Política de Uso Aceitável do Usuário (Código de Conduta de TI)

Título de política	Política de Uso Aceitável do Usuário (Código de Conduta de TI)
Categoria Política	Segurança de TI
Proprietário de apólices	Massimiliano Ferrazzi (Diretor de Informações)
Aprovador de Políticas	Attilio Bonadonna (Diretor de Recursos Humanos), Dino Lanari (Diretor de Qualidade)
Políticas Relacionadas	-
Procedimentos Relacionados	-
Data efetiva	01/03/2022
Próxima data de revisão	01/03/2023

Histórico de Revisão

Versão	Mudar	Autor	Data da Mudança
1.0	Documento criado	Imagem de espaço reservado de Massimiliano Ferrazzi	04/10/2021

Nota: Este documento contém diretrizes gerais que se aplicarão em integração com o Código de Conduta ética, contratos de trabalho, leis locais, regulamentos ou acordos coletivos de trabalho

ou seja, GDPR italiano

Conteúdo

Propósito

A Pieralisi fornece muitas ferramentas de negócios para seus funcionários e contratados para aumentar sua produtividade e empregos. Essas ferramentas incluem computadores, software, ferramentas de comunicação (e-mail, chat), acesso a redes internas (intranet), acesso a redes externas (internet), bem como sistemas telefônicos, correio de voz, fax, fotocopiadoras, etc. Pieralisi exige que esses sistemas sejam utilizados de forma responsável, ética e em conformidade com todas as legislações e outras políticas e contratos da Pieralisi. O não cumprimento pode ter um impacto severo e negativo sobre a empresa, seus funcionários e seus clients. Esta política não tenta antecipar todas as situações que possam surgir e não alivia ninguém que acesse o sistema de sua obrigação de usar o bom senso e o bom senso.

- Os indivíduos da Pieralisi são incentivados a usar o systcorporativo e recursos para promover as metas e objetivos de negócios da organização. Os tipos de atividades incentivadas incluem:
- Comunicando-se com colegas, parceiros de negócios da Pieralisi e clientes da Pieralisi no contexto das responsabilidades atribuídas a um indivíduo.
- Aquisição ou compartilhamento de informações necessárias ou relacionadas ao desempenho das responsabilidades atribuídas de um indivíduo.
- Participação em atividades educativas ou de desenvolvimento profissional.

Âmbito

Apolítica de Thi é aplicável a todos os funcionários da Pieralisi, incluindo funcionários temporários, em tempo integral, meio período e temporários; empreiteiros; alunos; e estagiários. Os requisitos definidos nesta política são aplicáveis a todos os dados, sistemas e serviços de propriedade e/ou gerenciados pela Pieralisi.

Definições

- **Shadow IT:** A aquisição e o uso de sistemas de tecnologia da informação e/ou serviços dentro da organização que não foram aprovados pelo Departamento de TI. Muitas vezes, o Departamento de T não está ciente dessas soluções que estão sendo implementadas.

- **Malware:** Um programa que é inserido em um sistema, geralmente secretamente, com a intenção de comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicativos ou sistema operacional da vítima, ou de outra forma irritante ou perturbando a vítima.

- **Engenharia social:** O "jogo contra"; a arte de manipular usuários finais para fornecer informações confidenciais ou pessoais. Um exemplo é o "phishing", onde os hackerspré-seem a serem organizações confiáveis, como bancos, fornecedores de empresas, funcionários de TI ou operadoras móveis, a fim de obter suas informações pessoais, como dados de cartão de crédito ou informações corporativas confidenciais.

- **Mídia removível:** Qualquer tipo de dispositivo de armazenamento que possa ser removido de um computador enquanto o sistema estiver em execução. Exemplos incluem pendrives/pen drives USB, cartões de memória, CDs/DVDs, discos rígidos externos ou dispositivos móveis usados para fins de armazenamento, como mp3 players ou smartphones. Embora existam propósitos comerciais para esses dispositivos, eles também são conhecidos por serem fontes comuns de infecções por malware e suscetíveis a perdas ou roubos, levando a violações de informações

confidenciais.

- **Service Desk:** A equipe de suporte interna do balcão de atendimento da Pieralisi, que pode ser contatada por e-mail em itsupport@pieralisi.com

Política

A. Uso aceitável de ativos

1. Os ativos incluem, mas não se limitam a, equipamentos físicos, como computadores de mesa, servidores, impressoras, laptops, telefones, dispositivos móveis e mídia removível (como pen drives USB), bem como sistemas e serviços, como rede organizacional, internet, voz ail, e mais. Os dados organizacionais também são considerados um ativo. Todos os dispositivos e sistemas são propriedade da Pieralisi e todo o uso deve estar de acordo com políticas, normas e diretrizes.
2. Pieralisi permite o uso limitado da rede, sistemas e devícios por razões pessoais (correspondências pessoais, bancos on-line etc.), mas o uso pessoal não deve ser abusado. O uso pessoal é aceitável desde que esteja limitado às seguintes considerações:
    a) Não tem um impacto negativo na produtividade geral dos funcionários.
    b) Não causa despesas adicionais à empresa.
    c) Não compromete a empresa de forma alguma.
    d) Isso não interrompe o desempenho da rede de forma alguma.
    e) Não contradiz nenhuma outra política pieralisi de forma alguma.
3. Os bens e sistemas pieralisi não podem ser usados para fins ilegais ou ilegais, incluindo violação de direitos autorais, obscenidade, ganho pessoal, difamação, calúnia, fraude, difamação, plágio, intimidação, falsificação, personificação, jogo ilegal, solicitação de esquemas de pirâmide, e adulteração de computador (por exemplo, espalhando vírus de computador).
4. Os usuários não devem acessar e/ou comprar tecnologia, dispositivos, aplicativos ou serviços que não sejam formalmente autorizados e aprovados pela TI. (Está evasão do Departamento de TI é conhecida como Shadow IT.)
5. Os ativos de TI, como laptops e dispositivos móveis, destinam-se a be usados apenas pelas pessoas a quem foram emitidos. Se outro funcionário ou não empregado (por exemplo, membro da família) estiver usando o dispositivo, o uso deve ser monitorado para garantir que nenhum dado sensível seja acessado pela parte não autorizada. A pessoa a quem o dispositivo foi emitido é, em última instância, responsável por quaisquer ações realizadas com o dispositivo.
6. Os usuários protegerão todos os ativos de TI gerenciados por empresas o tempo todo, mantendo-os fisicamente e logicamente protegidos e sob o controle do usuário, incluindo, mas não se limitando a:
    a) Trancando laptops com um cabo de bloqueio ou armazenando-os em uma gaveta ou armário trancado ao deixá-los no escritório.
    b) Garantir que a estação de trabalho esteja bloqueada (tela/teclado) sempre que se afastar dela.
7. O acesso aos sistemas e dispositivos Pieralisi é controlado por meio de contas individuais e senhas, conforme descrito na seção Padrão de Senha deste documento e na Política de Controle de Acesso.
8. As mídias removíveis, como pendrives USB, CDs etc., podem ser usadas com os seguintes requisitos:
    a) As informações só devem ser armazenadas em mídia removível quando necessário no

desempenho da função do usuário (por exemplo, USB compartilhada entre dois funcionários durante uma conferência).

b) O uso de mídia removível para introduzir malware ou outro software não autorizado no ambiente Pieralisi é estritamente probido.

c) Dispositivos móveis (por exemplo, smartphones, tablets) não são permitidos ser usados como mídia removível para transferir ou armazenar qualquer dados de negócios ou clientes.
d) Qualquer mídia removível desconhecida que seja encontrada sem vigilância deve ser reportada ao Departamento de TI e NÃO inserida em qualquer dispositivo emitido pela Pieralisi.
e) Os usuários finais são encorajados a tomar asures razoáveis para proteger a mídia removível (por exemplo, armazená-la em um local seguro/bloqueado quando não estiver em uso; não compartilhar com usuários não autorizados).
f) O uso de mídia removível não é permitido em sistemas externos ou não emitidos pela empresa.
g) Após o preenchimento das funções atribuídas, todos os dados serão excluídos, de acordo com a mídia removível.
h) Todas as mídias removíveis devem ser entregues ao Service Desk para descarte adequado quando não for mais necessário para uso comercial.

B. Comunicação Eletrônica e Uso da Internet

O uso desistemas e serviços de comunicação e internet da Pierali (incluindo e-mail, mensagens instantâneas, correio de voz, fóruns, mídias sociais e muito mais) é fornecido para desempenhar funções regulares de trabalho. O uso é um privilégio, não um direito e, portanto, deve ser usado com respeito, bom senso e de acordo com os seguintes requisitos:

1. Os sistemas de e-mail e outros serviços de mensagens usados na Pieralisi são de propriedade da empresa e são desua propriedade. Isso dá à Pieralisi o direito de monitorar todo e qualquer tráfego de e-mail que passe pelo seu sistema de e-mail. Esse monitoramento pode incluir, mas não se limita a, leitura inadvertida pela equipe de TI durante o curso normal de gerenciamento do e-mail system, revisão pelo RH e equipe jurídica durante a fase de descoberta de e-mail de litígios e observação por parte da gerência em casos de suspeita de abuso ou ineficiência dos funcionários.

2. Pieralisi geralmente fornece comunicações oficiais por e-mail. Como resultado, espera-se que os funcionários da Pieralisi com contas de e-mail verifiquem seus e-mails de forma consistente e oportuna para que estejam cientes de anúncios e atualizações importantes da empresa, bem como para cumprir negócios e orientados para papéis Tarefas.

3. Acooperação eletrônica e a internet não devem ser usadas para fins ilegais ou ilegais, incluindo, mas não se limitando a, violação de direitos autorais, obscenidade, difamação, difamação, fraude, difamação, plágio, assédio (incluindo conteúdo ofensivo e/ou insultante), nação discrimi, intimidação, falsificação, personificação, jogo ilegal, solicitação de esquemas de pirâmide ilegal e adulteração de computador (por exemplo). espalhando vírus de computador).

4. As plataformas de comunicação pieralisi e a internet não devem ser usadas para fins que poderiam ser razoavelmente esperados para pressionar o armazenamento ou a largura de banda (por exemplo, enviar anexos grandes em vez de apontar para um local em uma unidade compartilhada). O uso individual de recursos não interferirá no uso de outros sistemas e serviços de e-mail da Pieralisi.

5. Os usuários estão proibidos de usar contas que não pertencem a eles e são proibidos de usar plataformas para se passar por outras.

    a) Os usuários não devem dar a impressão de que estão representando ou

fornecendo opiniões em nome da Pieralisi, a menos que seja autorizado de outra forma.

6. Os usuários não devem abrir anexos de mensagens ou clicar em hiperlinks enviados de fontes desconhecidas ou não assinadas através de qualquer plataforma (e-mail, mensagem instantânea, mídia social, etc.). Anexos/links são a principal fonte de malware e engenharia social e devem ser tratados com a máxima cautela.

7. Pieralisi proíbe o uso de e-mails ou outras mensagens platforms para correspondências não solicitadas em massa, cartas em cadeia e atividade comercial competitiva, a menos que pré-aprovada por Pieralisi.

8. Quaisquer alegações de uso indevido devem ser prontamente relatadas ao Service Desk. Se você receber um e-mail ofensivo ou suspeito, não encaminhe, exclua ou responda à mensagem. Em vez disso, denuncie-o diretamente ao Service Desk.

9. Os usuários de e-mail são responsáveis pelo gerenciamento da caixa de correio, incluindo organização e limpeza. Se um usuário assinar uma lista de discussão, ele deve estar ciente de como cancelar a inscrição da lista e é responsável por fazê-lo no caso de seu endereço atual email mudar.

10. Podem existir cópias de arquivamento e backup de mensagens de e-mail, apesar da exclusão do usuário final, em conformidade com a Política de Retenção da Pieralisi.

11. É estritamente proibido baixar, arquivar, armazenar ou exportar e-mails (PST, OST etc.) em unidades pessoais como o DISCO USB ou em dispositivos locais.

12. O acesso por e-mail será encerrado quando o funcionário ou terceiros encerrar sua associação com a Pieralisi, a menos que outros acordos sejam feitos. A Pieralisi não tem obrigação de armazenar ou encaminhar os ontents da caixa de entrada /outbox de e-mail de um indivíduo após o término do prazo de seu emprego.

13. Os usuários não devem enviar informações confidenciais que não sejam adequadamente protegidas (criptografadas). (Os meios apropriados de proteção incluem, mas não se limitam ao OneDrive ou anexos criptografados por e-mail.)

    a) Os usuários devem tomar precauções extras ao transmitir informações da empresa, cliente e/ou outras informações regulamentadas por meiode comunicações eletrônicas. O material sensível deve ser marcado e criptografado adequadamente. Tenha em mente que todas as mensagens de e-mail enviadas para fora de Pieralisi se tornam propriedade do receptor.

14. Os usuários não podem encaminhar automaticamente e-mails recebidos por sua conta Pieralisi para um endereço de e-mail externo ou outro sistema de mensagens.

15. O uso de endereços privados e/ou webmail (caixas de e-mail acessíveis através da web gerenciadas por provedores externos, como outlook.com, yahoo, gmail, etc.) não é permitido, exceto para excepções especificamente autorizadas pela TI. Portanto, não é permitido, enviar dados, documentos ou arquivos de qualquer tipo com conteúdo corporativo ou origem para o e-mail pessoal privado de alguém próprio ou de terceiros.

16. A Pieralisi não se responsabiliza por danos diretos e/ou indiretos decorrentes do uso do sistema e serviços de e-mail da Pieralisi. Os usuários são os únicos responsáveis pelo

conteúdo que divulgam. A Pieralisi não é responsável por qualquer reclamação de terceiros, demand ou danos decorrentes dos sistemas de e-mail ou serviços da Pieralisi.

a) No entanto, espera-se que os usuários de e-mail se lembrem que o e-mail enviado das contas de e-mail da empresa reflete na empresa. Por favor, cumpra os padrões normais de cortesia e conduta profissional e pessoal.

17. A Pieralisi pode monitorar qualquer/todas as atividades de internet originárias de equipamentos ou contas da empresa ou que ocorramredes da empresa. Se a Pieralisi descobrir atividades que não estejam em conformidade com a lei aplicável ou a política corporativa/departamental, os registros recuperados poderão ser usados para documentar o conteúdo indevidamente de acordo com o devido processo legal.

18. Os usuários podem acessar remotamente a rede corporativa enquanto estão fora do local. Os usuários devem usar os serviços VPN aprovados. Somente usuários autorizados podem acessar a rede através de VPN.

19. As contas de mídia social pieralisi podem ser usadas apenas para fins comerciais. Ospropósitos incluem a construção de imagem positiva da marca, o atendimento ao cliente, o monitoramento da opinião pública, o networking profissional e muito mais. Os seguintes requisitos são impostos para o uso adequado das mídias sociais:

    a) O acesso às mídias sociais será aberto aos funcionários que receberam aprovação de seu gerente. A aprovação será fornecida dado um propósitode negócios le gitimate.

    b) Todas as ações e comunicações através das mídias sociais devem aderir a todo o uso aceitável previamente definido das comunicações eletrônicas. Os funcionários que representam Pieralisi nas redes sociais devem participar do treinamento obrigatório.

    c) É proibido o uso de contas pessoais de redes sociais e IDs de usuário para uso da empresa.

    d) O uso de IDs de usuários de redes sociais Pieralisi para uso pessoal é proibido.

C. Segurança de dados

Manter a confidencialidade, integridade e disponibilidade de dados organizacionais é primordial para a segurança e o sucesso da organização. Os seguintes requisitos são definidos para manter os dados seguros e manuseados adequadamente.

1. Todos os dados organizacionais pertencem à Pieralisi e, como tal, todos os usuários são responsáveis por respeitar e proteger adequadamente todos os ativos de dados.

2. Os usuários devem manter todos os dados seguros tomando precauções sensatas e seguindo os requisitos definidos nesta política.

3. Os usuários não podem visualizar, copiar, alterar ou destruir dados, software, documentação ou comunicações de dados pertencentes a Pieralisi ou outro indivíduo sem permissão autorizada.

4. Os usuários só acessarão dados fornecidos a eles para deveres relacionados com seu

emprego ou engajamento e de acordo com seus termos e condições de emprego ou equivalente. O acesso a alguns aplicativos e fontes de informação será rotineiramente registrado e/ou monitorado para este fim.

5. A extração, manipulação e emissão de relatórios dos dados da Pieralisi devem ser feitos apenas para fins comerciais.

    a) É proibido o uso pessoal de dados organizacionais, incluindo dados derivados, em qualquer formato e em qualquer local.

6. Os usuários seguirão todos os procedimentos de remoção de dados sancionados pela empresa para apagar permanentemente os dados dos dispositivos uma vez que seu uso não seja mais necessário, conforme definido no [Padrão de Classificação de Dados]. Os dados devem ser retidos pelo tempo definido na [Política de Retenção de Dados].

D. Uso de dispositivos móveis

Os funcionários da Pieralisi podem usar seus próprios dispositivos pessoais para acessar a internet pelo site de comentários sem fio do hóspede corporativo e enviar/receber e-mails. O uso de dispositivos móveis pessoais é um privilégio, não um direito e, portanto, deve ser usado com respeito, bom senso e de acordo com os seguintes requisitos:

1. É responsabilidade de qualquer funcionário da Pieralisi que usa um dispositivo móvel para acessar recursos corporativos para garantir que todos os protocolos de segurança normalmente utilizados na gestão de dados sobre infraestrutura convencional de armazenamento também sejam aplicados aqui. É imprescindível que qualquer dispositivo móvel usado para conduzir os negócios da Pieralisi seja usado de forma adequada, responsável e ética. O não cumprimento resultará na suspensão imediata da conta desse usuário.

2. A TI reserva-se o direito de recusar, pormeios físicos e não físicos, a capacidade de conectar dispositivos móveis a infraestrutura corporativa e conectada a empresas. A TI se envolverá em tal ação se esses equipamentos forem usados de forma a colocar em risco os sistemas, dados, usuários e clientes da organização.

3. Todos os dispositivos móveis utilizados para acesso a sistemas e/ou dados da empresa (como e-mail) devem ser protegidos por um forte controle de acesso (por exemplo, senha alfanumérica ou autenticação biométrica). Os funcionários são incentivados a nunca divulgar suas senhas a ninguém, mesmo aos familiares, se o trabalho de negócios for realizado a partir do dispositivo móvel.

4. Todos os usuários de dispositivos móveis devem empregar medidas razoáveis de segurança física. Espera-se que os usuários finais garantam todos esses dispositivos se eles estão realmente em uso e/ou sendo transportados.

5. Quaisquer computadores não corporativos usados para sincronizar ou fazer backup de dados em dispositivos móveis terão instalado software antivírus e anti-malware atualizado.

6. Dados confidenciais (por exemplo, dados do cliente) e senhas não devem ser armazenados em dispositivos móveis.

7. No caso de um dispositivo móvel perdido ou roubado que tenha acesso aos recursos da Pieralisi (por exemplo, e-mail, OneDrive, Authenticator), cabe ao usuário relatar o incidente ao Service Desk imediatamente.

8. Todos os dispositivos móveis pessoais que tentarem se conectar à rede corporativa através da internet serão inspecionados usando tecnologia gerenciada centralmente pelo Departamento de TI da Pieralisi.

Dispositivos que não são aprovados pela TI, não estão em conformidade com as políticas de segurança da TI, ou representam qualquer ameaça à rede corporativa ou aos dados não poderão se conectar.

Dispositivos móveis inteligentes, como smartphones, tablets e laptops, acessarão a rede corporativa e os dados usando o software VPN móvel instalado no dispositivo por TI.

E. Mesa limpa e impressão

Uma política de mesa limpa é uma ferramenta importante para garantir que todos os materiais sensíveis, como informações sobre um funcionário, um cliente ou propriedade intelectual, sejam removidos de um usuário final espaço de trabalho e trancado quando os itens não estão em uso ou um funcionário deixa sua estação de trabalho. Isso reduzirá o risco de violações de segurança no local de trabalho e faz parte dos controles básicos de privacidade padrão.

1. Os funcionários são obrigados a garantir que todas as informações confidenciais em hardcopy ou formulário eletrônico estejam seguras em sua área de trabalho no final do dia e quando esperam ficar fora por um período prolongado.

    a) As estações de trabalho do computador devem ser bloqueadas (tela/teclado) quando o espaço de trabalho estiver desocupado.

    b) Os laptops devem ser bloqueados com um cabo de bloqueio ou trancados em uma gaveta se não forem levados para casa no final do dia de trabalho.

2. Quaisquer informações confidenciais (por exemplo, dados do cliente) devem ser removidas da mesa e trancadas em uma gaveta quando a mesa estiver desocupada e no final da jornada de trabalho.

3. Senhas não devem ser anotadas em qualquer lugar ou em qualquer circunstância.

4. Os armários de arquivos contendo informações confidenciais devem ser mantidos fechados e bloqueados quando não estiver em uso ou quando não forem atendidos.

5. As chaves/crachás usados para acesso a informações confidenciais não devem ser deixadas em uma mesa autônoma.

6. As impressões que contenham informações confidenciais devem ser imediatamente removidas da impressora.

7. Após a eliminação, documentos sensíveis devem ser triturados.

8. Quadros que contenham informações confidenciais devem ser apagados.

F. Padrões de senha

O acesso aos sistemas e dispositivos Pieralisi é controlado por meio de contas individuais e senhas. Os seguintes requisitos estão em vigor para proteger essas senhas e acesso a dados e sistemas confidenciais:

1. Os usuários não podem compartilhar informações de conta ou senha com outra pessoa. As contas devem ser usadas apenas pelo usuário atribuído da conta e apenas para fins autorizados. Tentar obter a senha da conta de outro usuário é estritamente proibido.

2. Um usuário deve entrar em contato com o Service Desk para obter uma redefinição de senha se tiver razões para acreditar que qualquer pessoa não autorizada tenha aprendido sua senha. Os usuários devem tomar todas as precauções necessárias para evitar o acesso não autorizado aos serviços e dados da Pieralisi.

3. Os usuários não devem usar senhas corporativas para outros serviços. Caso outros serviços sejam comprometidos, pode deixar as contas corporativas comprometidas também.

4. A complexidade da senha será aplicada pela TI por meio de políticas aplicadas pelo sistema para garantir senhas fortes e higiene adequada da senha:

    a) As senhas expirarão a cada 90 dias e os usuários serão forçados a alterá-las. Os usuários são encorajados a redefinir suas senhas antes da data de validade para minimizar qualquer interrupção no acesso à rede.

    b) Uma vida útil mínima de 1 dia é aplicada para evitar alterações de senha muito frequentes.

    c) As 4 senhas anteriores não podem ser reutilizadas.

    d) Os requisitos de complexidade de senhas reforçam o uso de um mínimo de 3 categorias (Maiúscula, minúscula, números e caracteres especiais.)

        i. Não contêm o nome da conta do usuário ou partes do nome completo do usuário que excedem dois caracteres consecutivos
        ii. Ter pelo menos seis caracteres de comprimento
        iii. Conter caracteres de três das quatro categorias a seguir:
        iv. Caracteres maiúsculo ingleses (A a Z)
        v. Caracteres minúsculos em inglês (a a z)
        vi. Base 10 dígitos (0 a 9)
        vii. Caracteres não alfabéticos (por exemplo: ! , $, #, %)
        viii. Os requisitos de complexidade são aplicados quando as senhas são alteradas ou criadas.

    e) Após 5 tentativas de login fracassadas, as contas serão bloqueadas por 30 minutos. As contas podem ser desbloqueadas entrando em contato com o Service Desk ou aguardando os 30 minutos para serem desastradas.

    f) A redefinição da senha pode ser realizada através do portal passwordreset.pieralisi.com

G. Resposta e Relatórios de Incidentes

Pieralisi tem um programa de resposta a incidentes para uma remediação eficiente de incidentes de segurança da informação. Espera-se que os funcionários cumpram os seguintes requisitos, a fim de garantir uma remediação eficaz e eficiente dos incidentes:

1. Os usuários devem reportar qualquer incidente de segurança suspeito ao Service Desk, incluindo, mas não se limitando a equipamento perdido/roubado, suspeita de infecção por malware, credenciais comprometidas e quaisquer outros possíveis compromissos de sistemas e/ou dados Pieralisi.

2. Os usuários devem cooperar com processos de resposta a incidentes, como a perda de seus equipamentos para o Service Desk para investigação se ele estiver potencialmente comprometido.

H. Conscientização e Treinamento de Segurança

Erro humano e negligência são fontes comuns de problemas de segurança. Pieralisi adota uma abordagem proativa, exigindo consciência e treinamento de segurança:

1. Durante o onboarding, todos os usuários serão obrigados a passar por conscientização e treinamento de segurança da informação. Após a conclusão, os usuários serão obrigados a assinar uma declaração de que concluíram o treinamento, que serão exigidos e procedimentos específicos ensinados e pretendem cumprir as políticas e procedimentos previstos.

2. Os usuários devem completar a conscientização e o treinamento contínuos de segurança, conforme programado pelo Departamento de TI. Os funcionários serão mantidos atualizados sobre novas melhorias e ameaças emergentes.

I. Usos inaceitáveis de segurança

A TI gerenciará as políticas de segurança, a rede, o aplicativo e o acesso de dados centralmente usando qualquer solução tecnológica considerada adequada. Qualquer tentativa de violar ou contornar a segurança será considerada uma tentativa de intrusão e estará sujeita a ações disciplinares. As seguintes restrições e requisitos são aplicadas na Pieralisi para estabelecer e manter a confidencialidade, integridade e disponibilidade de sistemas e dados:

1. Os usuários não devem introduzir programas maliciosos na rede ou em um sistema (por exemplo, vírus, worms, cavalos de Tróia, bombas de e-mail, etc.).

2. Os usuários não devem introduzir ou contribuir para violações de segurança ou interrupções na comunicação de rede.

    a) As violações de segurança incluem, mas não se limitam a acessar dados dos quais o funcionário não é um destinatário pretendido ou fazer login em um sistema ou conta que o funcionário não está expressamente autorizado a acessar, a menos que essas ações estejam dentro do escopo de deveres regulares. Para efeitos desta seção, "interrupção" inclui, mas não é limitadoa, sniffing de rede, inundações de ping, falsificação de pacotes, negação de serviço e informações forjadas de roteamento para fins maliciosos.

3. A varredura de portas ou varredura de segurança é expressamente proibida a menos que a autorização prévia seja concedida por escrito pelo Chefe Information Officer.

4. Os usuários não devem executar qualquer forma de monitoramento de rede que intercepte dados não destinados ao host do funcionário, a menos que essa atividade faça parte do trabalho/dever normal do funcionário.

5. Os usuários não devem contornar a autenticação ou a segurança do usuário de qualquer host, rede ou conta.

6. Os usuários não devem introduzir honeypots, honeynets ou tecnologia semelhante na rede corporativa.

7. Nenhum servidor (ou seja, executando serviços web ou FTP a partir de estações de trabalho do usuário) ou dispositivos que ouçam ativamente o tráfego de rede pode ser colocados na rede corporativa sem autorização prévia por escrito pelo Diretor de Informações.

8. Os usuários não devem interferir ou negar serviço a qualquer usuário (por exemplo, ataque de negação de serviço).

J. Ownership e Problemas de Privacidade

Os sistemas são propriedade da Corporação, bem como, para fins de acesso e segurança, as informações que eles contêm. Respeitamos o direito à privacidade de nossos funcionários; no entanto, concedemos acesso aos nossos sistemas para uso empresarial. Os funcionários não devem esperar que as informações contidas nesses sistemas sejam privadas. A Empresa reserva-se o direito, de tempos em tempos, por razões comerciais, legais ou válidas, de ler, monitorar, controlar e acessar arquivos e mensagens de usuário criados, salvos, transmitidos ou recebidos. No caso de atividade ilegal interceptada, vamos trazê-los ao conhecimento da autoridade sem notificação prévia ao remetente ou receptor.

K. Descumprimento

As violações destas políticas serão tratadas como outras alegações de irregularidades em Pieralisi e serão investigadas por procedimentos estabelecidos.

As sanções podem incluir, mas não se limitam a um ou mais dos seguintes:

1. Aviso oral e/ou escrito
2. Liberdade condicional, suspensão ou rescisão do emprego
3. Ação judicial por leis aplicáveis e acordos contratuais

Qualquer usuário que descubra o uso de instalações de TI incompatíveis com este Código de Conduta de TI e outras regras, instruções, políticas e diretrizes da Pieralisi deve notificar imediatamente a TI e/ou RH assim que um usuário se conscientiza de qualquer violation e abuso, o não cumprimento pode resultar em ações disciplinares.

Data e Localização	Empregado
Louveira, 20/03/2023	Rafael Beliero