Política de Segurança da Informação (PSI)

1. Objetivo

Estabelecer as diretrizes para a proteção das informações geradas, tratadas e armazenadas pela Casa & Terra acerca de seus clientes, parceiros, fornecedores e colaboradores, assegurando a conformidade com a Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018) e normas internacionais, como a ISO/IEC 27001:2022 e o NIST Cybersecurity Framework. A PSI também visa orientar a criação, armazenamento, processamento, segurança, integridade, confidencialidade e disponibilidade das informações.

2. Princípios

Princípios sobre a preservação das informações do Casa & Terra:

a) Confidencialidade: Garantia de que o acesso seja obtido somente por pessoas autorizadas.

b) Disponibilidade: Garantia da geração da informação através dos dados e fontes do Casa & Terra e que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

c) Integridade: Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda, transmissão ou publicação, contra alterações indevidas, intencionais ou acidentais.

3. Termos e Definições

• Canais de *Broadcast* – Meio usado para transmitir informações ou dados sem distinção de remetentes.

• Dados Públicos – Informações que não possuem restrições de acesso e estão disponíveis para qualquer pessoa, sem necessidade de autorização.

• Dados Confidenciais – Informações internas da empresa que são acessíveis apenas por pessoas autorizadas, devido ao seu valor estratégico ou potencial impacto em caso de divulgação não autorizada.

• Dados Sensíveis – Dados pessoais relacionados à origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dado genético ou biométrico, filiação a sindicato, entre outros definidos no artigo 5º, II, da LGPD, que, em caso de vazamento ou mau uso, podem causar discriminação, prejuízo ou danos aos titulares.

• *Data Protection Officer* – Também conhecido como DPO ou Encarregado, nos termos da Lei nº 13.709/2018 ("LGPD"), é o responsável da empresa para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

• E-mail *Bombing* – Forma de ataque que consiste em enviar um volume muito alto de e-mails para um endereço de e-mail específico tendo como objetivo interromper o serviço de correio eletrônico do destinatário.

• *Peer-to-Peer* (P2P) - Arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central. Permite a realização de downloads de arquivos de múltiplas fontes simultaneamente para distribuição de carga de tráfego.

• *Sniffers* – Programas de computador que capturam tráfego de rede e analisam. •

VPN - Rede de comunicações privada e criptografada construída sobre uma rede de comunicações pública para acesso seguro entre dois pontos.

• RISI – O Relatório de Incidentes de Segurança da Informação é um documento que registra e detalha incidentes relacionados à segurança da informação. • Patch de Segurança – São criados para fazer atualização ou correção de software e resolver falhas de segurança em um sistema, aplicativo ou rede.

4. Escopo

Aplica-se a todos os colaboradores, terceiros, fornecedores e parceiros que tenham acesso às informações e recursos tecnológicos do Casa & Terra. Engloba dados em formato físico e digital, sistemas de TI, dispositivos e redes corporativas.

5. Responsabilidades

5.1. Da Gerência e Diretoria

• Analisar e aprovar os instrumentos normativos e operacionais relacionados à adoção desta Política de Segurança da Informação e aos treinamentos necessários para manter a segurança da informação;

• Avaliar criticamente, periodicamente, esta política e os indicadores de segurança da informação.

5.2. Dos Integrantes

• Se manter atualizado em relação a esta política e aos seus procedimentos e normas relacionadas, buscando orientação do seu gestor, da Diretoria de Tecnologia da Informação ou do Encarregado sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações;

• Proteger os ativos e informações que estejam sob sua custódia e arcar por todos os atos executados com sua identificação de acesso (não repúdio).

5.3. Dos Gestores

• Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;

• Aprovar ou solicitar os acessos dos colaboradores aos dados, informações, processos e sistemas do Casa & Terra;

• Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviço ou de parceria, a responsabilidade do cumprimento desta Política.

5.4. Do Encarregado de Proteção de Dados (DPO)

• Analisar e aprovar, em conjunto com a Gerência e Diretoria, os instrumentos normativos e operacionais relacionados à Segurança da Informação; • Avaliar criticamente e periodicamente esta política e os indicadores de segurança da informação e sua coerência com a política de privacidade disposta pelo mesmo; • Comunicar e coletar aprovações junto ao Comitê de Segurança da Informação de assuntos referentes aos dados pessoais, inclusive comunicações da ANPD; • Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

5.5. Do Comitê de Segurança da Informação

O Comitê de Segurança da Informação é composto por três membros, a ser definido pelo Conselho de Administração da Companhia e será coordenado pela área de Controles Internos e Auditoria a fim de assegurar o cumprimento desta política por todas as partes responsáveis.

6. Termo de Confidencialidade

Todos os colaboradores, terceiros, fornecedores e parceiros devem assinar o Termo de Confidencialidade ao iniciar suas atividades com o Casa & Terra. Este termo reforça a obrigação de:

- Proteger informações sensíveis;
- Não divulgar dados pessoais ou corporativos sem autorização;
- Garantir a devolução ou destruição de dados após o término da relação contratual.

7. Da Política De Privacidade

Os dados pessoais coletados, criados, repassados, excluídos ou modificados dentro da empresa, seja por meio tecnológico, físico, visual ou voz devem ser autorizados pelo proprietário e informados ao DPO, contendo:

• Finalidade e forma de uso;

• Especificação dos dados;

• Mapa de Dados (onde está armazenado e como serão utilizados);

• Dicionário de dados (o que é cada dado, tamanho do campo e tipo do campo);

• Temporalidade dos dados pessoais (quanto tempo deverá ser mantido e qual o procedimento de descarte da informação);

• Forma de coleta de consentimento do Titular dos dados;

• Forma de atendimento ao Titular dos Dados Pessoais;

• Integração e interoperabilidade com a ANPD.

Todos os sistemas e serviços informatizados devem possuir características de rastreabilidade e auditabilidade, inclusive para verificar quem efetuou pesquisa de determinado dado pessoal, com, no mínimo, usuário, origem, horário e ação.

7.1. Consentimento

O Casa & Terra garante que o consentimento dos titulares dos dados seja obtido de maneira clara e inequívoca, com linguagem acessível, explicando:

• A finalidade da coleta;

• A forma de utilização e armazenamento dos dados;

• O direito de revogar o consentimento a qualquer momento.

Todo consentimento deve ser registrado e armazenado de forma rastreável, incluindo a data e hora em que foi concedido.

7.2. Retenção e Descarte de Dados

Os dados pessoais e corporativos devem ser armazenados apenas pelo tempo necessário para as finalidades legítimas. Após o período definido, será realizada a exclusão ou anonimização segura, conforme procedimentos documentados e rastreáveis.

7.3. Transferência Internacional de Dados

A transferência internacional de dados pessoais será realizada apenas para países ou organizações que garantam níveis adequados de proteção, em conformidade com os requisitos estabelecidos pela LGPD. A empresa buscará celebrar cláusulas contratuais específicas e implementar garantias adicionais, quando necessário.

8. Diretrizes

8.1. Segurança do Ambiente Físico

Os locais que guardam equipamentos físicos que armazenam os sistemas utilizados pelo Casa & Terra ou equipamentos de rede devem estar devidamente protegidos, com acesso controlado e monitorado. A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e funcionários sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

O acesso às dependências da empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou equipamentos similares só pode ser feito mediante autorização da Diretoria de Tecnologia da Informação, com supervisão. Exceto para eventos e treinamentos organizados pela própria empresa.

8.2. Gestão de Acessos

No momento da criação de usuários, são concedidos automaticamente acessos mínimos iniciais respeitando o princípio de menor privilégio.

Qualquer outro acesso deve ser solicitado mediante abertura de chamado.

Os gerentes e o DPO serão responsáveis por definir as permissões de acesso às informações de sua área, e caso não estejam disponíveis, as limitações serão definidas pelo superior imediato.

Diante da necessidade de criação ou modificação de contas de usuários, sejam eles fixos, temporários, de serviço ou terceiros, os gestores das áreas deverão enviar a solicitação para a área de Gestão de Acessos, que detém permissão para tal.

Imediatamente no momento da demissão, todas as credenciais associadas ao usuário são desativadas. No entanto, para garantir a segurança contínua, após o prazo de 24 horas, procedemos com a revogação de todos os acessos, incluindo eventuais contas secundárias vinculadas ao colaborador.

É vetado a usuários com acesso privilegiado realizar modificações que não constem no escopo da função ou que sejam para benefício próprio.

8.2.1. Acesso de Prestadores de Serviço

Todo acesso de prestadores de serviço deve ser solicitado por meio da abertura de um chamado na ferramenta PortalCT, sendo detalhado e enviado pelo responsável do terceiro.

A conta será desativada imediatamente após o término do período autorizado de 90 dias ou mediante desligamento do terceiro, após esse período deverá ser aberto um novo chamado para regularização. Caso o terceiro não necessite mais de acesso antes do período previamente autorizado, a conta será desativada imediatamente a pedido do responsável ou pela equipe de Segurança da Informação.

8.3. Senhas

Por ser um instrumento de validação de identidade, fica proibido o compartilhamento de quaisquer senhas ou identificação de uso pessoal com outros usuários, bem como o armazenamento em locais visíveis a esses.

Na ocorrência de identificação de vazamento de credenciais, o colaborador deverá

alterar a senha imediatamente. Caso não ocorra a troca em tempo hábil, os acessos serão bloqueados e a senha será alterada sem aviso prévio pela equipe de Segurança da Informação.

A criação e troca de senhas deve atender os seguintes requisitos:

a) Conter no mínimo 8 caracteres e combinar letras maiúsculas, minúsculas, números e caracteres especiais, além de não utilizar as últimas 3 senhas. b) Não utilizar palavra referente ao nome fantasia das empresas do grupo (Exemplos: Casa & Terra, Casa, CT, Terra, CTERRA).

c) Não utilizar datas e números em sequência e/ou repetidos (Exemplos: 123456, 1212, 2020).

d) Expirar a cada 45 dias.

8.4. Computadores e Recursos Tecnológicos

Entende-se como recurso tecnológico qualquer ferramenta, sistema, dispositivo, software ou infraestrutura que utiliza a tecnologia para facilitar, otimizar ou melhorar uma atividade ou processo.

Os recursos tecnológicos, os dados e informações que os complementam devem ser utilizados pelos integrantes para fins exclusivos de realização das atividades profissionais concernentes ao cargo e função que ocupam na estrutura do Grupo Casa & Terra, cabendo a cada integrante utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

O Casa & Terra, por meio da Diretoria de Tecnologia da Informação, registrará todo o uso dos equipamentos, sistemas e serviços, visando garantir a segurança das informações e de sua infraestrutura. Toda tentativa de alteração dos parâmetros de segurança, por qualquer integrante, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao gestor responsável, quando aplicável.

Em suma, é vetado ao usuário:

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

• Burlar quaisquer sistemas de segurança e monitoramento;

• Acessar informações confidenciais sem explícita autorização do proprietário;

• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (*sniffers*);

• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio, perturbação, manipulação ou supressão de direitos ou propriedades intelectuais sem a devida autorização legal do titular;

• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

• Propagar qualquer programa ou código maliciosos;

• Utilizar software pirateado/não licenciado.

8.4.1. Uso de Computadores Pessoais

É proibido o uso de qualquer equipamento pessoal para realização de tarefas corporativas dentro ou fora do ambiente do Casa & Terra. A utilização de equipamentos (notebooks, celulares, tablets, etc.) pessoais para realização das atividades corporativas, somente será permitida mediante a aprovação do gestor, autorização da Diretoria de Tecnologia da Informação e assinatura do Termo de Aceite de Risco, sendo certo que o tratamento de dados no uso do equipamento será monitorado e ainda passível de auditoria de segurança antes do ingresso à rede ou após o encerramento das atividades do profissional no Casa & Terra. Caso o equipamento auditado não atenda aos requisitos mínimos de segurança, o mesmo

não terá acesso à rede corporativa.

Ao ser autorizado o uso de equipamentos pessoais, fica a cargo do proprietário do equipamento arcar com o licenciamento de todos os softwares necessários. O proprietário deverá arcar com as penalidades previstas na legislação sobre uso de softwares pirateados.

Sendo constatada a inconformidade com a diretriz apresentada, medidas administrativas serão tomadas sob prescrição do RISI (Repository of Industrial Security Incidents).

8.4.2. Uso de Computadores Corporativos

O integrante deve utilizar os equipamentos fornecidos pela Casa & Terra apenas para a realização de suas rotinas de trabalho junto à empresa. Mesmo esse tendo o computador sob sua responsabilidade não poderá modificar o software e o hardware sem autorização prévia e acompanhamento do time de tecnologia.

Todos os computadores deverão seguir o padrão de configuração descrito no Anexo I desta política, adendo os seguintes requisitos:

- Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor;
- Todos os computadores de uso individual deverão ter senha de BIOS para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Diretoria de Tecnologia da Informação da Casa & Terra, que terá acesso a elas para manutenção dos equipamentos;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do Casa & Terra ou por terceiros devidamente contratados para o serviço;
- O integrante deverá manter a configuração do equipamento disponibilizado, seguindo os devidos controles de segurança exigidos;

• Deverão ser protegidos por senha (bloqueados), todas as estações de trabalho e impressoras quando não estiverem sendo utilizados;

• Todos os recursos tecnológicos adquiridos pelo Casa & Terra devem ter imediatamente suas senhas padrões (*default*) alteradas;

• Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso; •

Os servidores e computadores devem ter versões do software antivírus instalados, ativados e atualizados permanentemente. Caso seja observado a tentativa de remoção de qualquer patch de segurança, o RISI será enviado e o usuário será responsabilizado. Qualquer suspeita de vírus ou similares, o time de tecnologia deverá ser acionado.

As estações de trabalho não serão objeto de procedimentos de backup.

8.4.3. Servidor de Arquivos (*File Server*)

Todas as informações, documentos e dados técnicos que constituem o capital intelectual do Casa & Terra, independentemente de sua classificação (públicos, confidenciais ou sensíveis), devem ser salvos nas unidades de rede. Caso essas sejam armazenadas em outros locais não aprovados previamente pela Diretoria de Tecnologia de Informação, tais como: disco local do computador, HD externos, pen drive, correio eletrônico, drivers virtuais (One Drive pessoal, Dropbox, iCloud, etc.), cópias físicas, dentre outros, as mesmas não terão sua integridade e confidencialidade garantidas. E, em caso de perda, o integrante que realizou o uso indevido será responsável por todos os danos ou prejuízos causados ao Casa & Terra e a terceiros.

Fica proibido o armazenamento de arquivos que não estejam relacionados diretamente ou não sejam pertinentes ao negócio do Casa & Terra, tais como arquivos de filmes, fotos pessoais ou de terceiros, músicas, vídeos, etc., em suas estações de trabalho, nos equipamentos portáteis (notebooks, smartphones, pen drives, etc.), nos servidores, sistemas da rede e nos diretórios compartilhados. Fica

concedido o direito aos responsáveis da Diretoria de Tecnologia da Informação da Casa & Terra e do Encarregado de remover, quando encontrados esses arquivos, sem aviso prévio, e o direito de utilizá-los em procedimentos de auditoria e prestação de contas à Autoridade Nacional de Proteção de Dados, se necessário.

8.5. Internet

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política de Segurança da Informação.

A internet disponibilizada pela instituição aos seus integrantes deve ser utilizada com moderação, pautada nos princípios éticos e morais da instituição. A utilização da internet para acessar sites e utilizar aplicativos que contrariem as leis vigentes é terminantemente proibida, assim como a realização de qualquer download, exposição, armazenamento, edição, distribuição e impressão relacionados a práticas sexuais, ilegais, abusivas ou imorais por meio de qualquer recurso.

Os integrantes detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Diretoria de Tecnologia da Informação.

Não é permitido o acesso a sites de proxy ou a ferramentas de VPN não autorizadas pela empresa nos equipamentos fornecidos.

8.6. Acesso Remoto

A solução de VPN corporativa é um recurso para acesso remoto à rede Casa & Terra, sendo obrigatória quando houver necessidade de acesso de outros países.

A solicitação de acesso deverá ser aberta na ferramenta CSC e aprovada pelo gestor do setor e pela Gerência da Tecnologia da Informação. Devem ser informadas no chamado as tarefas do integrante que levam à necessidade do acesso com VPN. Após a aprovação da solicitação aberta, o notebook corporativo do integrante deverá

ser encaminhado ao departamento de Tecnologia da Informação para auditoria, instalação do cliente, configurações e orientações de uso para o acesso.

O integrante deve manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço, devendo abster-se de usar a funcionalidade para quaisquer outras atividades. Cada vez que o integrante se ausentar de seu equipamento, deve executar *logoff* ou bloquear a estação de trabalho.

Não é permitido o uso da VPN corporativa em computadores pessoais ou que não estejam no domínio da Casa & Terra, assim como conceder o uso da sessão a quaisquer outros funcionários.

8.7. Correio Eletrônico e Chat Corporativo

O uso do correio eletrônico (e-mail Google Workspace) e do chat (Chats ou Meet) é para fins corporativos e relacionados às atividades do integrante dentro da instituição, sendo proibida sua utilização para fins pessoais. Para assegurar o uso correto, é vedado ao integrante:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Redirecionar automaticamente os e-mails corporativos para endereços externos;
- Enviar mensagens utilizando o endereço eletrônico de seu departamento, que não esteja autorizado, ou usando o nome de usuário ou o endereço eletrônico de outra pessoa;
- Enviar qualquer mensagem que torne seu remetente e/ou a empresa e o Grupo Casa & Terra vulnerável a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas,

documentos e afins sem autorização expressa e formal concedida pela empresa do Casa & Terra;

• Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

• Apagar mensagens pertinentes de correio eletrônico quando o Grupo Casa & Terra estiver sujeito a algum tipo de investigação;

• Utilizar o e-mail como repositório de documentos;

• Produzir, transmitir ou divulgar mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Casa & Terra;
- Contenham ameaças eletrônicas, como: spam, e-mail *bombing*, vírus e etc.;
- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise a obter acesso não autorizado a outro computador, servidor ou rede;
- Vise a interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise a burlar qualquer sistema de segurança;
- Vise a vigiar secretamente ou assediar outro usuário;
- Vise a acessar informações confidenciais sem explícita autorização do proprietário;
- Vise a acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) de 15MB para recebimento (internet)
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física, mental ou outras situações protegidas;
- Inclui material protegido por direitos autorais sem a permissão do detentor dos direitos.

8.8. Dispositivos de Armazenamento

O armazenamento de informações corporativas em mídias removíveis é expressamente proibido, e, por padrão, as portas USB devem ser bloqueadas para a utilização de dispositivos de armazenamento (consideram-se celulares, HDs, pen drives, cartões de memória etc.) em todas as máquinas. Isso impede o acesso não autorizado, a introdução de malware, o roubo de dados ou outras atividades maliciosas. Informações corporativas devem ser transmitidas utilizando as ferramentas corporativas (e-mail, rede de dados, software de mensageria etc.), que providenciam a segurança requerida.

Os usuários devem submeter solicitações formais para obter a liberação das portas USB para dispositivos de armazenamento através do portalCT. As solicitações devem ser aprovadas pelo gestor e pela equipe de tecnologia. Cada solicitação deve incluir uma justificativa clara para a necessidade da liberação.

As exceções serão analisadas caso a caso, e o Termo de Responsabilidade de Uso de Dispositivos de Armazenamento Externo será enviado ao colaborador no momento do atendimento do chamado, o qual deverá assinar se responsabilizando pelos riscos e pela reparação à empresa por eventuais danos materiais e imateriais decorrentes do uso do dispositivo a ser liberado, ou que venha a contribuir para a perda/vazamento de informações confidenciais e/ou permitir a entrada de vírus e similares na rede corporativa.

A liberação será feita por um período máximo de 90 dias. É recomendado que os arquivos sejam criptografados durante o uso, devendo ser deletados posteriormente. Um novo chamado deve ser aberto após a expiração.

9. Gestão de Conteúdo

Qualquer informação acessada, transmitida, recebida ou produzida como resultado da atividade profissional exercida no âmbito do Casa & Terra está sujeita a divulgação e auditoria pela Diretoria de Tecnologia da Informação e pelo Encarregado, sendo de propriedade exclusiva da empresa. As exceções devem ser explicitadas e formalizadas em instrumento apartado.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em canais não oficiais de comunicação definidos pela empresa, sendo também vedada a divulgação de informações sobre as operações de quaisquer das empresas do Casa & Terra fora do ambiente de trabalho. Somente os integrantes devidamente autorizados a falar em nome das empresas do Casa & Terra para os meios de comunicação poderão se manifestar, seja por e-mail, entrevista online, seja por documento físico, entre outros. Da mesma forma, apenas os integrantes autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e aos demais dispositivos legais.

Como é do interesse do Casa & Terra que seus integrantes estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio. O acesso a softwares *peer-to-peer* (uTorrent, BitTorrent e afins) e serviços de streaming (rádios online, canais de *broadcast* e afins) não serão permitidos, salvo os integrantes que o acesso a estes serviços é necessário para a execução das atividades.

As soluções de armazenamento e gestão de conteúdo, fornecidas e providenciadas pela Diretoria de Tecnologia da Informação e pelo Encarregado, deverão ser prontamente atendidas pelos usuários, não cabendo o direito a soluções alternativas.

10.Aquisição de Software

A aquisição de novos softwares somente ocorrerá após avaliação de segurança, conformidade com as leis vigentes, custo de licenciamento, eficiência operacional e compatibilidade com nossos sistemas operacionais, assim como a viabilidade de manutenção e suporte.

Os contratos de aquisição devem incluir cláusulas que abordem segurança, com responsabilidade do fornecedor por correções e atualizações. Mesmo que gratuitos ou sob licença GNU (Licença Pública Geral), todo e qualquer software deve ser encaminhado para a equipe de TI para avaliação, aprovação, disponibilização do executável e instalação.

Todos os softwares estão sujeitos ao bloqueio se forem encontradas divergências com os parâmetros da Política de Segurança da Informação, e, caso seja identificado o uso, instalação, cópia ou distribuição de programa não licenciado ou não autorizado, que tenham direitos autorais, marca registrada ou patente, serão desinstalados sem aviso prévio.

É de responsabilidade da Diretoria de Tecnologia da Informação implementar ferramentas de monitoramento proativo para identificar o uso não autorizado de softwares, permitindo uma intervenção rápida e eficaz.

11.Auditoria e Monitoramento

O Casa & Terra realizará auditorias periódicas de sistemas e práticas de segurança, abrangendo:

- Controle de acesso físico e lógico;
- Rastreamento de atividades em sistemas críticos;
- Identificação de não conformidades com a PSI.

Os resultados das auditorias serão documentados e reportados à alta gestão, com planos de ação corretiva sempre que necessário.

12.Solicitações

Toda e qualquer solicitação e/ou comunicação deve ser feita exclusivamente na ferramenta portalCT na opção “Chamados de TI” ou pelo telefone (61)3221-5711.

Situações não previstas nesta política serão deliberadas pelo diretor da Diretoria de Tecnologia da Informação.

15.Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27001:2022: **Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos**. Brasília, 2025.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 11 Julho. 2025.

16.Histórico de Revisões

Revisão	Histórico	Área responsável pela elaboração/Revisão	Cargo do aprovador	Data
01	Versão Inicial	Tecnologia da Informação	Diretor	11/07/2025

ANEXO I
PADRONIZAÇÃO WINDOWS

Todas as instalações do sistema operacional Windows 10/11 em estações de trabalho (Desktop/Notebook) deverão seguir os seguintes padrões:

Preparação

- A senha default deve ser alterada para inibir o acesso a pessoas não autorizadas. O usuário “Administrador” (local) do sistema operacional deverá ser ativado e deve ser adicionada a senha padrão estabelecida pela Diretoria de Tecnologia da Informação.

Essa senha será de responsabilidade e guarda exclusiva do técnico e, em hipótese alguma, será passada ao usuário.

• Todas as máquinas deverão ter as configurações de rede configuradas para DHCP.

• Antes de formatar, verificar a etiqueta com a chave do Sistema Operacional e do Microsoft Office.

Instalação

• A máquina deverá ser formatada, ou seja, não deverá ser feito 'upgrade' do sistema operacional anterior.

• O disco deverá ser formatado exclusivamente em NTFS.

• O disco terá apenas uma partição, designada como "C:" para sistema operacional. •

Será instalado o Windows, com o 'Service Pack' mais recente. • O Windows deverá ser ativado**.**

• Atualizar o Windows (Patch Segurança) antes de colocar a estação de trabalho no domínio.

• Inserir a máquina no domínio (casaeterra.intranet).

• Será instalado o "Microsoft Office". Deve-se observar/anotar a licença que estava configurada no equipamento. A chave de licença fica fixada no equipamento. O Office deverá ser ativado.

• Instalar e configurar pelo menos 1 impressora laser (a que estiver mais próxima do micro); endereçando-a por um endereço de rede (tipo **"**servidor de impressão**"**) ao invés do endereço IP diretamente. Também instalar o software para serviço de cópia e scanner.

Programas

Todos as estações de trabalho, deverão ter os seguintes softwares:

• WinRAR (Versão 24.09 ou superior);

• Adobe Reader (Versão 24 ou superior);

• Antivírus Kaspersky;

• AppController (Acesso Remoto – Versão 6.2 ou superior);

• Firefox (Última versão);

• FortiClient VPN (Versão 7.0 ou superior);

• Google Chrome (Última versão);

• Java (Versão 8.0 ou superior);

• Microsoft Office (Verificar versão anteriormente instalada);

• TeamViewer (Versão 15 ou superior).

O técnico deve verificar se há necessidade de instalação de outros softwares (ZWCAD, Autocad, etc) e a necessidade de licenças. Esse também deve conferir se a estação de trabalho está listada no Software de Inventário.

Usuário

• Será criado, única e exclusivamente, o usuário “Administrador” – criado automaticamente pela instalação.

• Desativar todos os demais usuários como “Convidados” e outros administradores.

• Grupo administradores: apenas “Administrador” e o grupo “Admins do Domínio”.

Nenhum outro usuário local deverá ser criado sem a prévia autorização e nenhum senão o “Administrador” terá direitos de administração local.

O colaborador não deverá ter conhecimento dos usuários administradores e suas senhas.

Configurações Finais e Validação

• Configurar Teclado no Layout ABNT2 (testar pontuação, acentos, etc); •

Testar entradas USB;

• Testar conexão de rede através da LAN e WLAN;

• Testar saída som (Alto Falante e fone);

• Testar Microfone (se possível);

• Testar câmera (se possível);

• Testar touchpad com as barras de deslizamento (quando Notebook); •

Verificar na instalação se não há nenhum conflito de hardware;

• Certificar que todos drives foram instalados;

• Verificar o desempenho da estação de trabalho;

• Limpar a máquina.

Caso seja necessário a aquisição de um software, o usuário deverá entrar em contato com a Diretoria de Tecnologia da Informação (61 3221-5711) para solicitar a homologação do novo software.