Política de Segurança da Informação

Departamento	Data de atualização	Código
TI/ Privacidade	06/08/2024	GRCPL2.18

Sumário

1. Pontos Importantes

A seguir apresentamos o resumo das principais orientações contidas nesta Política. Porém, a leitura integral da Política é necessária.

O que fazer:

- Seguir as Diretrizes da Equipe de T.I e Privacidade estabelecidas nessa Política;
- Contatar o Time de T.I e Privacidade sempre que surgir alguma dúvida sobre o conteúdo desta política;
- Na contratação de novos Fornecedores e Serviços ou na adoção de novos Procedimentos e Tecnologias, sempre responder o "Formulário de Privacidade Desde o Início".

O que não fazer:

- Deixar de cumprir as diretrizes de segurança estabelecidas nesta Política;
- Realizar qualquer ação em desacordo com nossas Políticas de Segurança da Informação e Privacidade.

2. Objetivo

A Política de Segurança da Informação ("Política de S.I ou PSI) da Cyrela Brazil Realty S.A Empreendimentos e Participações ("Cyrela ou Companhia") tem como principal objetivo estabelecer as diretrizes corporativas, responsabilidades e os limites de atuação dos colaboradores, prestadores de serviços e parceiros de negócios da Companhia em relação à segurança da informação. Preservar as informações da Cyrela ou sob sua responsabilidade quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Prevenir e reduzir impactos gerados pelos incidentes de segurança da informação, assegurando a confidencialidade, integridade, disponibilidade no desenvolvimento das atividades profissionais.

3. Abrangência

As diretrizes aqui estabelecidas devem ser observadas por todos os colaboradores, prestadores de serviços e parceiros de negócio da Companhia aqui, quando em conjunto mencionados, denominados genericamente como "parceiros", que realizam o tratamento de informações e dados pessoais, e aplicam-se ao tratamento em qualquer meio ou suporte, seja físico ou digital.

4. Diretrizes

a) Toda informação produzida ou recebida pelos parceiros e colaboradores Cyrela como resultado da atividade profissional contratada pela Cyrela pertence à empresa. As exceções devem ser explícitas e formalizadas em contrato entre a Cyrela e seus parceiros.

b) Os equipamentos de informática e comunicação, sistemas e informações devem ser utilizados pelos parceiros e colaboradores somente para execução de suas atividades profissionais;

c) A Cyrela, por meio da Gerência de TI, poderá registrar todo o uso dos sistemas e serviços, visando assegurar a disponibilidade e a segurança das informações e dados utilizados.

5. Classificação da informação

a) **Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral;

b) **Uso interno:** É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização;

c) **Confidencial:** É toda informação que pode ser acessada por usuários da organização e por parceiros da organização especificamente autorizados. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro;

d) **Restrita:** É toda informação que pode ser acessada somente por usuários da organização quando explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

6. Atribuições e Responsabilidades

6.1. Diretoria

a) Aprovar a Política de Segurança da Informação, bem como apoiar a sua efetiva implementação.

6.2. Área de tecnologia da informação

a) Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;

b) Acordar com gestores o nível de serviço e os procedimentos de resposta aos incidentes;

c) Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores, parceiros ou prestadores de serviços (em caráter excepcional e desde que aprovado previamente com a Diretoria da Cia) com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI e Normas de Segurança da Informação complementares;

d) Garantir rastreabilidade através de logs e trilhas de auditoria nas aplicações geridas pela TI;

e) Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

f) Administrar e proteger as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Cyrela;

g) Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

h) Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

    i) Contas (logins) individuais dos colaboradores serão de responsabilidade do próprio colaborador.

    ii) Contas de sistemas devem ser relacionadas a uma pessoa física responsável pela aplicação a ela associada.

i) Proteger continuamente os ativos de informação da empresa contra código malicioso, e garantir que os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado;

j) Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

k) Definir regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa;

l) Adotar medidas técnicas e organizacionais de prevenção à tentativas de atividades maliciosas externas;

m) Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, distrato contratual, incidente, investigação ou outra situação em que caiba medida restritiva para fins de salvaguardar os ativos da empresa;

n) Monitorar todo o ambiente de TI e tráfego de dados, gerando indicadores de utilização da capacidade instalada, tempo de resposta, períodos de indisponibilidade, incidentes de segurança e atividades no acesso à rede;

Importante: Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

6.3. Gestores

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

b) Atribuir aos parceiros, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Companhia.

c) Exigir dos colaboradores e prestadores de serviços a assinatura do Termo de Compromisso e Ciência, de modo eletrônico, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Cyrela.

d) Antes de conceder acesso às informações da empresa, deve ser exigido a assinatura do Acordo de Confidencialidade (NDA) dos parceiros que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

6.4. Colaboradores, prestadores de serviço, parceiros de negócio

Manterem-se atualizados em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Será de inteira responsabilidade do usuário, todo prejuízo ou dano que vier a sofrer ou causar à Companhia e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

7. Monitoramento e Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, a Companhia realiza:

a) O monitoramento das estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

b) A inspeção física nos ativos de sua propriedade, a qualquer tempo.

A Cyrela pode disponibilizar as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou de apurações internas por solicitação das áreas de Compliance e do Jurídico.

8. Uso de Internet

a) Qualquer informação ou dado que é acessado, transmitido, recebido ou produzido na internet está sujeita a divulgação e auditoria. Portanto, a Cyrela, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

b) Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede ou nuvem, visando assegurar o cumprimento de sua PSI.

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

d) Somente os colaboradores que estão devidamente autorizados a falar em nome da Cyrela para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros. Apenas os usuários autorizados pela Companhia poderão copiar, captar, imprimir ou enviar imagens de telas para terceiros.

e) É proibida a divulgação e/ou o compartilhamento indevido de informações ou dados institucionais em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo, aplicativos de mensagens instantâneas ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

f) Os usuários com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades na Cyrela e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Equipe de Ti.

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

h) Os usuários não poderão em hipótese alguma utilizar os recursos da Companhia para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

i) O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, as contas serão definidas em grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores.

j) Como regra geral, materiais de cunho sexual não devem ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso da Cyrela.

k) Usuários com acesso à internet não devem efetuar upload de qualquer software licenciado a Cyrela ou de dados de sua propriedade sem expressa autorização do responsável pelo software ou pelos dados.

l) Os usuários não devem utilizar os recursos da Cyrela para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

m) O acesso a softwares peer-to-peer (Kazaa, BitTorrent, Utorrent e afins) são de uso restritos. Já os serviços de streaming (Youtube, canais de broadcast e afins) são permitidos mediante a autorização do Gestor (a) do departamento e autorização da equipe de infraestrutura a grupos específicos no Active Directory. Porém, os serviços de comunicação instantânea (MSN, ICQ, WhatsApp e afins) e as mídias sociais (Facebook, Instagram e Twitter) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor (a) requisite formalmente à Equipe de TI.

n) Sites de proxy são proibidos.

9. Correio Eletrônico (E-Mail)

O uso do e-mail é para fins corporativos e relacionado às atividades profissionais do usuário junto a empresa. É proibido aos colaboradores e aos parceiros de negócio o uso do correio eletrônico por ventura concedidos em virtude do desempenho da atividade:

a) Utilizar o e-mail para outras atividades profissionais que não estejam relacionadas ao trabalho ou contrato específico;

b) Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da empresa;

c) Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

d) Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Companhia ou suas unidades vulneráveis a ações civis ou criminais;

e) Divulgar dados pessoais e/ou informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

f) Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

g) Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das empresas da Cyrela estiver sujeita a algum tipo de investigação;

h) Produzir, transmitir ou divulgar mensagem que:

i) Contenha qualquer ato ou forneça orientação que contrarie os interesses da Companhia;

ii) Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

iii) Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

iv) Vise obter acesso não autorizado a outro computador, servidor ou rede;

v) Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

vi) Vise burlar qualquer sistema de segurança;

vii) Vise vigiar secretamente ou assediar outro usuário;

viii) Vise acessar informações confidenciais sem explícita autorização do proprietário;

ix) Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

x) Inclua imagens criptografadas ou de qualquer forma mascaradas;

xi) Contenha conteúdo considerado impróprio, obsceno ou ilegal;

xii) Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

xiii) Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

xiv) Tenha fins políticos locais ou do país (propaganda política);

xv) Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Não é permitido o envio e recebimento de informações corporativas a partir de e-mail particular, ou outros repositórios particulares como: OneDrive, SharePoint, Google Drive, etc.

A caixa postal corporativa disponibilizada pela Cyrela ou por empresas do Grupo deve ser imediatamente:

a) Bloqueada para acesso em caso de suspeita de qualquer evento ou incidente de segurança da informação;

b) Revogada em caso de encerramento do contrato do colaborador, preservando as mensagens e histórico de atividades;

c) Sempre que necessário, o pedido de revogação deve ser acompanhado por solicitação de backup e de redirecionamento da caixa postal corporativa utilizada pelo colaborador para outro indicado pelo seu Gestor imediato;

d) A caixa postal corporativa utilizada pelo colaborador deve ser mantida para fins de auditoria e prova legal das obrigações assumidas de acordo com a função executada e a natureza das informações que tinha acesso, observada a criticidade da disponibilidade da informação, os requisitos legais, fiscais e de auditoria;

e) Na ocorrência de férias, afastamento, licença ou ausência do colaborador por um período superior a 2 (dois) dias, este deve inserir resposta automática de ausência temporária,

divulgando endereço de e-mail e contato do colaborador responsável pelo recebimento das mensagens;

f) A Cyrela pode, a seu exclusivo critério, desabilitar a caixa postal durante período de férias, afastamento, licença ou ausência do colaborador, além de bloquear mensagens com arquivos que comprometam o uso ou exponham a riscos sua infraestrutura tecnológica, ou que atrapalhem o andamento dos trabalhos

g) A Cyrela pode disponibilizar as informações dos correios eletrônicos, no caso de exigência judicial ou de apurações internas por solicitação das áreas de Compliance e do Jurídico.

10. Identificação (Login)

a) Os dispositivos de identificação e senhas protegem a identidade do parceiro usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Companhia e/ou terceiros. O presente documento visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os parceiros.

b) Todos os dispositivos de identificação utilizados na Companhia, como o número de registro do colaborador, o crachá do parceiro, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

c) O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a empresa e a legislação (cível e criminal).

d) Todo e qualquer dispositivo de identificação é pessoal, portanto, não deve ser compartilhado com outras pessoas em nenhuma hipótese.

e) É proibido o compartilhamento de login. Se existir login de uso compartilhado por mais de um parceiro, a responsabilidade perante a Cyrela e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

f) É proibido o compartilhamento de login, inclusive para funções de administração de sistemas.

g) Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares, parceiros de negócio e prestadores de serviços, sejam eles pessoas

físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

h) Todos os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (Oito) caracteres, mínimo de 3 caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).

i) É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

j) As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

k) Em caso de bloqueio em função de falha de autenticação, é necessário que o colaborador entre em contato com o Service Desk através da central de atendimento (11 3839-7001) e o desbloqueio será realizado mediante a confirmação do número de CPF e/ou data de nascimento e/ou RG.

l) Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido a sua conta.

m) Todas as contas de sistemas devem ser bloqueadas quando se tornarem desnecessárias. Contas de colaboradores contratados pelo regime CLT são desativadas automaticamente através de integração do sistema de folha de pagamento com o Active Directory quando estes são desligados da Companhia. Contas dos demais parceiros são desativadas mediante a solicitação da área contratante à Equipe de TI.

n) Caso o colaborador esqueça sua senha, esta deverá ser redefinida mediante o contato através do Service Desk (11 3839-7001) e confirmação de dados para garantir a autenticidade.

11. Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos parceiros são de propriedade da Cyrela, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

Ao retirar o equipamento, colaboradores e prestadores de serviço deverão assinar um termo de entrega contendo as orientações gerais de utilização, sendo de sua responsabilidade a devolução ao departamento pessoal ou à equipe de TI ao final do contrato de trabalho ou prestação de serviço.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Equipe de TI da Cyrela, ou de quem este determinar.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente podem ser feitas após a devida validação no respectivo ambiente de homologação pela TI, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico) não é permitida, exceto e com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da Companhia (fotos, músicas, vídeos, etc.) não devem ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles devem ser excluídos definitivamente sem a necessidade de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos parceiros da empresa deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), ou qualquer outro local, mesmo em nuvem corporativa, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os parceiros e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Equipe de Ti.

No uso dos computadores, equipamentos e recursos de informática, as regras abaixo devem ser observadas:

a) Os colaboradores e prestadores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

b) É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Equipe de Ti da Cyrela ou por terceiros devidamente contratados para o serviço.

c) O usuário deverá manter a configuração do equipamento disponibilizado pela Cyrela, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da empresa, assumindo a responsabilidade como custo diante de informações.

d) Deverão ser bloqueados todos os terminais de computador quando não estiverem sendo utilizados.

e) Todos os recursos tecnológicos adquiridos pela Cyrela devem ter imediatamente suas senhas padrões (default) alteradas.

f) Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

g) É proibido o uso de computadores e recursos tecnológicos da Companhia para:

h) Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

i) Burlar quaisquer sistemas de segurança.

j) Acessar informações confidenciais sem explícita autorização do Gestor da informação.

k) Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

l) Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

m) Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

n) Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

o) Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

12. Inteligência Artificial

Inteligência Artificial (IA) refere-se à capacidade de máquinas e sistemas computacionais realizarem tarefas que normalmente exigiriam inteligência humana. Essas tarefas incluem, mas não se limitam a, aprendizado, reconhecimento de padrões, resolução de problemas, tomada de decisão e processamento de linguagem natural. A IA é um campo interdisciplinar que combina ciência da computação, matemática, engenharia e outras áreas para criar sistemas capazes de realizar atividades de maneira autônoma ou assistida.

Existem várias subáreas dentro da IA e IA generativa, incluindo:

a) **Aprendizado de Máquina (Machine Learning - ML):** Um método de análise de dados que automatiza a construção de modelos analíticos. Utiliza algoritmos que aprendem a partir dos dados, identificando padrões e fazendo previsões ou decisões sem serem explicitamente programados para isso;

b) **Processamento de Linguagem Natural (Natural Language Processing - NLP**): A capacidade dos sistemas de IA de entender, interpretar e gerar linguagem humana;

c) **Visão Computacional:** Envolve a capacitação dos sistemas de IA para interpretar e processar informações visuais do mundo real;

d) **Modelos de Linguagem Natural**: Exemplos proeminentes são o GPT-3 e GPT-4, que podem gerar texto coerente e contextualmente relevante com base em uma entrada inicial;

e) **Redes Generativas Adversariais (Generative Adversarial Networks - GANs):** Compostas por duas redes neurais em competição, as GANs podem criar imagens, vídeos e outros conteúdos visuais realistas.

f) **Modelos de Transformação:** Utilizados em tradução automática e outras tarefas de NLP, esses modelos transformam uma entrada de um tipo de dados em outra.

12.1. Medidas de Segurança

A Companhia não é contrário à utilização de Inteligência Artificial ou Inteligência Artificial Generativa, porém, devemos tomar alguns cuidados como medida de segurança, são eles:

a) **Conformidade Legal e Regulatória:** Certifique-se de que o uso de IA esteja em conformidade com todas as leis e regulamentos aplicáveis, incluindo privacidade de dados (como GDPR, LGPD);

b) **Transparência:** Mantenha registros detalhados sobre como os sistemas de IA são usados e quais dados são processados;

c) **Criptografia:** Quando possível, utilize criptografia robusta para dados em trânsito e em repouso;

d) **Dados Pessoais:** Nunca forneça seus Dados Pessoais ou de qualquer colaborador, cliente ou parceiro, no uso das ferramentas de IA, a menos que finalidade desse processo tenha passado pela avaliação da Equipe de Ti e de Privacidade;

e) **Dados Comerciais:** Além dos Dados Pessoais, não devemos compartilhar com a IA qualquer dado relacionado à Companhia, sejam eles, dados financeiros, códigos fonte de softwares ou produtos, estratégias de negócios e planos de marketing e novos negócios;

f) **Avaliação de Riscos:** Todo novo projeto que utilize novas tecnologias ou IA, necessita da avaliação de riscos da Equipe de T.I e Privacidade, para isso, preencha o Formulário de Privacidade Desde o Início pelo link: https://forms.office.com/r/S89uSegwmC;

g) **Aplicações Seguras:** Devemos utilizar apenas aplicações seguras de IA, com confirmações de mercado e certificações de códigos seguros. Caso tenha dúvidas se a empresa fornecedora é segura, entre em contato com a Equipe de Ti e/ ou de Privacidade.

h) **Cuidados:** Atenção aos resultados. Antes de utilizar ou tornar público qualquer *output*, avalie seus resultados, sempre de forma individualizada.

i) **Diversidade e inclusão:** A IA pode replicar ou amplificar padrões discriminatórios. Sempre revise os resultados obtidos com a IA, para confirmar que não estejam enviesados.

13. Dispositivos Móveis

A Política de BYOD (Bring Your Own Device) tem como principal objetivo estabelecer as diretrizes para o uso seguro de dispositivos móveis pessoais bem como sua estruturação, a fim de aprimorar o entendimento sobre a importância da segurança dos ativos da Cyrela e gerenciamento dos mesmos em todos, bem como, a segurança das senhas desses sistemas da Companhia e demais sociedades do grupo.

A Política de BYOD é um conjunto de diretrizes que visam garantir que os recursos de informação da empresa sejam acessados somente por pessoas autorizadas, bem como, o uso seguro de dispositivos externos é essencial para garantir a segurança e a confidencialidade das informações da empresa.

Para saber mais sobre essa Política, você pode acessar o Cyrela On, ou entrar em contato com a nossa Equipe de TI por meio do e-mail informaticaadm@cyrela.com.br.

14. Datacenter

O acesso ao Datacenter somente deve ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros. O acesso por meio de chave, apenas deve ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando. Todo acesso pelo sistema de autenticação deve ser registrado (usuário, data e hora) mediante software próprio. O acesso de visitantes ou terceiros deve ser realizado somente com acompanhamento de um colaborador autorizado.

O Datacenter deve ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração de Facilities. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável. A entrada ou retirada de quaisquer equipamentos do Datacenter deve ser realizada somente por um colaborador da Equipe de TI. No caso de desligamento de empregados ou distrato de parceiros que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados.

15. Backup, Retenção e Descarte

Todos os backups devem ser automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup devem realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

Os backups possuem períodos padrão de retenção para o restore de arquivos e documentos, sendo que períodos de retenção adicionais podem ser avaliados e implementados caso haja necessidade específica, após aprovações das diretorias de TI e Jurídica.

A retenção das informações é parte essencial do ciclo de vida da informação física e lógica e visa garantir que as informações de propriedade ou sob a responsabilidade da Cyrela sejam armazenadas pelo período correto, de acordo com a legislação atual aplicável.

Para retenção das informações de dados pessoais, deverão ser observadas as hipóteses de tratamento previstas na Lei Geral de Proteção de Dados, conforme a 'Tabela de Temporalidade'. Para saber mais sobre essa Tabela, você pode acessar o Cyrela On, ou entrar em contato com a nossa Equipe de TI por meio do e-mail informaticaadm@cyrela.com.br.

O descarte seguro é parte essencial do ciclo de vida da informação física e lógica, e visa garantir que o conteúdo de propriedade ou sob a responsabilidade da Cyrela não seja recuperado ou acessado por pessoas não autorizadas. As informações físicas ou lógicas devem ser descartadas de modo que impossibilite sua recuperação por meio de processos de sanitização.

16.Gestão de Incidentes de Segurança

A gestão dos incidentes de segurança da informação deve ser realizada com base nas seguintes etapas:

16.1. Identificação

Consiste em detectar ou identificar de fato a existência de um incidente de segurança.

Baseia-se na identificação de incidentes internos ou externos, seja na detecção de alertas provenientes do sistema de monitoramento da rede da Cyrela ou por notificações realizadas por qualquer pessoa relatando ser de seu conhecimento ou mesmo vítima de atividade suspeita ou em desacordo com a Política de Segurança da Informação ou da Política de Gestão de Dados Pessoais.

É obrigação de todos os colaboradores, prestadores de serviço ou parceiros de negócio, sempre que detectarem um incidente de segurança, ainda que não confirmado, ou qualquer outra situação que potencialmente viole as políticas e normas internas de segurança da informação e proteção de dados pessoais, procederem a imediata notificação do Encarregado.

As notificações internas ou externas devem ser realizadas por meio de:

a) Pelo Canal do DPO no e-mail: dpo@cyrela.com.br; ou

b) Com os Pontos Focais das regionais:

   i) **Corporativo SP:** Alberto Luiz Nogueira;

   ii) **Vendas SP:** Aline Augusta;

   iii) **Corporativo RJ:** Julio Alves;

   iv) **Vendas RJ:** Carlos Eduardo;

   v) **Corporativo Sul:** Fernando Zafanelli;

vi) **Vendas Sul:** Lucas Henrique Escouto; e

vii) **Norte/ Nordeste:** Paulo Ferreira Ramos.

c) Pelo Help Desk/Service Desk TI, por meio do telefone 11 3839-7001 e pelo e-mail pontosfocais.ti-dpo@cyrela.com.br.

16.2. Triagem

Etapa onde a equipe de TI, com apoio de Compliance, deve realizar a análise inicial do evento, e avaliar eventual notificação ou denúncia visando a sua confirmação como incidente e classificando a sua relevância sobre as atividades da Cyrela. Nesta etapa devem ser identificados os sintomas do evento, suas características e os potenciais danos causados.

Confirmado que um incidente foi detectado, ele deve ser analisado antes de qualquer ação seja tomada, principalmente para confirmar se é um incidente válido.

A análise realizada consiste na coleta, aquisição e análise de dados, informações e demais evidências sobre o incidente para investigar o ativo de rede ou sistema de informação que gerou o incidente detectado ou denunciado.

Nesta etapa, devem ser apresentadas as ações que serão priorizadas com base na categoria e no impacto do cenário encontrado e realizar as comunicações necessárias.

Caso o incidente detectado envolva ou tenha a suspeita de envolver qualquer tratamento de dados pessoais, a equipe de TI deve notificar imediatamente o Encarregado de Proteção de Dados (DPO) para avaliar se o incidente informado deve ser comunicado à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, seguindo o "Plano de resposta à Incidentes de Dados Pessoais".

16.3. Mitigação

Etapa que busca a solução do incidente por meio de um ciclo básico composto pelas seguintes fases:

a) Análise dos dados;

b) Pesquisa de solução;

c) Ação proposta e realizada (contenção);

d) Comunicação;

e) Solução efetiva ou de contorno, e;

f) Recuperação do ambiente.

Devem ser realizados procedimentos iniciais para contenção do incidente visando evitar a sua propagação e posteriormente em restabelecer o ativo, mesmo que com uma solução temporária, até que a solução definitiva seja implementada.

A Equipe de TI, com apoio de Compliance, deve buscar a solução definitiva, ou seja, identificar a causa raiz de um incidente e eliminá-lo para assegurar que o ativo esteja seguro e confiável para que os procedimentos de recuperação sejam iniciados.

16.4. Resposta ao Incidente

A Equipe de TI e Compliance devem documentar e arquivar as conclusões do tratamento do incidente, descrevendo:

a) O que aconteceu;

b) Como o incidente foi detectado, ou seja, foi relatado por pessoa natural ou por um alerta de sistema automatizado;

c) As etapas tomadas a partir da detecção do evento até o estágio de recuperação dos ativos;

d) O status do incidente à medida que ele se move ao longo do processo de solução;

e) Qualquer dado que seja coletado durante o processo de solução que possa ser usado como evidência;

f) Definir a categorização final do incidente;

g) Comentários e sugestões da equipe envolvida na resolução.

16.5. Pós Incidente

A etapa de pós incidente tem o seu início após a resolução e encerramento do incidente, onde serão analisadas pelas equipes de TI e Compliance as causas que motivaram a sua ocorrência e quais são as medidas que podem ser tomadas com objetivo que o fato não ocorra novamente. O objetivo desta etapa é melhorar os procedimentos realizada na etapa de resposta e aprimorar os ativos para protegê-los de futuros incidentes.

17. Disposições Gerais

Esta Política, bem como os demais documentos que a complementam, encontra-se disponíveis na intranet e, em caso de indisponibilidade, podem ser solicitados ao Departamento Jurídico. Qualquer dúvida relativa a este documento deve ser encaminhada a Equipe de TI por meio do e-mail informaticaadm@cyrela.com.br. Esta Política entra em vigor na data de sua publicação.

Esta Política tem validade a partir da data de sua publicação, podendo ser alterada a qualquer tempo e critério pela área de Compliance.

Esta Política deve ser lida e entendida em conjunto com as demais políticas que fazem parte do Programa de Integridade, disponíveis no Cyrela On e no Portal de Integridade.

18. Histórico de mudanças

Revisão	Descrição	Data
1.0	- Elaboração da PLTSI01-Política de Segurança da Informação	30/11/2022
2.0	- Alteração de formatação; - Indicação das mídias sociais no item 8; - Indicação dos Pontos Focais indicados no Procedimento de Resposta à Incidentes de Segurança; - Indicação da Política de BYOD (Bring Your Own Device); - Medidas de Segurança para IA.	06/08/2024

CYRELA

São Paulo, 06 de agosto de 2024.

Rafaella Carvalho
Diretora Jurídica

Miguel Mickelberg
Dir. Financeiro

CYRELA LIVING vivaz RESIDENCIAL INSTITUTO CYRELA SELLER RJZ CYRELA CYRELA | GOLDSZTEIN