



Manual de Segurança da Informação do Grupo Benner

SUMÁRIO

1. OBJETIVO.....	3
2. CAMPO DE APLICAÇÃO.....	3
3. DEFINIÇÕES.....	3
4. PAPÉIS E RESPONSABILIDADES	4
5. DESCRIÇÃO	5
5.1. Gestão de Riscos	5
5.2. Classificação e Tratamento da Informação	5
5.3. Proteção de Dados	6
5.3.1. Acordos de Confidencialidade e Não Divulgação.....	6
5.3.2. Manuseio de Informações	6
5.3.3. Armazenamento de Arquivos	6
5.3.4. Impressão Segura	7
5.3.5. Criptografia	7
5.3.6. Mídias Externas e Dispositivos Móveis	8
5.3.7. Mesa e Tela Limpas	8
5.3.8. Devolução permanente ou disponibilização de equipamentos de TI para reparos externos	8
5.4. Gestão de Acessos.....	9
5.4.1. Acesso Físico	9
5.4.2. Acesso Lógico.....	10
5.5. Aquisição de Hardwares e Software.....	11
5.6. Uso Aceitável dos Ativos de TI.....	12
5.6.1. Diretrizes Gerais.....	12
5.6.2. Utilização dos Computadores.....	12
5.6.3. Controle de hardware e software adicionado aos computadores	13
5.6.4. Acesso remoto aos recursos de TI da Empresa	13
5.7. Equipamentos de Terceiros	14
5.8. Postura em Canais de Comunicação	14
5.9. Gestão da Continuidade de Negócios.....	16
5.10. Aquisição, desenvolvimento e manutenção de sistemas de informação	17
5.11. Registro e Tratamento de Eventos de Tecnologia da Informação.....	17
5.12. Monitoramento, Auditoria e Conformidade.....	18
5.13. Tratamento de Exceções	18
5.14. Responsabilidade por Conduta Inadequada.....	19
6. DOCUMENTOS DE REFERÊNCIA	19
7. CONSIDERAÇÕES FINAIS.....	20
8. REGISTRO DE ALTERAÇÕES	20
9. FORMALIZAÇÃO	20

1. OBJETIVO

Este Manual é o desdobramento e leva em conta as orientações da Política de Segurança da Informação (PSI). Tem como objetivo estabelecer as diretrizes gerais para proteção dos ativos de informação de propriedade do Grupo Benner e/ou sob sua custódia, definindo e monitorando a responsabilidade de todos os entes envolvidos.

2. CAMPO DE APLICAÇÃO

Aplicável a todos os colaboradores, próprios ou terceiros, que possuem ou possuíram acesso aos dados e/ou à infraestrutura tecnológica do **Grupo Benner***.

* Denominação utilizada para designar as empresas: Benner Sistemas S.A., Benner Tecnologia e Sistemas em Saúde Ltda., Benner Tecnologia e Serviços em Saúde Ltda., Itessa Tecnologia e Serviços S/A, Otto HX Tecnologia e Sistemas Ltda.

3. DEFINIÇÕES

Ameaça: Um conjunto de circunstâncias que têm o potencial de causar uma quebra em um ou mais requisitos de segurança da informação.

Ativos de Informação: Toda e qualquer pessoa, processo, tecnologia ou ambiente que manipule, processe, armazene, transporte, transmita e descarte informações corporativas.

Autenticidade: É um processo em que se estabelece a validade de uma mensagem, transação, indivíduo ou identidade. Normalmente obtida por meio de mecanismos de autenticação ou por utilização de certificados digitais.

Canais de Comunicação: Veículos e/ou ferramentas utilizados para transmitir mensagens, conteúdos e comunicações, tanto dentro quanto fora da Empresa.

Computador: Todo equipamento que possua dispositivos de processamento e armazenamento de dados e conexão à rede e/ou internet, tais como: servidores, estações de trabalho (desktops), notebooks, tablets e smartphones.

Confidencialidade: Propriedade de que a informação não esteja disponível ou seja revelada a indivíduos, entidades ou processos não autorizados. Somente as partes autorizadas acessam determinado ativo de informação.

Disponibilidade: Propriedade que garante a acessibilidade e usabilidade da informação para quem esteja autorizado. Os ativos são acessíveis às partes autorizadas nos momentos apropriados.

Dispositivos móveis: Equipamentos que, devido às suas dimensões reduzidas, podem também ser utilizados pelo colaborador fora do ambiente empresarial.

Grupos de Informação: Conjuntos de informações inerentes a um processo de negócio que precisam ser identificados e classificados de acordo com o seu grau de sigilo e de sensibilidade.

Integridade: Propriedade que garante a exatidão e completude na origem, no trânsito e no destino da informação. Ativos podem ser modificados somente pelas partes autorizadas e somente das formas autorizadas.

Incidente de Segurança da Informação: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação ou rede de computadores, que acarretam a perda de um ou mais princípios básicos de Segurança da Informação: Autenticidade, Confidencialidade, Disponibilidade, Integridade ou Irrefutabilidade.

Irrefutabilidade: Propriedade que garante o não repúdio (ou negação da autoria) de uma transação. As partes envolvidas em uma transação são capazes de provar, posteriormente, o evento ocorrido.

Recurso de TI: Todo hardware, software, infraestrutura de rede e internet disponibilizados pelo Grupo Benner aos seus colaboradores, para desempenho das atividades a que foram designados.

Risco: É a probabilidade de ocorrência de um evento e seus impactos resultantes. Riscos de TI são aqueles associados ao uso, gerenciamento, operação, suporte, inovação, influência ou adoção das soluções de TI para realizar as atividades de negócios da organização.

Segurança da Informação (SI): Preservação da confidencialidade, integridade e disponibilidade da informação; desta forma contribuindo para a continuidade do negócio. Outras propriedades, tais como autenticidade e irrefutabilidade, podem também estar envolvidas.

Siscon: Sistema utilizado para registro e atendimento de chamados relativos à infraestrutura de TI do Grupo Benner. Acessível por meio do endereço: <https://siscon.benner.com.br/>.

Sigilo: Propriedade que garante a não divulgação da informação a indivíduos, entidades ou processos não autorizados. Similar à Confidencialidade.

TCOM - Termo de Compromisso, no qual o colaborador se compromete a seguir as normas e diretrizes de segurança da informação definidas pela Empresa.

Vulnerabilidade: Fragilidade (interna) de um ativo ou grupo de ativos de informação, que pode ser explorada por uma ou mais ameaças (externas), gerando uma falha de segurança.

4. PAPÉIS E RESPONSABILIDADES

Definições dos papéis, atividades e responsabilidades no contexto de segurança da informação estão detalhadas na Seção 6. (Papéis e Responsabilidades) da PSI - Política de Segurança da Informação.

5. DESCRIÇÃO

As diretrizes de segurança da informação estão divididas em:

- **Diretrizes gerais (S):** são as diretrizes padrão (standard) de segurança da informação. Compreendem os requisitos mínimos que devem ser observados por todos os colaboradores.
- **Diretrizes específicas (P):** constituem o modo protegido de segurança da informação, cujos requisitos devem ser observados em determinadas áreas ou para determinados ativos da informação. Requerem um nível mais elevado de proteção.

É importante mencionar que, tendo em vista a priorização e a maturidade dos processos relacionados, alguns itens descritos neste documento podem estar ainda em fase de planejamento ou desenvolvimento.

5.1. Gestão de Riscos

A gestão de riscos é uma atividade contínua e sistemática dentro da Gerência de Tecnologia da Informação. Tem como objetivo identificar e responder adequadamente às ameaças e vulnerabilidades que possam comprometer a segurança dos ativos de informação.

Os riscos a que estão sujeitos os ativos de informação devem ser avaliados criteriosamente, de forma a reduzir a probabilidade e/ou o impacto de interrupções nos sistemas que suportam os processos de negócio do Grupo Benner.

Para que os riscos possam receber adequada identificação, avaliação e tratativa, os colaboradores devem informar previamente à Gerência de TI a respeito de quaisquer modificações nos ativos de informação existentes, e ainda a respeito de projetos que incluirão novos ativos de informação no ambiente corporativo.

Cabe à Gerência de TI as atividades relativas à gestão dos riscos percebidos na operação (continuidade); modificação (mudanças) e inclusão (projetos) de recursos de TI.

5.2. Classificação e Tratamento da Informação

Toda informação produzida ou recebida pelos colaboradores como resultado de sua atividade profissional pertence ao Grupo Benner. As exceções devem ser explícitas e formalizadas por meio de contrato ou instrumento similar, firmado entre as partes envolvidas.

As informações de propriedade do Grupo Benner ou sob a sua custódia devem ser devidamente classificadas e receberem o tratamento adequado, de acordo com as diretrizes e procedimentos de classificação e tratamento da informação.

5.3. Proteção de Dados

Os Colaboradores devem proteger os dados e informações do Grupo Benner e de seus clientes contra acessos, modificações, destruição ou divulgação não autorizada pelo Grupo Benner.

5.3.1. Acordos de Confidencialidade e Não Divulgação

O colaborador assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções, mesmo depois de terminado o vínculo contratual mantido com a empresa.

É vedado aos colaboradores copiar e/ou distribuir informações de propriedade de clientes ou outros parceiros comerciais. A transferência e/ou a divulgação de qualquer software, base de dados, programas ou arquivos-fonte para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada mediante autorização formal, com a devida identificação do solicitante e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

5.3.2. Manuseio de Informações

Quaisquer alterações ou exclusões executadas em sistemas, diretórios de rede, aplicações, bancos de dados ou códigos-fonte, que não tenham sido expressamente autorizadas, poderão gerar responsabilidade civil e penal, nos termos da legislação vigente.

Quando autorizadas, a utilização, cópia, manuseio, transferência, armazenamento e descarte de ativos de informação do Grupo Benner devem respeitar as diretrizes e procedimentos de classificação e tratamento da informação.

5.3.3. Armazenamento de Arquivos

Arquivos pessoais e/ou não pertinentes ao negócio (fotos, músicas, vídeos etc.) não deverão ser copiados ou movidos para os diretórios de rede, pois podem infringir regras de proteção de dados pessoais, propriedade ou licenciamento. Caso seja identificada a existência desses arquivos, eles serão excluídos de forma definitiva e sem a necessidade de autorização. Ainda assim, tanto o colaborador responsável quanto o seu Gestor Imediato poderão ser notificados.

É proibido o uso ou a guarda de arquivos e programas obtidos ilegalmente, constituindo-se crime previsto na legislação vigente. No caso de penalidade imposta por decisão administrativa ou judicial, as despesas daí decorrentes serão de responsabilidade da área da empresa onde ocorrer a infração.

Os arquivos corporativos, gerados pelas áreas usuárias, devem ser armazenados nos servidores da rede de dados. Sempre que possível, a criptografia deve ser utilizada, como meio adicional de proteção de dados sensíveis ou confidenciais.

Os documentos e arquivos digitais armazenados em estações de trabalho, notebooks, smartphones e outros dispositivos móveis devem ser transferidos o quanto antes para o local apropriado, de acordo com as diretrizes de armazenamento definidos no esquema de classificação da informação. Esta medida é importante para assegurar os níveis de proteção e disponibilidade adequados para os ativos de informação do Grupo Benner, uma vez que não existem meios disponíveis para recuperação dos dados mantidos somente no disco rígido dos computadores. É importante enfatizar que a perda de dados e informações corporativas devido à inobservância das diretrizes de armazenamento constitui uma violação da Política e demais normas de Segurança da Informação.

Os usuários – excetuando-se os que tenham autorização específica para esse fim, em razão de seu perfil ou função – não podem permitir ou causar qualquer alteração e/ou destruição de sistemas operacionais, dados ou documentos de propriedade ou sob custódia do Grupo Benner.

As pastas públicas (ou similares) não deverão ser utilizadas para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza específica. Devem ser utilizadas somente para armazenar informações de interesse geral, as quais serão periodicamente removidas, para que não haja acúmulo desnecessário de informações.

Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que possam comprometer o desempenho e funcionamento dos sistemas.

Cabe à área de TI definir e manter as estratégias de cópias de segurança (“backup”) das informações armazenadas nos diretórios da rede corporativa, nas aplicações corporativas e nos sistemas de informação utilizados no Grupo Benner. Cabe ao Gestor Imediato definir as diretrizes de disponibilidade e proteção das informações produzidas e manipuladas no departamento sob sua responsabilidade, incluindo aquelas que forem geradas ou alteradas por meio de trabalho remoto, fora das dependências da empresa.

É proibido armazenar informações da Empresa em sites de armazenamento em nuvem pública, tais como: Google Drive e DropBox, entre outros, salvo aplicações que compõem a suíte Microsoft 365 (OneDrive), disponibilizada pelo Grupo Benner.

5.3.4. Impressão Segura

A Gerência de TI é responsável por definir e implantar mecanismos de impressão segura, de modo a preservar a confidencialidade dos documentos impressos.

5.3.5. Criptografia

A criptografia de disco rígido será aplicada a todos os notebooks do Grupo Benner, podendo ser estendida aos desktops que forem identificados como protegidos. Essa medida visa proteger os dados armazenados nos equipamentos contra o acesso não autorizado, em caso de perda ou roubo do dispositivo.

5.3.6. Mídias Externas e Dispositivos Móveis

As mídias externas de armazenamento (tais como: *pen drive* e HD externo) e os dispositivos móveis (tais como *notebooks*, *smartphones* e *tablets*) somente poderão ser utilizados e conectados ao ambiente corporativo caso tenham sido configurados e disponibilizados pela área de TI do Grupo Benner.

Fica expressamente proibida a utilização de mídias externas e dispositivos móveis particulares para o desenvolvimento das atividades profissionais, bem como a cópia e/ou transferência de informações ou dados de propriedade do Grupo Benner para estes dispositivos.

5.3.7. Mesa e Tela Limpas

Nos escritórios e demais áreas de trabalho dentro e fora da empresa, os colaboradores devem adotar a política de mesa e tela limpas, de forma a evitar que mídias e documentos contendo informações confidenciais ou restritas fiquem expostos para pessoas não autorizadas, nas mesas ou nas telas dos computadores.

É expressamente proibido o consumo de alimentos, bebidas ou manuseio de substâncias nas estações de trabalho e/ou próximo aos equipamentos.

Antes de ausentar-se do seu local de trabalho, o usuário deverá certificar-se de proteger os sistemas, dados e informações contra o acesso de pessoas não autorizadas. Para isso, deve adotar uma das seguintes medidas: fechar todos os programas em uso, efetuar o logout/logoff da rede ou bloquear o computador através de senha.

Ao utilizar as salas de reunião na Empresa, o colaborador deve assegurar que todo o material, documentos e equipamentos foram recolhidos. As anotações feitas nos quadros e/ou *flipcharts* devem ser apagadas ou recolhidas ao término da reunião.

5.3.8. Devolução permanente ou disponibilização de equipamentos de TI para reparos externos

Os equipamentos de TI a serem devolvidos de forma permanente ou disponibilizados para reparos externos devem obedecer às seguintes regras:

Cabe ao Colaborador assegurar que todos os arquivos e dados da Empresa foram transferidos para o local apropriado de armazenamento, antes de entregá-lo à Gerência de TI. Além disso, o usuário deve assegurar que eventuais arquivos pessoais foram removidos dos equipamentos e dispositivos.

Em seguida, colaborador deve entregar o equipamento à Gerência de TI, para que sejam tomadas as providências necessárias e a atualização do inventário de ativos de TI.

Cabe à Gerência de TI providenciar a completa eliminação de todas as informações, utilizando ferramentas de deleção permanente, para evitar que eventuais dados (da empresa e/ou do colaborador) armazenados nos equipamentos sejam recuperados ou utilizados de forma indevida por terceiros.

5.4. Gestão de Acessos

Somente Colaboradores autorizados no exercício de suas funções ou cujas atividades estejam formalizadas em contrato poderão ter acesso às informações de propriedade ou sob custódia do Grupo Benner.

O acesso físico às dependências do Grupo Benner é absolutamente restrito aos Colaboradores e Visitantes autorizados.

Os Colaboradores possuem uma identificação única, pessoal e intransferível, que permite a sua identificação física e virtual no Grupo Benner. Quaisquer senhas, dispositivos de acesso ou meios de identificação deverão ser mantidos em sigilo e protegidos pelo Colaborador, sendo terminantemente proibido o seu compartilhamento com terceiros.

Havendo qualquer suspeita de acesso indevido por terceiros às credenciais de acesso (físico ou lógico), o Colaborador deverá registrar imediatamente um chamado no sistema Sicon.

5.4.1. Acesso Físico

Os Colaboradores são responsáveis por adotar medidas de segurança no uso de seus objetos, dispositivos e mecanismos, com o objetivo de prevenir o acesso de pessoas não autorizadas às dependências da empresa, especialmente em garagens e ambientes restritos.

Visitantes: A identificação e o controle de acesso de terceiros às dependências do Grupo Benner somente serão realizados mediante autorização de um Colaborador interno, (anfitrião), o qual será responsável pelo visitante durante a sua permanência na Empresa.

Proteção adicional de ativos de informação: Cabe ao gestor do processo de negócio identificar os ativos de informação sob sua responsabilidade que requerem um nível diferenciado de proteção. Se necessário, medidas adicionais devem ser providenciadas pelas áreas envolvidas para garantir adequado nível de proteção física destes ativos.

Áreas restritas: As instalações de processamento da informação (datacenter) e os locais onde ativos de informação estão armazenados de forma permanente ou provisória terão acesso restrito e controlado pela Gerência de TI. Solicitações de acesso a estas áreas restritas deverão ser aprovadas pelo nível gerencial na área solicitante e pelo Gestor da área de TI.

Será mantida uma lista de colaboradores que possuem permissão de acesso às áreas restritas da TI, a qual deverá ser periodicamente revisada e aprovada pelo Gerente de Tecnologia da Informação.

No caso de desligamento de usuários que possuam acesso a áreas restritas, as permissões de acesso deverão ser bloqueadas imediatamente nos sistemas de controle, bem como a atualização da lista de usuários autorizados.

Prestadores de serviços e outros colaboradores que não constem na lista de autorizados deverão estar acompanhados por um colaborador autorizado durante todo o tempo em que permanecerem nas áreas restritas.

É proibido o consumo de alimentos ou bebidas, ou armazenamento de materiais não pertinentes – ainda que de forma temporária – dentro das áreas restritas da TI.

Todo e qualquer acesso às áreas restritas da TI será registrado por meio de sistema específico de controle de acesso. O acesso por outros meios somente poderá ocorrer em casos de indisponibilidade do sistema específico, para os quais deverá haver um registro de incidente relacionado à falha no dispositivo de segurança.

5.4.2. Acesso Lógico

Registro e aprovações: O acesso às bases de dados, aplicações e/ou sistemas de informação de propriedade ou sob custódia do Grupo Benner somente será atendido pela área de TI mediante registro da solicitação, contendo as devidas aprovações. Dependendo do ativo em questão, poderá ser requerida a aprovação do Gestor responsável pela aplicação, além do Gestor Imediato do Colaborador.

O acesso aos recursos de TI da Empresa deve estar vinculado à assinatura do TCOM - Termo de Compromisso, no qual o colaborador se compromete a seguir as normas e diretrizes de segurança da informação definidas pela Empresa.

Condições de uso: As credenciais de acesso à rede corporativa e aos demais sistemas de informação utilizados no Grupo Benner – compostas pela identificação do usuário e a senha de acesso - são pessoais, intransferíveis e de uso exclusivo do Colaborador, que assume integral responsabilidade por sua guarda e sigilo.

É expressamente proibido utilizar as credenciais de acesso para as seguintes finalidades:

- a) compartilhar com terceiros as credenciais de acesso aos sistemas;
- b) utilizar credenciais de terceiros para acessar diretórios, arquivos ou sistemas;
- c) tentar transpor os mecanismos de autenticação da rede e dos sistemas de informação;
- d) tentar interferir no funcionamento dos serviços de rede, das aplicações e dos sistemas de informação, utilizando quaisquer mecanismos ou dispositivos não autorizados.

Usuários genéricos e/ou temporários: Solicitações para criação de usuários genéricos ou temporários deverão ser justificados pela área requisitante e aprovados pela Gerência de TI. Quando necessário, o Comitê de Segurança da Informação e Privacidade (CSIP) poderá ser acionado.

Controles de autenticação: Para os acessos realizados mediante autenticação de código de usuário e senha, a Gerência de TI implantará mecanismos para assegurar a complexidade e prazo de expiração das credenciais de acesso.

Controle de acesso lógico: Os eventos que podem ter impacto na rotina normal dos colaboradores, tais como: afastamentos por período igual ou superior a 15 dias, licenças prolongadas, alterações contratuais, desligamentos, entre outros, deverão ser comunicados à Gerência de TI para que as medidas necessárias sejam providenciadas.

Segregação de funções: Sempre que possível, as atividades de um processo serão divididas entre os usuários, como medida de prevenção de erros ou fraudes nas transações de negócio e nas atividades de

administração do ambiente de TI. A segregação das funções tem o objetivo de preservar a integridade e a autenticidade das transações realizadas no ambiente corporativo.

Acesso privilegiado: A Gerência de TI é responsável por controlar todo acesso aos recursos de TI do Grupo Benner, inclusive o acesso privilegiado. Tal acesso é concedido aos colaboradores que realizam a função de administração de sistemas operacionais, bancos de dados, ativos de rede e aplicações de negócio. Também envolve usuários que acessam utilitários e programas que podem se sobrepor aos controles de segurança existentes.

As credenciais para acesso privilegiado deverão ser diferentes das utilizadas pelo usuário para os recursos comuns de TI. Será mantida uma lista de usuários com acesso privilegiado, a qual deverá ser periodicamente revisada.

Princípio de mínimo privilégio: Com exceção dos usuários com permissão de acesso privilegiado, o acesso à rede, às aplicações e aos sistemas de informação da Empresa deve estar baseado no princípio de mínimo privilégio. Dessa forma, os acessos concedidos estarão restritos às informações e transações necessárias para execução das tarefas sob responsabilidade do Colaborador. Eventuais perfis de substitutos devem ser atribuídos de acordo com a necessidade e somente pelo período necessário para substituição do titular.

Com o objetivo de mitigar o risco de instalações indevidas e/ou não autorizadas, não será concedido privilégio de administração local aos usuários dos computadores. Exceções, quando justificáveis, deverão ser aprovadas pelo Gestor da área solicitante e pela Gerência de TI.

Acesso de terceiros: O acesso de terceiros à rede corporativa e/ou a sistemas de informação da Empresa deve ser solicitado somente para os casos em que a sua utilização seja indispensável. As solicitações devem ser aprovadas pelo gestor responsável pelo respectivo contrato e validado pela Gerência de TI. Cabe ao gestor do contrato informar à Gerência de TI sobre quaisquer modificações contratuais junto aos prestadores de serviço, incluindo as alterações na lista de colaboradores que acessam ativos de informação da Empresa, para garantir que as listas de acesso estejam atualizadas. Neste contexto, é importante levar em consideração tanto os recursos de TI que são acessados remotamente quanto aqueles que são acessados nas dependências da Empresa, por colaboradores das empresas prestadoras de serviço.

5.5. Aquisição de Hardwares e Software

Para garantir que as aquisições estejam aderentes aos padrões definidos pela Empresa, os colaboradores devem encaminhar à Gerência de TI todas as solicitações de aquisição de hardware e software, detalhando os requisitos funcionais necessários à adequada utilização desses ativos.

Cabe à Gerência de TI avaliar os requisitos funcionais necessários às áreas de negócio, em conjunto com os requisitos da infraestrutura de TI e de segurança da informação.

As especificações técnicas devem ser elaboradas pela Gerência de TI, visando otimizar as demandas do negócio e assegurar que as aquisições estejam em conformidade com normas internas e regulamentos externos.

Todas as aquisições devem ser aprovadas por nível gerencial compatível com o valor do investimento, seguindo os níveis de alçada definidos pela Empresa.

5.6. Uso Aceitável dos Ativos de TI

O Grupo Benner utiliza apenas equipamentos e softwares devidamente homologados, em conformidade com a legislação vigente e com as diretrizes internas definidas nas normas e políticas relacionadas.

5.6.1. Diretrizes Gerais

Os recursos de TI, incluindo equipamentos, computadores, programas, sistemas e softwares são disponibilizados pelo Grupo Benner como ferramentas para uso em atividades relacionadas ao trabalho. Todo colaborador deve utilizá-los e manuseá-los corretamente e cumprir as recomendações que constam neste manual, na Política de Segurança da Informação e nas demais normas e procedimentos aplicáveis.

Registros de uso (logs) da internet, rede, e-mail e demais sistemas de informação utilizados na Empresa são mantidos pela Gerência de TI. Visando à proteção dos ativos de informação da Empresa, a Gerência de TI pode bloquear ou desativar qualquer dispositivo, arquivo, site, correio eletrônico, domínio ou aplicação, estejam eles no computador do usuário ou na rede corporativa.

Os computadores fornecidos pela Empresa aos seus colaboradores devem possuir mecanismos de bloqueio automático e proteção de tela. Devem também ser providos de ferramentas de segurança da informação definidas e homologadas pela Gerência de TI, tais como: credenciais de acesso, diretivas de segurança, softwares de antivírus, firewall, registro de eventos (log), dentre outras, que devem estar permanentemente habilitadas e atualizadas.

As ferramentas de segurança da informação não poderão ser substituídas, desabilitadas ou removidas pelo usuário; quaisquer alterações em seu funcionamento devem ser reportadas à Gerência de TI por meio da abertura de um chamado no sistema Sicon.

Toda tentativa não autorizada de modificação dos parâmetros de segurança ou violação no funcionamento de qualquer recurso de TI fornecido pela Empresa será classificada como conduta inadequada e tratada como tal.

5.6.2. Utilização dos Computadores

É responsabilidade de cada Colaborador zelar pela segurança e integridade física dos computadores que lhe forem disponibilizados pela Empresa. Para isso, deve observar as orientações fornecidas pela Gerência de TI para uso adequado e seguro dos equipamentos.

Além das ferramentas e mecanismos de proteção, tais como antivírus, firewalls etc., todos os usuários são também responsáveis pela segurança da informação. Sendo assim, havendo suspeitas de que uma determinada mensagem ou anexo possam estar contaminados por código malicioso, estes deverão ser imediatamente eliminados.

Casos comprovados de uso inadequado ou inobservância das normas de proteção dos equipamentos poderá sujeitar o usuário ao ressarcimento de eventuais prejuízos.

A concessão de dispositivos móveis (tais como: *notebooks*, *smartphones* e *tablets*) aos colaboradores deve atender a ambos os critérios de necessidade e pertinência. O uso desses dispositivos móveis fornecidos pela Empresa deve ser justificado pelo Gestor da área solicitante e conter as aprovações definidas de acordo com as normas vigentes.

Os colaboradores não podem conectar os computadores da Empresa na rede de Visitantes, tendo em vista que esta rede tem a finalidade de conectar somente equipamentos de terceiros à internet.

5.6.3. Controle de hardware e software adicionado aos computadores

A gestão dos recursos de TI de propriedade da Empresa é de responsabilidade **da Gerência de TI**. Somente os recursos de TI registrados e homologados podem ser utilizados no ambiente computacional da Empresa. Não é permitido ao usuário final realizar modificações no hardware ou software dos recursos de TI que lhe forem fornecidos pela Empresa.

Somente softwares avaliados e homologados pela Gerência de TI podem ser instalados e utilizados nos computadores da Empresa. Qualquer necessidade de utilização de software ou aplicação, mesmo que gratuitos, deve ser solicitada à Gerência de TI, para que sejam avaliados os riscos e a aderência à política de segurança da informação.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares externos (mesmo os gratuitos), de conteúdos protegidos por direito autoral (DVDs, filmes, músicas) ou de aplicações desenvolvidas internamente são expressamente proibidos. Instalações indevidas detectadas nos computadores da Empresa poderão ser excluídas pela Gerência de TI sem a necessidade de prévia notificação. Ainda assim, o Gestor imediato do Colaborador poderá ser notificado.

5.6.4. Acesso remoto aos recursos de TI da Empresa

Quaisquer necessidades de acesso remoto aos recursos de TI da Empresa devem ser solicitadas à Gerência de TI, devidamente aprovadas pelo Gestor da área solicitante. A Gerência de TI providenciará a concessão de dispositivos móveis, ou ainda a instalação e configuração de aplicações adicionais para garantir a segurança em conexões externas.

Os colaboradores autorizados a utilizarem dispositivos móveis e/ou acesso remoto das aplicações deverão cumprir rigorosamente todas as regras e diretrizes estabelecidas neste Manual, nas demais normas e procedimentos aplicáveis.

Na qualidade de proprietária dos dispositivos móveis eventualmente fornecidos aos colaboradores, a Empresa reserva-se o direito de inspecioná-los a qualquer tempo, além de realizar intervenções de segurança, sempre que forem necessárias.

É importante ressaltar que a utilização dos recursos de TI por meio de acesso remoto, de acesso web, de dispositivos móveis, dentre outros, é uma concessão da Empresa para facilitar o trabalho de seus Colaboradores. A eventual disponibilidade de acesso não implica na obrigação de sua utilização por parte do Colaborador, nem representa solicitação da empresa para qualquer tipo de trabalho que exceda à jornada diária permitida por lei. A mera utilização desses recursos pelo Colaborador, por si só, não configura sobreaviso ou sobrejornada, sendo um ato de liberalidade, proatividade ou iniciativa.

5.7. Equipamentos de Terceiros

É vedado o uso de recursos de tecnologia de propriedade de terceiros, que não tenham sido formalmente homologados pela área de TI ou pelo Comitê de Segurança da Informação e Privacidade (CSIP) do Grupo Benner. Isto inclui computadores, dispositivos, programas, sistemas, jogos, softwares e outros recursos de TI. Os equipamentos de propriedade dos colaboradores e eventuais visitantes (incluindo computadores portáteis, smartphones, pen drives, players, entre outros dispositivos), não terão acesso à rede corporativa da Empresa. Para estes casos, o acesso à internet será concedido por meio da rede sem fio de Visitantes.

Equipamentos de propriedade das empresas que prestam serviço ao Grupo Benner e necessitam de acesso à rede corporativa deverão ser submetidos à Gerência de TI, para avaliação e homologação dos requisitos mínimos de segurança da informação.

São vedadas as conexões simultâneas dos computadores de terceiros à rede corporativa da Empresa e a outras redes, tanto internas quanto externas.

5.8. Postura em Canais de Comunicação

Tanto os canais de comunicação internos quanto os externos podem trazer danos à imagem da companhia ou de seus colaboradores, se não forem utilizados de forma adequada.

O Grupo Benner, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos de seus colaboradores aos canais de comunicação, quando tais acessos são realizados utilizando os recursos de TI da Empresa.

A empresa disponibilizará ferramenta de comunicação interna (mensageria) aos colaboradores. O uso é exclusivo para atividades relacionadas com os objetivos da empresa.

A utilização da Internet com os recursos de TI fornecidos pela Empresa deve ser restrita às atividades relacionadas com o negócio da empresa. Ainda que o acesso a sites que não estejam diretamente relacionados à atividade laborativa do usuário não seja proibido, o seu uso deve ser feito de maneira equilibrada e responsável, para assegurar ao usuário e à Empresa máxima segurança e performance no trabalho.

A gestão e a divulgação corporativa de conteúdos em mídias sociais oficiais da Empresa, bem como em seu nome, devem ser publicadas exclusivamente pela área de Comunicação. Em caso de dúvidas ou caso receba alguma solicitação externa, o colaborador deverá encaminhá-la à área responsável.

Apenas os colaboradores autorizados pela empresa 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.

Ao se identificar online como colaborador da Empresa, deve-se evitar publicações que façam referência a condutas repudiadas pela empresa.

É expressamente proibida a divulgação e/ou o compartilhamento de processos operacionais e estratégicos em listas de discussão, redes sociais, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que seja disponibilizada na internet.

Com a finalidade de evitar mensagens indesejadas e dificultar práticas de engenharia social, o endereço de e-mail de domínios da Empresa não deve ser fornecido em mídias sociais, aplicativos ou listas de distribuição externas à Organização. Da mesma forma, não é permitido compartilhar com terceiros informações de contato dos colaboradores da Empresa.

Todos os downloads de arquivos da internet efetuados pelos colaboradores estão sujeitos à verificação automática de segurança, utilizando as ferramentas de TI disponíveis no ambiente. Caso representem uma ameaça à segurança da informação ou à legislação vigente, os arquivos poderão ser excluídos sem que haja uma prévia notificação ao usuário.

É proibida a utilização do e-mail corporativo para quaisquer outros assuntos não relacionados ao trabalho, tais como: assuntos pessoais, piadas, correntes etc.

É proibido o uso dos recursos de TI fornecidos pela Empresa com as seguintes finalidades:

1. enviar mensagens não solicitadas para múltiplos destinatários (spam);
2. enviar mensagens utilizando outra conta de usuário diferente da sua conta individual, exceto para os casos expressamente autorizados;
3. enviar qualquer mensagem que torne o remetente e/ou a Companhia vulneráveis a ações civis ou criminais;
4. acessar softwares P2P (peer-to-peer), redes sociais, serviços de streaming e serviços de comunicação instantânea;
5. divulgar dados, informações, imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário da informação;
6. falsificar informações de endereçamento, adulterar cabeçalho e/ou conteúdo de mensagens enviadas ou recebidas por sua conta de e-mail ou de terceiros;
7. produzir, armazenar ou compartilhar conteúdos que:
 - a) contenham arquivos e/ou informações de Propriedade Intelectual da Empresa ou de Terceiros sem autorização expressa das partes afetadas.
 - b) contenham qualquer ato ou forneçam orientação que conflite ou contrarie os interesses da Empresa;
 - c) contenham ameaças eletrônicas, tais como: spam, phishing scam, vírus de computador ou qualquer outra espécie de malware;

- d) contenham arquivos com código executável (com extensões .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra que represente um risco à segurança da informação, com exceção para os colaboradores autorizados;
- e) visem obter acesso não autorizado à rede ou a outro computador, dentro ou fora da empresa;
- f) visem interromper um serviço, servidor ou rede de computadores (interna ou externa) utilizando qualquer método ilícito ou não autorizado;
- g) visem burlar qualquer sistema de segurança, tanto interno quanto externo;
- h) visem vigiar secretamente ou assediar outro usuário;
- i) visem acessar informações confidenciais de forma não autorizada;
- j) visem acessar indevidamente informações que possam causar prejuízos ou danos a qualquer pessoa;
- k) sejam considerados impróprios, obscenos ou ilegais;
- l) sejam de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros;
- m) contenham perseguição preconceituosa baseada em gênero, orientação sexual, raça, religião, naturalidade, incapacidade física, mental ou outras situações protegidas;
- n) sejam de cunho político ou ideológico;
- o) incluam material protegido por direitos autorais.

Qualquer exceção às regras definidas nesta seção de postura em canais de comunicação, que seja de legítimo interesse da Empresa, deverá ser avaliada de acordo com o descrito no item **5.13. Tratamento de Exceções** deste Manual.

5.9. Gestão da Continuidade de Negócios

A Gestão da Continuidade busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas da infraestrutura de TI e dos sistemas que suportam os processos críticos de negócio.

Cabe ao Gestor de cada departamento assegurar que as informações de negócio sejam mantidas adequadamente, de acordo com as diretrizes definidas no esquema de classificação das informações sob sua responsabilidade.

Cabe à Gerência de TI elaborar o Plano de Recuperação de Desastres e Política de Backup, com o objetivo de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

Tanto o Plano de Recuperação de Desastres quanto a Política de Backup devem ser submetidos a testes periódicos, com o objetivo de assegurar a sua efetividade. Além disso, toda documentação relativa à Gestão da Continuidade dos negócios, sob a ótica dos serviços de responsabilidade da Gerência de TI, deve estar devidamente atualizada e disponível para acesso.

5.10. Aquisição, desenvolvimento e manutenção de sistemas de informação

Toda necessidade de aquisição, desenvolvimento (interno ou externo) ou manutenção dos sistemas de informação utilizados na Empresa deve seguir a Norma de Gestão de Mudanças e demais procedimentos relacionados. O objetivo é garantir que os aspectos técnicos, funcionais, os riscos e as ações de mitigação sejam devidamente considerados antes de realizar as modificações e, desta forma, minimizar impactos indesejáveis ao ambiente computacional da Empresa.

Quaisquer mudanças nos sistemas existentes, bem como o desenvolvimento de novas funcionalidades, devem ser justificadas e aprovadas pelos proprietários dos processos afetados.

Ambientes específicos devem ser utilizados para desenvolvimento e testes em sistemas e aplicações de negócio. Não é permitida a realização de testes ou desenvolvimentos diretamente no ambiente de Produção da Empresa. As mudanças realizadas somente serão admitidas no ambiente produtivo mediante aceite formal dos testes realizados pelos usuários envolvidos.

As equipes envolvidas devem assegurar que a documentação técnica e funcional dos sistemas implantados ou alterados esteja atualizada e disponível antes do encerramento do projeto. As necessidades de treinamentos também devem ser consideradas, tanto para os usuários finais quanto para as equipes de suporte técnico.

A Gerência de TI é responsável pela adequada manutenção dos ativos de informação sob sua custódia. Para isso, deve assegurar as condições físicas e ambientais para o adequado acondicionamento dos equipamentos, bem como providenciar as atualizações de segurança necessárias para o correto funcionamento dos sistemas de informação.

5.11. Registro e Tratamento de Eventos de Tecnologia da Informação

Existem dois tipos de eventos que são tratados pelas equipes de TI: as requisições de serviço e os incidentes. As requisições de serviço visam promover uma alteração programada em algum recurso de TI, enquanto os incidentes referem-se a eventos adversos que causam indisponibilidade, instabilidade ou falha no funcionamento dos recursos de TI da Empresa.

É necessária a abertura de um chamado no sistema Siscon para toda requisição de serviço a ser atendida pela equipe de TI.

Da mesma forma, qualquer incidente identificado pelo usuário deverá ser imediatamente registrado no Siscon para encaminhamento à Área de TI. Os incidentes serão avaliados pela equipe de TI quanto à sua abrangência e magnitude, e as respostas serão planejadas de modo a minimizar os impactos aos processos de negócio e aos usuários finais.

Quando necessário, normas, procedimentos e práticas de Segurança da Informação poderão ser atualizados e reforçados, após o tratamento de algum incidente que comprometa a segurança das informações de propriedade ou sob custódia do Grupo Benner.

5.12. Monitoramento, Auditoria e Conformidade

As normas e procedimentos da Empresa devem estar alinhadas e em conformidade com leis e regulamentos específicos, cláusulas contratuais e acordos comerciais, no que diz respeito à Segurança da Informação.

Para garantir o cumprimento desta Norma, sistemas de monitoramento serão utilizados nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou *wireless* e outros componentes de propriedade da Empresa. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como arquivos manipulados.

A Gerência de TI deve implantar mecanismos de proteção para assegurar a disponibilidade e a integridade das trilhas de auditoria geradas, de modo a torná-las juridicamente válidas como evidências em casos de necessidade.

A Gerência de TI pode disponibilizar as informações obtidas pelos sistemas de monitoramento e auditoria nos seguintes casos: solicitação dos gestores, auditorias (interna ou externa) ou quando determinado pelo Comitê de Segurança da Informação e Privacidade para cumprimento de exigência judicial ou outro motivo legítimo.

Cabe aos gestores avaliar periodicamente a conformidade dos procedimentos internos sob sua responsabilidade, em relação à política, às normas e procedimentos de segurança da informação da Empresa. Sempre que necessário, os gestores deverão solicitar à Gerência de TI qualquer necessidade de adaptação da documentação relativa à segurança da informação aos requisitos provenientes de novas demandas corporativas.

Sempre que o objeto for pertinente nos contratos firmados entre o Grupo Benner e as empresas parceiras, deverão constar cláusulas de confidencialidade e concordância com as normas e procedimentos de segurança da informação.

Adicionalmente, deverá ser avaliada a necessidade de inclusão de cláusula de direito de auditoria às instalações, processos e registros mantidos por parceiros de negócio. Tal medida tem como objetivo habilitar a verificação da conformidade com os requisitos de segurança da informação na cadeia de suprimentos, especialmente com os fornecedores considerados críticos para a continuidade dos sistemas e serviços de TI.

5.13. Tratamento de Exceções

Quaisquer exceções às normas de segurança da informação, da forma como foram estabelecidas, deverão ser formalizadas e aprovadas pelo gestor da área solicitante. Considerando os aspectos funcionais, técnicos e de segurança da informação, a Gerência de TI emitirá um parecer para cada solicitação, podendo considerá-la: totalmente aprovada, parcialmente aprovada (com ressalvas) ou rejeitada. Quando necessário, o Comitê de Segurança da Informação poderá auxiliar na tomada de decisão. Todas as exceções autorizadas serão registradas e mantidas pela área de Segurança da Informação, para fins de auditorias ou revisões independentes.

5.14. Responsabilidade por Conduta Inadequada

Todos os colaboradores devem cumprir rigorosamente as políticas, normas e procedimentos vigentes, sob pena de serem responsabilizados por comprovados prejuízos ou danos que vier a sofrer ou causar à Empresa e/ou a terceiros, em decorrência da não observação das diretrizes e normas estabelecidas pelo Grupo Benner. Em nenhuma hipótese o Colaborador poderá alegar o desconhecimento das normas e diretrizes de segurança da informação, como justificativa para eventuais violações ou descumprimento.

A empresa poderá, a qualquer tempo, revogar credenciais de acesso concedidas aos Colaboradores, em virtude do descumprimento da Política de Segurança da Informação ou das normas e procedimentos dela decorrentes.

Em casos comprovados de conduta inadequada, um incidente de segurança da informação deverá ser registrado e endereçado pela Gerência de TI. Tanto o Colaborador quanto o seu Gestor Imediato serão notificados a respeito do incidente, dos riscos relacionados e das medidas adotadas.

Dependendo da gravidade da violação, sanções e/ou penalidades poderão ser aplicadas, de acordo com as normas internas, os dispositivos constantes na CLT (Consolidação das Leis do Trabalho), nas cláusulas contratuais ou nas decisões deliberadas pelo Comitê de Segurança da Informação e Privacidade - CSIP.

O uso de qualquer recurso de TI da Empresa para atividades ilícitas poderá acarretar a abertura de processos judiciais ou extrajudiciais. Em ambos os casos, o Grupo Benner cooperará ativamente e de forma irrestrita com as autoridades competentes.

6. DOCUMENTOS DE REFERÊNCIA

A seguir, são apresentadas as normas que suportam o sistema de gestão de segurança da informação do Grupo Benner:

- **PSI - Política de Segurança da Informação**

Documento que declara o comprometimento da organização com a Segurança da Informação (SI). Descreve como a SI está organizada, por meio da definição de papéis e responsabilidades, e define as diretrizes gerais para elaboração das normas e dos procedimentos relacionados.

- **CSIP - Comitê de Segurança da Informação e Privacidade**

Regimento interno que formaliza a instituição do Comitê de Segurança da Informação e Privacidade, descrevendo: a organização, o funcionamento, as atribuições e responsabilidades, os deveres e prerrogativas do Comitê e seus membros. O Anexo I traz a composição dos membros (Titulares e Suplentes) do CSIP.

- **MSI - Manual de Segurança da Informação**

Refere-se a este documento, que serve como um guia de acesso rápido, indicando as principais orientações e a documentação disponível para cada tópico específico. Material de suporte para os programas de conscientização, acompanhado de um Termo de Compromisso (TCOM) destacável, que deve ser assinado pelo colaborador e mantido como evidência do controle de treinamento.

▪ **NGA - Norma de Gestão de Ativos**

Descreve as regras para inventário, propriedade e uso de ativos da informação (infraestrutura e usuário final).

▪ **NGM - Norma de Gestão de Mudanças**

Descreve as regras e controles necessários para a gestão de mudanças no ambiente de TI.

▪ **NCI - Norma de Classificação da Informação**

Descreve as regras para classificação, rotulagem e tratamento dos ativos de informação, desenvolvidas de acordo com os requisitos da LGPD.

▪ **NAL - Norma de Acesso Lógico**

Estabelece as regras para a gestão e controle de acesso aos sistemas de informação utilizados na organização, incluindo: ciclo de vida dos acessos, política de senhas, gestão de acesso privilegiado em sistemas operacionais, recursos de rede e aplicações de negócio.

▪ **NAF - Norma de Acesso Físico**

Define as regras e os controles aplicáveis aos ambientes restritos de processamento de informações, incluindo a segurança física e os controles ambientais aplicáveis.

▪ **NGI - Norma de Gestão de Incidentes**

Define as regras e os procedimentos para gestão de incidentes de TI, com ênfase especial aos incidentes de segurança da informação.

7. CONSIDERAÇÕES FINAIS

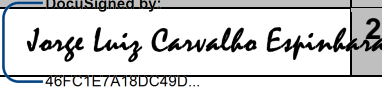
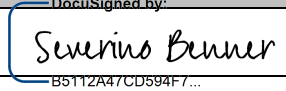
Este Manual tem caráter normativo e as condutas aqui estabelecidas constituem-se diretrizes para o melhor funcionamento e resultado do Grupo Benner.

O cumprimento das diretrizes contidas neste documento deve ser um compromisso constante de todos aqueles que fazem parte do Grupo Benner, bem como dos Prestadores de Serviços.

8. REGISTRO DE ALTERAÇÕES

Versão	Data	Etapas	Responsável
1.0	20/04/2023	Elaboração e Aprovação.	Governança de TI e CEO

9. FORMALIZAÇÃO

ELABORAÇÃO/REVISÃO		APROVAÇÃO	
Jorge Espinhara – Governança de TI		Severino Benner - CEO	
20/04/2023		20/04/2023	



MSI
TCOM

ANEXO I - TERMO DE COMPROMISSO E RESPONSABILIDADE
MANUAL DE SEGURANÇA DA INFORMAÇÃO

IDENTIFICAÇÃO DO COLABORADOR:

Nome completo:	
Empresa:	Identificação: (matrícula ou CPF)

1. Declaro que conheço e estou de acordo com as diretrizes da Política e do Manual de Segurança da Informação do Grupo Benner, em sua versão vigente.
2. Estou ciente de que a Empresa é proprietária exclusiva dos dados e informações, sistemas, tecnologias ou mesmo criações que resultem do exercício do meu trabalho, cedido ou elaborado em seu favor, e renuncio expressamente ao meu direito de reivindicar a propriedade, judicial ou extrajudicialmente, a qualquer tempo.
3. Reconheço que os recursos de tecnologia da informação que me foram disponibilizados pela Empresa são ferramentas de trabalho de sua propriedade e, por esse motivo, deverão ser utilizados para realizar as atividades inerentes à minha contratação.
4. Comprometo-me a manter a confidencialidade e zelar pela proteção e salvaguarda das informações que eu possa ter acesso e estou ciente de que, em caso de comprovado descumprimento de tal regra, serei responsabilizado, inclusive legalmente, pelo uso indevido ou divulgação não autorizada desses dados e informações.
5. Estou ciente de que as credenciais de acesso físico e lógico que me forem concedidas são de propriedade da Empresa e de meu uso exclusivo, pessoal e intransferível. Tais credenciais possuem o objetivo de proteger-me, bem como à Empresa, uma vez que elas possibilitam comprovar as ações realizadas enquanto usuário dos recursos de TI do Grupo Benner.
6. Visando assegurar o seu ambiente tecnológico, evitar danos aos recursos de informação e cumprir as diretrizes operacionais e seus aspectos legais, estou ciente de que a Empresa se reserva o direito de monitorar as atividades de seus usuários, enquanto estiverem utilizando os recursos de informação de sua propriedade.
7. Estou ciente de que a Empresa poderá retirar ou suspender o acesso a e-mail, internet, sistemas e demais recursos de TI que me forem disponibilizados, quando utilizados indevidamente ou em desacordo com as normas internas.
8. Estou ciente de que o não cumprimento ou violação de quaisquer diretrizes contidas na documentação relativa à Segurança da Informação, bem como a utilização indevida dos recursos de TI da Empresa, serão classificados e tratados como conduta inadequada, que poderão acarretar sanções administrativas ou disciplinares, além de eventuais medidas judiciais, nos termos da Lei.
9. Comprometo-me a informar, imediatamente, ao CSIP (Comitê de Segurança da Informação e Privacidade), ao meu Gestor imediato ou ao Gestor do meu contrato de prestação de serviços, qualquer indício ou falha de segurança que possa colocar em risco a confidencialidade, integridade ou disponibilidade dos ativos de informação do Grupo Benner.
10. Por fim, declaro que o presente termo, bem como as medidas nele descritas, não ferem minha liberdade de trabalho ou a minha privacidade, sendo um instrumento necessário para a preservação dos interesses e estratégias da Empresa. Declaro, ainda, que recebi treinamento adequado sobre a política e diretrizes de segurança da informação, no qual tive oportunidade de esclarecer dúvidas e questionamentos e não tenho qualquer ponto obscuro ou mal compreendido, estando claras e objetivas as regras a serem seguidas.

Data: ____/____/____

Assinatura: _____