Política de Segurança da Informação

1. INTRODUÇÃO

1.1. A **Tecnologia da Informação (TI)**, é o principal meio pelo qual empresas, clientes e fornecedores realizam negócios e trocam informações relevantes, utilizando a tecnologia como grande facilitador de suas operações, sendo de vital importância a definição de normas de segurança que visem disciplinar o uso destes recursos e a salvaguarda dos dados.

1.2. A EMPRESA 3XDATA inspirada pelas normas NBR ISO/IEC 27.000, bem como em práticas, políticas, normas e leis complementares que visam regular ou propor processos e posturas desejáveis sobre o assunto estabelece a sua **Política de Segurança da Informação (PSI)**.

1.3. A presente política deve ser de conhecimento e responsabilidade de todos, sendo avalizada pela alta diretoria da companhia visando adotar medidas técnicas e administrativas aptas a proteger e garantir a segurança dos dados que circulam em meios físicos ou digitais, bem como evitar acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação.

1.4. Aplica-se a esta política as medidas previstas em leis e regulamentos de privacidade que visam evitar o tratamento inadequado ou ilícito de informações pessoais ou sensíveis em sistemas ou arquivos pertencentes a 3XDATA.

2. OBJETIVO DA PSI

2.1. Definir responsabilidades e orientar a conduta de usuários, fornecedores ou pessoas ligadas à companhia, que em algum momento tenham acesso a algum tipo de informação, relevante ou não, pertencente a empresa 3XDATA.

2.2. A presente política visa garantir a segurança dos dados, divulgar claramente o comportamento desejado e a estabelecer mecanismos viáveis para a continuidade dos negócios, por meio da aplicação dos pilares da confidencialidade, da integridade, da disponibilidade, da autenticidade e do não-repúdio das informações.

3. CONCEITOS RELACIONADOS À PSI

3.1. USUÁRIO: refere-se a todos os colaboradores, profissionais autônomos, temporários ou de empresas prestadoras de serviço que obtiverem a aprovação do responsável hierárquico para utilização de recursos tecnológicos ou acesso à dados (digitais ou físicos) pertencentes a empresa 3XDATA.

3.2. DISPONIBILIDADE: refere-se à informação estar disponível quando for necessária para o fim ao qual foi destinada.

3.3. CONFIDENCIALIDADE: refere-se à informação estar disponível e acessível somente a quem for autorizado para tal.

3.4. INTEGRIDADE: refere-se à plenitude da informação, estando de acordo com as características para as quais foi desenvolvida, sem sofrer qualquer dano ou adulteração.

3.5. AUTENTICIDADE: refere-se à identidade do emissor ou receptor da informação, necessitando garantir que ambas as partes sejam quem estiver afirmando ser.

3.6. NÃO-REPÚDIO: refere-se à impossibilidade de negar a responsabilidade por um ato quando há mecanismos suficientes de identificação.

3.7. BYOD: Sigla extraída do inglês *Bring Your Own Device* (traga o seu próprio dispositivo) e refere-se ao uso de equipamentos pessoais nas atividades corporativas.

3.8. DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

3.9. DADO SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

3.10. TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

3.11. TRATAMENTO: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

3.12. ATIVO: equipamento ou componente de tecnologia que é utilizado para a entrega de um serviço pelo Departamento de Tecnologia da Informação.

3.13. ATIVO DE INFORMAÇÃO: qualquer ativo que utilize como forma de entrega de serviço o armazenamento de dados ou informações pertencentes a empresa 3XDATA.

3.14. INCIDENTE DE SEGURANÇA: qualquer incidente que comprometa os pilares da Segurança da Informação (disponibilidade, integridade, confidencialidade, não-repúdio e autenticidade).

3.15. DESASTRE: evento inesperado ou indesejável que afeta negativamente as operações críticas do negócio, ocasionando perdas

financeiras, danos à reputação ou à imagem da empresa, podendo torná-los totalmente inoperantes.

4. PAPÉIS E RESPONSABILIDADES

4.1. CEO, Investidores e membros do Conselho de Administração

- ✓ Incentivar e avalizar a PSI, seguindo-a em suas atividades de modo que possam guiar os demais colaboradores pelo exemplo;
- ✓ Definir políticas de incentivo para que a PSI seja cumprida, dirimindo quanto a casos omissos ou não-conformidades;
- ✓ Tomar conhecimento de Incidentes Graves de Segurança e patrocinar contramedidas necessárias para proteger a informação e os processos de negócio da empresa 3XDATA.

4.2. Equipes de Operação e Equipes de Apoio Administrativo/RH/Marketing

- ✓ Seguir a PSI e realizar suas atividades levando em consideração a previsibilidade das normas de segurança para preservação dos pilares de Segurança da Informação.
- ✓ Sugerir melhorias e auxiliar na correta visualização e equilíbrio da PSI com a produtividade da empresa 3XDATA.
- ✓ Incentivar a adoção da PSI por todos os colaboradores e visitantes.

4.3. Fornecedores e Terceirizados

- ✓ Participar do repasse de conhecimento das normas previstas na PSI tão logo seja possível após o início de suas atividades e quando aplicável.
- ✓ Aplicar a PSI e zelar pela segurança de todas as informações pertencentes a empresa 3XDATA nas quais tomar conhecimento.
- ✓ Destruir e não-reter qualquer informação pertencente a empresa 3XDATA que estiverem em seu poder após o término do vínculo de prestação de serviços, bem como, responsabilizar-se civil e criminalmente pela não aplicação desta regra.

4.4. Analistas, Desenvolvedores de Solução, Equipes de Suporte e Apoio do Departamento de Tecnologia da Informação

- ✓ Propor metodologias, sistemas e processos específicos visando aprimorar a Segurança da Informação.
- ✓ Promover a conscientização dos colaboradores em relação à relevância da PSI, apoiando na avaliação e adequação de controles de Segurança da Informação para projetos e ações em sistemas ou serviços.
- ✓ Alinhar todas as ações promovidas no Departamento de Tecnologia da Informação com as diretrizes corporativas da empresa 3XDATA.

4.5. Comitê de Segurança e Privacidade (CSP)

- ✓ Reunir-se a cada **6 (seis) meses** para debater assuntos relacionados às Políticas criadas para salvaguarda das informações da empresa 3XDATA**.**
- ✓ Criar orientações e políticas de incentivo para que os colaboradores adotem a PSI em suas atividades.
- ✓ Dirimir sobre questões relacionadas à Privacidade de Dados, conforme as leis e regulamentos aplicáveis, bem como aplicar sanções e direcionar planos de ação em casos de não conformidade.

5. APLICAÇÃO LEGAL DA PSI

5.1. A informação produzida ou recebida como resultado de sua atividade profissional pertence a empresa 3XDATA não sendo possível sua cópia ou armazenamento em desacordo com esta PSI.

5.2. Divulgar informações confidenciais ou estratégicas é passível de responsabilização civil ou criminal previsto nas leis de propriedade intelectual, industrial (Lei nº 9279), direitos autorais (Lei nº 9610), Lei Geral de Proteção de Dados (Lei nº 13709), bem como normativas, regulamentos ou outros dispositivos aplicáveis.

5.3. A segurança da informação será eficaz quando aplicada por pessoas comprometidas e em consonância com bons processos gerenciais de controle e sistemas de apoio à proteção de dados.

5.4. Todo usuário está sujeito a responder pelo prejuízo ou dano que vier a provocar a empresa 3XDATA ou à terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

5.5. Não será aceita qualquer justificativa de desconhecimento das normas vigentes.

5.6. Atualizações ou melhorias eventuais realizadas na PSI serão divulgadas pelos canais de comunicação da empresa. Recomenda-se que todo usuário leia e informe-se constantemente sobre a sua aplicação e procure seu gestor imediato em caso de dúvidas.

5.7. A empresa 3XDATA, por meio de seus prepostos autorizados pela alta direção da companhia, reserva-se o direito de tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação de gestores e diretores.

6. COMITÊ DE SEGURANÇA E PRIVACIDADE (CSP)

6.1. Composto por colaboradores da empresa 3XDATA, sem mandato definido e podendo ser alterado conforme a conveniência e a necessidade de aperfeiçoar os controles e as Políticas de Segurança. A participação do CIO é obrigatória, uma vez que diversas ações na presente PSI referem-se a ele.

6.2. Atualmente o CSP conta com os seguintes membros permanentes:

- ✓ Nome do Encarregado de Dados e CIO: Yúri Nicolas Petry (Encarregado de Dados)
- ✓ Nome do Gerente de Operações: Anderson Rodrigues

6.3. O CSP também poderá contar com consultores e membros convidados conforme o debate e a pauta preparada para o dia.

6.4. Um dos membros do Comitê deverá ser nomeado para organizar as pautas e garantir as agendas dos encontros ordinários (trimestrais), bem como, convocar reuniões extraordinárias.

6.5. Nas agendas ordinárias, devem ser debatidos pelo menos:

- ✓ Leitura da ata do encontro anterior
- ✓ Revisão dos Planos de Ação definidos no último comitê
- ✓ A revisão da Matriz de Riscos
- ✓ A verificação das atualizações das Políticas de Segurança
- ✓ Pautas relacionadas à Segurança

6.6. Um encontro extraordinário deverá ser agendado sempre que um Incidente de Segurança considerado GRAVE ocorra, com o intuito de debater os controles implantados e possíveis ações para evitá-los no futuro. Não haverá necessidade de agenda extraordinária caso um encontro ordinário esteja previamente agendado e considere-se estar dentro de um prazo razoável para debater tal assunto.

6.7. Para um encontro do comitê ser considerado válido, todos deverão ser convidados, no entanto, a presença de 2/3 membros será mandatória para que ele tenha poder deliberativo. Do contrário, o encontro será meramente consultivo.

6.8. Todos os encontros deverão ter ata redigida com posterior envio por e-mail. As atas deverão ser salvas em diretório específico e ficar à disposição para consulta de qualquer membro do comitê ou partes interessadas previamente autorizadas, sempre que necessário.

7. UTILIZAÇÃO DE ESTAÇÕES DE TRABALHO

7.1. Toda estação de trabalho é disponibilizada em favor do usuário na atribuição de suas atividades corporativas e dos interesses da empresa 3XDATA. Por isso, este ativo deve ser utilizado exclusivamente para atividades relacionadas às atividades de trabalho. O uso particular de estações de trabalho, sem prévio consentimento de gestores ou diretrizes específicas, constitui uma violação à PSI.

7.2. São vetados acessos a comunicadores instantâneos, Rádios on-line, blog, Flog, TVs on-line, ou qualquer outra comunidade da Internet que tenha relação com comunicadores instantâneos ou qualquer endereço que faça

streaming de áudio/vídeo.

7.3. Os únicos programas de Bate papo autorizados são o Microsoft Teams, Watsapp, Google Meeting, Telegram. Havendo alterações, estas serão amplamente divulgadas pela área responsável bem como será atualizada esta PSI.

7.4. As redes sociais (Facebook , Linkedin, Instagram e ou outras que possam surgir) podem ser liberadas para os colaboradores que sejam pertinentes e de uso exclusivo de trabalho, mediante autorização dos gestores da área, a solicitação de liberação será atendida apenas por chamado do gerente.

7.5. - O acesso ao site de áudio/vídeo youtube.com ou youtube.com.br pode ser liberado para usuários específicos, mediante autorização do Gerente da área e para uso exclusivo de trabalho, caso seu acesso se torne abusivo poderá ser desativado sem prévia autorização;

7.6. É proibida a criação e/ou utilização de domínios de e-mail (Gmail, Hotmail, Yahoo, Outlook, etc.) que contenha ou tenha algum tipo de relação com a empresa 3XDATA;

7.7. O uso de sistemas WEBPROXYES externos, redirecionadores ou qualquer outra tecnologia/processo que contrarie os itens acima não é permitido.

7.8. Não é permitido efetuar cópia/download de materiais gráficos, logomarcas, documentos, músicas e outros que possam caracterizar pirataria e/ou violação de direitos autorais

7.9. Todo o usuário que utilizar estações de trabalho deverá responder pela guarda e proteção deste recurso, garantindo que a operação realizada por meio dele siga práticas recomendáveis de manuseio. Em caso de dúvidas, o SAC do Departamento de Tecnologia da Informação deverá ser acionada imediatamente.

7.10. Cabe aos gestores da empresa 3XDATA, independente do seu departamento, auxiliar cotidianamente seus colaboradores na correta utilização dos recursos disponíveis de hardware e software, bem como, assegurar-lhes treinamento para o uso correto destes recursos, repassar as normas previstas na PSI para novos colaboradores e acionar o SAC do Departamento de Tecnologia da Informação em caso de dúvidas ou dificuldades técnicas.

7.11. O Departamento de Tecnologia da Informação deverá estar empenhado na proteção de todas as estações de trabalho contra códigos maliciosos ou vírus. Auditorias mensais sobre o estado de atualização de softwares antivírus deverão ser realizadas e ações proativas de correção executadas mediante abertura de chamado e comunicação ao usuário responsável. Esta norma se aplicará sempre que houver meios técnicos empregados e capazes de apoiar tal ação, podendo ser regulada por Instrução de Trabalho Específica.

7.12. É proibida a intervenção do usuário na manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, bem como a transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, sem que este procedimento seja acompanhado e validado por um profissional do SAC do Departamento de Tecnologia da Informação.

7.13. Não será permitido ao usuário o download ou instalação de jogos, softwares não-homologados, softwares piratas, *cracks*, *keygens*, filmes, séries, músicas ou qualquer outro conteúdo protegido por direitos autorais. Essa regra aplica-se mesmo que os acessos à internet ou à dispositivos removíveis permitam que a ação seja tecnicamente possível.

7.14. Os softwares liberados ao uso da empresa 3XDATA são somente os descritos abaixo:

- ✓ Sistema operacional que está instalado no computador e registrado;
- ✓ Suíte de escritório Microsoft Office;
- ✓ Adobe Acrobat Reader ou similar Free;
- ✓ Programa compactador de arquivos Free;
- ✓ Microsoft teams ou Google meet;
- ✓ Antivírus definido pela equipe de informática;
- ✓ Sistema Operacional da Empresa - Kaspersky;
- ✓ 3CX Phone;
- ✓ Programas de uso cotidiano para acesso as ferramentas de trabalho;
- ✓ Ferramentas de acesso a equipamentos proprietários;
- ✓ Software de acesso remoto licenciado – Anydesk;

7.15. Caso haja alguma alteração/adição/remoção de software será divulgado em comunicado para a área interessada no referido software, e atualizada nesta PSI para consulta pública;

7.16. A instalação de qualquer outro programa nos computadores da empresa fica obrigatoriamente restrita a prévia análise e homologação da equipe técnica da empresa. Já os computadores particulares e de empresas terceirizadas também estão sujeitos a essas restrições, por estarem dentro da rede corporativa da empresa 3XDATA;

7.17. A instalação de software de propriedade dos usuários, ainda que registrados em seu nome ou de terceiros, não é permitida em computadores da empresa 3XDATA, e o usuário está sujeito às penas e sanções previstas na lei 9.609 de 19/02/98.

7.18. As portas USB das estações de trabalho são bloqueadas por diretivas corporativas. Caso necessário, uma liberação especial (momentânea ou permanente) poderá ser realizada mediante justificativa razoável, que atenda aos interesses da empresa 3XDATA e devidamente

aprovada pelo gestor imediato.

7.19. Caso um ou mais arquivos estejam em um pen drive e havendo a necessidade de utilização destes para atividade de um colaborador ou seja recebido por uma empresa terceira em função de entrega de um trabalho contratado, este pen drive deverá ser encaminhada ao setor tecnologia para disponibilização do arquivo dentro da rede no servidor de arquivos, com a devida verificação de vírus e outras que se fizerem necessárias.

7.20. Cada gestor de departamento deve estar atento aos computadores em desuso que deverão, o mais rápido possível, serem encaminhados ao Departamento de Tecnologia da Informação para a remoção das informações, descarte ou reuso. Não é permitida a retenção de estações de trabalho sob o pretexto de possível utilização futura. Arranjos eventuais sobre o assunto deverão ser acordados mediante abertura de chamado, solicitando e justificando a retenção, podendo o CIO, após avaliar os argumentos, aprovar ou não, tal solicitação.

7.21. A Empresa 3XDATA implementará padrões e meios técnicos nas estações de trabalho visando o cumprimento da **Política de Mesa Limpa, Tela Limpa e Descarte de Informações** prevista nesta PSI.

7.22. Cumpre ressaltar que qualquer autorização especial concedida por meio de avaliação de gestores imediatos poderá ser revogada pelo CIO caso comprove-se que foi dada em desacordo com a PSI, ou ainda, que em determinado momento estejam ocorrendo abusos ou mal uso do direito concedido. Essa normativa aplica-se à toda a PSI.

8. UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS (CELULARES, TABLETS E NOTEBOOKS DA EMPRESA 3XDATA)

8.1. Aplica-se aos dispositivos móveis corporativos todas as regras que foram transcritas no item **Utilização de Estações de Trabalho** e assim como qualquer outro equipamento corporativo, os mesmos devem ser utilizados com zelo e apenas para fins profissionais. No ato da entrega de equipamentos móveis, o usuário assinará e aceitará os termos previstos no **Termo de Entrega de Equipamento**.

8.2. Recomenda-se que os dispositivos móveis sejam transportados de forma segura, a fim de evitar danos, furto, roubo ou extravio. Caso uma dessas situações ocorra, o colaborador deve acionar imediatamente a Central de Serviços do Departamento de Tecnologia da Informação que lhe instruirá como proceder.

8.3. Todo dispositivo móvel fornecido pela empresa 3XDATA, deverá ser protegido por senha e HD Criptografado, seguindo as orientações e boas práticas de uso de senhas previstas no item **Controles de Acesso** desta PSI.

8.4. Notebooks podem ser utilizados em redes externas, entretanto o

colaborador deverá garantir que o antivírus está ativo e atualizado. Ao se conectar a uma nova rede a mesma deve ser definida com o perfil "rede pública", onde as opções de compartilhamento de arquivos e impressoras e descoberta de rede estão desativados. Em caso de dúvidas sobre como realizar esta definição, entre em contato com a Central de Serviços do Departamento de Tecnologia da Informação.

8.5. Os softwares/aplicativos instalados deverão ser de uso profissional e devidamente homologados e autorizados pelo Departamento de Tecnologia da Informação que estarão disponíveis por padrão, conforme a função do colaborador. Caso haja necessidade de utilização de um aplicativo não homologado a solicitação deve ser feita via chamado à Central de Serviços do Departamento de Tecnologia da Informação.

8.6. Os dispositivos móveis não devem conter informações de cunho particular, tais como contatos pessoais, fotos, vídeos, mensagens ou qualquer outro conteúdo que não esteja relacionado com os interesses da empresa 3XDATA.

8.7. Cabe ao usuário, quando encerrar seu vínculo com a empresa, devolver o equipamento e não reter qualquer informação contida nele, bem como não será dado prazo ou permissão, após o comunicado formal do fato, para realização de cópias dos arquivos, independente da origem, autoria, objetivo ou conteúdo.

8.8. Os equipamentos fornecidos devem ser transportados de forma segura a ponto de evitar danos ou roubo, conforme orientações fornecidas pelo gestor imediato no ato da entrega dos aparelhos ou dispositivos.

8.9. A carga da bateria dos aparelhos deve ser utilizada apenas com o carregador fornecido com o aparelho ou homologado pelo fabricante. Não deve ser conectado na USB do computador pessoal ou de terceiros.

8.10. O Bluetooth está liberado, porém deve ser desativado quando não estiver em uso.

8.11. O pacote de dados e franquia de voz, eventualmente fornecidos em nome da empresa 3XDATA, devem ser exclusivamente utilizados para fins profissionais. A utilização deste benefício será auditada e possíveis abusos poderão ser coibidos mediante ressarcimento financeiro da despesa gerada ou procedimentos administrativos previstos por normas do Departamento Pessoal.

8.12. Em caso de furtos ou roubos, o colaborador responsável pelo dispositivo deverá entrar em contato imediatamente com a Central de Serviços do Departamento de Tecnologia da Informação ou com seu gestor imediato. O procedimento passará pela abertura do chamado técnico e a abertura de boletim de ocorrência junto à uma delegacia de polícia ou via internet, sendo o colaborador responsável por aquilo que relatar no documento ou à autoridade policial.

8.13. Em caso de danos em dispositivos móveis corporativos, tão logo o Departamento de Tecnologia da Informação tome conhecimento do fato, será providenciada a limpeza dos dados, bloqueio, reparo e substituição do aparelho, quando necessário.

8.14. Para casos em que for constatado o mau uso do dispositivo como um facilitador de uma perda ou dano, o gestor responsável será comunicado para que possa proceder com as medidas administrativas cabíveis.

9. POLÍTICA DE BYOD

9.1. A utilização da modalidade de BYOD será permitida desde que previamente autorizadas pelo gestor imediato e em conformidade com as normas previstas neste item da PSI.

9.2. Usuários que utilizam equipamentos particulares em benefício das atividades de interesse da empresa 3XDATA devem manter uma postura que não venha causar riscos, inconvenientes ou danos para a empresa tais como acesso à conteúdo ilícito, protegidos por direitos autorais, que causem perturbação ao ambiente de trabalho, dentre outros.

9.3. Não será permitido que seja retido em unidades de armazenamento local de seu dispositivo qualquer informação pertencente A empresa 3XDATA. O uso das informações corporativas será permitido somente com acesso por usuário/senha em dispositivos de armazenamento corporativo previamente indicados pelo Departamento de Tecnologia da Informação.

9.4. Os equipamentos pessoais utilizados deverão ser validados previamente pelo Departamento de Tecnologia da Informação, a fim de garantir que atendam requisitos técnicos necessários ao cumprimento de suas obrigações. No ato da validação, deverá ser concedido acesso completo ao equipamento, sem qualquer restrição, para que sejam instalados os softwares de produtividade, softwares de proteção e realizadas as configurações de política de senhas e diretivas corporativas.

9.5. Ao optar pelo BYOD, o usuário deverá garantir que todos os sistemas previamente instalados em seu dispositivo foram adquiridos legalmente e que não ferem qualquer conduta ou lei de proteção de direitos autorais. O Departamento de Tecnologia da Informação poderá solicitar documentação comprobatória, tais como notas fiscais ou ordens de compra, podendo ser motivo de reprovação do seu uso para fins corporativos.

9.6. A descoberta de armazenamento de dados protegidos por direitos autorais, tais como jogos, fotos, músicas, vídeos que não seja comprovadamente adquirido será motivo de invalidação do equipamento para uso na modalidade BYOD.

9.7. Fica o usuário ciente de que o uso particular de seu equipamento poderá

ser limitado por diretivas corporativas e que, não será possível justificar tal dificuldade, para obter liberações extras ou exceções, ficando livre para cessar a adoção do BYOD e solicitar, o mais breve possível, um equipamento corporativo.

9.8. A Empresa 3XDATA não será responsabilizada por furtos, danos, roubo ou apreensão legal do equipamento, ou ainda, perda, vazamento ou corrompimento de dado pessoal, dado sensível ou qualquer outro que pertença exclusivamente ao usuário e que esteja armazenado em equipamento utilizado na modalidade BYOD, mesmo que tais incidentes ocorram em horário de trabalho ou em atividades corporativas.

9.9. A hipótese acima não se aplica quando comprovadamente ocasionado por um preposto da empresa 3XDATA e em desacordo com qualquer postura ou norma previamente estabelecida nesta PSI, bem como em outras normas, regulamentos, leis civis ou criminais que se aplicarem ao ato. Neste caso, a empresa 3XDATA compromete-se a ressarcir os danos e a instaurar procedimento disciplinar contra o infrator.

9.10. O Departamento de Tecnologia da Informação poderá estabelecer um contrato de BYOD com o usuário detalhando outras normas ou regulamentos técnicos acerca do uso de equipamentos particulares em atividades da empresa 3XDATA.

9.11. Equipamentos ou dispositivos utilizados na modalidade BYOD não receberão qualquer tipo de suporte técnico do Departamento de Tecnologia da Informação em seu hardware (sendo o usuário o único responsável por garantir o bom funcionamento de seu dispositivo), bem como todo o suporte ficará restrito aos aplicativos e sistemas utilizados para desenvolvimento das atividades corporativas. Os aplicativos de mensageria configurados com contas particulares, tais como WhatsApp, Telegram, Facebook Messenger, dentre outros, não receberão qualquer suporte, independendo do uso em atividades corporativas ou não.

10. POSTURAS DOS COLABORADORES NO APOIO A SEGURANÇA DA INFORMAÇÃO

10.1. Independentemente da localização do escritório de trabalho da empresa 3XDATA onde o colaborador atue ou quando o colaborador estiver em *roaming*, a PSI se aplicará. Portanto, cabe a todos reforçarem a adoção desta política em todas as suas atividades, bem como em suas equipes de trabalho.

10.2. Ressalta-se que informação não é somente o que circula em papéis ou sistemas, mas também o que é falado ou discutido. Recomenda-se que diálogos ou conversas telefônicas que tratem de assuntos sensíveis, tais como discussões sobre a estrutura do produto, decisões/definições da empresa, matérias de cunho jornalístico, emissão de opiniões sobre as funcionalidades dos produtos da empresa 3XDATA**,** ou ainda, que

possuam conteúdo prolongado e possam criar distúrbios desnecessários no ambiente de trabalho, sejam realizadas em ambientes reservados.

10.3. A ninguém será permitido tirar fotos de qualquer informação referente aos produtos da empresa 3XDATA ou manter em dispositivos pessoais qualquer informação a ele pertencente, mesmo que sob pretexto de aplicação do BYOD.

10.4. Todos são responsáveis pelas informações que manipulam ou às quais possuem acesso. Vazamentos, utilização indevida, repasse não-autorizado, obtenção de vantagem, independente do meio de comunicação utilizado, será considerada falta grave. A conduta de todos os colaboradores deve ser no sentido de preservar e manter sigilo de tais dados.

10.5. Qualquer tipo de transgressão à PSI será reportado ao gestor imediato que não poderá se eximir ou negligenciar ações disciplinares a tal conduta, devendo acionar o Departamento Pessoal da empresa 3XDATA, quando cabível. O DPO poderá ser acionado e deliberar com seu superior, sobre fatos ou condutas que sejam consideradas graves sempre que necessário.

11. CONTROLES DE ACESSO

11.1. Todos os sistemas pertencentes a empresa 3XDATA devem ser acessados por meio de senhas. Quando o acesso for por credencial nominal (será chamada na PSI de "senha individual"), a senha deverá ser pessoal e intransferível, sendo o seu dono o responsável por tudo que ocorrer no ambiente com o uso de suas credenciais, conforme o Código Penal Brasileiro, artigo 307, falsa identidade.

11.2. Para sistemas onde exista restrição de quantidade de usuários (tal como um custo fixo por usuário cadastrado) ou sua natureza não permita a utilização de senha individual (tal como uma senha de conexão ao banco de dados da aplicação), a mesma deverá ser compartilhada somente entre os membros da equipe de desenvolvimento que manipula o produto (será chamada na PSI de "senha compartilhada").

11.3. Todas as senhas, independente da sua natureza, devem respeitar requisitos mínimos de segurança que seguem:

- ✓ Mínimo de 8 caracteres;
- ✓ Deve conter pelo menos um caractere alfanumérico (!@#$%^&*.,/\);
- ✓ Deve conter pelo menos um algarismo (0,1,2,3,4,5,6,7,8,9);
- ✓ Deve conter letras MAIÚSCULAS e minúsculas;
- ✓ Não deve utilizar o nome do próprio usuário, ser um número de documento, data de nascimento ou conter palavras contidas do vocabulário cotidiano;

- ✓ Para senhas compartilhadas, recomenda-se uma aleatoriedade e quantidade maior nos caracteres. Podem ser utilizados geradores de senha para estes casos;
- ✓ Recomenda-se a troca de todas as senhas individuais a cada 90 dias, ou de acordo com os parâmetros de expiração do sistema e ou aplicativo utilizado, não havendo repetição de expressões em comparação com a senha anterior;
- ✓ Recomenda-se a troca de todas as senhas compartilhadas a cada 180 dias ou após o desligamento de algum colaborador que eventualmente teve acesso a essa credencial (o que vier primeiro). Assim como em senhas individuais, não deve haver repetição de expressões em comparação com a senha anterior;
- ✓ Não manter nenhum tipo de registro físico ou eletrônico de suas senhas, exceto quando o armazenamento for feito de forma segura;

11.4. Caso exista a necessidade de terceiros, tais como fornecedores ou prestadores de serviço, acessarem os sistemas e ambiente de tecnologia da empresa 3XDATA, fica definido que:

- ✓ As credenciais de acesso de cada um deverão conter somente as permissões necessárias para a realização do trabalho ao qual foram contratados;
- ✓ Qualquer fornecedor que realizar intervenções diretas ou acessar informações sigilosas da empresa 3XDATA, deverá estar acompanhado de um colaborador-monitor que irá monitorar o acesso, a não ser que exista uma permissão especial;
- ✓ As permissões especiais para acessos não-monitorados deverão ser concedidas pelo CIO da empresa 3XDATA ou por quem ele designar, e deverão ser expressas por meio de documento, seja ele, e-mail, contrato ou termo assinado;
- ✓ Caso um fornecedor realize ações com uma senha individual de um colaborador da empresa 3XDATA, este último se responsabilizará por todas as alterações de ambiente realizadas em seu nome;

11.5. Qualquer fornecedor da empresa 3XDATA será corresponsável, em conjunto com o colaborador-monitor, por incidentes ou prejuízos que causar no ambiente de produção ou desenvolvimento de produto, por não respeitar uma orientação expressa, ou também por imperícia ou negligência. Fica excluído deste item qualquer intervenção que ocorra em decorrência de uma ação com riscos reconhecidos e aceitos por ambas as partes.

11.6. A empresa 3XDATA disponibiliza equipamentos para seus colaboradores, não sendo possível a utilização de equipamentos particulares. Caso haja alguma alteração neste procedimento este está coberto nesta PSI no item 9.

11.7. Sempre que possível, os sistemas da empresa 3XDATA deverão conter registros de logs de acesso para monitoramento e avaliação de intervenções por parte dos interessados.

11.8. Caso um colaborador, fornecedor ou visitante da empresa 3XDATA receba um login de acesso, o mesmo deverá ser desativado após **60 dias sem utilização**. A mesma regra aplica-se a senhas compartilhadas. Auditorias periódicas serão conduzidas pela Central de Serviços do Departamento de Tecnologia da Informação para garantir essa prática.

11.9. É de responsabilidade de cada colaborador garantir que suas senhas individuais estejam ativas e presentes na proteção de serviços de e-mail ou no Sistema Operacional, sob a orientação da Central de Serviços do Departamento de Tecnologia da Informação, podendo acioná-lo sempre que necessário para garantir tal prática.

11.10. As senhas individuais serão fornecidas ao colaborador no ato de sua contratação e bloqueadas no processo de desligamento. Caberá ao Departamento Pessoal garantir tais solicitações, bem como, avaliar com a Central de Serviços do Departamento de Tecnologia da Informação, possíveis necessidades de alteração de acessos quando houver mudanças internas de função. Todas as criações, alterações ou revogações de acesso deverão ser registradas por meio de chamado.

11.11. Ao receber uma solicitação de novo acesso ou alteração de permissões, a Central de Serviços do Departamento de Tecnologia da Informação deverá criar as credenciais podendo usar como base alguns modelos de identidade lógica ou copiar permissões de outro colaborador com funções idênticas. O Departamento Pessoal deverá esclarecer com a maior riqueza de detalhes possível os acessos necessários e apontar perfis semelhantes que possam agilizar esse processo.

11.12. Recomenda-se que as senhas não sejam anotadas em arquivos eletrônicos ou papéis. Caberá a cada usuário a memorização de sua própria senha, podendo acionar a Central de Serviços do Departamento de Tecnologia da Informação caso esqueça-a e necessite redefini-la.

11.13. Os usuários devem proceder com a troca de senha, caso suspeitem

de fraude ou quebra de confidencialidade por terceiros. A tentativa de burlar senhas de acesso por meio de tentativa e erro repetidas vezes (o que é nominado "ataque por força bruta") ou ainda, apropriar-se indevidamente de credenciais de acesso, chaves de criptografia ou identificação biométrica será alvo de ação disciplinar.

11.14. Os acessos externos à rede de informações da empresa 3XDATA fora do expediente de trabalho são liberados por meio de medidas técnicas viáveis, atendendo a Lei 12.551 (Tele Trabalho) que altera o Art. 6° da CLT, exceto para cargos de confiança. Qualquer trabalho externo deverá ser autorizado pelo supervisor direto.

12.SEGURANÇA NO ACESSO ÀS INSTALAÇÕES

12.1. Os acessos ao ambiente de trabalho da empresa 3XDATA devem ser feitos somente por pessoas autorizadas e devidamente acompanhadas por algum colaborador. As instalações de uso comum e os Datacenters Corporativos possuem segurança por câmeras e as suas gravações podem ser utilizadas para auditoria ou investigação.

12.2. Para acesso recorrente às dependências da empresa 3XDATA por terceiros, poderá ser concedida uma autorização especial por um gestor. A autorização deverá ser solicitada por meio de abertura de chamado e ser direcionada à ciência do CIO. Caberá exclusivamente a quem solicitou tal privilégio a responsabilidade por todas as ações realizadas em decorrência dessa permissão.

12.3. Para os casos em que não houver concessão de autorização especial, um colaborador-monitor deverá acompanhar a visita e será responsável por:

- ✓ Garantir a boa conduta do visitante, inclusive advertindo-o, se necessário, caso alguma prática não-recomendada ocorra durante a visita;
- ✓ Evitar que o visitante tenha acesso visual às telas dos desenvolvedores de solução, da equipe técnica, bem como tome em seu poder, sem autorização, algum documento que pertença a Empresa 3XDATA;
- ✓ Informar quanto às restrições para fotografias, caso necessário;
- ✓ Acompanhar o visitante desde a entrada nas dependências do escritório da empresa 3XDATA e acompanhá-lo até a saída quando a visita for concluída;

12.4. Cabe ao CIO ou a quem ele nomear, instruir a recepção dos prédios ao qual estejam situados os escritórios administrativos quanto à alguma restrição de visitas ou informar quanto a autorizações especiais para visitantes, fornecedores ou prestadores de serviço poderem acessar as

instalações da empresa 3XDATA sem a necessidade de acompanhante.

12.5. O acesso físico ao Datacenter de Servidores Legado deverá ser realizado por meio de biometria registrada e restrita à colaboradores designados para manutenção das operações neste ambiente. Não será concedida, sob nenhuma hipótese, acesso sem monitoramento a quem não possuir credencial biométrica, mesmo que sejam colaboradores, gestores ou diretores da empresa 3XDATA. Qualquer ação realizada fisicamente neste ambiente deverá ser conduzida por, pelo menos, dois colaboradores autorizados.

12.6. Não será tolerada a remoção de qualquer equipamento, componente ou ativo de um dos Datacenters de Servidores Legado sem que haja registro em chamado e justificativa razoável. O DPO deverá avaliar tais ocasiões e emitir pareceres em casos de não conformidade.

12.7. Em caso de necessidade justificada de remoção de ativo, caberá a quem o autorizar, garantir que não há dados sigilosos, pessoais ou sensíveis que possam ser copiados do equipamento, e em caso de impossibilidade de apagá-los ou destruí-los previamente, um termo de confidencialidade deverá ser lavrado, apontando responsabilidades civis em caso de vazamento não autorizado de tais informações. O documento lavrado deverá ser anexado ao chamado que foi registrado para essa ação.

13. SEGURANÇA E GESTÃO DE CAPACIDADE DOS ATIVOS E DOS DATACENTERS CORPORATIVOS

13.1. O Departamento de Tecnologia da Informação tem como dever a aplicação de políticas, técnicas e tecnologias capazes de proteger todos os ativos de informação da empresa contra códigos maliciosos e/ou vírus. Para tanto, possui autonomia para instalar sistemas de proteção, preventivos e detectáveis, visando a garantia da segurança das informações e dos perímetros de acesso.

13.2. Todo colaborador da empresa 3XDATA deve estar ciente que ao manipular ativos ou utilizá-los direta ou indiretamente para suas atividades, o uso será auditado pelo Departamento de Tecnologia da Informação, por meio de (mas não restritos à) sistemas de monitoramento nas estações de trabalho, servidores, conexões com a internet, sites visitados, e-mails recebidos/enviados, upload/download de arquivos, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

O Departamento de Tecnologia da Informação deverá monitorar o ambiente de TI, a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos da empresa

3XDATA, bem como reportar e seguir as diretrizes previstas na PSI para incidentes de segurança ou tomar as medidas proativas cabíveis para evitar efeitos negativos sobre o ambiente de produção.

14. SEGURANÇA NAS COMUNICAÇÕES

14.1. Fica proibido o compartilhamento (independendo do meio de comunicação) de qualquer informação referente ao desenvolvimento ou plataforma dos produtos da Empresa 3XDATA para pessoas externas à organização, a não ser que o destinatário possua permissão especial (comprovável documentalmente) pelo responsável hierárquico.

14.2. A Internet Corporativa deve ser utilizada para viabilizar a busca de informações e agilizar processos de negócio em favor da empresa 3XDATA, não sendo permitido o uso alheio a este fim durante o horário de trabalho. A liberação técnica do recurso para fins pessoais não justificará tal prática e o uso indevido do acesso à Internet é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado legalmente por eventuais danos causados.

14.3. Auditorias dos acessos à Internet serão conduzidas sem aviso prévio e de forma transparente aos usuários pelo Departamento de Tecnologia da Informação e poderão ser solicitadas pelos responsáveis hierárquicos, pelo CIO Corporativo, pela própria Gestão de Tecnologia ou pelo DPO. Os relatórios produzidos levarão ao conhecimento dos interessados informações, tais como, nomes dos usuários, páginas consultadas, tempo de consulta, e o conteúdo navegado.

14.4. O uso de ferramentas de mensageria, tais como Microsoft Teams, Whatsapp e Telegram, é amplamente permitido, estando regulamentado com as mesmas práticas de conduta e auditoria previstos para outras ferramentas de comunicação, se utilizados em equipamentos corporativos.

14.5. Não é permitido o envio de mensagens de cunho político-partidário, religioso, discriminatório, ofensivo, contrários às leis e regulamentos vigentes, que infrinjam direitos de propriedade ou que contraponha as regras de conduta ou os valores da Empresa 3XDATA, por meio das ferramentas de comunicação corporativas. Não é permitido o uso destas ferramentas para fins particulares, sendo de pleno direito a auditoria de seu uso, conforme viabilidade técnica e sem prévio aviso.

14.6. Não é permitido o envio de mensagens onde não seja explícita a identidade do remetente.

14.7. Quaisquer comunicados em massa, propagandas, informativos, imagens, dentre outros, deverão ser previamente aprovados pelo CIO ou por quem ele nomear, a fim de não serem tratados como Spam ou comprometerem o funcionamento dos sistemas de e-mail.

14.8. Mensagens recebidas de origem desconhecida deverão ser eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos, bem como, evitar clique em links apontando para sites externos, mesmo que a mensagem pareça verdadeira. Em caso de dúvidas, solicite uma avaliação prévia da Central de Serviços do Departamento de Tecnologia da Informação.

14.9. Qualquer colaborador da empresa 3XDATA deve estar ciente de que é unicamente o responsável pelas informações que são enviadas por meio de sua conta de e-mail ou qualquer outra ferramenta cedida em seu nome para uso destinado ao trabalho.

14.10. A empresa 3XDATA buscará por meios técnicos viáveis garantir a salvaguarda dos e-mails e seu conteúdo anexo, no entanto, não será responsável por eventuais perdas ou danos acarretados pelo uso de tal ferramenta como principal fonte de armazenamento de informação. Para casos em que reter o dado será crítico para o desenvolvimento de uma determinada atividade, os mesmos deverão ser copiados para drives específicos, seguindo as orientações desta PSI no item **Política de Armazenamento de Dados**, ficando a responsabilidade de tal prática exclusiva do usuário.

14.11. O uso de software de e-mail, mensagens instantâneas e correio interno não homologados pelo Departamento de Tecnologia da Informação são passíveis de sanções em caso de dano real causado por tal prática.

A empresa 3XDATA provê acesso ao Correio Eletrônico para usuários autorizados com a finalidade de agilizar os contatos de negócio, o seu uso é um privilégio que pode ser retirado a qualquer momento, caso sua utilização se torne abusiva.

14.12. O uso do Correio Eletrônico deve ser feito somente através dos softwares homologados no item 7.16 desta PSI e do Webmail da empresa 3XDATA;

14.13. A empresa 3XDATA se reserva ao direito de acesso, auditoria, revisão, eliminação, revelação ou uso de todas as mensagens e outras informações armazenadas ou transferidas no sistema de Correio Eletrônico a qualquer momento e sem notificação prévia.

14.14. O uso indevido do e-mail é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado pelos danos causados.

14.15. A simples resposta a um e-mail fora do horário de expediente não configurará hora extra. Para que isto ocorra é necessário que a empresa 3XDATA tenha exigido na demanda enviada por e-mail, a realização de uma tarefa fora do horário de trabalho.

14.16. O colaborador ou terceiro é inteiramente responsável por sua defesa quando realizar comunicações que venham a causar prejuízos a outrem em assuntos que não tenham qualquer relação com o trabalho ao

qual foi contratado para realizar, independente da utilização de ferramentas pessoais ou corporativas para tal, acometidos em horário de expediente ou não. O critério também se aplica para infrações de conduta moral, ou transgressões previstas na legislação vigente.

15. POLÍTICA DE MESA LIMPA, TELA LIMPA E DESCARTE DE INFORMAÇÕES

15.1. O Departamento de Tecnologia da Informação é responsável por gerenciar o descarte de informações a pedido dos custodiantes que estejam armazenados em dispositivos eletrônicos e poderá emitir informações, recomendações ou emitir regulamentos quanto ao bom uso de informações em papel.

15.2. Cada usuário deve cuidar para que papéis, mídias e imagens nos monitores não fiquem expostas ao acesso não autorizado, bem como fica responsável por possíveis bilhetes colados sobre o monitor, teclado ou gabinete, devendo garantir que tais papéis não contenham senhas, informações sigilosas, dados pessoais ou dados pessoais sensíveis.

15.3. Mídias contendo informações referentes a empresa 3XDATA deverão ser destruídas antes de seu descarte. CD's, DVD's e documentos em papel deverão passar pelo triturador antes de serem encaminhadas ao lixo. HD's deverão ser encaminhados ao Departamento de Tecnologia da Informação para a destruição da informação antes do descarte ou reutilização.

15.4. Todos devem evitar manter sobre a mesa de trabalho, qualquer papel que contenha detalhes sobre o código fonte do produto, estrutura dos dados ou comunicados contendo informações que possam remeter ao conhecimento total ou parcial do Planejamento Estratégico da empresa 3XDATA;

15.5. Ao utilizar as impressoras, preferir aquela que estiver mais próxima de sua mesa e evitar o acúmulo de papéis na bandeja de impressão. Ao enviar um comando para imprimir, retire imediatamente o documento. Qualquer colaborador que perceber a impressora em uso por outra pessoa, não deve se apropriar do documento, copiar ou ler seu conteúdo, sob nenhuma hipótese.

15.6. Folhas impressas com informação considerada confidencial ou estratégica para a empresa 3XDATA ou contendo **dados pessoais** ou **dados pessoais sensíveis** de pessoas não deverão sob nenhuma hipótese serem reaproveitadas como rascunho.

15.7. O simples apoio no transporte de papéis ou dispositivos entre unidades ou departamentos pertencentes a empresa 3XDATA**,** não dá o direito ao colaborador que estiver transportando, tomar conhecimento ou acessar os dados contidos em tais conteúdos. Qualquer transgressão neste sentido será alvo de ação disciplinar.

15.8. Ao sair de sua estação de trabalho todo colaborador deverá, obrigatoriamente, bloquear sua estação de trabalho pelos comandos **Windows+L** ou **CTRL+ALT+DEL > Bloquear a Tela (quando utilizar Windows)** ou comando similar em outro sistema operacional em uso, sendo responsável por garantir que o desbloqueio ocorra mediante o uso de login e senha**.** Adicionalmente, ao terminar o expediente ou realizar intervalo para o almoço, o monitor deverá ser desligado.

16. POLÍTICA DE ARMAZENAMENTO DE DADOS

16.1. Este capítulo da PSI aplica-se a todas as informações geradas pela empresa 3XDATA, independente do formato. Para tanto, ressalta-se que toda a informação contida em servidores de rede, estações de trabalho, unidades de armazenamento lógico, armários físicos e locais de destinação de arquivo morto que pertencem a empresa A52 e está destinado somente à dados de seu interesse.

16.2. É proibido a qualquer usuário, utilizar-se dos espaços disponíveis para armazenamento de dados ou documentos físicos para seu benefício pessoal e em caso de desligamento ou encerramento de contrato de trabalho, não será dada a oportunidade de reaver tais itens. A empresa irá disponibilizar gavetas ou armários próprios para armazenar itens pessoais que não estejam em desacordo com qualquer outra norma de conduta vigente.

16.3. Ao substituir um computador e remanejá-lo a outro colaborador, o Departamento de Tecnologia da Informação procederá com a remoção das informações existentes no equipamento e garantirá que o novo usuário não tenha acesso aos documentos pertinentes ao usuário anterior.

16.4. A criação de pastas departamentais nos servidores de rede refletirá a estrutura organizacional da empresa 3XDATA**.** Qualquer novo diretório a ser criado, precisará de solicitação via chamado técnico pelo responsável hierárquico e constar as permissões de acesso. Essa solicitação será avaliada pela Central de Serviços do Departamento de Tecnologia da Informação que informará o Departamento Pessoal sobre as novas permissões concedidas, bem como poderá rejeitá-la, caso perceba que a solicitação é abusiva ou já é contemplada por outro diretório existente. Salienta-se a proibição de criação de pastas pessoais nos servidores de rede.

16.5. Qualquer nova permissão concedida em diretórios de rede deverá ser prontamente informada ao Departamento Pessoal para que possam efetuar o devido controle.

16.6. Qualquer usuário que perceba em sua estação de trabalho ou em diretórios de rede em que possua acesso, a existência de arquivos que não são de interesse da empresa 3XDATA**,** deverá comunicar

imediatamente o Departamento de TI, que auditará por meios técnicos viáveis a existência de arquivos que não condizem com os interesses da empresa e procederá com a exclusão sem aviso prévio aos donos.

16.7. Armazenamento de fotografias ou vídeos será permitida somente sob orientação e autorização do DPO, uma vez que pode gerar riscos significativos às leis de privacidade e direitos autorais vigentes no Brasil.

16.8. Todo colaborador deverá garantir que seus documentos de trabalho estão salvos em drives corporativos de rede específicos para este fim. Dados não devem ser armazenados na **Área de Trabalho** ou em pastas de armazenamento local (Exemplos de diretórios: **Documentos, Downloads, C:,** dentre outros).

16.9. Em caso de falhas eventuais em estações de trabalho ou dispositivos móveis, não será realizado *backup* de documentos salvos em discos locais ou em desacordo com o item anterior. Essa regra se aplicará, independente do teor do conteúdo dos documentos ou de sua relevância.

17. CONSIDERAÇÕES DA PSI NA AQUISIÇÃO DE NOVOS EQUIPAMENTOS E SOFTWARES

17.1. Todo novo hardware ou software deverá ser adquirido mediante abertura de chamado e aprovação do CIO, que poderá dispor sobre regras ou políticas específicas para garantia de melhores condições de oferta no ato de aquisição de novos ativos.

17.2. A instalação de novos equipamentos ou softwares adquiridos deverá ser igualmente registrado podendo ser documentado no mesmo chamado de solicitação de aquisição.

17.3. Os softwares homologados e instalados nos computadores e servidores de rede são de propriedade exclusiva da empresa 3XDATA, sendo proibidas as cópias integrais, ou mesmo as parciais, bem como a instalação de softwares piratas.

17.4. Pirataria é considerada crime e softwares piratas causam prejuízos tanto materiais como funcionais, além de denegrir a imagem da Instituição, constituindo crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98. Quem infringir tal lei estará sujeito às sanções disciplinares previstas nos códigos de conduta da empresa 3XDATA, bem como às penas de detenção e multa previstas na referida lei.

17.5. A empresa 3XDATA mantém contratos especiais com alguns fabricantes de software do mercado e poderá estender a utilização de alguns destes softwares nos computadores enquadrados nas regras de BYOD previstas nesta PSI, desde que estejam plenamente autorizados pelo gestor imediato e pela Gestão de Tecnologia.

17.6. Todo fornecedor de hardware ou software da empresa 3XDATA

deverá estar ciente das condutas éticas fomentadas pela empresa. Por isso, quando houver fornecimento de produto ou serviço mediante contrato, ele deverá constar cláusulas padrão anticorrupção, cláusula de confidencialidade e cláusulas de direito de privacidade (em cumprimento à Lei Geral de Proteção de Dados). Quando houver dispensa de contrato por motivo razoável, tais condutas devem ser repassadas por e-mail ou qualquer outro meio escrito que demonstre de maneira inequívoca a ciência do prestador quanto a essas posturas.

17.7. Caberá ao DPO dirimir sobre cláusulas padrão e criar meios para orientar os colaboradores quanto à prática prevista acima.

17.8. Antes de adquirir ou contratar qualquer sistema ou serviço, deverá o responsável pela aquisição, garantir que o fornecedor e seu produto estão aderentes à PSI e demais normas vigentes na empresa 3XDATA**.**

17.9. Para aquisição de produtos que trarão novidade em termos de funcionalidade ou que manipulem dados em serviços críticos, recomenda-se que um teste ou avaliação seja realizada previamente, levando em consideração a forma como o produto/serviço adquirido trata a Segurança da Informação. Seus resultados deverão ser apreciados e aprovados pelo DPO.

17.10. Não será recomendada a aquisição de qualquer produto/serviço que esteja em desacordo com a PSI. No entanto, o DPO poderá autorizar o risco inerente à esta aquisição, avaliando impactos positivos ou negativos sobre o negócio. Neste caso, será necessária uma reavaliação sobre os controles implantados neste documento para comportar o novo cenário que levou a considerar tal decisão.

17.11. Qualquer aquisição de produto/serviço que manipulará ou armazenará informação pessoal ou informação sensível aos clientes da empresa 3XDATA (tais como dados sobre a intimidade, vida privada, honra e imagem) deverá conter documentação expressando claramente os processos de tratamento para estar em conformidade com **Lei Geral de Proteção de Dados (Lei 13.709/18)**;

18. CONSIDERAÇÕES DE SEGURANÇA NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

18.1. O desenvolvimento das soluções da empresa 3XDATA deverá ser realizado, respeitando boas práticas de mercado quanto à não-existência de vulnerabilidades ou brechas de segurança no código fonte que poderiam ser exploradas maliciosamente.

18.2. Um produto da empresa 3XDATA poderá ser lançado para produção e comercialização somente quando passar por testes de segurança e privacidade. Estes testes deverão ser considerados como parte integrante e importante do processo de fabricação da solução.

18.3. Os testes de segurança e privacidade deverão garantir o cumprimento da legislação e a privacidade dos dados dos usuários, possuindo rastreabilidade para consultas futuras e avaliação da eficácia a quem interessar.

18.4. A manutenção de sistemas da empresa 3XDATA deve garantir o menor impacto e indisponibilidade possível sobre as operações dos usuários, evitando vulnerabilidades ou fragilidades no ambiente de produção.

19. GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

19.1. Um Incidente de Segurança pode ser informado por qualquer meio válido e por qualquer usuário ou indivíduo que possua alguma relação com a empresa 3XDATA. Ao tomar conhecimento do fato, a Central de Serviços do Departamento de Tecnologia da Informação deverá analisar sua gravidade.

19.2. Caso o Incidente de Segurança seja classificado como severidade **Baixa**, o CIO deverá ser informado do fato e ser copiado na solução. Se o tema for recorrente ou representar algum risco em potencial, o tema deve ser levado à próxima reunião ordinária do DPO.

19.3. Caso o Incidente de Segurança afete algum serviço crítico, ele será classificado como **Alto** ou **Urgente**, de acordo com a previsibilidade do acordo supracitado. Neste caso, o CIO ou pessoa autorizada por ele, deverá organizar uma força-tarefa a fim de mitigar os efeitos, analisar causas e documentar as ações. Neste caso, após a reestabelecer os serviços em sua totalidade, uma reunião extraordinária pelo DPO deve ser convocada para analisar as ações tomadas ou dirimir sobre o ocorrido.

19.4. É possível que o Incidente de Segurança não afete diretamente um serviço em produção. Isso ocorrerá tipicamente em tentativas malsucedidas de invasão ou vazamentos não autorizados. Nestes casos, o DPO deverá ser convocado para discutir o fato e tomar as contramedidas necessárias. Caso, o incidente afete a privacidade de indivíduos, também será necessário aplicar o procedimento previsto na **Política de Privacidade** da empresa 3XDATA no que tange a comunicação à Agência Nacional de Proteção de Dados (ANPD), bem como a abertura de Boletim de Ocorrência, quando aplicável.

19.5. Ao constatar-se (a qualquer momento) que houve ação deliberada de pessoas envolvidas diretamente com os negócios da empresa 3XDATA (colaborador, fornecedor, visitante, investidor e etc), o caso deve ser informado imediatamente ao Departamento Pessoal e ao gestor hierárquico imediato para que, cientes do fato, tomem as medidas administrativas cabíveis.

19.6. Todo Incidente de Segurança considerado **Alto** ou **Urgente** deverá, obrigatoriamente, gerar uma lição aprendida e uma revisão nos

mecanismos de segurança, incluindo a PSI, por parte do DPO;

20. ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NO GERENCIAMENTO DE CONTINUIDADE DE NEGÓCIO

20.1. A Continuidade do Negócio trata de todos os mecanismos que servem para perpetuidade do negócio. A PSI, o **Plano de Continuidade de Serviços**, bem como, seus mecanismos de retenção e proteção da informação, apoiam a Continuidade do Negócio, que somados, ajudam a garantir a proteção de um dos ativos mais importantes da a empresa 3XDATA, que é a informação.

20.2. A Empresa 3XDATA mantem uma **Política de Backup** para administrar, proteger e testar as cópias de segurança dos programas e dados do negócio, de modo a garantir a Continuidade dos Serviços de Tecnologia com a menor perda de informação possível em cenários considerados como "desastre".

20.3. Todo desastre, será considerado um "Incidente de Segurança" e será tratado como tal.

20.4. Os mecanismos previstos na PSI deverão apoiar e ser apoiados pela **Matriz de Riscos** que deverá ser revisada tantas vezes forem necessárias e mandatoriamente pelo DPO.

20.5. O **Plano de Continuidade de Serviços** deve levar em consideração a **Matriz de Riscos** e prever os testes para garantia e eficácia dos controles utilizados. Cabe ao DPO garantir a informação ao corpo diretivo da empresa com relação aos riscos residuais ou solicitar a aprovação de riscos potenciais.

20.6. O Departamento de Tecnologia da Informação terá o compromisso de criar e manter cópias de segurança (*backups*) apenas dos dados armazenados nos serviços disponibilizados em rede, excluindo dados em discos ou dispositivos locais, levando em consideração os recursos disponíveis para tal. Sempre que necessário, será sua obrigação, por meio do CIO solicitar novas aquisições, seguindo a política de compras da empresa. A decisão positiva ou negativa deverá servir de subsídio para atualização da **Matriz de Riscos.**

21. CONSIDERAÇÕES DA PSI QUANTO À PRIVACIDADE DE DADOS

21.1. Todo o colaborador da empresa 3XDATA deve estar ciente que em suas atribuições poderá manipular uma série de dados pessoais ou dados pessoais sensíveis para cumprimento de atividades e processos corporativos. Neste caso, o colaborador terá uma série de obrigações e normas a seguir, estando de pleno acordo com a **Política de Privacidade**.

21.2. A **Política de Privacidade** da empresa 3XDATA constitui o

documento máximo de regulação da aplicação das leis de privacidade na companhia, em especial a Lei Geral de Proteção de Dados e estabelece normas no uso de dados pessoais.

21.3. O DPO deverá aprovar qualquer novo processo, projeto ou atualização que utilize o tratamento de dados pessoais. A **Política de Privacidade** detalha os aspectos considerados pelo DPO e quais documentos serão produzidos.

21.4. A não conformidade com a **Política de Privacidade** constitui falta grave, uma vez que fere os códigos de conduta da companhia e representam riscos consideráveis à imagem da empresa e aos seus clientes.

22. AUDITORIAS DE CONFORMIDADE

22.1. As Auditorias de Conformidade constituem uma ação proativa a fim de evitar posturas indesejadas e não conformidades com relação à PSI. Um programa de auditorias pode ser estabelecido pelo DPO e cumprido durante determinado período e de acordo com a conveniência. O Departamento de Tecnologia da Informação também poderá realizar auditorias sempre que julgar necessário.

22.2. O Departamento de Tecnologia da Informação, por meio do CIO, deve restringir a quantidade de pessoas com permissão de acesso aos logs de auditoria de sistema, bem como, garantir meios para verificar se existem adulterações nos arquivos. Para tanto, os logs de auditoria de sistema devem ser gerados e mantidos com nível de detalhe suficiente para rastrear exclusão não-autorizada, falhas ou fraudes.

22.3. As auditorias serão realizadas de acordo com programação estabelecida pelo DPO e relatórios serão gerados periodicamente, sendo apreciados pelo próprio comitê e pelo CIO da Empresa 3XDATA.

22.4. O CIO da empresa 3XDATA poderá solicitar relatórios de auditoria contendo o nome, mensagens trafegadas, acessos a Internet e demais informações do usuário conforme resolução do TST (Tribunal Superior do Trabalho).

23. RESPONSÁVEIS PELA POLÍTICA

- ✓ **Dono do documento:** Yúri Nicolas Petry.
- ✓ **Apoiadores:** Membros do Comitê de Segurança e Privacidade.
- ✓ **Partes Interessadas:** CIO
- ✓ **Aplicabilidade:** Toda a Companhia.

24. DOCUMENTOS COMPLEMENTARES

- ✓ Matriz de Riscos
- ✓ Política de Backup
- ✓ Política de Privacidade
- ✓ Plano de Continuidade de Serviços
- ✓ Termo de Entrega de Equipamento

25. HISTÓRICO DE REVISÃO

Revisão	Histórico	Data
00	Rascunho	05/11/2020
01	Revisão 1 – Jeronymo Luiz	14/03/2022
02	Revisão 2 – Jeronymo Luiz	17/3/2022
03	Lida em conjunto até o item 14 – Yúri Petry	17/03/2022
04	Encaminhada para revisão – Yúri Petry	24/03/2022
05	Revisão final – Yúri Petry	11/05/2022