JORDÃO
SOLUÇÕES EM ENERGIA

7

# Política de Segurança da Informação

Versão 01
10 de março de 2023

# Política de Segurança da Informação

A Política de Segurança da Informação (“PSI”), é o documento que orienta e estabelece diretrizes corporativas da JORDÃO CONSULTORIA E PROJETOS LTDA inscrita no CNPJ/MF sob o n° 02.445.475/0001-17 com sede à Avenida Rio Branco, nº120, sala 830, Centro, Rio de Janeiro/RJ, CEP 20.040-001, para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

Esta PSI está baseada nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001 e 27002, bem como está de acordo com as leis vigentes em nosso país.

As informações da JORDÃO CONSULTORIA E PROJETOS LTDA, dos seus sócios, beneficiários, colaboradores e parceiros comerciais são bens que requerem proteção e tratamento de forma ética e sigilosa, de acordo com a legislação vigente e as normas internas da Empresa, evitando-se o mau uso, a perda e a exposição indevida.

O efetivo cumprimento da Política de Segurança da Informação – PSI é uma importante ferramenta para combater ameaças a estes ativos da Entidade.

## 1. OBJETIVOS

1.1. Conscientizar e orientar os colaboradores, parceiros e clientes da JORDÃO CONSULTORIA E PROJETOS LTDA, para uso seguro da informação, garantindo a observância aos princípios inerentes à segurança da informação.

1.2. Nortear a definição de normas e procedimentos específicos de segurança da informação, como também a implementação de controles e processos para seu atendimento.

1.3. Preservar as informações da JORDÃO CONSULTORIA E PROJETOS LTDA, quanto à:

1.3.1. **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

1.3.2. **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

1.3.3. **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

1.3.4. **Autenticidade**: garantia de que seja identificado e registrado o usuário que está enviando ou modificando a informação.

1.4. As orientações aqui apresentadas são os princípios fundamentais e representam como a JORDÃO CONSULTORIA E PROJETOS LTDA exige que a informação seja utilizada.

## 2. ABRANGÊNCIA

2.1. Esta Política se aplica a todos os colaboradores da empresa cientificando-os de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados, em qualquer tempo e circunstância.

2.2. É obrigação de cada colaborador se manter atualizado em relação a esta Política e aos procedimentos e normas a ela relacionadas, buscando orientação do seu Gestor ou da área de TI sempre que não estiver seguro quanto às diretrizes aqui apresentadas.

2.3. Deverá constar em todos os contratos com parceiros da JORDÃO CONSULTORIA E PROJETOS LTDA, Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela empresa.

2.4. O cumprimento da Política de Segurança pelos colaboradores, clientes, e parceiros poderá ser auditado pela JORDÃO CONSULTORIA E PROJETOS LTDA.

## 3. DIRETRIZES PARA A SEGURANÇA DA INFORMAÇÃO

3.1. Esta Política define as Diretrizes para a Segurança da Informação, visando preservar a integridade, confidencialidade, autenticidade e disponibilidade das informações sob gestão da JORDÃO CONSULTORIA E PROJETOS LTDA. Descreve a conduta considerada adequada para o manuseio, controle e proteção das informações, contra acessos não autorizados, destruição, modificação e divulgação indevida, seja acidental ou intencionalmente. As condutas aqui estabelecidas estão em total consonância com o Código de Ética da Empresa.

3.2. Propriedade da Informação

3.2.1. Toda informação produzida, acessada, recebida, manuseada ou armazenada pelos colaboradores, como resultado da atividade profissional, bem como, a reputação, a marca e demais ativos são de propriedade e de direito de uso exclusivos da JORDÃO CONSULTORIA E PROJETOS LTDA, sendo, portanto, proibidas as cópias, reproduções ou distribuição sem a devida autorização. As exceções devem ser explícitas e formalizadas por meio de manual específico.

3.2.2. A utilização da marca, identidade visual e demais sinais distintivos da JORDÃO CONSULTORIA E PROJETOS LTDA, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só poderá ser feita para atender às atividades profissionais da Empresa.

3.3. Classificação da Informação

3.3.1. É de responsabilidade de cada gestor estabelecer critérios relativos ao nível de confidencialidade da informação gerada ou recebido por sua área, de acordo com os critérios a seguir:

3.3.1.1. Pública: Informações da Empresa com linguagem e formato dedicado à divulgação ao público em geral, sendo de caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação;

3.3.1.2. Corporativa: Informações cujo conhecimento é de interesse de toda Empresa, podendo ser divulgada para beneficiários, participantes e parceiros;

3.3.1.3. Uso Interno: Informações de conhecimento exclusivo dos colaboradores da Empresa e deve ser divulgada apenas para o público interno;

3.3.1.4. Restrita: É toda informação que pode ser acessada somente por colaboradores de áreas previamente definidas em manual específico;

3.3.1.5. Confidencial: É uma informação crítica para os negócios da Empresa ou de parceiros, devendo haver indicação do nome ou cargo do colaborador responsável. A divulgação não autorizada desta informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e/ou criminais.

3.4. Utilização, Guarda e Descarte de Documentos

3.4.1. Documentos que contenham informações classificadas como uso interno, restrito ou confidencial não podem ficar expostos na estação de trabalho, em impressoras, fax, scanner, telas de computadores, áreas comuns, locais de trânsito de pessoas, refeitório e nas salas de reunião.

3.4.2. Documentos que contenham informações classificadas como restrita ou confidencial devem ser acondicionados em armários de acesso controlado, sua destruição, quando for o caso, deverá ser feita por meio de triturador de papel.

3.4.3. Nenhuma das informações restritas ou confidenciais podem ser repassadas para terceiros sem consentimento formalizado pela Diretoria Executiva da JORDÃO CONSULTORIA E PROJETOS LTDA.

3.4.4. É expressamente proibida a divulgação de informações de clientes e colaboradores sem as devidas autorizações e finalidades.

3.4.5. As áreas devem observar a exigência e o prazo legal definido em tabela vigente à época, para manutenção dos documentos produzidos em razão de suas atividades. Decorrido o prazo para armazenamento, os documentos devem ser destruídos antes de descartados, mediante autorização prévia da diretoria responsável.

3.5. Backup (Cópias de segurança)

3.5.1. Os backups devem ser realizados por sistemas de agendamento e executados, preferencialmente, fora do horário comercial, período em que não há nenhum ou pouco acesso de usuários ou processos automatizados dos sistemas de informática. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida, sugestões de melhorias, entre outros.

3.5.2. Além dos backups normalmente realizados no servidor, deverá ser feito backup adicional mantido em dispositivo externo com as informações codificadas (criptografadas) em ambiente seguro para armazenagem fora da JORDÃO CONSULTORIA E PROJETOS LTDA.

3.5.3. A rotina implementada de backup deve estar formalmente documentada para consultas e auditorias.

3.6. Controle de Acessos/Logins

3.6.1. Para cada colaborador da JORDÃO CONSULTORIA E PROJETOS LTDA deverá ser fornecido dispositivo de identificação pessoal, como crachás, códigos de acesso e senhas, os quais, não poderão ser compartilhados, divulgados ou transferidos a outra pessoa. O colaborador é responsável por todas as atividades desenvolvidas por meio de seus dispositivos de identificação pessoal. É vedada, a qualquer colaborador, a utilização de dispositivos de identificação pessoal de outro colaborador mesmo quando cedida por este.

3.6.2. É de responsabilidade de cada colaborador da Empresa a guarda dos dispositivos de identificação que lhe forem designados, bem como, a memorização de sua própria senha, não devendo anotar ou armazená-las em arquivos eletrônicos sem utilizar um meio de proteção definido pela Equipe de Segurança, como, por exemplo, criptografia.

3.6.3. As senhas não devem ser baseadas em informações pessoais, como o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome do Instituto, nome do departamento e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

3.6.4. As senhas de acesso deverão ser trocadas semestralmente.

3.6.5. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Empresa e a legislação (cível e criminal) será dos colaboradores que dele se utilizarem.

3.6.6. A concessão de acessos deverá seguir o critério de menor privilégio, no qual os colaboradores têm acesso apenas às informações imprescindíveis para o pleno desempenho de suas atividades.

3.6.7. Cada Diretoria deverá, através de e-mail, solicitar à Equipe de Segurança inclusões, alterações ou exclusões de acesso a usuários, definindo os serviços que deverão ser incluídos, alterados ou excluídos e justificando quanto à necessidade da solicitação.

3.6.8. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, por ocasião do desligamento de qualquer colaborador, a Equipe de Segurança da Informação deverá providenciar o imediato cancelamento de todas as suas senhas de acesso a equipamentos e sistemas corporativos, bem como de seu e-mail.

3.6.9. A Equipe de Segurança da Informação deverá, pelo menos semestralmente, efetuar testes de verificação de acesso aos recursos de TI e bloqueio automático de senha.

3.7. Segurança do Ambiente Físico

3.7.1. É vedado o acesso de pessoas não autorizadas ao Centro de Processamento de Dados – CPD, ou equivalente, da JORDÃO CONSULTORIA E PROJETOS LTDA.

3.7.2. O acesso de visitantes à Área Técnica ou às áreas internas da JORDÃO CONSULTORIA E PROJETOS LTDA deverá ser supervisionado diretamente por um colaborador.

3.7.3. É fundamental que, durante a jornada de trabalho e nas dependências da JORDÃO CONSULTORIA E PROJETOS LTDA, os colaboradores utilizem crachá de identificação. As áreas de acesso restrito, somente podem ser acessadas por colaboradores devidamente autorizados.

3.7.4. O acesso às dependências da Empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, para fins de gravação dos ambientes de trabalho, somente poderá ser realizado a partir de autorização da Responsável pela Comunicação e mediante supervisão.

3.7.5. Não é permitido aos colaboradores tirar fotos, gravar, filmar, publicar e/ou compartilhar imagens dos ambientes internos da JORDÃO CONSULTORIA E PROJETOS LTDA que possam:

3.7.5.1. Comprometer a segurança dos demais colaboradores;

3.7.5.2. Comprometer o sigilo das informações;

3.7.5.3. Impactar negativamente a imagem da JORDÃO CONSULTORIA E PROJETOS LTDA, outros colaboradores, clientes, parceiros e/ou visitantes.

3.8. 3.7 Mesa limpa/Tela limpa

3.8.1. Deve ser seguido o princípio estabelecido na Norma ABNT NBR/ISO/IEC 27001 da Mesa limpa/Tela limpa. Este princípio tem como objetivo a redução dos riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente. A adoção de uma política de “mesas limpas” para os papéis e mídias de armazenamento removível e, igualmente, uma política de “telas limpas”, contra, por exemplo, o perigo de ter um usuário já autenticado/registrado, porém ausente e com sua sessão de trabalho aberta.

3.8.2. A política de Mesa Limpa/Tela Limpa busca resguardar a JORDÃO CONSULTORIA E PROJETOS LTDA, assim como o próprio usuário, contra o acesso não autorizado a informações como, por exemplo, terceiros observando dados expostos em mesas ou telas. Assim, sinteticamente, entre outros:

3.8.2.1. Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos sempre que possível fora da superfície da mesa (mesa limpa);

3.8.2.2. Informações restritas ou confidenciais devem ser trancadas em local separado (idealmente em um arquivo, armário ou gaveteiro) quando não necessárias, especialmente quando o ambiente fica vazio;

3.8.2.3. Computadores e notebooks não devem ser deixados autenticados/ registrados quando não houver um colaborador (operador) junto e devem ser protegidos por senhas e outros controles quando não estiverem em uso. (tela limpa);

3.8.2.4. Informações restritas ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;

3.8.2.5. Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;

3.8.2.6. Papéis, livros ou qualquer informação restrita ou confidencial não devem ser deixados na mesa;

3.8.2.7. Informações restritas ou confidenciais devem ser mantidas em local apropriado (longe dos olhos de curiosos);

3.8.2.8. Um protetor de tela que solicite uma senha para acesso deve ser usado;

3.8.2.9. Todos os documentos e meios eletrônicos no final do dia de trabalho devem ser devidamente guardados/organizados, com proteção adequada;

3.8.2.10. Documentos contendo informações pessoais devem ser mantidos trancados.

3.9. Segurança dos Equipamentos

3.9.1. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da Área de TI ou de quem esta determinar.

3.9.2. Os sistemas e computadores devem ter versões de software antivírus instalados, ativados e atualizados permanentemente. Em caso de suspeita de incidência de vírus ou problemas de funcionalidade de hardware ou software, o colaborador deverá acionar a Área de TI do Instituto.

3.9.3. Os colaboradores deverão proteger o acesso a seus computadores por meio de tela de bloqueio a ser liberada mediante senha, quando os mesmos não estiverem em uso. Ao final do expediente de trabalho diário, o computador deverá ser desligado.

3.10. Utilização da Rede

3.10.1. A JORDÃO CONSULTORIA E PROJETOS LTDA, possui uma rede integrada de computadores com servidores e um microcomputador para cada colaborador da área administrativa.

3.10.2. O acesso à rede da JORDÃO CONSULTORIA E PROJETOS LTDA, só poderá ser efetivado após o registro obrigatório de computadores e usuários, de acordo com os sistemas de registro implementados.

3.10.3. O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso.

3.10.4. Os colaboradores da JORDÃO CONSULTORIA E PROJETOS LTDA, não deverão obter ou disponibilizar material sem a licença adequada através da rede.

3.10.5. O usuário é responsável pela própria e devida autenticação nos sistemas de redes disponibilizados pela JORDÃO CONSULTORIA E PROJETOS LTDA, não podendo fornecer e/ou compartilhar seu usuário, senha e/ou acesso à rede com outros usuários.

3.10.6. O usuário está comprometido a utilizar as redes públicas e ou privadas da JORDÃO CONSULTORIA E PROJETOS LTDA, para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence.

3.10.7. É vedada a utilização de proxies que permitam o tráfego de informações a redes privadas externas.

3.10.8. Os usuários devem administrar suas pastas, excluindo arquivos desnecessários.

3.10.9. Material sexualmente explícito ou contrário à legislação brasileira não podem ser expostos, armazenados, distribuídos, editados ou gravados, através do uso dos recursos computacionais da rede corporativa da Empresa.

3.10.10. Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos etc..) nos drivers de rede, pois estes ocupam espaço comum limitado. Caso identificada a existência desses arquivos, eles serão imediatamente excluídos, em definitivo e sem prévia comunicação.

3.11. Utilização dos Sistemas Corporativos

3.11.1. Os Sistemas Corporativos são os sistemas utilizados na gestão da JORDÃO CONSULTORIA E PROJETOS LTDA os quais buscam trazer maior transparência, tempestividade e confiabilidade para as informações, abrangendo todos os segmentos da administração do Instituto e permitindo o gerenciamento isolado de cada parte e a interligação desta com o todo, produzindo relatórios analíticos, sintéticos e estatísticos, sendo acessados por meio de uma rede interna ou externa.

3.11.2. É expressamente proibida a divulgação e/ou o compartilhamento indevido das informações contidas nos Sistemas Corporativos da Empresa.

3.11.3. Todos os usuários dos ativos de informação de propriedade da JORDÃO CONSULTORIA E PROJETOS LTDA, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do mesmo, mantendo conduta profissional.

3.11.4. O acesso às informações contidas nos Sistemas Corporativos deve ser efetuado sempre através de identificação segura (chave e senha).

3.11.5. Para cada usuário devem ser atribuídas permissões específicas, por módulo e/ou operação.

3.11.6. A concessão de acesso às bases de dados para prestadores de serviço e colaboradores deverá sempre seguir o critério do menor privilégio possível.

3.11.7. As bases de dados do ambiente de desenvolvimento devem estar anonimizadas evitando-se o acesso desnecessário a informações pessoais de participantes e beneficiários.

3.12. Utilização dos Equipamentos de Informática a Informação

3.12.1. Os equipamentos de informática e de comunicação são utilizados pelos colaboradores do Instituto para a realização das atividades profissionais. Excepcionalmente, o uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

3.12.2. A JORDÃO CONSULTORIA E PROJETOS LTDA, por meio de sua área de TI, poderá registrar todo e qualquer uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas. A responsabilidade em relação à segurança da informação será comunicada na fase de contratação dos colaboradores, os quais deverão assinar um termo de responsabilidade.

3.12.3. As estações de trabalho possuem códigos internos (IP), que permitem a rastreabilidade de todas as atividades executadas, assim como, é possível à área de TI monitorar todo acesso realizado por meio de sua rede, sendo de responsabilidade de cada colaborador zelar pelos seus respectivos acessos.

3.13. Utilização da Internet

3.13.1. Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

3.13.2. A internet, via cabo ou Wi-fi, deverá ser utilizada para fins profissionais, como ferramenta de busca de informações, que contribuam para o desenvolvimento das atividades da JORDÃO CONSULTORIA E PROJETOS LTDA.

3.13.3. O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso. Em particular, o usuário deverá observar os termos de licença de uso do material obtida através da internet.

3.13.4. Os colaboradores da JORDÃO CONSULTORIA E PROJETOS LTDA não deverão:

3.13.4.1. Utilizar a Internet com objetivos ou meios para a prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses da Instituição ou de terceiros;

3.13.4.2. Utilizar a Internet com objetivo de danificar, inutilizar, sobrecarregar ou deteriorar os recursos de tecnologia da informação e dados de qualquer tipo, de uso corporativo, pessoal ou de terceiros;

3.13.4.3. Acessar a sites de proxy com o objetivo de burlar os mecanismos de segurança existentes;

3.13.4.4. Acessar sites de pornografia, pedofilia e outros contrários à lei. O acesso a esses sites é terminantemente proibido, ainda que os mesmos não estejam bloqueados no sistema de segurança da Instituição.

3.13.5. Os equipamentos fornecidos para o acesso à internet são de propriedade da JORDÃO CONSULTORIA E PROJETOS LTDA, que poderá analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede ou internet, estejam eles em disco local ou na rede.

3.13.6. Assim, a Empresa, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.

3.14. Utilização de E-mail (correio eletrônico)

3.14.1. Os serviços de correio eletrônico são oferecidos como um recurso profissional pela JORDÃO CONSULTORIA E PROJETOS LTDA para seus colaboradores no cumprimento de seus objetivos nas áreas de atuação.

3.14.2. O uso pessoal poderá ser permitido, mas não priorizado, desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas suas atividades, não interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de correio eletrônico da JORDÃO CONSULTORIA E PROJETOS LTDA, não incorra em gastos adicionais para a Instituição, ou viole qualquer outra lei ou norma vigente.

3.14.3. Portanto, cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal. Deve ser considerado que o correio eletrônico é inerentemente uma forma insegura de comunicação, não garantindo sigilo ou entrega.

3.14.4. A JORDÃO CONSULTORIA E PROJETOS LTDA poderá fornecer recursos adequados para melhorar o nível de segurança no uso do correio eletrônico, como, por exemplo, chaves de criptografia e assinatura digital.

3.14.5. O acesso às mensagens nos servidores de correio eletrônico deve ser feito usando protocolos seguros.

3.14.6. Os colaboradores e parceiros com acesso, aos serviços de mensagem eletrônica disponibilizados pela JORDÃO CONSULTORIA E PROJETOS LTDA devem observar o seguinte:

3.14.6.1. Todos os usuários dos ativos de informação de propriedade da JORDÃO CONSULTORIA E PROJETOS LTDA, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da Empresa, mantendo uma conduta ética e profissional;

3.14.6.2. Todas as contas de e-mail terão uma titularidade, sendo o usuário titular o responsável direto pelas mensagens enviadas por intermédio do seu endereço de e-mail;

3.14.6.3. Os usuários poderão ser titulares de uma única caixa postal individual no servidor de e-mail, com direitos de envio/recebimento de mensagens, via Intranet e Internet;

3.14.6.4. Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens;

3.14.6.5. O usuário deve utilizar o e-mail de forma adequada e diligente;

3.14.6.6. É vedado o envio, armazenamento ou manuseio de material que caracterize a divulgação, incentivo ou prática de atos que:

3.14.6.6.1. Contrariem o disposto na legislação vigente, ética, moral e de ordem pública;

3.14.6.6.2. Sejam proibidos pela presente Política, lesivos aos direitos e interesses da JORDÃO CONSULTORIA E PROJETOS LTDA ou de terceiros;

3.14.6.6.3. De qualquer forma, possam danificar, inutilizar, invadir, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

3.14.6.6.4. Promovam ameaças, difamação ou assédio a outras pessoas;

3.14.6.6.5. Contenham conteúdo considerado impróprio, obsceno ou ilegal;

3.14.6.6.6. Sejam de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

3.14.6.6.7. Contenham a prática de qualquer tipo de discriminação relativa à raça, sexo, credo religioso, incapacidade física ou mental ou outras situações protegidas;

3.14.6.6.8. Caracterizem violação de direito autoral garantido por lei.

3.14.6.7. É vedada ainda a utilização do e-mail, nas situações abaixo:

3.14.6.7.1. Acesso não autorizado à caixa postal de outro usuário;

3.14.6.7.2. Uso para atividades com fins comerciais ou políticos e o uso extensivo para assuntos pessoais ou privados;

3.14.6.7.3. Envio de mensagens do tipo “corrente” e “spam”;

3.14.6.7.4. Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;

3.14.6.7.5. Utilização de listas e/ou caderno de endereços da JORDÃO CONSULTORIA E PROJETOS LTDA para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;

3.14.6.7.6. Divulgação de informações em não conformidade com a diretriz de Classificação de Informações prevista nesta política;

3.14.6.7.7. Envio de qualquer mensagem que torne a empresa vulnerável a ações civis ou criminais;

3.14.6.7.8. Exclusão de mensagens relacionadas às atividades profissionais, quando o Instituto ou pessoas a ele relacionadas estiverem sujeitos a algum tipo de investigação.

3.15. Utilização de Software de Mensagens Instantâneas/Redes Sociais

3.15.1. Os serviços de comunicação instantânea instalados nos equipamentos serão inicialmente disponibilizados aos colaboradores que necessitem dessa ferramenta e poderão ser bloqueados, caso o gestor requisite formalmente à área de TI da Empresa.

3.15.2. O uso de aplicativos de comunicação pelos colaboradores, a partir de recursos da JORDÃO CONSULTORIA E PROJETOS LTDA, para compartilhar informações profissionais, deverá ser feito de forma responsável para evitar riscos desnecessários, que possam comprometer as atividades, os projetos ou a própria Empresa.

3.15.3. O colaborador deve, ainda, sempre que possível, preservar o sigilo e a confidencialidade das informações, atender aos requisitos de segurança previstos nesta Política e respeitar a legislação vigente.

3.16. Utilização de Dispositivos Móveis Corporativos

3.16.1. Dispositivos móveis corporativos são equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória.

3.16.2. É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações de uso interno, restritas ou confidenciais por meio de dispositivos móveis corporativos.

3.16.3. O usuário deve utilizar os dispositivos móveis corporativos de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

3.16.4. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis corporativos, tanto por sua guarda quanto pelos conteúdos neles instalados.

3.16.5. Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel corporativo.

3.16.6. Não é permitida a alteração da configuração dos sistemas operacionais dos equipamentos, em especial, os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um colaborador da área de TI.

3.16.7. O colaborador deverá responsabilizar-se em não utilizar quaisquer programas e/ou aplicativos, inclusive gratuitos, que não tenham sido instalados ou autorizados por um colaborador da área de TI.

3.16.8. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela JORDÃO CONSULTORIA E PROJETOS LTDA, notificar imediatamente seu gestor e a área de TI. Também deverá, assim que possível, registrar um Boletim de Ocorrência na Delegacia de Furtos de Roubos (BO).

3.16.9. O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao Instituto e/ou a terceiros.

3.16.10. Em caso de desligamento, o colaborador deve realizar imediata devolução de seus dispositivos móveis à área de TI.

3.17. Utilização de Mídias Removíveis

3.17.1. O uso de mídias removíveis deve ser tratado como exceção à regra, pois a porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais.

3.17.2. Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que tais dispositivos possam vir a causar, uma vez que esse tipo de mídia pode conter vírus e softwares maliciosos, capazes de danificar e corromper dados.

3.18. Acesso Remoto ao Hosting

3.18.1. Para garantia da integridade dos dados da JORDÃO CONSULTORIA E PROJETOS LTDA e utilização em caso de contingência, as informações armazenadas na rede interna devem estar replicadas em servidores virtuais externos (nuvem). O acesso a redes remotas permite ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto.

3.18.2. A boa utilização destes serviços é de responsabilidade de cada usuário, os que utilizam a rede da JORDÃO CONSULTORIA E PROJETOS LTDA e/ou terceiros que utilizam serviços de acesso remoto. Cabe ressaltar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse da Empresa.

3.18.2.1. Por se tratar de solução de contingência devem ser utilizados de acordo com o estabelecido nos normativos específicos;

3.18.2.2. O usuário somente poderá realizar as atividades em período estipulado pela JORDÃO CONSULTORIA E PROJETOS LTDA.

3.19. Acesso Remoto à Rede da JORDÃO CONSULTORIA E PROJETOS LTDA.

3.19.1. A interconexão entre redes privadas a distância permite ao usuário utilizar-se de redes e serviços de redes disponibilizados por terceiros. O acesso a redes remotas disponibilizadas por redes privadas externas permite ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto.

3.19.2. Por se tratar de um acesso entre redes privadas, a segurança e integridade da informação trafegada dependem das configurações da rede. Logo, este tópico tem como objetivo estipular um conjunto de diretrizes e recomendações aos diferentes usuários da JORDÃO CONSULTORIA E PROJETOS LTDA.

3.19.3. A boa utilização destes serviços é de responsabilidade de cada usuário, os que utilizam a rede da JORDÃO CONSULTORIA E PROJETOS LTDA e/ou terceiros que utilizam serviços de acesso remoto. Cabe enfatizar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse da JORDÃO CONSULTORIA E PROJETOS LTDA.

3.19.3.1. O usuário somente pode realizar acesso interativo entre redes onde a permissão esteja autorizada. A autorização depende das atividades profissionais relacionadas a função exercida;

3.19.3.2. O usuário deve utilizar somente o local e o ambiente físico aprovado pela JORDÃO CONSULTORIA E PROJETOS LTDA;

3.19.3.3. O usuário externo deve configurar de forma adequada o firewall e a proteção antivírus na rede externa à rede da JORDÃO CONSULTORIA E PROJETOS LTDA;

3.19.3.4. O usuário somente poderá realizar as atividades em período estipulado pela JORDÃO CONSULTORIA E PROJETOS LTDA.

3.20. Instalações de Softwares

3.20.1. O colaborador da JORDÃO CONSULTORIA E PROJETOS LTDA é proibido de instalar todo e qualquer programa não autorizado em seu computador e em qualquer outro dispositivo computacional pertencente à Empresa, salvo as instalações de programas que contenham prévia autorização da Diretoria Executiva ou da Área de TI. Este comando também é aplicado a programas com conteúdo de atualização conhecidos como patches.

3.20.2. O usuário é proibido de remover toda e qualquer versão de software obsoleto, mesmo em casos onde exista uma versão atualizada da aplicação utilizada.

3.20.3. Caso o usuário necessite instalar ou remover qualquer software, deverá entrar em contato com o gestor responsável e/ou com a área de TI da empresa.

3.20.4. Não é permitida a instalação/uso de softwares ilegais (sem licenciamento), sendo que a Área de TI poderá valer-se desta Política para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

3.20.5. É proibido executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da Empresa.

3.21. Comunicação Dentro e Fora da Empresa

3.21.1. Somente os colaboradores que estão devidamente autorizados a falar em nome da JORDÃO CONSULTORIA E PROJETOS LTDA, para os meios de comunicação, podem fazê-lo em nome da Empresa.

3.21.2. A fim de evitar exposição desnecessária da JORDÃO CONSULTORIA E PROJETOS LTDA, os colaboradores não devem tratar de assuntos internos em locais públicos ou dentro das instalações físicas do Instituto, quando próximos a visitantes ou terceiros.

## 4. DAS RESPONSABILIDADES ESPECÍFICAS

4.1. Dos Colaboradores em Geral

4.1.1. Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da empresa.

4.1.2. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à JORDÃO CONSULTORIA E PROJETOS LTDA e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

4.2. Dos Colaboradores em Regime de Exceção (Temporários)

4.2.1. Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

4.2.2. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

4.3. Dos Gestores de Pessoas e/ou Processos

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

4.3.2. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da JORDÃO CONSULTORIA E PROJETOS LTDA.

4.3.3. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da JORDÃO CONSULTORIA E PROJETOS LTDA.

4.3.4. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

4.3.5. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Política de Privacidade e do Plano de Resposta a Incidentes.

## 5. DOS CUSTODIANTES DA INFORMAÇÃO

5.1. Da Área de Tecnologia da Informação

5.1.1. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

5.1.2. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

5.1.3. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares.

5.1.4. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

5.1.5. Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

5.1.6. Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

5.1.7. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

5.1.8. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a JORDÃO CONSULTORIA E PROJETOS LTDA.

5.1.9. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

5.1.10. O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

5.1.11. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

5.1.12. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

5.1.13. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

5.1.13.1. os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

5.1.13.2. os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

5.1.14. Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

5.1.15. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

5.1.16. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

5.1.17. Realizar auditorias periódicas de configurações técnicas e análise de riscos.

5.1.18. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

5.1.19. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

5.1.20. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

5.1.21. Monitorar o ambiente de TI, gerando indicadores e históricos de:

5.1.21.1. uso da capacidade instalada da rede e dos equipamentos;

5.1.21.2. tempo de resposta no acesso à internet e aos sistemas críticos da JORDÃO CONSULTORIA E PROJETOS LTDA;

5.1.21.3. períodos de indisponibilidade no acesso à internet e aos sistemas críticos da JORDÃO CONSULTORIA E PROJETOS LTDA;

5.1.21.4. incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

5.1.21.5. atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

5.2. Do Comitê de Segurança da Informação

5.2.1. Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano.

5.2.2. A composição mínima deve incluir um colaborador de cada uma das áreas: TI, DPO, OPERAÇÃO, RH, COMUNICAÇÃO E JURÍDICO.

5.2.3. Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a JORDÃO CONSULTORIA E PROJETOS LTDA.

5.2.4. O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

5.2.5. Cabe ao CSI:

5.2.5.1. propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;

5.2.5.2. propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas

complementares;

5.2.5.3. avaliar os incidentes de segurança e propor ações corretivas;

5.2.5.4. definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

## 6. DAS DISPOSIÇÕES FINAIS

6.1. Este documento é válido a partir do dia 10 de março de 2023.

6.2. O proprietário deste documento é a área de TI, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.