

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA
ELABORADO POR:		REVISADO POR:		APROVADO POR:	
Gestão de Processos e Qualidade (GPQ)		Gestão de Processos e Qualidade (GPQ)		Rafael Chaves	
Gestão de Processos e Qualidade (GPQ)		Gestão de Processos e Qualidade (GPQ)			
Documento analisado criticamente e aprovado quanto à adequação.		Documento assinado eletronicamente.			

SUMÁRIO

Sumário

1. OBJETIVOS	2
2. APLICAÇÃO	2
3. TERMOS / DEFINIÇÕES E PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO	2
4. ABREVIATURAS	4
5. RESPONSABILIDADES	4
6. PROCEDIMENTO	7
7. INCIDENTES E CANAIS DE COMUNICAÇÃO	9
8. HISTÓRICO DE REVISÕES	10
9. ANEXOS	10

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

1. OBJETIVOS

- Esta política tem por objetivo estabelecer diretrizes e Políticas de Segurança e Privacidade da Informação que permitam aos colaboradores da CONTREI adotar padrões de comportamento seguro, adequados às metas e necessidades da CONTREI;
- Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança e Privacidade da Informação;
- Resguardar as informações da CONTREI, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;
- Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros; e
- Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da CONTREI como resultado de falhas de segurança.

2. APLICAÇÃO

Esta política se aplica a todos os usuários da informação da CONTREI, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a CONTREI, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da CONTREI e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da CONTREI.

3. TERMOS / DEFINIÇÕES E PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

3.1 Termos e Definições

3.1.1 Controle de Acesso

Significa assegurar que o acesso físico e lógico aos ativos seja autorizado e restrito com base em requisitos de negócio e de segurança da informação.

3.1.2 Ativo

Qualquer coisa que tenha valor para a organização.

3.1.3 Ataque

Tentativa não autorizada, bem-sucedida ou malsucedida, de destruir, alterar, desabilitar, obter acesso a um ativo ou qualquer tentativa de expor, roubar ou fazer uso não autorizado de um ativo.

3.1.4 Autenticação

Provisão de garantia de que uma característica alegada de uma entidade está correta.

3.1.5 Cadeia de Custódia

Demonstrável posse, movimento, manuseio e localização de material de um ponto no tempo até outro.

3.1.6 Informações Confidenciais

Informações que não se destinam a ser disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados.

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

3.1.7 Violação de Segurança da Informação

Comprometimento de segurança da informação que leva à destruição indesejada, perda, alteração, divulgação de, ou acesso a, informações protegidas transmitidas, armazenadas ou tratadas de diversas formas.

3.1.8 Evento de Segurança da Informação

Ocorrência indicando uma possível violação de segurança da informação ou falha de controles.

3.1.9 Incidente de Segurança da Informação

Um ou múltiplos eventos de segurança da informação relacionados e identificados que podem prejudicar os ativos (3.1.2) da organização ou comprometer suas operações.

3.1.10 Sistema de Informação

Conjunto de aplicações, serviços, ativos de tecnologia da informação ou outros componentes de manuseio de informações.

3.1.11 Parte Interessada Stakeholder

Pessoa ou organização interessada que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.

3.1.12 Não Repúdio

Capacidade de comprovar a ocorrência de um evento ou ação declarada e suas entidades originárias.

3.1.13 Dados Pessoais DP

Qualquer informação que (a) possa ser usada para identificar a pessoa natural à qual tal informação se relaciona ou (b) é ou pode ser direta ou indiretamente vinculada a uma pessoa natural.

3.1.14 Titular de DP

Pessoa natural a quem se referem os dados pessoais.

3.1.15 Política

Intenções e direção de uma organização, expressa formalmente por sua alta direção.

3.1.16 Procedimento

Modo especificado de realizar uma atividade ou um processo.

3.1.17 Processo

Conjunto de atividades inter-relacionadas ou interativas que utilizam entradas para entregar um resultado pretendido.

3.1.18 Registro

Informações criadas, recebidas e mantidas como evidência e como um ativo por uma organização ou pessoa, em busca de obrigações legais ou na transação de negócios.

3.1.19 Informações Sensíveis

Informações que precisam ser protegidas contra indisponibilidade, acesso, modificação ou divulgação pública não autorizada devido a potenciais efeitos adversos em um indivíduo, organização, segurança nacional ou segurança pública.

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

3.1.20 Ameaça

Causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização

3.1.21 Usuário

Partes interessadas com acesso aos sistemas de informação da organização

3.1.22 Vulnerabilidade

Fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças.

3.1.23 Segurança da informação

A segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação.

3.1.24 Princípios de Segurança da Informação

A segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação.

4. ABREVIATURAS

SGI – Sistema de Gestão Integrado

CSPI - Comitê de Segurança e Privacidade da Informação.

ESPI – Encarregado de Segurança e Privacidade da Informação.

GPQ – Gestão de Processos e Qualidade (da CONTREI).

5. RESPONSABILIDADES

5.1 Gestores da Informação

É responsabilidade dos Gestores da Informação, mas não se limitam a:

- Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, identificação, rotulagem, classificação, manuseio e descarte conforme as normas estabelecidas pela CONTREI;
- Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem delas conforme necessário;
- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;
- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela CONTREI.

5.2 Usuários da informação

É responsabilidade dos Usuários da Informação, mas não se limitam a:

- Ler, compreender e cumprir os termos da Política Geral de SGI, bem como as demais normas e procedimentos aplicáveis;

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

- Comunicar ao Compliance CONTREI qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança e privacidade das informações ou dos recursos computacionais da CONTREI;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de SGI e suas Normas e Procedimentos ao Compliance CONTREI;
- Assinar o Termo de Uso de Sistemas de Informação da CONTREI;

5.3 ESPI - Encarregado da Segurança e Privacidade da Informação

São responsabilidades do Encarregado da Segurança e Privacidade da Informação da CONTREI, nos termos do art. 41 da Lei nº 13.709/2018 ("LGPD"), bem como perante o SGI, as descritas a seguir, mas não se limitam a:

- assegurar que o SGI está em conformidade com os requisitos da Norma NBR ISO IEC 27001;
- relatar sobre o desempenho do SGI para a Alta Direção;
- conduzir a gestão e operação da segurança e privacidade da Informação;
- Elaborar e propor as normas e procedimentos de segurança e privacidade da informação, incluindo as responsabilidades pertinentes, necessários para se fazer cumprir a SGI;
- identificar e avaliar as principais ameaças ao SGI junto aos Líderes, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- tomar as ações cabíveis para se fazer cumprir os termos das políticas e demais normas do SGI e da CONTREI;
- realizar a gestão dos incidentes do SGI, garantindo tratamento adequado;
- ser o elo de comunicação entre a CONTREI, os titulares de dados e a ANPD;
- aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar providências (art. 41, §2º, I da LGPD);
- receber comunicações da ANPD e adotar providências (art. 41, §2º, II da LGPD);
- orientar os funcionários e os contratados da CONTREI a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (art. 41, §2º, III da LGPD); e
- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (art. 41, §2º, IV da LGPD).
- **Gestão de Riscos:** Coordenar e apoiar a avaliação de riscos de segurança da informação associados a novos e existentes fornecedores e ao uso de serviços em nuvem.
- **Revisões da Política:** Conduzir revisões periódicas da política e seus procedimentos, propondo ajustes com base em auditorias, incidentes e mudanças no cenário de ameaças.
- **Comunicação de Violações:** Comunicar ao CSPI quaisquer tentativas ou violações dos termos desta política relacionadas a fornecedores ou nuvem.

5.4 CSPI - Comitê de Segurança e Privacidade da Informação

É responsabilidade do CSPI incluem, mas não se limitam a:

- Acompanhar a implementação e a manutenção do Sistema de Gestão da Segurança e Privacidade da Informação (SGI) da CONTREI;
- Contribuir para que a conformidade seja obtida, por exemplo, quanto à privacidade, segurança, regulamentos administrativos e à legislação aplicável.
- Propor, apreciar e criticar as políticas, normas e procedimentos relacionados ao SGI;
- Apoiar a aplicação das políticas de segurança e privacidade da informação e as normas recomendadas, procedimentos e padrões técnicos relacionados;

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

- Apoiar o atingimento dos objetivos do SGI;
- Participar da análise de incidentes de segurança e privacidade, bem como outros temas do SGI, sempre que solicitado.
- Apresentar demandas relacionadas ao SGI de suas respectivas áreas, quando houver.
- Reportar ao ESPI temas de segurança da informação e privacidade, considerados relevantes.

5.5 Alta Direção

É responsabilidades da Alta Direção incluem, mas não se limitam a:

- Estabelecer a Política de Segurança e Privacidade da Informação;
- Garantir a integração dos requisitos do sistema de gestão do SGI dentro dos processos da CONTREI;
- Estar comprometida com uma gestão efetiva do SGI na CONTREI;
- Adotar todas as medidas para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização;
- Prover recursos necessários para o SGI e;
- Promover a melhoria contínua do SGI.

5.6 Recursos Humanos

É responsabilidades do RH incluem, mas não se limitam a:

- Dar apoio a gestão e a unidade de compliance;
- Cumprir as normas de antes, durante e pós contrato estabelecidas no SGI e;
- Quando necessário aplicar as sanções e punições cabíveis, decididas em conjunto com o Comitê e a Gestão.

5.7 Tecnologia da Informação

É responsabilidades da unidade Tecnologia da Informação incluem, mas não se limitam a:

- Administrar e gerenciamento de redes de computadores e servidores
- Administração e gerenciamento de cyber segurança do ambiente
- Administração e gerenciamento de backups
- Administração e gerenciamento de banco de dados
- Gestão dos controles de acessos
- Garantir o armazenamento seguro dos dados
- Estabelecer a Política de Segurança e Privacidade da Informação
- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

5.8 Software

É responsabilidades da unidade Software incluem, mas não se limitam a:

- Gestão dos controles de acessos;
- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade.

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

6. PROCEDIMENTO

A CONTREI entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados a seus clientes.

A CONTREI compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação pela aplicação de um processo de gestão de riscos, e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

Dessa forma, a CONTREI estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas, leis e Políticas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

6.1 Política Geral de Segurança da Informação

A CONTREI considerando a segurança da informação **estabelece e documenta através da sua Política Integrada** a seguinte política de segurança da informação:

“A CONTREI garante a Qualidade dos Serviços e a Segurança da Informação quanto à integridade, confidencialidade e disponibilidade, satisfazendo os requisitos aplicáveis dos clientes e demais partes interessadas, comprometida com a melhoria contínua do Sistema de Gestão Integrado”.

6.2 Diretrizes

A Política Geral de Segurança da Informação é comunicada dentro da CONTREI para conhecimento de todos os colaboradores, sócios e está disponível para as partes interessadas, conforme apropriado, através da rede interna da CONTREI, campanhas internas, treinamentos e no site da CONTREI.

Esta Política Geral de Segurança da Informação é complementada por políticas específicas definindo as diretrizes para a operação do SGI, incluindo, dentre outras:

Código	Título
POL 000-23	Política Integrada
POL 001-23	Política Geral de Segurança da Informação
POL 002-25	Política de Nomeação do ESPI
POL 003-25	Política de Nomeação do CSPI
POL 004-25	Política de Gestão de Segurança de Redes e Sistemas
POL 005-25	Política de Gestão de Continuidade de Negócios e Resiliência
POL 007-25	Política de Gestão de Fornecedores e Terceiros
POL 008-25	Política de Gestão de Incidentes e Resposta a Eventos de Segurança
POL 009-25	Política de Conformidade e Requisitos Legais

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

Código	Título
POL 010-25	Política de Gestão de Pessoal e Conscientização em Segurança
POL 011-25	Política de Gestão de Ativos e Inventário
POL 012-25	Política de Gestão de Mudanças e Configurações
POL 013-25	Política de Gestão de Acesso e Identidade
POL 014-25	Política de Gestão de Segurança de Dados e Informações
POL 015-25	Política de Gestão de Segurança Física e Ambiental
POL 016-25	Política de Cookies

6.3 Confidencialidade, Integridade e Disponibilidade.

A Segurança da Informação compreende a preservação da confidencialidade, Integridade e Disponibilidade da Informação, onde:

- A disponibilidade é a propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada;
- A Confidencialidade implica que a informação não esteja disponível ou revelada para pessoas não autorizadas, entidades ou processos;
- A Integridade é a propriedade relativa à acuracidade e completeza da informação.

Informações confidenciais da CONTREI, independentemente da mídia ou ambiente onde estejam sendo mantidas, devem ser protegidas contra acessos não autorizados ou acessadas com a devida autorização.

Os gestores devem informar a todos da CONTREI, os clientes, os fornecedores, usuários em geral dos sistemas de informação e dos processos, que todas as informações armazenadas, transmitidas ou manuseadas por estes processos e sistemas, são de propriedade da CONTREI, de seus clientes ou licenciadas por terceiros. Sempre que permitido pela legislação, a CONTREI reserva o direito de revisar e monitorar estas informações para fins administrativos, de segurança ou legais.

Comportamento Seguro

Independentemente do meio ou da forma, a informação está presente no trabalho de todos os colaboradores. Portanto, é fundamental para a proteção e salvaguarda das informações que os colaboradores adotem comportamento seguro e consistente com o objetivo de manter e proteger as informações.

6.4 Termo de Uso dos Sistemas Internos

Os colaboradores devem estar cientes da Política Geral de Segurança da Informação e das demais Políticas Específicas que compõem o sistema, conforme a necessidade. Para isso são treinados e assinam o FSI 007-23 Termos de Uso dos Sistemas Internos.

6.5 Processo Disciplinar

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança e privacidade, serão passíveis de processo disciplinar.

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

A existência de normas, políticas e procedimentos é condição essencial para o sucesso da empresa.

A aplicação de penalidades deve ser feita, tanto quanto possível, logo em seguida à falta cometida, sob pena de caracterizar o perdão tácito. Admite-se um período maior para a aplicação de penalidade quando a falta requerer apuração de fatos e das devidas responsabilidades. As sanções devem ser justas, razoáveis e proporcionais à falta cometida. Faltas semelhantes devem receber sanções semelhantes.

O processo disciplinar apresenta uma resposta de forma gradual, que leva em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito ou delito repetido, se o infrator foi ou não adequadamente treinado, as legislações relevantes, os contratos do negócio e outros fatores, conforme requerido. O processo disciplinar formal busca assegurar um tratamento justo e correto aos colaboradores envolvidos em supostas violações de segurança e privacidade da informação.

6.6 Controles Utilizados

O SGI da CONTREI implementa e aplica controles relativos à segurança da informação conforme estabelecida na NBR ISO IEC 27002:2022, compreendendo:

- Controles organizacionais (Seção 5).
- Controles de pessoas (Seção 6).
- Controles físicos (Seção 7).
- Controles tecnológicos (Seção 8).

Trata-se de um conjunto de 93 controles descritos na Aplicativo da Matriz de Aplicabilidade (Access). Ver Anexos I e II desta Política.

6.7 Procedimentos para rever e atualizar a política conforme necessário.

Esta política é analisada quanto à pertinência, revisada e atualizada com periodicidade anual na reunião de Análise Crítica ou conforme o entendimento do ESPI, sempre que necessário. Será reemitida somente em caso de alteração.

6.8 Procedimentos para monitorar e avaliar a eficácia da política;

Esta política é monitorada e avaliada quanto à sua eficácia e conscientização através, dos seguintes meio:

- Avaliação de eficácia dos treinamentos da Política Geral;
- Indicador de treinamento;
- Auditorias internas;
- Pesquisa Interna;
- Auditorias externas.

7. INCIDENTES E CANAIS DE COMUNICAÇÃO

Incidentes, Dúvidas e Reclamações

Em caso de incidentes do SGI, dúvidas e/ou reclamações entre em contato com a GPQ (Gestão de Processos e Qualidade) da CONTREI conforme os canais de comunicação a seguir.

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

Canais de Comunicação

A CONTREI conta com canais de comunicação, gerenciados pela área de GPQ/TI, por meio dos quais os colaboradores e demais terceiros interessados podem denunciar, de forma anônima ou identificada, práticas irregulares eventualmente ocorridas na empresa. Os Canais de Comunicação são acessíveis a todos os interessados, que deverão procurar a GPQ/TI por algum dos seguintes meios:

- E-mail: dpo@contrei.com
- Tel. (31) 3228-2250
- Endereço de correspondência: Rua Gonçalves Dias, nº 229, Bairro Funcionários - CEP 30140-090 - Belo Horizonte/MG

8. HISTÓRICO DE REVISÕES

Esta política é revisada com periodicidade anual na reunião de Análise Crítica ou conforme o entendimento do Encarregado da Segurança e Privacidade da Informação.

REVISÃO	DATA	HISTÓRICO
01	02/05/2025	Emissão Inicial do documento.

9. ANEXOS

- Anexo I - Descrição dos controles usados para proteger a informação.
- Anexo II – Aplicativo da Matriz de Aplicabilidade (Access)

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

Anexo I - Descrição dos controles usados para proteger a informação.

A5.01 - Políticas de Segurança da Informação	A7.05 – Proteção contra ameaças físicas e ambientais
A5.02 – Funções e responsabilidades de segurança da informação	A7.06 – Trabalhando em áreas seguras
A5.03 – Segregação de funções	A7.07 – Limpar mesa e limpar a tela
A5.04 – Responsabilidades da direção	A7.08 – Localização e proteção do equipamento
A5.05 – Contato com autoridades	A7.09 – Segurança de ativos fora das instalações
A5.06 – Contato com grupos de interesses especiais	A7.10 – Mídia de armazenamento
A5.07 – Inteligência de ameaças (Novo)	A7.11 – Utilitários de apoio
A5.08 – Segurança da informação na gestão de projetos	A7.12 – Segurança de cabeamento
A5.09 – Inventário de informações e outros ativos associados	A7.13 – Manutenção de Equipamento
A5.10 – Uso aceitável de informações e outros ativos associados	A7.14 – Descarte seguro ou reutilização de equipamentos
A5.11 – Devolução de ativos	A8.01 – Dispositivos de endpoint de usuário
A5.12 – Classificação da informação	A8.02 – Direitos de acesso privilegiado
A5.13 – Rotulagem de informações	A8.03 – Restrição de acesso à informação
A5.14 – Transferência de informação	A8.04 – Acesso ao código-fonte
A5.15 – Controle de acesso	A8.05 – Autenticação segura
A5.16 – Gerenciamento de identidade	A8.06 – Gerenciamento de capacidade
A5.17 – Informação de autenticação	A8.07 – Proteção contra malware
A5.18 – Direitos de acesso	A8.08 – Gestão de vulnerabilidades técnicas
A5.19 – Segurança da informação nas relações com fornecedores	A8.09 – Gerenciamento de configurações (Novo)
A5.20 – Abordando a segurança da informação nos acordos com fornecedores	A8.10 – Exclusão de informação (Novo)
A5.21 – Gerenciando a segurança da informação na cadeia de suprimentos de TIC	A8.11 – Mascaramento de dados (Novo)
A5.22 Monitoramento, revisão e gestão de mudança de serviços de fornecedores	A8.12 – Prevenção de vazamento de dados
A5.23 – Segurança da informação para uso de serviços em nuvem (Novo)	A8.13 – Backup de informação
A5.24 – Planejamento e preparação do gerenciamento de incidentes de segurança da	A8.14 – Redundância de instalações de processamento de informações
A5.25 – Avaliação e decisão sobre eventos de segurança da informação	A8.15 – Logging
A5.26 – Resposta a incidentes de segurança da informação	A8.16 – Atividades de monitoramento (Novo)
A5.27 – Apreendendo com os incidentes de segurança da informação	A8.17 – Sincronização de relógio
A5.28 – Coleta de evidências	A8.18 – Uso de programas utilitários privilegiados
A5.29 – Segurança da informação durante a interrupção	A8.19 – Instalação de software em sistemas operacionais
A5.30 – Prontidão de TIC para continuidade de negócios	A8.20 – Segurança de redes
A5.31 – Requisitos legais, estatutários, regulamentares e contratuais	A8.21 – Segurança de serviços de rede
A5.32 – Direito de propriedade intelectual	A8.22 – Segregação de redes
A5.33 – Proteção de registros	A8.23 – Filtragem da web (Novo)
A5.34 – Privacidade e proteção de PII	A8.24 – Uso de criptografia
A5.35 – Revisão independente da segurança da informação	A8.25 – Ciclo de vida de desenvolvimento seguro
A5.36 – Conformidade com políticas, regras e padrões de segurança de informações	A8.26 – Requisitos de segurança do aplicativo
A5.37 – Documentação dos procedimentos de operação	A8.27 – Arquitetura de sistema segura e princípios de engenharia
A6.01 – Seleção	A8.28 – Codificação segura (Novo)
A6.02 – Termos e condições de contratação	A8.29 – Teste de segurança em desenvolvimento e aceitação
A6.03 – Conscientização, educação e treinamento de segurança da informação	A8.30 – Desenvolvimento terceirizado
A6.04 – Processo disciplinar	A8.31 – Separação de ambientes de desenvolvimento, teste e produção
A6.05 – Responsabilidades após rescisão ou mudança de emprego	A8.32 – Gestão de mudanças

	SISTEMA SGI		POL 001 - 23		
	TÍTULO DO DOCUMENTO		REVISÃO	DATA	CLASSIFICAÇÃO
	Política Geral de Segurança e Privacidade da Informação		01	02/05/2025	PÚBLICA

A6.06 – Acordos de confidencialidade ou não divulgação	A8.33 – Informação de teste
A6.07 – Trabalho remoto	A8.34 – Proteção de sistemas de informação durante os testes de auditoria
A6.08 – Relatório de eventos de segurança da informação	
A7.01 – Perímetros de segurança física	
A7.02 – Entrada física	
A7.03 – Protegendo escritórios, salas e instalações	
A7.04 – Monitoramento de segurança física (Novo)	

Proibido reproduzir ou ceder a terceiros sem autorização da CONTREI.