Ferragut Soluções em T.I

Documentação interna:

Política de segurança da informação.

CNPJ: 17.052.388/0001-77
Cel. (14) 9 9767-2972
ferragut.com.br

Soluções de TI
Ferragut

A Ferragut

Ajudamos a melhorar o desempenho do seu negócio ao abordarmos uma estratégia que ao mesmo tempo visa buscar melhorias e agilidade para suas agendas de negócio e como as agendas de TI. Atuamos diretamente com a Diretoria de Tecnologia da Informação e com profissionais de diversas áreas de especialização, a fim de buscar uma organização de TI mais eficaz permitindo que a mesma promova processos eficientes na organização como um todo buscando formas assim transformar o seu negócio.

Ferragut Soluções de TI

Versionamento

Informações sobre este documento			
Autor:	Ferragut Soluções em T.I.		
Data de criação:	18 de janeiro de 2021		
Última alteração:	20 de fevereiro de 2021	**Feita por:**	Caio A. M. Ferragut
Última Impressão:			
Versão:	1.2		

CNPJ: 17.052.388/0001-77
Cel. (14) 9 9767-2972
ferragut.com.br

Ferragut Soluções de TI

Sumário

Ferragut Soluções de TI

OBJETIVO

A Política de Segurança da Informação é uma declaração formal da Ferragut Soluções em T.I. acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários.

ABRANGÊNCIA

Todos os funcionários, diretores, executivos, acionistas, colaboradores, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos da Ferragut Soluções em T.I. , suas Unidades, subsidiárias e/ou coligadas.

MISSÃO

Garantir a integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios da Ferragut Soluções em T.I..

DOCUMENTOS DE REFERÊNCIA

NBR ISO/IEC 17799:2005

ABNT 21:204.01-010

Lei 9.609/98 – Lei do Software

TERMOS E DEFINIÇÕES

TI: Tecnologia da Informação

Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

Software não licenciado: Programa de computador sem autorização de uso ou sem uma licença válida pelo desenvolvedor.

Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.

USB: É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.

Softwares de Mensageria: São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

FileServer: É um dispositivo de uma rede de computadores que tem por objetivo de realizar o compartilhamento de arquivos na rede, nele se encontram todos os arquivos compartilhados na rede.

Active Directory (AD): O Active Directory (AD) é uma ferramenta da Microsoft utilizada para o gerenciamento de usuários de rede, denominada serviço de diretório. Um diretório nada mais é do que um banco de dados contendo informações dos usuários de uma organização, tais como nome, login, senha, cargo, perfil e etc.

Spam: É o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Usuário: Colaboradores que fazem uso dos recursos de TI da empresa.

DIRETRIZES

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Conforme definição da norma NBR ISO/IEC 17799: 2005, a informação é um ativo que, como qualquer outro ativo importante para os negócios, têm um valor para a organização e,consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é aqui caracterizada pela preservação da:

a) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

b) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) Disponibilidade, a Política de Segurança da Informação deve ser divulgada a todos os funcionários e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes pró-ativas e engajadas no que diz respeito à proteção das informações.

Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle destas diretrizes.

A Política de Segurança da Informação da empresa é aprovada e revisada anualmente pela Diretoria Executiva.

ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Definição

Cabe a todos os envolvidos na execução das atividades da da Ferragut Soluções em T.I. (funcionários, estagiários, prestadores de serviços,...) cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela empresa; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a empresa quando do descumprimento ou violação desta política, através do canal de ética.

Diretorias, Gerências e Coordenações

Cabe às Diretorias, Gerências e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança

da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação através do canal de denúncia.

Área de Governança de TI e Governança Corporativa

Cabe às duas áreas propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Gestores.

ENGENHARIA SOCIAL

Engenharia social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas.

A Engenharia Social manifesta-se de diversas formas, e podemos dividi-los em dois grupos. No entanto, o grande ponto onde engenheiros sociais se baseiam é na falta de conscientização do usuário com relação à Segurança da Informação e na exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes, e como uma simples informação poderia trazer prejuízos à empresa:

Diretos: São aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido.

Indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir, como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a fazer é ignorar a oferta tentadora e apagar o e-mail imediatamente.

CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área.

A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

O acesso às dependências da empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da área de Segurança Patrimonial e mediante supervisão. Exceto para eventos e treinamentos organizados pela própria empresa.

Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL DENTRO E FORA DA EMPRESA

Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas.

Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento às pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da empresa.

REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

Diretrizes Gerais

Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

Diretrizes Específicas

Sistemas.

Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

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

Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha “robusta”.

Máquinas – Estação de Trabalho.

As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

O acesso à estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.

Quando se ausentar da mesa, deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os funcionários com estações de trabalho, incluindo equipamentos portáteis.

Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da empresa, só devem ser utilizadas em equipamentos com controles adequados.

Os usuários de TI devem utilizar apenas softwares licenciados pela área de Suporte Técnico – Infraestrutura TI, nos equipamentos da empresa.

6.6.2.2.7. A área de Infraestrutura de TI deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

Boas práticas de segurança para aparelhos eletrônicos.

Quando em deslocamentos de carro, coloque-os no porta-malas ou em local não visível.

Ao movimentar-se com notebook ou tablets, se possível, não utilize malas convencionais e sim mochilas ou malas discretas.

Não coloque os aparelhos em carrinhos de aeroportos ou despacho junto à bagagem.

Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), caso seja necessário a utilização do equipamento, mantenha-o próximo e sempre à vista, não se distanciando do mesmo.

Evite utilizar equipamentos eletrônicos em locais públicos.

Nos hotéis, preferencialmente, guarde-os no cofre do seu apartamento.

Avalie se em pequenas viagens é realmente necessário levar o aparelho.

Utilização de equipamentos particulares / terceiros dentro da empresa.

Notebooks particulares para serem usados dentro da rede das empresas abrangidas neste documento, precisam ser avaliados pelo pessoal responsável de TI.

Equipamentos de terceiros devem ser informados ao suporte para serem verificadas atualização do antivírus e existência de vírus.

É responsabilidade da área contratante encaminhar os terceiros sob sua responsabilidade para esta verificação.

Boas práticas de segurança para Impressão.

Documento enviado para a impressão deverá ser retirado imediatamente.

A impressão de documentos sigilosos deve ser feita sob supervisão do responsável.

Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora para retirada, ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora da empresa.

Ferragut Soluções de TI

A Instalação de Softwares

Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado à área de Suporte Técnico – Infraestrutura TI, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim ser disponibilizado para a área requerente.

A empresa respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na empresa.

A Gerência de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

Diretrizes quanto à utilização da Rede Corporativa.

Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

Somente os empregados que estão devidamente autorizados a falar em nome da empresa para os meios de comunicação podem escrever em nome da empresa em sites de BatePapo (Chat Room) ou Grupos de Discussão (fóruns, newsgroups). Em caso de dúvidas, procurar a área de Comunicação.

Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos. O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante citar que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.

Arquivos que estão nas pastas públicas com mais de 15 meses sem acesso serão excluídos.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos drivers de rede, pois ocupam espaço comum limitado do departamento.

Arquivos digitalizados para a pasta de digitalização são excluídos diariamente por questões de segurança da informação.

Diretrizes quanto ao uso de Mídias Removíveis e da porta USB.

O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra.

A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, neste caso, os modens 3G e os pen drives merecem a atenção. Tal vulnerabilidade não pode ser contida com firewalls ou com programas antivírus já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa.

Para liberação das portas USB dos desktops e notebooks é necessário justificar o uso e a aprovação da chefia do departamento do solicitante. Para notebooks de gerentes e cargos acima esta liberação é efetuada por padrão.

Dentro da empresa dê preferência à utilização da rede evitando a utilização de modem 3G conectado à porta USB do computador, pois é considerada uma forma de burlar a segurança de rede, protegida por Firewall e regras de segurança. Assim o funcionário abre a porta para acesso sem qualquer controle.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados.

É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

Diretrizes quanto ao uso da Internet

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

O acesso às páginas e websites é de responsabilidade de cada usuário, ficando vedado o acesso a sites com conteúdos impróprios e de relacionamentos.

O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.

É vedado qualquer tipo de download. Como também o upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados.

Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

Recomendações sobre o uso do Correio Eletrônico (E-Mail).

É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico da empresa.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.

Evitar utilizar o e-mail da empresa para assuntos pessoais.

Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de

comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não enviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.

Utilizar o e-mail para comunicações oficiais internas, as quais não necessitam obrigatoriamente do meio físico escrito. Isto diminui custos com impressão e aumenta a agilidade na entrega e leitura do documento.

A utilização do e-mail/webmail da empresa fora do horário de trabalho para posições que possuam controle/reporte de jornada deve ser aprovado pelo Diretor da área.

Uso de Softwares de Mensageria.

Recomenda-se a utilização do Software Google Meet como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

A instalação de software de mensageria e a liberação do acesso são restritas e sua utilização deve ser justificada à Gerência de TI.

O uso de sistemas de mensageria é aceitável apenas quando for utilizado como ferramenta de produtividade para comunicação online, no exercício de sua função.

Enquanto o uso responsável dos sistemas de mensageria é estimulado, o seu abuso deve ser evitado.

Sistemas de mensageria possuem histórico de riscos associados à malwares (p.ex. vírus, worms etc), de forma que deve ser utilizado com zelo e cuidado.

O uso de sistemas de mensageria em redes de relacionamento pessoais deve ser evitado no ambiente corporativo, por conta da natural assincronia das mensagens instantâneas oriundas de terceiros sem finalidades laborais, o que usualmente torna-se contraproducente.

O grande problema de se utilizar este tipo de software é que, uma vez conectado, o computador fica altamente vulnerável. As portas de entrada/saída ficam abertas, sem qualquer restrição de leitura ou gravação. Desta forma, vírus que exploram esse tipo de vulnerabilidade não encontram empecilhos para se instalarem e iniciarem os processos danosos, não só para aquele dispositivo, mas para todos os que a ele estiverem conectados ou que estiverem em rede.

Exemplos de softwares de Mensageria: Microsoft Teams, Google Meet, Zoom, Skype, Skype for Business, WhatsApp, Telegram, etc.

Controle de Acesso a VPN.

O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet,

como se o usuário estivesse fisicamente nas instalações das empresas abrangidas neste procedimento.

Nunca deixar sessões VPN abertas. Cada vez que o usuário deixar o seu equipamento conectado via VPN, deve executar logoff ou bloquear seu equipamento.

Manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

Controle de Acesso Lógico (Baseado em Senhas).

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.

Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.

Não incluir senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função.

A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso.

A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário.

Soluções de TI
Ferragut

Sistemas Wireless

A utilização deste recurso está disponível para fins profissionais.

Não é permitido: Download de músicas, jogos, filmes, programas etc, utilização de meios alternativos para burlar o sistema de controle de acesso a Internet da empresa, acesso a sites com conteúdo impróprio, pornográficos e afins, utilização de programas de downloads P2P, como Limewire, Kazaa, Ares, Emule, uTorrent, biTorrent, entre outros, ligação de aparelhos a fim de redistribuir o acesso à rede wireless a terceiros, se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais.

Considera-se violação das regras o seguinte:

• Divulgar sua conta de usuário e sua senha de acesso para qualquer pessoa. Estas informações são de caráter pessoal e intransferível.

• Utilizar o serviço para fins ilícitos e proibidos.

• Utilizar o serviço para transmitir ou divulgar material ilícito, proibido ou difamatório que viole a privacidade de terceiros, ou que seja abusivo, ameaçador, discriminatório, injurioso ou calunioso.

• Acessar conteúdo pornográfico e jogos on-line.

• Utilizar o serviço para transmitir/divulgar material que incentive discriminação ou violência.

• Transmitir e/ou divulgar qualquer material que viole direitos de terceiros, incluindo direitos de propriedade intelectual.

• Obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço.

• Interferir ou interromper o serviço, as redes ou os servidores conectados ao serviço.

• Usar de falsa identidade ou utilizar dados de terceiros para obter acesso ao serviço.
• Tentar enganar ou subverter as medidas de segurança dos sistemas e da rede de comunicação.

• Utilizar o serviço para intimidar, assediar, difamar ou aborrecer qualquer pessoa.

• Utilizar serviço de proxy para burlar sites com acesso não autorizado.

• Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos.

• Utilizar o acesso à internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade Internet.

• Acessar sites pornográficos ou quaisquer outros sites que seu conteúdo não seja destinado a serviços.

• Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da empresa.

• Violar ou tentar violar os sistemas de segurança.

• Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da empresa.

• Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e worms, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional.

• Utilizar os recursos computacionais da empresa para ganho indevido.

• Utilizar os recursos computacionais da empresa para intimidar, assediar, difamar ou aborrecer qualquer pessoa.
• Consumir inutilmente os recursos computacionais da empresa de forma intencional.

• Desenvolver qualquer outra atividade que desobedeça às normas apresentadas acima.

O usuário é responsável por qualquer atividade a partir de sua conta (login) e também por seus atos no uso dos recursos computacionais oferecidos. Assim, o mesmo responderá por qualquer ação judicial e administrativa apresentada à instituição e que o envolva.

Em caso de descumprimento das regras, o usuário estará sujeita ao infrator as penalidades apresentadas a seguir:

• 1º infração: imediata suspensão do acesso por 7 dias;

• 2ª infração: suspensão do acesso por período de 30 dias;

• 3ª infração: suspensão permanente do uso da rede sem fio.

Os registros de reincidência serão armazenados enquanto perdurar o vínculo do usuário para controle e tomada de decisão.

Caso alguma violação de regra seja identificada, através do sistema de monitoramento, o usuário será bloqueado e notificado pelo e-mail de contato.

FileServer (Servidor de arquivos).

O file server da empresa é acessado pelos Colaboradores mediante login com usuário e senha próprios, tendo os usuários permissões diferenciadas de acordo com as funções e atividades desempenhadas por cada profissional. Dessa forma, os diferentes níveis de permissão viabilizam melhor controle de acesso e de reprodução dos dados e arquivos pelos profissionais.

VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.