Política de Segurança da Informação da ToBusiness +Qmarcas, let'smark & A+registros

PREÂMBULO

Somos a **ToBusiness**, um grupo empresarial composto pelas divisões +Qmarcas, let'smark & A+registros, com atuação em todo o território nacional, nos segmentos de registro de marcas, patentes, direitos autorais e intermediação de negócios, por meio da qual ainda intermediamos, sob demanda, serviços de assessoria e consultoria jurídica empresarial.

APRESENTAÇÃO

A **Política de Segurança da Informação**, também conhecida como **PSI**, é o documento que orienta e estabelece as diretrizes corporativas da **ToBusiness (+Qmarcas, let'smark & A+registros)** para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários dos seus serviços, razão pela qual deve ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI é baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

E de acordo com a definição da norma ISO 27001, que estabelece as diretrizes gerais para a gestão da informação de uma empresa, segurança da informação nada mais é que o ato de proteger os dados da empresa (especialmente aqueles confidenciais) contra diversos tipos de ameaças e riscos — espionagens, sabotagens, incidentes com vírus ou códigos maliciosos e até acidentes, como incêndio e inundação.

Chegamos, assim, à política de segurança da informação, definida como as regras que ditam o acesso, o controle e a transmissão da informação em uma organização. Lembrando que uma política de segurança não é um documento imutável ou inquestionável. Muito pelo contrário, requer atualização constante e participação não só da diretoria da empresa, mas também dos funcionários e da equipe de TI.

SOBRE A NOSSA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A PSI da **ToBusiness (+Qmarcas, let'smark & A+registros)** será obtida pela implantação de uma gama de controles que incluem procedimentos de rotina (como as verificações de antivírus), infraestrutura de hardware e software (como a gestão de soluções para assinatura eletrônica de documentos), além da criação de uma política devidamente documentada.

Para tanto, alguns princípios básicos serão observados, a saber: confidencialidade, integridade e disponibilidade – onde cada um deles denota uma postura diferente dentro da **ToBusiness (+Qmarcas, let'smark & A+registros)**, exigindo ações pontuais para que se mantenham sempre presentes.

CONFIDENCIALIDADE

O conceito de confidencialidade não foge muito à noção que o próprio termo nos passa. A confidencialidade, no contexto da segurança da informação, nada mais é do que a garantia de que determinada informação, fonte ou sistema é acessível apenas às pessoas previamente autorizadas a terem acesso.

Dessa forma, sempre que uma informação confidencial é acessada por um indivíduo não autorizado, intencionalmente ou não, ocorre o que se chama de quebra da confidencialidade. A ruptura desse sigilo, a depender do teor das informações, pode ocasionar danos inestimáveis para a empresa, seus clientes e até mesmo para todo o mercado.

INTEGRIDADE

Quando empresas lidam com dados, um dos seus grandes deveres é mantê-los intocados, de forma a preservar a sua originalidade e confiabilidade. Caso contrário, erros podem ocorrer na interpretação dessas informações, gerando também rupturas no *compliance* do negócio e, no pior dos casos, sanções penais pesadas.

Nesse contexto, garantir a integridade é, pois, adotar todas as precauções necessárias para que a informação não seja modificada ou eliminada sem autorização, isto é, que mantenha a sua legitimidade e consistência, condizendo exatamente com a realidade.

DISPONIBILIDADE

A relação da segurança da informação com a disponibilidade é basicamente a garantia de acesso aos dados sempre que necessário. Ou seja, é a possibilidade de os colaboradores e membros da organização acessarem os dados de maneira fluida, segura e eficiente.

No contexto corporativo, a disponibilidade das informações é matéria de extrema importância, visto que o negócio pode depender da disponibilidade dos seus dados e sistemas para fechar contratos, vendas e atender os clientes.

1. OBJETIVO

1.1. A maior finalidade dessa PSI consiste em definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio em que ela esteja contida.

1.2. A PSI também terá por escopo nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

1.3. Por fim, a PSI ainda visará preservar as informações sob guarda e responsabilidade da ToBusiness (+Qmarcas, let'smark & A+registros), sobretudo quanto à:

- **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;
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. APLICAÇÕES DA PSI

2.1. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores da ToBusiness (+Qmarcas, let'smark & A+registros), bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

2.2. Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

2.3. É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Sistemas sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3. RESPONSABILIDADE

3.1. Esta Política é de responsabilidade do Time de Tecnologia da ToBusiness (+Qmarcas, let'smark & A+registros), onde quaisquer mudanças nesta Política devem ser aprovadas pelo mesmo.

3.2. A alta administração da ToBusiness (+Qmarcas, let'smark & A+registros) tem o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

4. DATA DE ENTRADA EM VIGOR

4.1. Esta Política entrará em vigor imediatamente.

5. PÚBLICO ALVO

5.1. Esta Política se aplica à todas as divisões e a todos os colaboradores da ToBusiness (+Qmarcas, let'smark & A+registros.

6. DIRETRIZES GERAIS

6.1. Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela ToBusiness e suas divisões pertence à referida organização; onde as exceções devem ser explícitas e formalizadas em contrato entre as partes.

6.2. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais.

6.3. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

6.4. A ToBusiness, por meio do seu Time de Tecnologia, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

6.5. A informação sob custódia de qualquer divisão da ToBusiness, mesmo que pertencente a clientes ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas.

6.6. A geração, utilização, armazenamento, manutenção, distribuição e destruição da informação devem ser feitas de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados.

6.7. As divisões da ToBusiness (+Qmarcas, let'smark & A+registros) reservam-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais, onde devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

6.8. A informação deve ser armazenada, pelo tempo determinado pela instituição ou legislação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

6.9. O uso de redes externas de comunicação (Internet, redes privadas, etc.) deve ser controlado através de Servidores de *Firewalls*, Servidores de Acesso à Internet, Servidores de *AntiSpam*, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

6.10. O acesso externo aos sistemas da organização, quando realizado pelo pessoal da Área de Suporte Técnico ou por prestadores de serviço, deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização e restringindo-se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada.

6.11. A remessa de dados da organização, seja para atender requisitos de negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

6.12. Sistemas aplicativos (softwares, sistemas e API's) desenvolvidos dentro da organização devem ser documentados e controlados quanto às alterações ou correções feitas. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

6.13. Sistemas aplicativos desenvolvidos fora da organização, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes, etc.) sob custódia de ambas as partes, de.

6.14. O mau uso dos sistemas informáticos, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade.

6.14. Para minimizar o risco de falhas nos sistemas, deve-se fazer um planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos.

7. REQUISITOS DA PSI

7.1. Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da ToBusiness (+Qmarcas, let'smark & A+registros), a fim de que a política seja cumprida dentro e fora da organização.

7.2. Caso ainda não tenha sido criado, deverá ser composto um órgão multidisciplinar, o Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC), o qual, entre outras atribuições, será responsável pela gestão da segurança da informação.

7.3. Tanto a PSI quanto as normas deverão ser revistas e atualizadas anualmente, ou sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC).

7.4. Em todos os contratos da ToBusiness (+Qmarcas, let'smark & A+registros) deverá constar o anexo de **Acordo de Confidencialidade** ou **Cláusula de Confidencialidade**, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

7.5. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores, onde todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos intangíveis, a fim de reduzir possíveis riscos.

7.6. Todo colaborador, quando contratado e informado das presentes regras de Segurança da Informação, deve assinar um termo de responsabilidade.

7.7. Todo incidente que afete a segurança da informação deverá ser comunicado Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC) ou, caso ele ainda não tenha sido formado, ao responsável pela área de TI da organização.

7.8. ToBusiness exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores,

reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

7.9. Esta PSI será implementada na ToBusiness por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

7.10. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

8. CONFIDENCIALIDADE DAS INFORMAÇÕES

8.1. Cada um dos nossos colaboradores, no ato de sua contratação, sabe que em seu contrato há a exposição do termo de confidencialidade, onde todos, sem exceção, se obriga a manter o mais absoluto sigilo com relação a quaisquer dados, informações, materiais, produtos, sistemas, técnicas, estratégias, métodos de operação, pormenores, inovações, segredos comerciais, marcas, criações, especificações técnicas e comerciais da ToBusiness (+Qmarcas, let'smark & A+registros), a que venham a ter acesso, conhecimento ou que venha a lhe ser confiado, comprometendo-se, igualmente, a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, funcionários e/ou prepostos faça uso indevido desses Informações Confidenciais. Para tanto, é indispensável a todos:

- Abster-se de compartilhar, sob qualquer hipótese, nome de usuário (login) e senha da rede da ToBusiness que são pessoais e intransferíveis, atentando que qualquer ação indevida é de responsabilidade de quem compartilhou essas informações;
- Respeitar os direitos autorais e a legislação específica sobre propriedade intelectual, tanto das produções da ToBusiness como de terceiros;
- Resguardar os conteúdos e documentos internos da ToBusiness (informações, dados, relatórios) ompartilhando-os somente após a devida autorização e com quem os necessite para exercer as atividades definidas pela ToBusiness;
- Respeitar e proteger a condição de confidencialidade e sigilo de informações e a restrição de divulgação delas, tanto de matérias internas à ToBusiness como de propriedade de terceiros, mesmo após eventual desligamento da ToBusiness;
- Vetar o acesso a informações confidenciais por pessoas que não estejam para isso credenciadas;
- Utilizar os sistemas da ToBusiness zelando pela qualidade das informações imputadas e garantindo a sua confidencialidade;
- Zelar pelos registros acadêmicos de toda ordem, disponibilizando-as, a quem de direito, de acordo com os prazos e critérios requeridos segundo a finalidade das informações.

8.2. O mesmo dispositivo do item 8.1. aplica-se aos dados e informações dos clientes e dos fornecedores com os quais possamos ter acesso, uma vez que somos regidos por regras dispostas na Lei Complementar nº 105/2001, especificamente para a prestação de serviços com a utilização de informações financeiras dos clientes da **ToBusiness**, onde todos os colaboradores devem manter o mais absoluto sigilo sobre quaisquer situações bancárias dos clientes, bem como contas bancárias ativas, informações sobre saldos, extratos, transferências, movimentações de qualquer natureza ou qualquer dado que possa interferir na perfeita observância ou possa violar as normas previstas.

8.3. Se qualquer dos colaboradores der causa a violação de informação considerada como de caráter confidencial, ficará sujeito a indenizar a **ToBusiness** ou qualquer uma das suas sub-divisões (+Qmarcas, let'smark & A+registros), até a altura dos danos efetivamente causados, sem prejuízo das penalidades previstas na esfera penal e administrativa.

8.4. Para apuração de qualquer conduta que possa expor informações confidenciais, a **ToBusiness** dispõe de tecnologias de monitoramento de atividades de todos os seus colaboradores em seus terminais internos, ramais de comunicação internos e externos, celulares comerciais, intra e extra net, sistema integrados e prestadores de serviços, dentre outros; entretanto, ressalta-se que inexiste qualquer intenção obscura de fiscalizar cada passo dado por quaisquer dos colaboradores, mas é importante, ao menos periodicamente, checarmos as atividades desempenhadas se estão dentro dos padrões pregados e esperados pelo grupo.

8.5. Os colaboradores não podem e nem devem ter expectativa de privacidade, se as atividades privadas se desempenharem em nossos terminais ou mediante o uso dos recursos e tecnologias disponibilizadas para fins profissionais.

9. DO TRATAMENTO DAS INFORMAÇÕES

9.1. Toda informação deve ser utilizada apenas para fins profissionais, de interesse exclusivo da empresa.

9.2. Toda informação relevante deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda.

9.3. Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização.

9.4. É proibida a transmissão a terceiros, por qualquer meio, bem como sua divulgação, reprodução, cópia, utilização ou exploração de conhecimentos, dados e informações de propriedade das Instituições, utilizáveis nas atividades das mesmas, sem a prévia e expressa autorização da Diretoria responsável, e das quais os funcionários venham a tomar conhecimento durante a relação empregatícia, estendendo-se tal vedação ao período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

9.5. A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco.

9.6. As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da empresa.

9.7. Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

9.8. As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área de Tecnologia da Informação da ToBusiness (+Qmarcas, let'smark & A+registros), sempre que esse equipamento estiver em uso ou logado com a credencial do funcionário que necessita do suporte.

9.9. Quando forem vendidos, devolvidos ao fabricante, enviados para manutenção ou deslocados para outros usuários, as informações contidas em equipamentos que armazenem informações deverão ser destruídas antes da liberação do equipamento para o destino.

9.10. Todas as pessoas com acesso aos sistemas e informações, pertencentes ou em posse do grupo, deverão ter uma única identificação (*login*).

9.11. Os gestores devem determinar as regras de acesso e distribuição das informações, considerando os seguintes itens:

A. Riscos inerentes às informações:
    a. Acesso por pessoas não autorizadas;
    b. Divulgação indevida;
    c. Indisponibilidade; e
    d. Alteração indevida.
B. Consequências:
    a. Fraudes: Possibilidades de lesarem empresas do Conglomerado ou terceiros (clientes, fornecedores, etc.);
    b. Problemas legais: Possibilidades de gerar prejuízos, multas, penalidades ou embaraços às Instituições, Diretores e Funcionários do Conglomerado, a outras pessoas físicas ou jurídicas;
    c. Perda de negócio: Possibilidade de não realizar receitas previstas ou gerar perdas nos negócios implantados ou em fase de implantação;
    d. Prejuízo de imagem do Conglomerado: Possibilidades de prejudicar a imagem do Conglomerado ou de seus funcionários;
    e. Problemas de recuperação: Possibilidades de gerar custos de recuperação de informações perdidas ou danificadas.

10. DECLARAÇÃO DE RESPONSABILIDADE

10.1. É um compromisso de responsabilidade direta do funcionário para com as informações, equipamentos e outras propriedades da ToBusiness (+Qmarcas, let'smark & A+registros) a ele confiadas, devendo ser lida e assinada quando de sua admissão (Anexo 1).

10.2. Os prestadores de serviço à ToBusiness (+Qmarcas, let'smark & A+registros) deverão assinar uma declaração de responsabilidade sobre a confidencialidade das informações, onde tal declaração deve constar em uma das cláusulas do contrato com eles ajustados.

10.3. Os clientes também devem concordar com uma a declaração de responsabilidade a ser destacada em uma das cláusulas do termo de adesão ao serviço/produto por eles adquiridos - ou documento equivalente, se ao cliente for entregue alguma senha de acesso às informações.

10.4. A declaração de responsabilidade deve ser lida e assinada por todos os funcionários antes de ser arquivada na respectiva pasta funcional. O Departamento de Recursos Humanos deve garantir que todos os funcionários tenham sua declaração de responsabilidade assinada.

10.5. Poderá ser utilizado um Termo de Responsabilidade eletrônico, mediante aprovação do Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC) ou, caso o mesmo ainda não tenha sido criado, do responsável pela Tecnologia da Informação da ToBusiness (+Qmarcas, let'smark & A+registros).

11. DA SEGURANÇA DAS INFORMAÇÕES

11.1. Segurança Lógica de Computadores, Redes e Sistemas Aplicativos

11.1.1. Este item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse do Grupo.

11.1.2. Todo sistema aplicativo define um conjunto de operações aplicáveis às informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão, liberação etc.

11.1.3. Um perfil de acesso define que operações podem ser executadas por certa classe de usuários, usando um determinado tipo de informação.

11.1.4. Caso as operações e suas respectivas informações envolvam quantias, poderão ser criadas alçadas, que definem a quantia máxima envolvida em operações executadas por cada classe de usuários.

11.1.5. As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis, alçadas e classe de usuários, bem como os processos operacionais a serem utilizados para sua administração e controle.

11.2. Normas para segurança lógica de computadores, redes e aplicativos

11.2.1. Os acessos aos serviços e dados devem ser controlados com base nos requisitos de cada negócio, devem estar claramente definidos e documentados e todos os sistemas aplicativos devem estar direcionados para a implementação e manutenção desses controles.

11.2.2. Cada gestor da informação deve definir e manter atualizada uma política de acesso aos seus aplicativos.

11.2.3. As informações devem ser analisadas pelos respectivos gestores da informação, de forma a permitir que sejam definidas as regras de acesso, através de perfis e alçadas.

11.2.4. Os sistemas aplicativos devem possuir recursos que possibilitem a administração dos acessos, através dos perfis e alçadas definidos pelos respectivos gestores da informação.

11.2.5. Devem existir procedimentos formais que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários.

11.2.6. Em relação ao controle de acesso a computadores e redes, deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto.

11.2.7. O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados.

11.2.8. Os ambientes de produção, homologação e desenvolvimento devem estar segregados entre si, de forma a impedir acessos indevidos.

11.2.9. Um sistema efetivo de controle de acesso a computadores, redes e sistemas aplicativos deve ser criado e utilizado para autenticar os usuários, de modo que as principais características desse controle sejam:

- O acesso a computadores e redes deve ser protegido por senha;
- As senhas poderão ser alteradas pelos usuários em qualquer ambiente (operacional ou aplicativo);
- Os sistemas devem ser programados para nunca exibir a senha na tela;
- As senhas devem ser individuais e intransferíveis;
- A senha deve ser de uso exclusivo, pessoal e intransferível, sendo o compartilhamento proibido em quaisquer circunstâncias;
- As senhas não devem ser triviais e previsíveis;
- Os tipos de caracteres utilizados para a formação da senha devem ser:
    - Letras maiúsculas;
    - Letras minúsculas;
    - Números; e
    - Sinais ou símbolos especiais (Ex: @ # $ % & * - + = “ ´ ` ^ ~ { } [ ] / | \ ? !).

- As senhas deverão ter um tamanho mínimo de 8 (oito) caracteres, sendo obrigatória a utilização de no mínimo três dos quatro tipos de caracteres acima definidos, sendo mandatário o uso de no mínimo um sinal ou símbolo especial;
- Os sistemas devem prever um prazo para a expiração de senhas de no máximo 30 (trinta) dias;
- Caso algum sistema defina uma senha inicial, deverá obrigar o usuário a alterá-la no primeiro acesso;
- As senhas trocadas ou expiradas devem ser cadastradas para efeito de bloqueio de reutilização (mínimo de vinte e quatro senhas);
- Os arquivos de senhas devem ser criptografados e gravados separadamente dos arquivos de dados, em ambiente de acesso restrito;
- Após um máximo de cinco tentativas consecutivas sem sucesso, os acessos devem ser bloqueados até que seja solicitado o desbloqueio do usuário;
- Uma vez aprovada, a senha deve garantir acesso exclusivo do usuário na estação de trabalho. Portanto, um mesmo usuário não deverá utilizar simultaneamente mais de uma estação de trabalho.

11.2.10. Todos os sistemas aplicativos deverão contar com um monitoramento de uso e acesso aos sistemas, sendo ainda capaz de:

- Detectar tentativas de acesso não autorizado;
- Registrar eventos de entrada no sistema (login);
- Sempre que houver riscos que afetem o negócio devem ser gravadas trilhas de auditoria para futuras investigações, registrando os dados dos acessos, tais como: identificação do usuário, localidade, identificação do terminal ou estação de rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas;
- Emitir relatórios gerenciais de acessos (por usuário, módulo do aplicativo e funções).

11.3. Segurança no Acesso de Prestadores de Serviço

11.3.1. Visando estabelecer controles sobre recursos de processamento da informação da organização durante a execução de serviços por contratados externos, o Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC) deve fazer uma avaliação dos riscos envolvidos para determinar as implicações de segurança e os controles necessários diante de cada intervenção externa, nos computadores e sistemas informáticos da ToBusiness (+Qmarcas, let'smark & A+registros), onde, o que pautar como conveniente acordar deve ser explicitado no contrato a ser ajustado com tais prestadores de serviços.

11.3.2. É proibida a utilização de equipamentos próprios do prestador conectados à rede da ToBusiness (+Qmarcas, let'smark & A+registros) sem a devida autorização escrita e acompanhamento presencial por parte da área de segurança da informação que, de igual modo,

deverá avaliar a necessidade através de justificativa técnica, onde, se necessário e indispensável tal acesso, isso deve ser feito por meio de uma rede própria e com um "*firewall*" dedicado para controlar os acessos de tais prestadores.

11.3.3. Caso o prestador utilize softwares próprios em equipamentos da organização, deve-se apresentar documentação ou termo de responsabilidade garantindo direito de uso, que será mantido enquanto o software estiver instalado.

11.4. Segurança Física de Computadores e Demais Equipamentos

11.4.1. O Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC), em conjunto com o responsável da área de Tecnologia da Informação deve garantir que os colaboradores e usuários dos computadores físicos da ToBusiness (+Qmarcas, let'smark & A+registros) utilizem os terminais de computadores, assim como notebooks, laptops, netbooks, ultrabooks, tablets e smartphones, de maneira segura, e que sejam tomadas medidas adequadas para respeitar a confidencialidade, integridade e disponibilidade das informações que são armazenadas e manipuladas através desses equipamentos.

11.4.2. Os meios de armazenamento considerados como mídias removíveis devem ter o acesso controlado; e quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

11.4.3. Os computadores e demais equipamentos não ligados a uma rede, e que contenham informações importantes para os negócios da empresa, devem estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

11.4.4. Os usuários ligados a uma rede, e que tratam com informações importantes para os negócios da empresa, devem manter estas informações armazenadas nos servidores de rede.

11.4.5. O Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC) é responsável por elaborar e manter atualizado o inventário de hardware e software da ToBusiness (+Qmarcas, let'smark & A+registros) e suas divisões.

11.4.6. É proibida a utilização de qualquer equipamento particular, exceto smartphones, nas dependências das Instituições do Conglomerado.

11.4.7. É expressamente vedada a aquisição, reprodução, utilização e cessão de cópias não autorizadas de softwares ou de quaisquer programas e produtos, mesmo aqueles desenvolvidos pelas áreas técnicas do Conglomerado ou desenvolvidos por terceiros para o Grupo.

11.5. Segurança Física dos Servidores de Rede e Sistemas de Armazenamento de Dados

11.5.1. O Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC), em conjunto com o responsável da área de Tecnologia da Informação, deve garantir que a ToBusiness administre e

utilize os diversos sistemas operacionais, incluindo os servidores de rede e os sistemas de backup de maneira segura, tanto de forma operacional como contingencial, e que sejam tomadas medidas adequadas para garantir a confidencialidade de seus dados, a integridade e disponibilidade dos equipamentos e meios de armazenamento de dados.

11.5.2. As mídias removíveis de armazenamento devem ter acesso controlado, e quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

11.5.3. Os servidores de arquivos devem estar instalados em uma área que garanta a segurança física destes equipamentos incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

11.5.4. O Administrador Local da rede, quando existir, ou a Área de Tecnologia da Informação, é responsável por elaborar e manter atualizado o inventário de hardware e software; assim como por garantir o controle de acesso físico aos equipamentos.

11.5.5. Todas as redes que integram o grupo devem ser providas de uma sistema de firewall robusto e capaz de criar as barreiras necessárias contra os ataques externos.

11.5.6. Todos os terminais de computadores, inclusive notebooks, laptops, netbooks, ultrabooks, tablets e smartphones de uso interno, deve ser munidos de antivírus e antispyware capaz de proteger tais unidade e também a rede como um todo.

11.5.7. O Administrador Local da rede, quando existir, ou a Área de Tecnologia da Informação, visando administrar e utilizar os recursos de informática de maneira segura, tomando medidas adequadas que garantam recursos alternativos de processamento na eventualidade de perda dos dados, softwares ou sistemas, deve manter um sistema de backup redundante, de modo que os dados e informações importantes e sob sigilo e responsabilidade da ToBusiness, estejam armazenados em pelo menos dois backup's distintos.

11.5.8. O sistema de backup deverá levar em consideração o períodos de atualização dos dados e as particularidades de cada setor ou operação do gruo.

11.5.9. As informações consideradas imprescindíveis devem estar presentes nas rotinas de backups, levando-se em consideração a periodicidade de atualização dos dados.

11.5.10. As cópias de backup devem estar guardadas em local apropriado e seguro, e protegidas contra o acesso por pessoas não autorizadas.

11.5.11. Quando o prazo de retenção das cópias de backup's forem superiores ao especificado pelo fabricante para utilização do meio de armazenamento, deve-se adotar um procedimento para regravação dos dados em novo meio, periodicamente.

11.5.12. É de responsabilidade do administrador local da rede ou do responsável pela área de tecnologia da informação, manter e garantir a execução dos procedimentos de backup.

11.6. Controle Contra Pirataria

11.6.1. O Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC), em conjunto com o responsável da área de Tecnologia da Informação deve garantir que sejam tomadas as medidas adequadas para coibir a pirataria de softwares dentro das instalações do grupo e em relação à todos os usuários e administradores de servidores de redes ou computadores, inclusive portáteis, conectados ou não a uma rede.

11.6.2. A quantidade de licenças de softwares não pode ser inferior à quantidade de softwares instalados, mesmo que para fins de testes ou treinamentos, a não ser que esta situação esteja coberta contratualmente.

11.6.3. Não é permitido duplicar, replicar ou copiar software de propriedade da ToBusiness (+Qmarcas, let'smark & A+registros), a não ser com a finalidade de cópia de segurança e mesmo assim, somente por pessoas autorizadas.

11.6.3. As licenças de uso de softwares da ToBusiness (+Qmarcas, let'smark & A+registros) só pode ser instalada em computadores do próprio grupo.

11.6.4. Não é permitido executar ou instalar qualquer software (inclusive software livre e de domínio público), telas de "screen saver", “papéis de parede” etc., que não estejam autorizados para uso das empresas da ToBusiness.

11.6.5. Todo software de demonstração deve vir acompanhado de uma autorização formal da empresa proprietária, indicando onde pode ser instalado e por quanto tempo.

11.6.6. A utilização de software do tipo “shareware” só deve ser feita após a obtenção do registro junto ao autor e após homologação pelo Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC) em conjunto com o responsável da área de Tecnologia da Informação.

11.6.7. É proibida a utilização e reprodução não autorizada de manuais, livros, revistas, periódicos protegidos por direitos autorais.

11.6.8. É da responsabilidade do Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC), em conjunto com o responsável da área de Tecnologia da Informação, verificar se o software a ser instalado é original, conferindo o mesmo com as devidas licenças de uso e se a instalação foi devidamente autorizada; assim como é responsável ainda por implementar mecanismos que dificultem a pirataria através de qualquer meio.

11.7. Controle de Acesso à Internet

11.7.1. A Internet abrange vários aspectos e serviços (websites de serviços de parceiros, fornecedores, entidades governamentais, prestadores de serviço e outros) que devem ser disponibilizados de forma restrita ou controlados conforme as necessidades de negócio.

11.7.2. A restrição a websites não relativos aos negócios da organização deve ser implementada, garantindo o uso efetivo da rede de Internet.

11.7.3. O acesso à Internet deve ser rastreado a fim de permitir o monitoramento do uso indevido da tecnologia (Nome do usuário e endereço acessado são informações obrigatórias no rastreamento).

11.7.4. O usuário deve restringir o acesso aos websites ainda não bloqueados que possam denegrir a imagem da organização (por exemplo: pornografia, pedofilia, racismo etc.) e que não têm relação com os objetivos de negócio da organização (Webmail, jogos etc.).

11.7.5. O usuário deve também comunicar o endereço eletrônico desses websites à área de Segurança da Informação, que deverá realizar seu imediato bloqueio.

11.7.6. O acesso à Internet deve ser feito através de "Servidores de Acesso" protegidos por sistemas de Firewall.

11.7.7. Quando for necessário o acesso utilizando uma segunda conexão através de modem ou rede wi-fi, a configuração da máquina deve garantir o isolamento da rede normal de serviço da empresa, evitando assim que uma contaminação seja propagada.

11.7.8. Os requisitos de segurança destas máquinas em particular, sobretudo no que diz respeito a antivírus e firewall local, devem ser respeitados.

11.7.9. A **ToBusiness**, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

11.7.10. A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

11.7.11. Como é do interesse da **ToBusiness** (+Qmarcas, let'smark & A+registros) que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

11.7.12. Somente os colaboradores que estão devidamente autorizados a falar em nome da **ToBusiness** ou suas divisões para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

11.7.13. Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

11.7.14. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

11.7.15. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na **ToBusiness** e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC).

11.7.16. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de Sistemas.

11.7.17. Os colaboradores não poderão em hipótese alguma utilizar os recursos da **ToBusiness** (+Qmarcas, let'smark & A+registros) para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

11.7.18. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos.

11.7.19. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

11.7.20. Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à **ToBusiness** ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

11.7.21. Os colaboradores não poderão utilizar os recursos da **ToBusiness** (+Qmarcas, let'smark & A+registros) para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de tróia, spam, assédio, perturbação ou programas de controle de outros computadores.

11.7.22. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente ao responsável pela área de Tecnologia da Informação.

11.7.23. Não é permitido acesso a sites de proxy.

11.8. Acesso ao Correio Eletrônico e Aplicativos de Mensagens

11.8.1. A ToBusiness disponibiliza aos seus funcionários a tecnologia necessária a fim de facilitar a comunicação interna, comunicação com clientes, fornecedores e outros grupos que tenham relação comercial com a mesma.

11.8.2. É de responsabilidade do usuário a utilização da tecnologia de forma adequada, prudente, e de modo compatível com as leis e princípios aplicáveis aos negócios.

11.8.3. As mensagens de correio eletrônico, a fim de que sejam monitoradas para identificar o uso indevido da tecnologia, devem ser rastreadas, atender à esta política de segurança e permitir o respectivo monitoramento.

11.8.4. As mensagens de correio eletrônico institucionais devem trazer as informações sobre privacidade da informação (as quais devem ser preservadas).

11.8.5. O uso do correio eletrônico e mensagens de aplicativos da ToBusiness (+Qmarcas, let'smark & A+registros) é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição.

11.8.6. A utilização desses serviços para fins pessoais é permitida desde que feita com bom senso, não prejudique o grupo e também não cause impacto no tráfego da rede.

11.8.7. Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da ToBusiness (+Qmarcas, let'smark & A+registros):

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a ToBusiness ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da ToBusiness (+Qmarcas, let'smark & A+registros) estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
    - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do grupo;
    - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
    - contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    - vise obter acesso não autorizado a outro computador, servidor ou rede;
    - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    - vise burlar qualquer sistema de segurança;
    - vise vigiar secretamente ou assediar outro usuário;
    - vise acessar informações confidenciais sem explícita autorização do proprietário;
    - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
    - inclua imagens criptografadas ou de qualquer forma mascaradas;
    - contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet);
    - tenha conteúdo considerado impróprio, obsceno ou ilegal;
    - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
    - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
    - tenha fins políticos locais ou do país (propaganda política);
    - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

11.8.8. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Gerência ou departamento
- Nome da empresa
- Telefone(s)
- Correio eletrônico

12. COMITÊ DE ÉTICA, PRIVACIDADE, SEGURANÇA E CONTROLE (CEPRISC)

12.1. O **Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC)**, a ser composto por 3 (três) integrantes da ToBusiness (+Qmarcas, let'smark & A+registros), é um órgão deliberativo, consultivo e opinativo, o qual tem poderes para emitir pareceres, investigar condutas internas e transgressões normativas, propor advertências, suspensões, demissões ou qualquer outro tipo de punição e, de outro lado, pode também propor o reconhecimento de atos e iniciativas.

12.2. Este órgão tem caráter permanente e seus membros são indicados pela Diretoria Executiva.

12.3. É vedado aos membros receber qualquer tipo de favorecimento ou acréscimo salarial por conta desta função, os quais também não contam com nenhum tipo de estabilidade de cargo, função ou emprego.

12.4. É um comitê que abrange a ética, conduta, privacidade, segurança da informação, Prevenção e Controle Antifraude, Anticorrupção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

12.5. A cada ano (no mês de janeiro), o Diretor Executivo da ToBusiness (+Qmarcas, let'smark & A+registros) deverá substituir um dos mesmos do deste comitê, por outro integrante do grupo, de modo que haja um revezamento anual.

12.6. Sua composição deve respeitar:

- Mandato por tempo determinado (3 anos para cada membro);
- Rodízio entre os membros (1 a cada ano);
- Representantes dos diversos públicos da ToBusiness (+Qmarcas, let'smark & A+registros) (1 de cada departamento);
- Natureza interdisciplinar.

12.7. As principais responsabilidades do Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC) são:

- Esclarecer dúvidas em relação aos princípios contidos no Código;
- Apoiar os gestores na interpretação e encaminhamento de soluções para situações que se configurem violações ao Código;
- Decidir sobre a conveniência ou não de presentes recebidos pelos funcionários e que eventualmente entenderem como suspeitos de anormalidades;
- Assegurar a avaliação das situações de descumprimento do Código recebidas através dos canais de denúncia e encaminhar as diligências cabíveis;
- Garantir o anonimato das denúncias que chegarem sob essas condições;
- Analisar qualquer situação fora dos padrões morais e éticos e eventualmente não previstas neste Código;
- Revisar o Código de Ética anualmente e atualizá-lo, sempre que necessário.

12.8. Além das competências indicadas e designadas em cada código e/ou política que integram a ToBusiness (+Qmarcas, let'smark & A+registros), este Comitê terá por função precípua zelar pela integridade e imagem desta organização, primando pelos preceitos que nos une e nos alinham diante de uma conduta proba, reta e cercada de orgulho por estar sempre de olho na ética, na privacidade e segurança dos dados e informação, assim como na prevenção e controle antifraude, anticorrupção e combate à lavagem de dinheiro e ao financiamento do terrorismo,

razão pela qual lhe compete ainda atualizar, ajustar e corrigir os seguintes dispositivos normativos:

A. Código de Ética e Conduta
B. Política de Privacidade
C. Política de Segurança da Informação
D. Política de Prevenção e Controle Antifraude, Anticorrupção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo

12.9. O **CEPriSC**, sempre que entender necessário, pode acionar a Assessoria de Imprensa da ToBusiness (+Qmarcas, let'smark & A+registros) a fim de lhe auxiliar na missão de mitigar eventuais crises externas, sanar dúvidas, fazer comunicados à imprensa e/ou aos clientes, parceiros e fornecedores.

12.10. ATRIBUIÇÕES ESPECÍFICAS DO COMITÊ DE ÉTICA, PRIVACIDADE, SEGURANÇA E CONTROLE (CEPriSC) DIANTE DA SEGURANÇA DOS DADOS E DA INFORMAÇÃO

12.10.1. Além de outras atribuições mencionadas na presente política de segurança da informação, são atribuições do CEPRISC, o qual deve:

- Garantir que a presente política de segurança da Informação não seja apenas conhecida, mas compreendida por todos os funcionários e colaboradores, conscientizando-os sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando houver incidentes de Segurança de forma a atingir uma melhor utilização e proteção à informação.
- Elaborar um processo de treinamento continuado contemplando todos os níveis funcionais do grupo;
- Divulgar os diversos materiais e alertas referente à Segurança da Informação para funcionários, colaboradores e clientes;
- Criar procedimentos de aferição do nível de conhecimento dos usuários em geral;
- Promover a organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos aspectos de segurança em geral;
- Realizar a revisão periódica dessa política de segurança da informação, adequando as ações às novas necessidades, evitando torná-lo repetitivo.
- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação do grupo.
- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio do grupo, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

- Manter comunicação efetiva com o o responsável pela área de tecnologia da informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a ToBusiness.
- Buscar alinhamento com as diretrizes corporativas da instituição.
- Deverá o CEPRISC 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 o grupo.
- O CEPRISC poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.
- O CEPRISC poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.
- Cabe ainda ao CEPRISC:
    - Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
    - Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
    - Avaliar os incidentes de segurança e propor ações corretivas;
    - Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

13. DAS RESPONSABILIDADES ESPECÍFICAS

13.1. Dos Colaboradores em Geral

13.1.1. 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 instituição.

13.1.2. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à ToBusiness (+Qmarcas, let'smark & A+registros) e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

13.2. Dos Colaboradores em Regime de Exceção (Temporários)

13.2.1. Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC).

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.

13.3. Dos Gestores de Pessoas e/ou Processos

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

13.3.2. 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 ToBusiness (+Qmarcas, let'smark & A+registros).

13.3.3. 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 ToBusiness (+Qmarcas, let'smark & A+registros).

13.3.4. 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.

13.3.5. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

13.4. Da Área de Tecnologia da Informação

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

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

13.4.3. 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.

13.4.4. 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.

13.4.5. 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.

13.4.6. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a ToBusiness.

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

13.4.8. 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.

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

13.4.10. 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:

- Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

13.4.11. 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.

13.4.12. 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.

13.4.13. 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.

13.4.14. Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

13.4.15. 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.

13.4.16. 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.

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

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos do grupo;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos do grupo;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- 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).

14. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

14.1. Para garantir as regras mencionadas nesta PSI, bem como de sua versão educacional, a ToBusiness e suas divisões (+Qmarcas, let'smark & A+registros) poderão:

A. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
B. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Ética, Privacidade, Segurança e Controle (CEPriSC);
C. Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
D. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

15. CANAIS DE RELACIONAMENTO COM O CLIENTE

15.1. Os canais eletrônicos de relacionamento com os clientes devem ser contemplados por:

- Linha direta como nº de telefone
- Nº de WhatsApp
- Formulário eletrônico disponibilizados nos sites da ToBusiness (+Qmarcas, let'smark & A+registros)

16. DISPOSIÇÕES GERAIS

16.1. Ao utilizarem nossos *websites*, você manifesta sua concordância com esta Política de Privacidade, que poderá ser alterada periodicamente. Se você não concordar com esta Política de Privacidade, não utilizem os nossos *websites* nem os serviços nele oferecidos.

16.2. A ToBusiness (+Qmarcas, let'smark & A+registros) reserva-se o direito de alterar esta Política de Privacidade, o que será avisado aos nossos usuários por meios razoáveis, inclusive através de e-mail para o endereço informado e/ou publicando a notificação e a política alterada nos nossos *website*.

16.3. A continuação do uso dos nossos serviços e dos nossos *websites* após as alterações da Política de Privacidade implica em dizer que você também aceita e concorda com as mudanças realizadas.

16.4. As informações coletadas ou fornecidas depois da atualização da Política de Privacidade serão regidas por esta última cláusula (8.3.).

17. CONCLUSÃO

17.1. Esperamos que, com esta Política de Privacidade, e com a disponibilização de nossos canais de comunicação, possamos juntos estabelecer uma relação comercial e de parceria sadias, profissionais, éticas, corteses e sem quaisquer tipos de desvios de condutas por parte de nenhum de nós ou dos nossos colaboradores.

17.2. E assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da ToBusiness (+Qmarcas, let'smark & A+registros). Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

Curitiba-PR, 30 de junho de 2023.

Missao Tanizaki Jr.
Diretor de Comunicação

ANEXO I

Modelo de Termo de Responsabilidade

Eu (Nome do Funcionário), código funcional Nº (número), CPF/MF Nº (número) declaro para os devidos fins e efeitos de direito que a(o) (Nome da Empresa) trouxe ao meu conhecimento o conteúdo das diretrizes, violações, normas e responsabilidades que regem sua Política de Segurança de Informação, que ora declaro ter lido, estando ciente e responsável pelo que segue:

1. Qualquer meio de acesso às informações ou instalações (como identificações de usuário, senhas, crachás, cartões, chaves, etc.) que a empresa me forneceu ou vier a fornecer são pessoais, intransferíveis, estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades perante o Conglomerado, devendo ser por mim devolvidos em caso de desligamento;

2. Todas as informações utilizadas no Conglomerado, sejam elas de sua propriedade ou de terceiros, possuem caráter confidencial e sigiloso, motivo pelo qual comprometo-me a manuseá-las de maneira segura e somente no exercício de minhas atividades, evitando sua perda, furto, cópia, utilização indevida ou divulgação não autorizada;

3. O Conglomerado está autorizado a consultar e analisar informações registradas em qualquer meio localizado em suas instalações e que tenham sido geradas ou recebidas utilizando seus recursos, inclusive correspondências recebidas em nome ou endereço da mesma;

4. Não devo adquirir, reproduzir, utilizar ou distribuir cópias não autorizadas ou legalmente adquiridas de softwares ou programas produtos, mesmo aqueles desenvolvidos internamente pelas áreas técnicas do Conglomerado;

5. Devo zelar pela segurança, uso correto e manutenção adequada dos equipamentos existentes no Conglomerado;

6. As informações por mim geradas ou recebidas durante minha jornada de trabalho deverão tratar apenas de assuntos profissionais e ligados exclusivamente ao exercício de minha função;

7. Descumprindo os compromissos por mim assumidos nesta declaração estarei sujeito as penalidades aplicáveis, como medidas administrativas/disciplinares internas e/ou ações penais/cíveis previstas em lei.

Curitiba-PR, data

Nome, CPF e Assinatura do Funcionário

ANEXO II

Modelo de Termo de Responsabilidade para Empresas Contratadas

As empresas prestadoras de serviço devem ser orientadas para que mantenham documento similar em seus arquivos, assinado pelos funcionários por ela contratados para prestar serviços ao ToBusiness (+Qmarcas, let'smark & A+registros), devendo o texto abaixo ser incluído nos contratos de prestação de serviço:

1. "Fica a Contratada, responsável pela orientação dos funcionários por ela indicados para trabalharem junto à contratante, no que diz respeito ao cumprimento das Políticas de Segurança da Informação da Contratante, cumprimento das Leis de Copyright e de Combate a Pirataria de Softwares.
2. Fica também a Contratada corresponsável pela utilização das senhas e uso das informações por parte dos funcionários por ela contratados e disponibilizados para atuação junto a Contratante, de acordo com o termo de responsabilidade assinado pelo funcionário da Contratada. Esta corresponsabilidade estende-se inclusive aos foros judiciais, sob todos os aspectos, inclusive o do direito das obrigações."

ANEXO III

Modelo de Termo de Confidencialidade

(Identificação e Qualificação) _____, por intermédio de seus representantes legais, doravante designada simplesmente RESPONSÁVEL, se compromete, por intermédio do presente TERMO DE CONFIDENCIALIDADE E NÃO DIVULGAÇÃO, a não divulgar, sem autorização, quaisquer informações de propriedade da ToBusiness **ToBusiness (+Qmarcas, let'smark & A+registros)** ou de qualquer de suas divisões, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA

O RESPONSÁVEL reconhece que tomou conhecimento de informações privadas da **ToBusiness (+Qmarcas, let'smark & A+registros)**, que podem e devem ser conceituadas como segredo de indústria ou de negócio.

Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios empregados da **ToBusiness (+Qmarcas, let'smark & A+registros)** e do RESPONSÁVEL, sem a expressa e escrita autorização do representante legal signatário do Contrato ora referido.

CLÁUSULA SEGUNDA

As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito da **ToBusiness (+Qmarcas, let'smark & A+registros)** e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Listagens e documentações com informações confidenciais, inclusive aquelas relativas ao sigilo bancário que o Banco do Nordeste deve observar, por imposição legal;
II. Documentos relativos a estratégias econômicas, financeiras, de investimentos, de captações de recursos, de marketing, de clientes e respectivas informações, armazenadas sob qualquer forma, inclusive informatizadas;
III. Metodologias, técnicas, processos, procedimentos, ferramentas, códigos fontes, softwares, relatórios e produtos e serviços, entre outros, desenvolvidos pela **ToBusiness** ou por ela mantido sob sua responsabilidade;
IV. Valores e informações de natureza operacional, financeira, administrativa, contábil e jurídica;
V. Outros documentos e informações porventura conhecidos durante a execução dos serviços.

CLÁUSULA TERCEIRA

O RESPONSÁVEL reconhece que as referências dos incisos da Cláusula Segunda deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham ser como tal definidas no futuro devem ser mantidas sob sigilo.

Em caso de dúvida acerca da natureza confidencial de determinada informação, o RESPONSÁVEL deverá mantê-la sob sigilo até que venha a ser autorizado expressamente pelo representante legal da **ToBusiness** a tratá-la diferentemente.

VI. Em hipótese alguma a ausência de manifestação expressa da ToBusiness (+Qmarcas, let'smark & A+registros) poderá ser interpretada como liberação e qualquer dos compromissos ora assumidos.

CLÁUSULA QUARTA

O RESPONSÁVEL recolherá, ao término do Contrato, para imediata devolução à ToBusiness, todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse seja de seus empregados, prepostos, prestadores de serviço seja de fornecedores, com vínculo empregatício ou eventual com o RESPONSÁVEL, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial a que teve acesso enquanto contratado pelo ToBusiness.

Parágrafo Único

O RESPONSÁVEL determinará a todos os seus empregados, prepostos e prestadores de serviço que estejam direta ou indiretamente envolvidos com a prestação de serviços objeto do Contrato, a observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA QUINTA

O RESPONSÁVEL obriga-se a informar imediatamente ao Banco do Nordeste qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

CLÁUSULA SEXTA

O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

CLÁUSULA SÉTIMA

As obrigações a que alude este instrumento perdurarão inclusive após a cessação do vínculo contratual entre o RESPONSÁVEL e o Banco do Nordeste e abrangem as informações presentes ou futuras.

CLÁUSULA OITAVA

O RESPONSÁVEL se compromete no âmbito do Contrato objeto do presente Termo, a apresentar ao ToBusiness declaração individual de adesão e aceitação das presentes cláusulas, de cada integrante ou participante da equipe que prestar ou vier a prestar os serviços especificados no Contrato.

Curitiba-PR, _____ de _____ de 20___.

DE ACORDO:

Nome e CPF