Política de Segurança da Informação

1. Objetivo

Esta Política de Segurança da Informação (**PSI**) tem como objetivo estabelecer as diretrizes que assegurem e reforcem o compromisso da **CIT - Companhia Industrial Têxtil** com as práticas e medidas preventivas garantidoras de segurança da informação, criar condições para manter e melhorar continuamente a gestão de segurança da informação, protegendo os ativos de informação, visando à confidencialidade, autenticidade e disponibilidade, e descrever as regras comportamentais e as diretrizes a serem seguidas quando da execução das atividades, de tal forma a garantir a prevenção de incidentes de segurança da informação e proteção de dados pessoais.

2. Área de Aplicação

2.1 Abrangência da Política de Segurança da Informação

2.1.1 A **PSI** deve ser seguida por todos que estejam a serviço da **CIT** em qualquer etapa do processo.

3. Documentos de referência

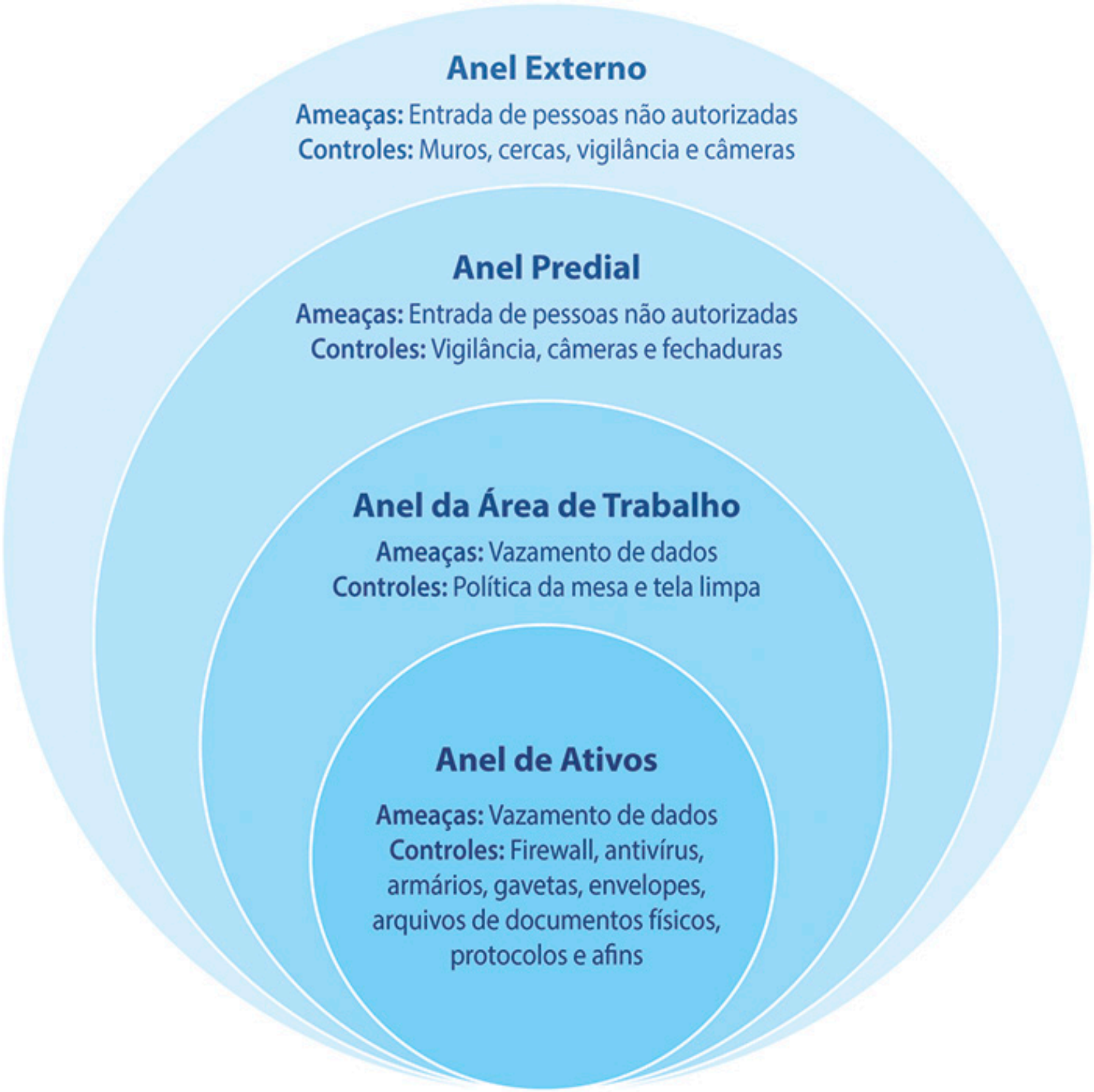
- *Lei 13.709/2018: Lei Geral de Proteção de Dados Pessoais – LGPD;*
- *ABNT NBR ISO 9001 Sistema de Gestão da Qualidade;*
- *ABNT NBR ISO/IEC 27002 Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação;*
- *MQ. CQUAL 0002 – Manual da Qualidade;*
- *PO. CQUAL.0001 – Elaboração, Revisão e Controle de Documentos da Qualidade;*
- *PO.CQUAL 0007 – Ação Corretiva;*
- *PO.CQUAL.0005 – Auditorias Internas da Qualidade;*
- *PO.GERAD.0003 – Arquivo de Documentos;*
- *PE GERAD 0043 – Segurança Patrimonial;*
- *PO.TI.0001 – Serviço de TIC.*

4. Descrição do Procedimento

4.1 Papéis e Responsabilidades de Segurança da Informação

Papel	Responsabilidades
Encarregado da Proteção de Dados (**DPO**)	Prestar esclarecimentos para os titulares de dados pessoais acerca da política de privacidade de dados e os direitos previstos na Lei Geral de Proteção de Dados (LGPD). Prestar esclarecimentos para a Autoridade Nacional de Proteção de Dados (ANPD), quando solicitado. Adequar e auditar as melhores práticas necessárias para a conformidade com a Lei Geral de Proteção de Dados (LGPD). Monitorar a tabela de temporalidade de documentos e o descarte das informações. Orientar e esclarecer sobre melhores práticas de segurança da informação no âmbito da CIT.
Membro do Comitê de Proteção de Dados	Assessorar o Encarregado da Proteção de Dados (DPO) sobre decisões que possam impactar a confidencialidade, disponibilidade e integridade de dados.
Equipe de Tecnologia da Informação (TI)	Manter os sistemas da informação disponíveis. Realizar cópias de segurança (backup) das informações da CIT. Proteger a infraestrutura de tecnologia da informação contra ameaças internas e externas sejam elas de ordem humana ou natural. Dar suporte a todos os papéis no uso da tecnologia da informação. Controlar a entrada de pessoal às dependências do Datacenter (Central de Processamento de Dados).
Colaborador, Prestadores de serviços temporários, Prestadores de serviços e terceirizados.	Ler, assimilar e praticar a PSI durante o período integral de trabalho e/ou durante a prestação de serviços em nome da CIT. Acionar o DPO no caso de dúvidas sobre a segurança das informações e proteção de dados pessoais. Acionar a equipe de tecnologia da informação no caso de suspeitas de ameaças no ambiente tecnológico. Não divulgar informações e dados da CIT e/ou informações que estejam provisoriamente sobre sua posse.
Fornecedores, Consultores, Auditores e Parceiros de negócio.	Ler, assimilar e praticar a PSI durante a prestação de serviços em nome da CIT. Acionar o DPO no caso de dúvidas sobre a segurança das informações e proteção de dados pessoais. Não divulgar informações e dados da CIT e/ou informações coletadas durante a prestação de serviços em nome da CIT.

4.2 Os anéis e o ambiente da ameaça de segurança da informação da CIT



4.3 Termos e definições

4.3.1 Para conhecer os termos utilizados nessa **PSI CIT** consultar a norma ABNT NBR ISO/IEC 27002 e ou a Lei 13.709/2018: Lei Geral de Proteção de Dados Pessoais – LGPD.

4.4 Gestão de ativos de informação

4.4.1 A **CIT** definiu procedimentos para a gestão dos seus ativos de informação de forma a garantir o uso seguro (proteção) e as atualizações recomendadas, prevenindo as ameaças e vulnerabilidades de forma a manter a disponibilidade destes;

4.4.2 A **CIT** deve criar, gerir e avaliar critérios de tratamento e **classificação da informação** de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor;

4.4.3 Os **ativos de informação (do tipo softwares)** devem possuir mecanismos que permitam a **auditoria** dos eventos. Esta **auditoria** deve estar sempre ativa (salvo quando explicitamente dispensado este requisito) e os registros devem ser armazenados pelo período de 12 meses.

4.5 Diretrizes de Segurança da Informação

4.5.1 Controle de acessos

4.5.1.1 A **CIT** definiu procedimentos específicos contendo parâmetros e regras para criação e gerenciamento de senhas, gestão de acesso aos seus sistemas, dados e informações;

4.5.1.2 As regras e procedimento para acesso as instalações da **CIT** estão previstos no **PE GERAD 0043 – Segurança Patrimonial;**

4.5.1.3 Os usuários da **CIT** são responsáveis por todos os atos praticados com suas identificações (credenciais), tais como: nome de usuário/senha (**pessoal e intransferível**), crachá, carimbo, correio eletrônico e certificado digital.

4.5.2 Segurança das comunicações da CIT

4.5.2.1 A **CIT** contempla no **MQ – CQUAL 0002 – Manual da Qualidade –** diretrizes de **segurança da informação** para a disponibilização e utilização de serviços de comunicação.

4.5.3 Comunicação no ambiente digital

4.5.3.1 A **CIT** definiu procedimentos específicos contendo diretrizes de segurança da informação para a disponibilização e utilização de serviços de comunicação relacionados aos ativos de informação (ferramentas de comunicação).

E-mail: É o meio de comunicação oficial. Devem ser utilizado em comunicação que necessitem de rastreabilidade, segurança e formalização.

Google Meet: Deverá ser priorizado quando do agendamento para reuniões virtuais.

Nota: *Poderão ser usadas ferramentas de comunicação auxiliares, como WhatsApp e Skype. Quando a informação exigir registro, o e-mail é obrigatório.*

4.5.3.2 As ferramentas oficiais de comunicação da **CIT** são **monitoradas** e as mensagens trocadas poderão ser **auditadas** a qualquer momento, sem comunicação prévia ao usuário.

4.5.3.3 Acesso à Internet

4.5.3.3.1 O uso da internet é **monitorado** e poderá ser **auditado** pela equipe de tecnologia da **CIT**. O usuário poderá vir a prestar contas de seu uso para o comitê de proteção de dados e ao **DPO**;

4.5.3.3.2 A internet deve ser utilizada para fins profissionais e de interesse da **CIT**;

4.5.3.3.3 Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados é proibido e a tentativa de burlar os bloqueios realizados pela equipe de tecnologia da informação da **CIT** é falta grave e será passível de punição;

4.5.3.3.4 É proibido: Download de softwares e conteúdos protegidos pela lei de propriedade intelectual, utilizar ferramentas de compartilhamento Peer-2-Peer (P2P) (kazaa, Morpheus, Torrent e afins).

4.5.3.4 Impressão e descarte de documentos

4.5.3.4.1 Verifique se é realmente imprescindível a **impressão** do documento;

4.5.3.4.2 Quando do **descarte** de documentos deverá ser realizado conforme previsto no **PO-GERAD-0003 – Arquivo de Documentos**;

4.5.3.4.3 No caso da utilização de impressora compartilhada, se dirija até a impressora imediatamente após autorizar a impressão;

4.5.3.4.4 Documentos que, possuam qualquer tipo de **dados pessoais**, como nomes, telefones, e-mails e afins, não poderão ser utilizados como rascunho, devendo ser descartados, preferencialmente triturados de forma que seja impossível identificar os dados ali contidos;

4.5.3.4.5 As informações impressas para a entrega a terceiros, fora do ambiente empresarial, deve ser realizado através da utilização de **envelope lacrado**, devidamente protocolado.

4.5.3.5 Política da Mesa e Tela Limpa

4.5.3.5.1 Jamais deixe documentos confidenciais, principalmente aqueles que contenham **dados pessoais**, visíveis sobre a sua mesa;

4.5.3.5.2 Após a utilização da documentação, guarde-a imediatamente em seu arquivo apropriado/determinado.

4.5.3.6 Uso de estação de trabalho e cópia de segurança (Backup)

4.5.3.6.1 A **CIT** definiu procedimento específico para o uso seguro das estações de trabalho e dos procedimentos necessários para garantir que as informações relevantes sejam objeto de backup;

4.5.3.6.2 Todos os dados relativos à empresa devem ser mantidos no servidor de arquivos, objeto do serviço de **backup** diário e confiável. A equipe de tecnologia da informação e o **DPO** não se responsabilizam por arquivos armazenados na estação de trabalho;

4.5.3.6.3 Informações salvas em estações de trabalho dos colaboradores, fornecedores, prestadores de serviços temporários, consultores, auditores e afins, são de responsabilidade dos mesmos, bem como em relação à integridade, confidencialidade e disponibilidade da informação.

4.5.3.7 Política Social

4.5.3.7.1 Não comente sobre as rotinas de trabalho na **CIT** para terceiros e/ou em locais públicos para evitar a prática de phishing;

Nota: *Phishing é uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito. São comunicações falsificadas que parecem vir de uma fonte confiável.*

4.5.3.7.2 Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa;

4.5.3.7.3 Somente aceite ajuda técnica de um membro da equipe de tecnologia da informação, previamente apresentado e identificado;

4.5.3.7.4 Nunca execute procedimentos técnicos cujas instruções não tenham sido previamente aprovadas pela equipe de tecnologia da informação da **CIT**;

4.5.3.7.5 Relate a equipe de Tecnologia da Informação pedidos externos ou internos que venham a discordar dos tópicos anteriores.

4.5.3.8 Vírus e códigos maliciosos.

4.5.3.8.1 É de responsabilidade do setor de Tecnologia da Informação a manutenção do software de antivírus atualizado. Caso perceba mensagens de alerta do seu software de antivírus, como ameaças ou necessidade de atualização, acione a equipe de Tecnologia da Informação imediatamente;

4.5.3.8.2 Informe comportamento suspeito em seu sistema operacional para a equipe de tecnologia da informação, para que possíveis códigos maliciosos possam ser identificados no menor espaço de tempo possível;

4.5.3.8.3 Suspeite de softwares recém-instalados na sua estação de trabalho sem o seu consentimento. Caso isto ocorra, acione imediatamente o setor de tecnologia da informação para confirmar a origem.

4.5.3.9 Trabalho remoto

4.5.3.9.1 O trabalho remoto só deverá ser realizado através de uma autorização formal concedida pelo seu gestor direto;

4.5.3.9.2 O trabalho remoto ocorrerá através do uso da solução de **VPN (*Virtual Private Network*)** que deverá ser solicitada ao setor de Tecnologia da Informação, quando necessário;

4.5.3.9.3 Durante o período de trabalho fora das dependências da **CIT**, cuide da estação de trabalho e não permita que estranhos tenham acesso;

4.5.3.9.4 Mesmo em trabalho remoto, a estação de trabalho deverá ser utilizada exclusivamente para fins profissionais e de interesse da **CIT**;

4.5.3.9.5 A utilização da estação de trabalho da **CIT** para prática de ***cybercrimes*** é passível de penalidades, inclusive, na esfera judicial.

> ***Nota:*** *Crime digital, crime informático, crime cibernético, cybercrime, crime eletrônico são termos aplicáveis a toda a atividade criminosa em que se utiliza de um computador ou uma rede de computadores como instrumento ou base de ataque.*

4.5.3.10 Uso de dispositivos móveis (Smartphones, tabletes e correlatos).

4.5.3.10.1 Os dispositivos móveis da **CIT** disponibilizados aos seus colaboradores estão autorizados para o uso empresarial;

4.5.3.10.2 Não é permitido utilizar o **celular / *smartphone* de uso pessoal** para registrar, por texto, áudio, vídeo ou foto, quaisquer informações empresariais ou confidenciais;

4.5.3.10.3 Não é permitido usar o celular para gravar conversas sem que todos os envolvidos na conversa tenham autorizado previamente a gravação;

4.5.3.10.4 É proibido utilizar o ***smartphone* da empresa** para atividades que infrinjam quaisquer leis ou normativas aplicáveis à pessoa física ou à empresa;

4.5.3.10.5 É proibido usar de linguagem imprópria, ou ter comportamentos considerados nocivos à imagem da empresa enquanto estiver em ligação ou envio de áudio no horário de trabalho, principalmente na presença de clientes, parceiros e colaboradores;

4.5.3.10.6 Não é permitido o uso de dispositivos móveis pessoais de prestador de serviços e/ou colaboradores na rede de dados da **CIT**.

4.5.3.11 Abertura de chamados de tecnologia da informação

4.5.3.11.1 Todas as demandas de tecnologia da informação serão tratadas através da abertura de chamado utilizando serviço de gestão de incidentes;

4.5.3.11.2 Todo e qualquer procedimento de tecnologia da informação repassado por terceiros não deve ser executado sem o prévio conhecimento e autorização do setor de tecnologia da informação.

4.5.3.12 Sanções e Punições

4.5.3.12.1 O não cumprimento das diretrizes da Política de Segurança da Informação acarretará em reciclagem obrigatória em segurança da informação e ou advertência emitida pelo **DPO** e formalizada pelo setor de **Departamento de Pessoal da CIT**, podendo culminar até mesmo no desligamento do colaborador ou rescisão contratual com fornecedores e prestadores de serviço, de acordo com a gravidade da ocorrência;

4.5.3.12.2 Tais penalidades não excluem a possibilidade de direito de regresso, através de ação judicial em desfavor do colaborador, terceirizado, prestador de serviço ou qualquer outra atuação de um profissional ou empresa em nome da **CIT**.

4.5.3.13 Casos omissos e exceções

4.5.3.13.1 Os casos omissos e exceções à Política de Segurança da Informação (**PSI**) serão tratados formalmente, através de um processo administrativo interno, liderado pelo **DPO** e Comitê da Proteção de Dados.

CIT

COMPANHIA INDUSTRIAL TÊXTIL

TECIDOS
CONSTÂNCIO VIEIRA
DESDE 1912

Sistema de Gestão da Qualidade ISO 9001

ISO 9001
BUREAU VERITAS
Certification

BUREAU VERITAS 1828

constanciovieira.com.br