10/2017 e seu anexo. Transferência eletronica / Transferência de midia de armazenamento físico / Transferência verbal.	DI-PLAN e DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização	Manual de Segurança da Informação, considerando dentre as politicas e diretrizes ali traçadas a politica de controle de acessos.	Gestão: DI-PLAN e DI-TI Execução: Todas as áreas

5.16	Gestão de identidade	O ciclo de vida completo das identidades deve ser gerenciado.	Sim	Resultante da análise de risco item aplicável ao escopo da organização	Gestão de identidades, considerando o foco no fornecer ou revogar o acesso as informações. Considerando a melhoria da politica de constrole de acessos. Manual de Segurança da Informação. Sistema Help Desk.	DI-TI e Ger-Gp
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	Resultante da análise de risco item aplicável ao escopo da organização	Poltica de Controle de Acessos, Manual de Segurança da Informação, Sistema de gerenciamento de senhas. Sistema Help Desk.	DI-PLAN, DI-TI, SEC-ADMIN e GER-GP
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	Resultante da análise de risco item aplicável ao escopo da organização	Poltica de Controle de Acessos, Manual de Segurança da Informação, Sistema de gerenciamento de senhas. Sistema Help Desk.	DI-PLAN, DI-TI, SEC-ADMIN e GER-GP
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	Resultante da análise de risco item aplicável ao escopo da organização	Manual de Segurança da Informação, Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação, Contratos firmados, gestão de contratos e Termos de Referência contratuais.	DI-PLAN, DI-TI e SEC-ADMIN
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	Resultante da análise de risco item aplicável ao escopo da organização	Manual de Segurança da Informação, Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação, Contratos firmados, gestão de contratos e Termos de Referência contratuais.	SEC-ADMIN e DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização	Manual de Segurança da Informação, Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação, Contratos firmados, gestão de contratos e Termos de Referência contratuais.	SEC-ADMIN e DI-TI

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	Resultante da análise de risco item aplicável ao escopo da organização	Reunião do Comitê - Gestão de Mudanças - Manual de Segurança da Informação, Termos de Responsabilidade e Aplicação da Cláusula de segurança da Informação, Contratos firmados, gestão de contratos e Termos de Referência contratuais.	Gestor de Contrato
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	Resultante da análise de risco item aplicável ao escopo da organização	Google Workspace: Controle de Acesso e Politica de backup do proprio google, Contrato de produto.	Di-Ti
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	Resultante da análise de risco item aplicável ao escopo da organização.	Gerir Incidentes de Segurança da Informação - Comunicação Via reuniões comitê - Ata´s de reunião e Registro de atividades do Redmine, Plano de Continuidade de TI, Manual de Segurança da Informação. Avaliar a precisão de papeis e responsabilidades, procedimentos de gestão de incidentes, procedimentos de emissão de relatórios.	DI-TI e Comitê de Segurança da Informação
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	Resultante da análise de risco item aplicável ao escopo da organização.	Gerir Incidentes de Segurança da Informação - Comunicação Via reuniões comitê - Ata´s de reunião, Plano de Continuidade de TI e Registro de atividades do Redmine	DI-TI e Comitê de Segurança da Informação
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	Resultante da análise de risco item aplicável ao escopo da organização.	Gerir Incidentes de Segurança da Informação - Comunicação Via reuniões comitê - Ata´s de reunião e Registro de atividades do Redmine, Repsostas a incidentes de Segurança, Contrato ISH e indicador de Getsão de incidentes.	DI-TI e Comitê de Segurança da Informação
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	Resultante da análise de risco item aplicável ao escopo da organização.	Gerir Incidentes de Segurança da Informação - Comunicação Via reuniões comitê - Ata´s de reunião e Registro de atividades do Redmine, Repsosatas a incidentes de Segurança, Contrato ISH e indicador de Getsão de incidentes. Gestão de Boas Práticas de Acidentes e Incdentes de Segurança. Planno de Contínuidade de TI.	DI-TI e Comitê de Segurança da Informação

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	Resultante da análise de risco item aplicável ao escopo da organização.	Gerir Incidentes de Segurança da Informação - Comunicação Via reuniões comitê - Ata´s de reunião e Registro de atividades do Redmine, Repsosatas a incidentes de Segurança, Contrato ISH e indicador de Getsão de incidentes. Gestão de Boas Práticas de Acidentes e Incdentes de Segurança. Planno de Contínuidade de TI.	DI-TI e Comitê de Segurança da Informação
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	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da Informação e PO Gerir Incidentes de Segurança da Informação, Plano de Continuidade de TI, Simulados de Incidentes de Segurança, Gestão de Boas Práticas geridas em reunião do comitê.	DI-TI e Comitê de Segurança da Informação
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	Resultante da análise de risco item aplicável ao escopo da organização.	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.	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Planilha de Requisitos Legais anexo ao PO Gerir Ativos.	Gestão: DI-TI Execução: Todas as áreas.
5.32	Direitos de propriedade intelectual	A organização deve implementar procedimentos adequados para proteger os direitos de propriedade intelectual.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da Informação - PO Gerir Desenvolvimento de Software, Licencimento de Aplicações e Sistemas	Di-Ti
5.33	Proteção de registros	Os registros devem ser protegidos contra perdas, destruição, falsifcação, acesso não autorizado e liberação não autorizada.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Controle de Registros operacionais gerenciados ao final de padrão operacional instituido. PO Gerir Processos de Trabalho	DI-PLAN e DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de Privacidade e proteção de dados pessoais, Manual de Segurança da Informação, Reuniões do Comitê de Segurança da Informação, Gestão de Boas Práticas por meio de documentos padronizados.	DI-TI, Di-Plan, Di-Com e SEC-Admin

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	Resultante da análise de risco item aplicável ao escopo da organização.	Ata´s de Reuniões analise critica de gestão e Reuniões do Comitê	DI-TI e Comitê de Segurança da Informação
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 específcos deve ser analisado criticamente a intervalos regulares.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Ata´s de Reuniões analise critica de gestão e Reuniões do Comitê	DI-TI e Comitê de Segurança da Informação
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	Resultante da análise de risco item aplicável ao escopo da organização.	Gestão de processos operacionais via site e via sgp, integração organizacional e reuniões de gestão.	DI-PLAN.
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	Resultante da análise de risco item aplicável ao escopo da organização.	Codigos de etica, Processos da GGP, Manual de função, Resolução Admin Regulamentação de funções no TCE 19/2022.	GGP
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	Resultante da análise de risco item aplicável ao escopo da organização.	Termo de responsibilidade de segurança da informação assinados, Codigos de etica, Processos da GGP, Manual de função, Resolução Admin Regulamenta funções no TCE.	GGP
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	Resultante da análise de risco item aplicável ao escopo da organização.	Matriz de comunicação e treinamentos vinculados a segurança da informação	Di-Ti, Escoex e Di-Com
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	Resultante da análise de risco item aplicável ao escopo da organização.	Codigo de Ética, Resolução Administrativa nº. 8/2015	GGP
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	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de Controle de Acessos (ciclo de vida do usuário), Manual de Segurança da Informação.	Gestão: GGP Executa: Di-Ti
6.6	Acordos de confdencialidade 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	Resultante da análise de risco item aplicável ao escopo da organização.	Termo de responsabilidade. - Para equipe colaboradores na entrada do exercicio da função para terceiros no incio do contrato e a cada nova troca de equipe.	GGP

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	Resultante da análise de risco item aplicável ao escopo da organização.	Resolução Admisnitratva nº 18/2023 considerando padrões para o trabalho remoto	DI-PLAN, Di-Ti e GGP
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	Resultante da análise de risco item aplicável ao escopo da organização.	Help desk / Email /Grupo intermo de segurança da informação e canais diretos de comunicação	Di-Ti e Di-Com
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	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da informação - Politica de segurança fisica, Controle de Limites conforme padrão operacional da Assessoria Militar.	DI-PLAN, DI-TI, SEC-ADMIN e GER-GP
7.2	Entrada física	As áreas seguras devem ser protegidas por controles de entrada e pontos de acesso apropriados.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Fechaduras eletronicas - Politica de acesso - Controle imagens via CFTV - Monitoramento 24 horas.	DI-TI e SEC-ADMIN
7.3	Segurança de escritórios, salas e instalações	Segurança física para escritórios, salas e instalações deve ser projetada e implementada	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Controle de Portaria, Controle de Acesso Físico, Auto Responsabilidade e Atuação da equipe da Assessoria Militar do Estado de Goiás.	DI-TI e SEC-ADMIN
7.4	Monitoramento de segurança física	As instalações devem ser monitoradas continuamente para acesso físico não autorizado	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Moinitoramento por cameras e controle pelo CFTV, Controle de Portaria, Controle de Acesso Físico, Auto Responsabilidade e Atuação da equipe da Assessoria Militar do Estado de Goiás.	Di-Ti, Acessoria Militar e Sec-Admin
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	Resultante da análise de risco item aplicável ao escopo da organização.	Plano de continuidade de TI, PO Respostas a emergenia, manual de segurança da informação, Simulação de incidente de segurança.	Di-Ti e Serv-Manutenção Predial
7.6	Trabalho em áreas seguras	Medidas de segurança para trabalhar em áreas seguras devem ser projetadas e implementadas.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Controle de acesso, politica de controle de acesso (manual de segurança da informação), Fechaduras eletrônicas, circuito de CFTV monitorado 24 horas.	DI-TI e SEC-ADMIN
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	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de mesa limpa tela limpa, Manual de Segurança da Informação, Gestão de Incidentes, Sistema de comunicação rotineiros TCE -GO conforme o escopo.	DI-Ti, SEC-ADMIN e Di-Com

7.8	Localização e proteção de equipamentos	Os equipamentos devem ser posicionados com segurança e proteção.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de mesa limpa tela limpa, Anslise técnica de instalação de cameras com apoio da assessoria militar assim como da empresa de seguros.	SEC-ADMIN e Di-Com
7.9	Segurança de ativos fora das instalações da organização	Os ativos fora das instalações da organização devem ser protegidos.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Gestão por memorando e termo de controle patrimonial, conforme determinado em PO Gerir Patrimonio.	Di-Ti e Diplan
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.	Não	Resultante da análise de risco item não aplicável ao escopo da organização, considerando ainda a aceitabilidade do risco junto a organização.	Poliitca do uso de midias removiveis, atualizando considerando a não existencia das mesmas. Planilha de Ativos. PO Gerir Incidentes de Segurança da Informação. PO Gerir Ativos.	Di-Ti e GGP
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	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da Inofrmação e Plano de Continuidade do TI.	DI-TI e SEC-ADMIN
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	Resultante da análise de risco item aplicável ao escopo da organização.	Projeto eletrico do predio, Gestão e monioramento do manutenção predial.	Serv- Manutenção Predial
7.13	Manutenção de equipamentos	Os equipamentos devem ser mantidos corretamente para assegurar a disponibilidade, integridade e confdencialidade da informação.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Manutenção Logica / Atualização de sistemas / Manutenção Física (Data de trocas e gestão de manutenções por tempo de uso), Contrato de Manutenção Predial e de Equipamentos.	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Plano de gerenciamento de resíduos - PO Gerir Patrimonio - Laudo Técnico	DI-PLAN, DI-TI, SEC-ADMIN e GER-GP
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	Resultante da análise de risco item aplicável ao escopo da organização.	Código de etica / Termo Responsabilidade Manual de Segurança da Informação Antivírus Firewall SOC	Di-Ti e GGP

8.2	Direitos de acessos **privilegiados**	A atribuição e o uso de direitos de acessos privilegiados devem ser restritos e gerenciados	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	AD GPAC Git Aplicações internas e externas Politica de Controle de Acesso / Manual de Segurança da Informação	Di-Ti
8.3	Restrição de acesso à informação	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	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da Informação Logs AD GPAC GIT	Di-Ti
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.	Não	Resultante da análise de risco item não aplicável ao escopo da organização, conisderando que acessos de leitura e escrita ao código-fonte, ferramentas de desenvolvimento e bibliotecas de software são gerenciados por meio de contrato terceirizado espcifico para o tema.	Contrato de terceirização e termo de referencia forncedor Indra	Gestão do Contrato Di-Ti
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	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da Informação	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	PDTI Zabbix SOC Reuniões internas de TI Manual de Segurança da Informação	DI-TI
8.7	Proteção contra malware	Proteção contra malware deve ser implementada e apoiada pela conscientização adequada do usuário.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da Informação Politca de proteção. Deep Security e Planilha de Gestão de Ativos. SOC	DI-TI
8.8	Gestão de vulnerabilidades técnicas	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	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de vulnerabilidade, Gestão de Ativos SOC Tenable.io	DI-TI

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	Resultante da análise de risco item aplicável ao escopo da organização.	Rotina de gestão de configuração Wiki PDTI / Zabbix / SOC / Wiki / Redmine	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Tabela de temporalidade, Gestão de informações via controle de registros ao final de cada processo padrão. Manual do SGI.	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Mapa de dados e Banco de Dados e Política de Privacidade	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de Privacidade e proteção de dados pessoais, Manual de Segurança da Informação, Reuniões do Comitê de Segurança da Informação, Gestão de Boas Práticas por meio de documentos padronizados.	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Testes de integridade e PO de Gerir Backup.	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Plano de Continuidade do Negócio.	DI-TI
8.15	Log	Logs que registrem atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Contrato ISH, Portal de chamados ISH, Gestão de Incidentes via Redmine TCE Goiás. Logs de sistemas operacionais e serviços	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da Informação SOC - ISH Antivírus Firewall Logs	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	NTP, Manual de Segurança da Informação, PO Gerir Incodentes de Segurança da Informação	DI-TI

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	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de controle de acesso, Manual de Segurança da Informação, Termo de Responsabilidade, Cofre de Senha (PAM)	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Help desk / Servidor WSUS / Formlaizçaão de ações via Redmine/ Planilha de Gerir Ativos / PO Gerir Ativos / PO Gerir Incidentes de Seguraça da Informação / Manual de Segurança da Informação.	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de Privacidade de Dados, Gestão de Acesso a rede. SOC Regras de firewall, segregação de redes, antivírus, AD	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Politica de segurança de redes (antivirus, Firewall e Controle de Acesso)	DI-TI
8.22	Segregação de redes	Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Diagrama de rede, demonstrando segregação e arquitetura de redes. Cisco / Firewall	DI-TI
8.23	Filtragem da web	O acesso a sites externos deve ser gerenciado para reduzir a exposição a conteúdo malicioso.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Bloqueio via Firewall e Proxy	DI-TI
8.24	Uso de criptografa	Regras para o uso efetivo da criptografa, incluindo o gerenciamento de chaves criptográfca devem ser defnidas e implementadas.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Manual de Segurança da Inofrmação - Politica de criptografia	DI-TI

8.25	Ciclo de vida de desenvolvimento seguro	Regras para o desenvolvimento seguro de software e sistemas devem ser estabelecidas e aplicadas.	Não	Resultante da análise de risco item não aplicável ao escopo da organização, conisderando que regras para o desenvolvimento seguro de software e sistemas são aplicadas por meio de empresa terceirizada e monitoradas pela equipe de Di-Ti, sendo estas estabelecidas e aplicadas conforme descrito em TR da contratada.	Contrato de terceirização e termo de referencia forncedor Indra	DI-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	Resultante da análise de risco item aplicável ao escopo da organização.	PO Gerir Manutenção de software e Geriri Desenvolvimento de Software GitHub Redmine	DI-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	Resultante da análise de risco item não aplicável ao escopo da organização, conisderando que engenharia de sistemas seguros fazem parte do escopo de atividade terceirizada, a qual é devidamente monitorada pela Di-Ti conforme descrito em TR da Contratada	Contrato de terceirização e termo de referencia forncedor Indra	DI-TI
8.28	Codifcação segura	Princípios de codifcação segura devem ser aplicados ao desenvolvimento de software.	Não	Resultante da análise de risco item não aplicável ao escopo da organização, conisderando que princípios de codifcação segura fazem parte do escopo de atividade terceirizada, a qual é devidamente monitorada pela Di-Ti conforme descrito em TR da Contratada	Contrato de terceirização e termo de referencia forncedor Indra	DI-TI
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	Resultante da análise de risco item não aplicável ao escopo da organização, considerando que teste de segurança fazem parte do escopo de atividade terceirizada, a qual é devidamente monitorada pela Di-Ti conforme descrito em TR da Contratada	Contrato de terceirização e termo de referencia forncedor Indra	DI-TI

8.30	Desenvolvimento terceirizado	A organização deve dirigir, monitorar e analisar criticamente as atividades relacionadas à terceirização de desenvolvimento de sistemas.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Contrato Indra, Termos de Referência, Log´s, Firewall, VPN, GPO´s.	DI-TI
8.31	Separação dos ambientes de desenvolvimento, teste e produção	Ambientes de desenvolvimento, testes e produção devem ser separados e protegidos.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	Github Servidores Ambiente .gti.br – ambiente de homologação.	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	Ata´s de Reuniões analise critica de gestão e Reuniões do Comitê, Reunião de nalise estratégica Manual do SGI, Help Desk, Plano Diretor.	DI-PLAN, DI-TI, SEC-ADMIN e GER-GP
8.33	Informações de teste	Informações de teste devem ser adequadamente selecionadas, protegidas e gerenciadas.	Sim	Resultante da análise de risco item aplicável ao escopo da organização.	PO Gerir Manutenção de software e Gerir Desenvolvimento de Software Banco de Dados. Contrato e termo de referência empresa Indra.	DI-TI
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	Resultante da análise de risco item aplicável ao escopo da organização.	PO Gerir Manutenção de software e Gerir Desenvolvimento de Software SOC	DI-PLAN e DI-TI