Política da Segurança da informação e Cibernética

higher

higher

1. Objetivos

A Política de Segurança da Informação e Cibernética (“Política”) é o documento que define a forma que as informações e/ou sistemas de informação devem ser utilizados e manipulados, além de definir responsabilidades para os diferentes colaboradores da Higher Soluções Ltda.
A informação, assim como outros bens matérias ou imateriais da empresa, é de extrema valia para a Higher Soluções Ltda. e, dessa forma, a disponibilidade, a integridade e a confidencialidade dessas informações são absolutamente essenciais para o devido sucesso do negócio da empresa.
Além de preservar estes aspectos, a presente Política possui como objetivos:

- O combate ao vazamento de informações;
- O combate a fraudes e mitigação de erros e acidentes;
- Prevenção às ameaças inerentes à tecnologia da informação como vírus, spams, crimes virtuais, invasões etc.;
- Manutenção da disponibilidade da informação e dos sistemas;
- Garantia da privacidade dos funcionários e clientes;
- Atendimento às normas, leis e regulamentos.

Este é um documento de leitura obrigatória por todo e qualquer colaborador da Higher Soluções Ltda, sendo funcionário ou prestador de serviços, servindo como referência em caso de dúvidas e como base para qualquer treinamento ou palestra relacionada à Segurança da Informação. Todo colaborador deve zelar pela integridade das informações que manipula e garantir a confidencialidade dos dados passíveis de afetar o posicionamento da empresa no mercado, a produtividade ou a privacidade dos seus colaboradores e clientes.

Visando garantir a correta manipulação das informações, todo acesso e processamento de informações da Higher Soluções Ltda. devem estar de acordo com a presente Política.

A Higher Soluções Ltda. necessita garantir que suas informações e/ou sistemas de informação estejam protegidos e disponíveis para colaboradores e clientes e a presente Política é uma das ferramentas utilizadas para este fim.

As atualizações da Política são aplicadas conforme mudanças circunstanciais ou necessidades técnicas para a adequação aos parâmetros de segurança e melhores práticas.

Trata-se de uma norma de caráter geral e, principalmente, de cumprimento obrigatório por todos que tenham acesso ao ambiente da Higher Soluções Ltda.

2. Considerações

As diretrizes e regras estabelecidas nessa Política devem ser interpretadas como determinações obrigatórias.

Todos os colaboradores, consultores, prestadores de serviço, terceirizados e parceiros de negócio que possuam acesso às informações da Higher Soluções Ltda. devem estar cientes e anuentes com essa Política antes de obter qualquer informação pertencente à Higher Soluções Ltda.

Violações dessa Política podem levar a penalidades disciplinares ou contratuais.

3. Abrangência

As diretrizes definidas a seguir são destinadas a todos os colaboradores da Higher Soluções Ltda., sejam estes funcionários, prestadores de serviço, terceirizados ou parceiros de negócio.

O descumprimento desta Política poderá levar a penalidades disciplinares, contratuais ou judiciais, a depender do caso e sua gravidade.

4. Disposições Gerais

4.1 Adesão à Política de Segurança da Informação

Todos os colaboradores contratados por prazo indeterminado ou temporário, bem como estagiários, prestadores de serviços, terceirizados, e parceiros de negócio, que utilizem as dependências, ambiente e sistemas da Higher Soluções Ltda. para desempenhar seu trabalho, devem aderir a esta Política, manifestado sua ciência e concordância expressa

4.2 Solicitação de Acesso aos Sistemas de Informação

Todas as solicitações para criação, alteração e exclusão de acessos aos sistemas de informação da Higher Soluções Ltda, tais como: Acesso à Internet, correio eletrônico, aplicativos, sistemas, rede interna e telefonia somente serão atendidas pela área responsável pela Tecnologia da Informação, mediante abertura de chamado técnico.

5. Acesso à rede corporativa

5.1 Aviso de segurança

Os sistemas de informação da Higher Soluções Ltda só poderão ser utilizados por usuários autorizados.

Indivíduos que utilizarem os computadores (ou outros recursos computacionais) sem permissão ou que tentarem burlar a Norma de Segurança da Informação e as suas políticas complementares estarão sujeitos às sanções administrativas ou penalidades judiciais conforme o caso.

É terminantemente proibido conectar quaisquer equipamentos de colaboradores ou terceiros à rede do HIGHER SOLUÇÕES LTDA (móveis ou não – Ex. Desktops, Notebooks, Notepads, Celulares e etc.), seja por meios físicos ou lógicos, sem a prévia verificação e aprovação das áreas de Tecnologia e Segurança da Informação.

5.2 Identificação obrigatória

Não é permitida a utilização de computadores e/ou sistemas da Higher Soluções Ltda. sem a devida identificação de acesso.

5.3 Descanso de tela

Após 05 (cinco) minutos de inatividade no sistema (Windows), deverá ser acionada automaticamente a função de descanso de tela do Windows que somente é desabilitada após a inserção novamente de um usuário e senha.

5.4 Bloqueio do equipamento

Toda vez que o usuário se ausentar temporariamente de sua posição de trabalho, este deverá efetuar o bloqueio de seus equipamentos.

Ao final do expediente, o usuário deve sempre desligar o seu equipamento pela opção “Desligar” do Windows, o qual encerra todos os aplicativos abertos e desliga o computador.

Os procedimentos acima visam evitar que o login e/ou equipamento do usuário sejam acessados por terceiros durante a sua ausência, além da instalação e atualização de programas necessários nos equipamentos dos usuários.

Qualquer acesso ou danos causados por terceiros pela falta desse procedimento serão de responsabilidade do usuário.

6. Utilização de computadores

6.1 Configuração

As opções de configurações de proteção de tela, papel de parede, senhas locais e outras configurações estão desabilitadas por padrão. Os modelos de papel de parede e proteção de tela são padronizados de acordo com as diretrizes internas da Higher Soluções Ltda.

Não é permitido efetuar alterações nas configurações de softwares e sistema operacional (Windows) dos computadores da Higher Soluções Ltda. Quaisquer alterações necessárias deverão ser solicitadas a Tecnologia da Informação e aprovadas pela Gerência de Segurança da Informação.

É proibida a utilização de dispositivos USB e Drives particulares nos computadores. Qualquer necessidade de uso deverá ser solicitada previamentea à área competente para a devida liberação.

6.2 Manutenção

Todo usuário é responsável pela correta utilização do seu equipamento e periféricos (impressora, mouse, teclado, monitor etc.);

Os usuários que utilizam tais equipamentos deverão informar as razões de eventuais danos causados a estes.

7. Utilização de recursos

7.1 Uso pessoal de recursos

Os recursos e sistemas de informática e de comunicação da Higher Soluções Ltda (computadores, impressoras, Internet, Correio Eletrônico, telefone, smartphone, etc.) devem ser utilizados para a execução de atividades profissionais.

A Higher Soluções Ltda admite uso moderado e responsável dos seus ativos para fins pessoais conquanto que o colaborador não oponha resistência às regras de Segurança da Informação as quais já declara conhecer e concordar, em especial, no que tange a limitação de sua privacidade.

O simples uso moderado e responsável dos recursos da Higher Soluções Ltda para fins pessoais caracteriza seu aceite quanto a essa regra de exceção, não desonerando o mesmo colaborador das penalidades decorrentes dos excessos eventualmente praticados, que serão considerados, para todos os fins, como ato ilícito diante da Lei e das normas da Higher Soluções Ltda.

7.2 Modems e redes externas

Todo e qualquer acesso externo a partir da Rede Corporativa da Higher Soluções Ltda deverá ser feito através de seu sistema de acesso à Internet.

É proibida a utilização de modems ou redes wireless para acesso externo, sejam estes de propriedade da Higher Soluções ou não.

7.3 Grupos de usuários

Todas as limitações de acesso aos recursos computacionais da Higher Soluções Ltda são definidas através de grupos de usuários em uma visão departamental ou funcional.

8. Acesso à internet

8.1 Objetivo

Por ser uma ferramenta de trabalho, a Internet tem como objetivo prover informações e recursos que auxiliem na realização de tarefas e atividades relacionadas às funções de cada usuário da Higher Soluções Ltda.

8.2 Controle de acesso

Apenas terão acesso à Internet os usuários previamente identificados no sistema operacional Windows.

A identificação será realizada no momento do fornecimento do login e senha para entrada na estação de trabalho.

É proibido o compartilhamento de usuários e senhas para quaisquer finalidades.

8.3 Bloqueio de Sites e Mensagens Instantâneas

É terminantemente proibido o acesso a sites com conteúdo pornográfico, jogos, bate-papo, pedofilia, hackers, sabotagem, violência, racismo, drogas e similares ou qualquer outro site com conteúdo não autorizado. Estes sites são bloqueados e monitorados constantemente

A liberação de sites bloqueados, exceto aqueles de conteúdo nocivo como os acima citados, deverá ser solicitada previamente com uma justificativa aceita pela Higher Soluções Ltda.

Todos os colaboradores que utilizarem a ferramenta de WhatsApp para fins profissionais deverão respeitar as normas e procedimentos descrito nesta Política.

Resta convencionado que o tráfego de documentos oficiais, informações sensíveis ou não autorizadas e qualquer outro conteúdo que infrinja diretriz da Higher Soluções Ltda, via WhatsApp, deverá ser evitado, sempre que possível.

8.4 Monitoração

Todos os sites visitados pelos usuários são registrados, inclusive tentativas de acesso a sites não-autorizados. Estes registros são armazenados e eventualmente poderão ser encaminhados ao departamento competente para providências.

8.5 Confiabilidade

Como regra geral, toda e qualquer informação oriunda da Internet deve ser considerada suspeita. Como um meio aberto de publicação de informações, não há formas de garantir a confiabilidade destas.

8.6 Identificação

Toda e qualquer ação realizada pelo usuário da Higher Soluções Ltda na Internet deve ser devidamente identificada.

Ações anônimas na Internet utilizando o sistema da Higher Soluções Ltda são terminantemente proibidas.

9. Correio eletrônico (e-mail)

9.1 Utilização

O sistema de Correio Eletrônico (E-mail) da Higher Soluções Ltda. é uma ferramenta para comunicação e produtividade e como tal, deve ser utilizada apenas para a execução de atividades profissionais.

Qualquer dado que estiver nos servidores de e-mail da Higher Soluções Ltda, seja ele enviado ou recebido de um determinado destino ou localmente no computador do usuário, é de propriedade da instituição. A Higher Soluções Ltda reserva para si o direito de examinar, interceptar, acessar e revelar mensagens de e-mail e outras comunicações, bem como materiais contidos no seu sistema de e-mail com ou sem aviso, a qualquer momento (inclusive fora do horário de expediente) e por quaisquer motivos.

A utilização indevida da ferramenta de E-mail é monitorada, levando-se em conta: envio de informações confidenciais da Higher Soluções Ltda a terceiros, uso não-comercial da ferramenta ou qualquer outra ação que conflite com a correta utilização de Correio Eletrônico prevista nesta Política de Segurança.

A quebra de sigilo da caixa postal do usuário poderá ser efetuada, caso haja indícios de uso indevido verificados.

Neste caso, o e-mail em questão poderá ser enviado ao departamento de Recursos Humanos que fará as verificações necessárias do seu conteúdo.

Sendo constatado o mau-uso do correio eletrônico, o departamento de Recursos Humanos tomará as providências cabíveis, podendo para isso e se necessário, consultar o departamento Jurídico.

Estão terminantemente proibidas mensagens eletrônicas que possuam conteúdo ofensivo, preconceituoso ou discriminatório de qualquer natureza (ex: raça, sexo, religião, etc.), pornográfico ou obsceno, piadas, correntes, venda de produtos, pesquisas de campo particulares (ex.: questionários de pesquisa), caridade e etc.

9.2 Criptografia de Informações Sigilosas ou Confidenciais

Por definição, todas as mensagens enviadas para terceiros (fora do ambiente interno da Higher Soluções Ltda.) devem conter uma legenda de aviso de confidencialidade na sua parte inferior conforme abaixo:

“A informação transmitida destina-se apenas a pessoa ou entidade a quem foi endereçada e pode conter informação confidencial, legalmente protegida e para conhecimento exclusivo do destinatário. Se o leitor desta advertência não for o seu destinatário, fica ciente de que sua leitura, divulgação, distribuição ou cópia é estritamente proibida. Caso a mensagem tenha sido recebida por engano, favor comunicar ao remetente e apagar o texto do computador.”

"The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.”

9.3 Propriedade

Todas as mensagens eletrônicas enviadas ou recebidas e/ou armazenadas nos computadores são de propriedade da Higher Soluções Ltda.

Não é permitido o envio de cópias de mensagens eletrônicas internas contendo informações sensíveis ou confidenciais da instituição para endereços externos sem a prévia autorização da área responsável.

9.4 Identificação

Toda mensagem eletrônica enviada a partir da Higher Soluções Ltda. deverá ser devidamente identificada com o assunto em questão, o nome real do remetente e seu endereço eletrônico, não sendo permitido o envio de mensagens anônimas ou com origem forjada.

Todas as mensagens devem conter a assinatura de e-mail padrão da Higher Soluções.

O padrão de assinatura de e-mail é estipulado pela Higher Soluções Ltda e em nenhum momento deve ser alterado

9.5 Privacidade

Não é permitida a leitura ou o envio de mensagens eletrônicas, utilizando a caixa postal de outro usuário. Em caso de férias ou afastamento, é necessário que as mensagens recebidas neste período sejam direcionadas para o funcionário que assumirá suas funções no respectivo período. Caso seja necessário, a área responsável poderá requerer à Tecnologia da Informação o repasse automático dessas mensagens eletrônicas para outro endereço.

Ausências superiores a 30 dias, por qualquer motivo que seja, deverão ser comunicadas pelo departamento de Recursos Humanos a área de Tecnologia da Informação e a conta do usuário deverá ser bloqueada até o seu retorno.

9.6 Arquivos Anexados

E-mails recebidos de origem ou remetentes desconhecidos ou suspeitos, que possuírem links ou arquivos anexados aos e-mails, em hipótese alguma devem ser abertos sem antes consultar a Tecnologia da Informação a respeito. Tais arquivos podem conter vírus ou programas com conteúdo prejudicial ao sistema da instituição.

Eventualmente, e-mails recebidos com arquivos anexos específicos podem ser bloqueados pelo firewall interno, a fim de prevenir eventuais danos a segurança da informação. Nestes casos, o usuário deverá solicitar a liberação à área responsável.

9.7 Armazenamento

Recomenda-se que as mensagens eletrônicas que não forem descartadas, sejam armazenadas manualmente no arquivo morto provido pela própria ferramenta de correio eletrônico ou em pastas particulares (arquivos PST’s) criadas a parte. Com isso, ajuda-se a manter a segurança e evita-se o uso desnecessário dos recursos computacionais da empresa.

Em casos de reais necessidades e desde que aprovado pela área responsável, a Tecnologia da Informação poderá providenciar uma cópia desses arquivos de email em mídia devidamente protegido, utilizando o padrão de criptografia AES 256.

Faz-se necessário também esvaziar a pasta Mensagens Excluídas periodicamente, pois o simples ato de deletar uma mensagem, não a elimina por completo

9.8 Criptografia

A criptografia diz respeito a conceitos e técnicas utilizadas para codificar uma informação, de tal forma que somente seu real destinatário e o emissor da mensagem possam acessá-la, com o objetivo de evitar que terceiros interceptem e entendam a mensagem.

É importante que os usuários estejam cientes do limitado nível de segurança que mensagens eletrônicas sem criptografia possuem e desta forma, mensagens de teor sigiloso e confidencial devem estar devidamente criptografadas.

Por padrão, a Higher Soluções Ltda utiliza o método de criptografia AES 256 para que as informações confidenciais e/ou sigilosas possam ser protegidas da melhor maneira possível.

9.9 Spam

Além do envio e recebimento de mensagens eletrônicas, o servidor de correio eletrônico da Higher Soluções Ltda possui a funcionalidade de bloqueio automático de mensagens de origem duvidosa ou indesejada, denominada de SPAM, que também verifica a existência de vírus nestas mensagens eletrônicas.

Em determinadas situações, este servidor poderá bloquear mensagens eletrônicas que deveriam chegar ao seu destino, por reconhecê-las como possíveis ameaças a segurança da informação. Para esses casos, o usuário deverá solicitar o desbloqueio à área responsável.

10. Senhas

10.1 Confiabilidade

Os dados de acesso são a identificação pessoal do usuário em todos os sistemas de informação da Higher Soluções Ltda.

Em hipótese alguma as senhas do usuário deverão ser escritas ou divulgadas a terceiros, inclusive funcionários da Segurança da Informação.

Em caso de exposição, a senha deverá ser alterada imediatamente.

10.2 Função

A senha é utilizada para identificação do usuário na rede, sistema de correio eletrônico, acesso à Internet, sistemas internos e outras funcionalidades.

10.3. Obrigatoriedade

Só podem ter acesso aos computadores da Higher Soluções Ltda os usuários que se identificarem na rede utilizando sua senha pessoal e intransferível.

10.4. Responsabilidade

Após a identificação do usuário usando sua senha pessoal na rede ou nos sistemas da Higher Soluções Ltda, a responsabilidade por toda e qualquer atividade será única e exclusiva do usuário.

A senha do usuário não deverá ser utilizada por terceiros em nenhuma circunstância.

Quaisquer ações indevidas efetuadas através do acesso autenticado serão de total responsabilidade do usuário identificado, ainda que seja durante eventual uso de sua senha por terceiros, sujeitando o usuário às penalidades cabíveis.

11. Arquivos

11.1 Localização

Todos os arquivos críticos ou vitais para o negócio da Higher Soluções Ltda devem estar armazenados nos servidores de arquivos designados.

É terminantemente proibido o armazenamento destes arquivos nas pastas dos computadores locais

O funcionário não poderá copiar ou mover arquivos em diretórios fora da estrutura preparada para seu usuário.

É terminantemente proibida, e cabível de punição definida, a utilização das pastas em rede para armazenamento de arquivos pessoais e não relativos ao negócio da empresa

11.2. Identificação

Os arquivos devem ser identificados corretamente na rede, tendo seu nome relacionado com seu conteúdo e com a área da empresa. Deve-se evitar o uso de nomes comuns que podem facilmente criar duplicidade na rede e dificuldade de identificação destes.

11.3. Cópia de Segurança (Backup)

A responsabilidade pela cópia de segurança (backup) dos arquivos localizados nos servidores de arquivos da rede é da Tecnologia da Informação, não tendo esta nenhuma responsabilidade sobre arquivos armazenados localmente ou fora de seus diretórios de usuário.

Todos os colaboradores da Higher Soluções Ltda que possuem laptops e dispositivos móveis que contenham informações consideradas críticas, deverão reportar-se à Segurança da Informação para solicitar backup, caso contrário, tal área não se responsabilizará em caso de problemas com as informações contidas nestes dispositivos.

11.4. Controle de acesso

Os arquivos são armazenados através de estrutura departamental em diretórios restritos a cada departamento e a cada usuário.

Não é permitido o acesso a arquivos de outros departamentos ou usuários, a menos que estes estejam no diretório público do departamento ou da empresa.

11.5. Remoção

Arquivos que deixem de ter importância para a Higher Soluções Ltda devem ser removidos do sistema. Esta limpeza é de responsabilidade de cada usuário e deve ser realizada mensalmente.

11.6. Arquivamento

Periodicamente, será realizado o procedimento de arquivamento dos dados de cada departamento contidos nos servidores de arquivos da Higher Soluções Ltda.

12. Softwares

12.1. Instalação de Softwares

Somente devem ser instalados nos equipamentos da Higher Soluções Ltda. softwares homologados e aprovados pela Segurança da Informação.

12.2. Jogos e Softwares recreativos

Nenhum tipo de jogo ou software recreativo pode ser armazenado ou utilizado nos computadores da Higher Soluções Ltda. Caso essa prática seja detectada, o software será imediatamente removido e o usuário responsável identificado, sendo enviada uma comunicação ao departamento de Recursos Humanos, para eventuais providências.

12.3. Legalização

Nenhum tipo de software não legalizado ou não licenciado pode ser instalado nos servidores ou estações de trabalho da Higher Soluções Ltda.

12.4. Antivírus

Cada computador ou servidor da Higher Soluções Ltda executará automaticamente o software contra vírus de computador no momento de entrada do usuário.

A atualização e a manutenção da estrutura de antivírus são de responsabilidade da Tecnologia da Informação.

12.5. Utilização Indevida

Não é permitida a cópia ou o empréstimo de softwares pertencentes à Higher Soluções Ltda para uso pessoal de colaboradores.

Os programas adquiridos pela empresa são de uso corporativo e é contra a lei copiá-los para fins pessoais.

11.6. Arquivamento

Periodicamente, será realizado o procedimento de arquivamento dos dados de cada departamento contidos nos servidores de arquivos da Higher Soluções Ltda.

13. Acesso remoto

13.1. Forma de utilização

Todo acesso remoto à rede da Higher Soluções Ltda. deve ser realizado através do dispositivo de VPN (Rede Privada Virtual) que possibilita o acesso seguro e criptografado através da Internet para os sistemas da Empresa.

O acesso à VPN será liberado mediante uma solicitação e disponibilização pela Tecnologia da Informação.

13.2. Controle de acesso

Apenas usuários previamente autorizados poderão fazer uso do sistema de acesso remoto da Higher Soluções Ltda

14. Computadores e dispositivos portáteis

14.1. Prevenção de roubo

Colaboradores que façam uso de notebooks, laptops, smartphones, ipads e outros dispositivos móveis contendo informações da Higher Soluções Ltda., devem zelar pela segurança física do equipamento.

Tais dispositivos não devem ser expostos em locais públicos e deve-se tomar cuidados especiais para evitar-se perda ou roubo destes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Higher Soluções Ltda, notificar imediatamente à empresa. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

15. Mídia portátil

Dados em mídia removível (Cartões de Memória, CDs, DVD, pendrives, HDs externos), quando não utilizados, devem estar armazenados em locais seguros (cofres, gavetas com chave, etc).

Dados armazenados em mídias removíveis do tipo Cartões de Memória, Pendrive, Hard Drive Externo e armazenados em Hard Drive Internos deverão ser descartadas através do Software – Hard Drive Eraser impossibilitando a sua recuperação.

É vedada a utilização de dispositivos pessoais de mídia removível nas instalações da Higher Soluções Ltda.

15.1. Softwares de segurança

Computadores e telefones portáteis, contendo informações da Higher Soluções Ltda, deverão estar adicionalmente protegidos através de aplicativos que reforcem sua segurança contra utilização não-autorizada e eventual quebra de sigilo na ocorrência de furto do equipamento.

Todos os laptops e dispositivos móveis deverão ter senha de setup e boot habilitada por padrão, caso estes recursos estejam disponíveis no equipamento.

16. Disponibilização de informações

16.1. Informações em Mesas de Trabalho ou Salas de Reunião

Ao convocar reuniões, deve-se envolver somente as pessoas que efetivamente estejam relacionadas ao assunto abordado ou que necessitem ter acesso a tais informações pela natureza da posição que ocupam.

Para a realização de reuniões, internas ou externas, deve-se restringir o número de cópias dos documentos ao número de participantes.

Documentos contendo informações sigilosas ou importantes da Higher Soluções Ltda não podem ser deixados sobre as mesas de trabalho ou de reunião ao alcance de quaisquer outras pessoas.

16.2. Informações em locais públicos

O colaborador deve evitar conversas sobre informações confidenciais da empresa em locais públicos, táxis, bares, restaurantes, etc. Pessoas mal intencionadas podem escutar tais informações e usá-las de maneira incorreta, visando prejudicar a empresa.

16.3. Informações para a imprensa

Apenas os sócios, ou aqueles por ele delegados, têm autorização para representar a Higher Soluções Ltda junto aos meios de comunicação.

17. Auditoria

17.1. Responsabilidade

Todos os eventos passíveis de auditoria serão verificados através de usuários criados para esse fim em cada um dos sistemas da Higher Soluções Ltda.

17.2. Acesso Indevido a Arquivos

Qualquer tentativa de acesso a arquivos restritos a outro departamento ou a outros usuários nos sistemas da Higher Soluções Ltda é registrada.

Os registros serão encaminhados ao departamento de Recursos Humanos para notificação ao Gestor da Área e posteriormente serão tomadas eventuais ações cabíveis.

Nos casos em que o colaborador tenha conhecimento ou acesso involuntário a informações que não fazem parte do desempenho das suas funções, o mesmo deverá comunicar imediatamente o incidente para a Segurança da Informação.

17.3. Internet

Qualquer acesso à Internet, seja ele a sites permitidos ou não, é registrado. No registro constam informações de usuário, horário e site visitado.

18. Política de segurança cloud ou nuvem

A Higher Soluções Ltda. realiza, também, o devido arquivo de dados em nuvens, se inserindo em um modelo de gestão compartilhada de dados, mediante a contratação de pessoa jurídica provedora da nuvem, corresponsável, em virtude da prestação de serviços, pela segurança da informação. Diante disso, devem ser mensuradas as políticas de segurança instituídas pelos prestadores de serviços de nuvem, de forma a se determinar quais são as responsabilidades e suas divisões entre contratante e contratada (provedora cloud), sendo que no momento da contratação, a Higher Soluções Ltda. priorizará a contratação do fornecedor que possuir certificados de segurança internacional, emitidos por organização externa.

19. Identificação de riscos

A Higher SoluçõesLtda., mediante área interna ou por empresa prestadora de serviços de Tecnologia da Informação, mapeará, de forma constante, os riscos internos e externos dos softwares, equipamentos e demais itens de utilização pelos colaboradores para desempenho do efetivo trabalho.

Nesse sentido, com o devido mapeamento dos riscos, serão realizados as implantações e investimentos necessários para a regular e constante proteção e monitoramento cibernético das informações transitadas e armazenadas no ambiente da Higher Soluções Ltda.

20. Procedimentos de prevenção e proteção

Todos os procedimentos operacionais serão monitorados por área interna de Tecnologia de Informação ou por empresa terceirizada prestadora de serviços de TI.

Cabe destacar, nesse ponto, que o monitoramento e emissão de relatórios periódicos medirão a regularidade do ambiente cibernético da Higher Soluções Ltda. e destacarão eventuais pontos vulneráveis para a devida correção e atualização, caso necessário.

higher

Atendimento

@ relacionamento@highersolucoes.com

+55 (21) 3942.1002

Escritórios

Brasil

Rua Bandeira Paulista - 726 - 24º andar - Itaim Bibi, SP

Rua Humaitá 275, 7º andar - Lagoa, RJ

EUA

5729 Wallis Lane, Saint Cloud FL, Orlando

BANCO CENTRAL DO BRASIL

Correspondente Cambial Autorizado
Seguimos todas as regras, exigências de segurança
e processos do Banco Central do Brasil

Higher Câmbio Digital

A Sua Fintech de Câmbio

CNPJ: 39.695.312/0001-00

SISBACEN: 05218