POLÍTICA DE SEGURANÇA CIBERNÉTICA

VERSÃO	DATA DE APROVAÇÃO PELA DIRETORIA
2	13 de junho de 2022

INTRODUÇÃO:

A Política de Segurança Cibernética (a "Política" ou "PSC") é o documento que orienta e estabelece as diretrizes corporativas da UY3 SOCIEDADE DE CRÉDITO DIRETO S/A, para assegurar a confidencialidade, integralidade e a disponibilidade dos dados e dos sistemas de informação da Empresa. Deve, portanto, ser cumprida e aplicada em todas as áreas da Empresa, inclusive por todas as pessoas físicas e jurídicas, sejam sócios, diretores, administradores, empregados, prestadores de serviços, parceiros e/ou quaisquer outros terceiros (os "Colaboradores") que, no âmbito dessa relação, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade da Empresa, cujo acesso seja controlado.

Sumário

1. OBJETIVOS

A presente Política apresenta os princípios gerais de conduta e as obrigações a serem seguidas pelos Colaboradores, a fim de mitigar eventuais riscos relacionados às ameaças externas ou internas, deliberadas ou acidentais, que possam impactar os dados e sistemas de informação da **UY3** quanto à sua integridade, confidencialidade e disponibilidade.

2. APLICAÇÕES DA PSC

Esta PSC é aplicável a toda a Empresa, contemplando todo o uso de dispositivos, acesso e tratamento de sistemas de informações, aos servidores, conexões à rede e à internet e quaisquer outros usos de recursos tecnológicos ou que contenham informações da **UY3**.

Em razão da sensibilidade da informação trafegada na **UY3**, este poderá, nos limites da lei aplicável e conforme necessário, monitorar, gravar e registrar os ambientes, sistemas, serviços, computadores e redes da Empresa para garantir a disponibilidade e a segurança das informações utilizadas. É obrigação de cada Colaborador manter-se atualizado em relação a esta PSC, aos procedimentos e às normas relacionadas.

3. COMITÊ DE SEGURANÇA CIBERNÉTICA

A responsabilidade pela criação e atualização desta Política é do Comitê de Segurança Cibernética (o "CSC"), que é um órgão da **UY3** que tem a função de discutir e deliberar sobre assuntos relacionados à segurança cibernética da Empresa. Toda e qualquer dúvida sobre o conteúdo desta Política deve ser direcionada ao CSC.

4. INFORMAÇÕES PROTEGIDAS

Todo e qualquer dado ou informação que o Colaborador desenvolva ou venha a ter acesso em virtude do seu vínculo com a Empresa ou do desempenho de suas atividades contratadas pela Empresa (as "Informações Protegidas"), será considerada informação confidencial, de exclusiva propriedade da Empresa, salvo disposição contratual diversa, sendo expressamente proibida a sua reprodução, divulgação, publicação,

transmissão, cessão ou facilitação de acesso a quaisquer terceiros, direta ou indiretamente, total ou parcialmente, salvo se autorizado previamente e por escrito pelos representantes legais da Empresa.

O Colaborador poderá ser responsabilizado por eventual uso indevido da Informação Protegida. A Empresa reserva-se o direito de monitorar o uso das Informações Protegidas pelo Colaborador e analisar todos dados e evidências relacionados, para fins de obtenção de provas que poderão ser eventualmente utilizadas nos processos investigatórios e na adoção das medidas legais cabíveis.

A qualquer tempo, caso seja solicitado pela Empresa, ou em caso de término da relação do Colaborador com a Empresa, independentemente da causa, o Colaborador restituirá à Empresa todas as cópias, bancos de dados, reproduções ou adaptações que porventura tiver realizado das Informações Protegidas. O Colaborador reconhece, ainda, que as obrigações e proibições previstas nesta cláusula permanecerão válidas durante toda a existência do vínculo do Colaborador com a Empresa e mesmo após o término de tal vínculo, independentemente do motivo.

Qualquer Informação Protegida cuja divulgação seja exigida por Lei, ordem judicial, determinação de autoridades administrativas competentes ou acordos celebrados pela Empresa com terceiros somente poderá ser divulgada após análise e validação do Comitê de Segurança Cibernética da **UY3**.

5. CLASSIFICAÇÃO DAS INFORMAÇÕES PROTEGIDAS

Para assegurar a proteção adequada das Informações Protegidas, é necessário que sejam classificadas de acordo com a importância que representam para os negócios da Empresa, aplicando-se o grau de sigilo conforme sua classificação:

(i) **Informação Interna:** informação que guarde assuntos exclusivamente pertinentes à esfera interna da Empresa, cujo acesso é liberado apenas às pessoas internas da Empresa designadas para tal. Embora a Empresa não tenha interesse em divulgá-la a indivíduos externos, a disponibilização dessa informação não tem o potencial de causar danos sérios à Empresa;

(ii) **Informação Confidencial:** informação sigilosa que não deve ser divulgada. Seu uso é restrito a um determinado número de pessoas para desempenharem as suas atividades vinculadas à Empresa. A sua divulgação não autorizada pode causar prejuízos para a Empresa (tais como perda de clientes, danos financeiros, depreciação da imagem etc.), propiciando vantagens aos seus concorrentes e clientes, bem como revelando estratégias e resultados de negócios; e

(iii) **Informação Secreta**: informação sigilosa, com acesso controlado e liberado apenas às pessoas nomeadas para tanto, que contém matérias de ordem vital para a Empresa ou seus clientes, cuja divulgação, inexatidão e disponibilidade (total ou parcial) podem causar danos graves à Empresa, morais e/ou patrimoniais. **Sempre serão consideradas Informações Secretas** as informações de saúde dos pacientes, os procedimentos de segurança, dados pessoais e as outras informações de notável sensibilidade para os negócios da Empresa.

Além das Informações Protegidas, há também a **Informação Pública**, destinada ao público em geral e já divulgada pela Empresa, cuja utilização por quaisquer indivíduos independe de autorização e não pode gerar prejuízos para a Empresa ou para terceiros.

Sempre que a Informação for classificada como Interna, Confidencial ou Secreta, o Colaborador responsável por gerar ou obter tal informação, deverá, obrigatoriamente, antes de divulgá-la a qualquer outra pessoa, classificar tal informação e marcar tal classificação, de acordo com o tipo de suporte, da seguinte forma:

(i) documentos impressos: a classificação da informação deve ser indicada no topo de todas as páginas, de forma claramente visível, quando o documento for gerado dentro da Companhia; e marcado com uma etiqueta ou carimbo quando o documento for gerado externamente por outras organizações;

(ii) documentos eletrônicos: a classificação da informação deve ser indicada no nome do arquivo. Caso o arquivo eletrônico possa ser impresso, as regras descritas no subitem (i) deverão ser observadas;

(iii) e-mail: a classificação da informação deve ser indicada em letra maiúscula no assunto do e-mail e o rodapé de todos os e-mails enviados deve conter *disclaimer* igual ou equivalente a: *"A informação contida nesta mensagem e seus anexos é restrita e/ou confidencial, para uso exclusivo de seu destinatário. Caso Você não seja o destinatário desta mensagem, notifique o remetente e descarte esta mensagem.";*

(iv) bancos de dados e aplicações: a classificação deve estar indicada nos "metadados" dos registros. Eventuais relatórios oriundos dessas aplicações e banco de dados deverão seguir os padrões mencionados nos tópicos supra; e

(v) outros tipos de mídia: a classificação deverá ser visível pelos recursos que se façam necessários.

Caso o Colaborador receba uma informação que não esteja classificada, ele deve considerar, obrigatoriamente, essa informação como sendo, no mínimo, uma Informação Confidencial.

A classificação das Informações Protegidas é um importante procedimento voltado para a sua rastreabilidade. Portanto, se o Colaborador tiver conhecimento de que Informações Internas, Confidenciais ou Secretas estejam sendo tratadas inadequadamente, tal Colaborador deverá comunicar o CSC.

A **UY3** pode contratar terceiros para prestação de serviços de processamento e armazenamento de dados e de computação em nuvem. Se os dados que estão sendo processados envolvem Informações Protegidas, firmamos acordos contratuais apropriados e medidas organizacionais foram implementadas de acordo com a legislação aplicável para assegurar a confidencialidade, integridade, disponibilidade e recuperação dos dados e informações processadas ou armazenadas pelo prestador de serviços.

6. PRIVACIDADE E PROTEÇÃO DE DADOS

Esta PSC aplica-se a dados, incluindo dados pessoais e sensíveis, que podem ser coletados sobre os as pessoas físicas relacionadas à **UY3**, incluindo seus Colaboradores e clientes. É vedado, sem a prévia autorização da Empresa, o uso destes dados para finalidades diversas das expressamente determinadas nesta PSC ou dos motivos que ensejaram a coleta, o uso, o armazenamento e qualquer outra hipótese de tratamento dos dados.

O Colaborador garante que todos os dados pessoais a que tiver acesso não serão divulgados ou compartilhados sem autorização expressa da Empresa, bem como não serão transmitidos ou acessados por terceiros não autorizados. O Colaborador garante ainda que adotará as melhores práticas de segurança da informação durante todo o ciclo de vida dos dados dentro da Empresa.

7. MONITORAMENTO E AUDITORIA DO AMBIENTE

Todo ambiente físico e digital da empresa **é ou poderá ser monitorado, respeitados os limites previstos na legislação vigente**, incluindo o acesso, uso ou tráfego de informações em tal ambiente por qualquer meio (tal qual, por exemplo, e-mail) com o objetivo de **apurar o cumprimento das normas de segurança da empresa**.

Os colaboradores estão cientes de que a empresa poderá:

(i) Monitorar todos os servidores, redes, conexões de internet, softwares, equipamentos e dispositivos corporativos, móveis ou não, conectados à rede corporativa; e

(ii) Realizar inspeções físicas nos equipamentos e nas estações de trabalho do colaborador, periodicamente ou sob fundada suspeita de infração às normas internas da empresa.

O Colaborador também está ciente de que o monitoramento poderá identificá-lo e apresentar dados sobre o seu uso da infraestrutura técnica da Empresa e do material e conteúdo manipulado pelo Colaborador, sendo certo que todas as informações coletadas no curso do monitoramento são guardas nos backups da Empresa para fins de auditoria e poderão ser utilizadas como provas de eventual violação das regras e condições estabelecidas pela **UY3** ou pela legislação em vigor. Caso solicitado pelos órgãos competentes, essas informações oriundas do monitoramento poderão ser divulgadas na medida em que houver razão legal ou determinação judicial para tanto.

O Colaborador entende que o monitoramento é realizado para resguardar a segurança não só dos sistemas da Empresa e das Informações Protegidas, como também do próprio Colaborador. **Os dados e as informações monitoradas somente poderão ser acessadas pelos departamentos competentes e para finalidades legítimas**, como a apuração de denúncias e condução de investigações no ambiente laboral. Todo e qualquer tratamento de dados para estes fins será fundamentado no relatório de auditoria ou em outro instrumento apropriado para tanto, e cumprirá as normas específicas sobre privacidade e proteção de dados pessoais.

8. MANUSEIO DAS INFORMAÇÕES PROTEGIDAS

O Colaborador é responsável pelo uso que fizer das Informações Protegidas. Assim, as regras abaixo deverão ser observadas para garantir um nível mínimo de Segurança da Informação.

8.1. Cuidados com impressoras e copiadoras

Os Colaboradores estão cientes que todo e qualquer uso dos equipamentos como copiadoras e impressoras, deve ser feito exclusivamente no âmbito das suas atividades profissionais, sendo vedado seu uso para fins pessoais. Deve-se evitar imprimir documentos contendo Informações Secretas e, para todos os tipos de informação, os documentos impressos ou copiados devem ser retirados imediatamente dos equipamentos.

8.2. Uso de informações protegidas

O Colaborador deve tomar o máximo de cuidado com o uso que faz das Informações Protegidas, atentando-se para não deixar anotações ou manipular documentos que contenham Informações Protegidas em locais de circulação, como salas de reunião ou espaços públicos, como cafés e aviões. É proibida a reutilização de papéis para rascunho que contenham Informação Protegida.

Nos casos envolvendo a contratação de serviços de terceiros que justifiquem a necessidade de compartilhamento de Informações Protegidas pelo Colaborador, estas somente poderão ser compartilhadas após a assinatura de Acordo de Confidencialidade (NDA) ou de outros instrumentos contratuais pertinentes.

8.3. Comunicação verbal

Sempre que Informações Protegidas forem transmitidas por meio de comunicação verbal, o Colaborador deverá respeitar as regras dispostas abaixo, de acordo com o meio de transferência da informação:

(i) Presencial. Informações Internas, Confidenciais e Secretas somente podem ser discutidas em locais privados de acesso controlado, para impedir que terceiros não autorizados escutem a conversa e tenham acesso a tais informações. Quando não for possível a comunicação em ambiente privado, o Colaborador deverá tomar, no mínimo, as seguintes cautelas: (a) sempre verificar se alguém está escutando a conversa; e (b) nunca identificar a Empresa, o cliente ou o paciente durante o diálogo.

(iii) **Telefones, Celulares e Rádios.** É vedada a transmissão de Informações Confidenciais e Secretas por rádio ou telefone (fixo ou móvel). Caso o Colaborador não possa evitar que tais informações sejam transmitidas por ligações telefônicas ou pelos outros meios de transmissão, o Colaborador deve redobrar o cuidado, sendo objetivo e discreto ao transmitir tais informações. Da mesma forma, o Colaborador também não deve fornecer informações como senhas, telefones, endereços (físicos e eletrônicos) ou outras informações de acesso restrito por telefone ou outros meios de transmissão e deve estar atento para não repetir em voz alta essas informações quando forem lhe passadas por terceiros. Ainda, o Colaborador entende e concorda que é vedada a gravação de Informações Confidenciais e Secretas em equipamentos eletrônicos, como caixa postal, secretária eletrônica, áudios em aplicativos de conversa etc.

8.4. Recebimento, envio e compartilhamento de arquivos

O Colaborador é responsável pelos arquivos que recebe, envia e compartilha por meio eletrônico e pela infraestrutura tecnológica da Empresa, seja ela equipamentos de propriedade da Empresa disponibilizados para o uso do Colaborador, equipamentos do próprio Colaborador (quando autorizado pela Empresa, conforme as regras do item 15 - *Dispositivos*), ou ainda, serviços de *cloud* (nuvem).

Para garantir níveis mínimos de segurança da infraestrutura tecnológica da Empresa é vedado ao Colaborador:

(i) receber, enviar e compartilhar arquivos que: (a) tenham finalidades diversas e não relacionadas às atividades de interesse da Empresa ou relativas aos seus negócios; (b) contenham pornografia ou conteúdo de cunho racista, discriminatório ou qualquer outro que viole a legislação em vigor, a moral e os bons costumes; (c) violem direitos de terceiros, em especial direitos de propriedade intelectual, direitos autorais, direitos de imagem, entre outros; (d) caracterizem infração civil ou penal e/ou possam causar prejuízos à Empresa e a terceiros; e (e) configurem concorrência desleal ou quebra de sigilo profissional; e

(ii) enviar, compartilhar e baixar: (a) arquivos que contenham vírus, malware ou outros códigos maliciosos; (b) Informações Internas, Confidenciais ou Secretas em ambiente externo; e (c) qualquer arquivo executável (.exe) que não seja autorizado pela Empresa.

8.5. Guarda e deslocamento de informações

Todas as Informações Protegidas que devam ser armazenadas em suporte físico ou digital, quando da sua guarda pelo Colaborador, devem respeitar regras de ciclo de vida dos dados da Empresa, bem como os seguintes cuidados, de acordo com a classificação da informação:

(i) Suporte físico. Todos documentos contendo Informações Internas, Confidenciais e Secretas devem ser armazenados em arquivos físicos próprios indicados pela Empresa, de acordo com os métodos identificação do conteúdo, também indicados pela Empresa, incluindo sua data de arquivamento. Documentos utilizados pelo Colaborador em sua estação de trabalho, quando não estiverem sendo utilizados, devem sempre ser guardados em gaveta ou armário, garantindo que tais gavetas e armários permaneçam trancados quando se tratar de Informações Secretas. Nenhuma anotação relacionada às Informações Protegidas deve ser deixada à mostra, seja em cima da mesa, do computador ou em divisórias, mesmo quando o Colaborador estiver presente. Quando o Colaborador não estiver nas dependências da Empresa, os documentos contendo Informações Internas, Confidenciais e Secretas não devem ficar expostos.

(ii) Suporte digital. Todo e qualquer arquivo que contenha Informação Interna, Confidencial ou Secreta deve ser salvo na rede corporativa da Empresa, em diretório específico, que inviabilize o acesso por Colaboradores não autorizados. Caso o arquivo deva ser armazenado em dispositivo móvel (como, por exemplo, em notebooks, por conta de reuniões externas), é indispensável que o Colaborador remova o arquivo do dispositivo após a sua utilização.

Todo e qualquer documento ou arquivo que contenha Informações Confidenciais ou Secretas somente poderá ser movimentado se houver a possibilidade de recuperação ou análise dos registros de tal arquivo ou documento em caso de falhas de segurança que acarretem a perda ou o extravio das Informações Protegidas.

8.6. Descarte de informações

O descarte de um documento físico e/ou a exclusão de um arquivo digital da rede da Empresa que contenha Informações Protegidas deverá seguir as seguintes regras de descarte:

(i) Suporte físico: os documentos que tiverem Informações Públicas poderão ser descartados no lixo comum; já aqueles que possuírem Informações Internas, Confidenciais e Secretas devem ser destruídos manualmente ou, preferencialmente, por um aparelho fragmentador antes do descarte. No caso de Informações Secretas, o uso de aparelho fragmentador é obrigatório e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável.

(ii) Suporte digital: arquivos que contenham Informações Protegidas e estejam armazenados em suporte digital flexível, tais como CD ou DVD, deverão ser destruídos por meio de aparelho fragmentador e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável. Já aqueles arquivos armazenados em suporte digital rígidos, como disco rígido (HD) e pen drive, devem ser encaminhados ao setor de segurança da informação, em caixa lacrada, para destruição adequada, conforme o procedimento interno adotado.

Somente o responsável pela geração ou pelo armazenamento do arquivo, ou documento a ser descartado, tem competência para descartá-lo ou deletá-lo, salvo quando este conferir expressa autorização para que terceiro o faça. Ainda, todo descarte deve ser registrado, a fim de manter um histórico que possibilite a realização de auditorias, caso necessário.

9. E-MAIL CORPORATIVO

Os endereços de e-mail fornecidos pela Empresa aos Colaboradores são individuais e destinados exclusivamente para fins corporativos e relacionados às atividades do Colaborador dentro da Empresa. As mensagens de e-mail sempre deverão incluir assinatura com o formato padrão da **UY3**. Acrescentamos que é proibido aos Colaboradores o uso do e-mail da **UY3** para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Empresa;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a **UY3** vulneráveis a ações civis, trabalhistas ou criminais;

- divulgar informações não autorizadas, incluindo, mas não se limitando a imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo responsável;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas; e
- apagar mensagens pertinentes de e-mail quando a **UY3** estiver sujeito a algum tipo de investigação.

10. INTERNET

Todas as regras da **UY3** visam basicamente ao desenvolvimento de um comportamento ético e profissional no uso da internet. Para garantir a utilização racional desses recursos, bem como a segurança dos dados e sistemas, a Empresa se reserva o direito de utilizar ferramentas para verificar o conteúdo dos e-mails corporativos e monitorar o uso da internet e da rede corporativa.

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 as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Empresa cooperará ativamente com as autoridades competentes.

Os Colaboradores com acesso à internet poderão fazer o download somente de softwares ligados diretamente às suas atividades na **UY3** e deverão providenciar o que for necessário para regularizar a licença e o registro desses softwares, sempre buscando a aprovação do setor de Tecnologia da Informação.

Os Colaboradores não poderão: (i) utilizar os recursos da **UY3** para fazer o download ou a distribuição de software ou dados sem as licenças adequadas; (ii) efetuar *upload* ("subir") de qualquer software licenciado à **UY3** ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados; e (iii) utilizar a rede de visitantes (rede de Internet segregada) com seus dispositivos de trabalho, exceto se prévia e expressamente autorizado pelo departamento competente, hipótese em que serão aplicáveis todas as limitações de uso aqui previstas.

11. REDES SOCIAIS, WHATSAPP E E-MAIL PESSOAIS

O uso de redes sociais, serviços de e-mail, WhatsApp e outros mensageiros, para finalidades **pessoais**, é autorizado, desde que:

(i) não sejam utilizados para acesso ou divulgação de quaisquer Informações Protegidas;

(ii) não sejam utilizados para acesso ou divulgação de qualquer conteúdo não autorizado por esta Política;
(iii) não atrapalhe o exercício das atividades do Colaborador, bem como de qualquer outro Colaborador;
(iv) o Colaborador não compartilhe, poste, divulgue ou exponha qualquer imagem, foto, vídeo ou som captado no ambiente interno da Empresa; e
(v) o Colaborador não compartilhe, poste, divulgue ou exponha qualquer comentário ou texto que revele ou induza terceiros a acreditar que se trata de uma opinião ou posicionamento da Empresa.

O Colaborador é exclusivamente responsável pelo uso e pela guarda de suas senhas de acesso a redes sociais e e-mails pessoais, e a Empresa recomenda expressamente o uso de navegação anônima para aplicações particulares em equipamentos de propriedade da Empresa.

A Empresa poderá suspender, temporariamente e sem aviso prévio, o uso e o acesso a essas aplicações, nas dependências físicas da Empresa, a seu exclusivo critério, por questões de governança e/ou de segurança da informação.

12. COMUNICAÇÃO INTERNA

A Empresa pode disponibilizar para uso do Colaborador, por meio dos equipamentos corporativos, a aplicação Microsoft Teams, que possibilita troca de mensagens de texto em tempo real no ambiente de trabalho. Caso o Colaborador tenha acesso a tal ferramenta, ele está ciente de que o seu uso é destinado exclusivamente para fins profissionais, sendo vedado qualquer uso para finalidades pessoais, e desde já reconhece que todas as informações trocadas estão sujeitas a monitoramento.

Ao usar essa ferramenta, o Colaborador deve estar ciente de que não poderá: (i) enviar mensagens contendo Informações Confidenciais ou Secretas; (ii) enviar mensagens que violem a legislação em vigor ou cujo conteúdo verse sobre drogas, violência, racismo ou qualquer forma de discriminação, ameaça, pornografia ou qualquer outro que seja ofensivo e desrespeite a moral e os bons costumes; (iii) enviar mensagens de propagandas, correntes, boatos ou qualquer tipo de mensagem que, além de sobrecarregar os sistemas da Empresa com o tráfego excessivo, possa causar danos a terceiros; e (iv) interceptar mensagens de terceiros ou se fazer passar por qualquer outra pessoa forjando quaisquer mensagens.

13. ACESSO À REDE DE ARQUIVOS

O acesso às informações armazenadas na infraestrutura técnica da Empresa poderá ser realizado de maneira diferente (por meio físico, lógico ou remoto), a depender do tipo de formato. Para cada tipo de formato serão aplicadas regras de conduta distintas, a saber:

13.1. Acesso físico ao datacenter

Os locais onde estão instalados os datacenters da Empresa são considerados parte crítica da sua infraestrutura tecnológica, razão pela qual o cuidado com a proteção e segurança deve ser obrigatoriamente redobrado. Há diferentes tipos de acessos e, para cada, diferentes regras e restrições, conforme consta abaixo:

(i) acessos permanentes: permitidos somente aos empregados da Empresa que tenham a necessidade de acesso liberado para executar suas atividades;

(ii) acessos esporádicos: permitidos a outros Colaboradores ou a visitantes externos, mediante autorização prévia da UY3, com acesso registrado pela equipe de TI (nome, data e hora) e desde que haja acompanhamento em tempo integral pela equipe responsável; e

(iii) acessos externos: permitidos àqueles que não sejam Colaboradores da Empresa (contratantes externos), mediante autorização e desde que tenham contrato vigente com a Empresa que justifique esse acesso.

13.2. Acesso lógico

O acesso às informações armazenadas na infraestrutura tecnológica da Empresa será restrito a cada Colaborador, a depender do perfil de acesso que lhe for atribuído pelo Departamento de TI, conforme as regras dispostas no item 14 – *Identificação e Senhas*. Cada perfil pressupõe a liberação do acesso de determinados diretórios dentro da rede da Empresa, que são definidos a exclusivo critério do departamento de TI, ou seja, as informações poderão ser acessadas de acordo com o nível de acesso definido pela Empresa.

13.3. Acesso remoto

Quando o Colaborador não se encontrar nas dependências da Empresa, ele poderá acessar a rede privada da Empresa de forma remota, por meio de tecnologias autorizadas pela Empresa, que pode incluir o uso de VPN. O acesso remoto somente será concedido ao Colaborador nos casos em que houver necessidade comprovada. Verificada a necessidade, o acesso remoto somente será permitido após aprovação formal escrita da Empresa e será concedido apenas àquela parte da rede relacionada com o perfil do Colaborador, sendo vedado o acesso remoto à rede integral da Empresa.

O acesso remoto somente é permitido para execução das atividades profissionais do Colaborador que estejam vinculadas à Empresa, de forma que tal acesso não poderá ser realizado por dispositivo ou software particulares do Colaborador ou de propriedade de terceiros. O Colaborador é responsável por todas as atividades realizadas quando do seu acesso remoto, respondendo por qualquer uso irregular, inclusive por outra pessoa na posse de seu acesso. No caso de furto, roubo ou extravio de equipamento móvel que tenha o acesso remoto à VPN da Empresa configurado, o

Colaborador deverá imediatamente procurar uma autoridade policial para lavrar um boletim de ocorrência e, na sequência, comunicar o incidente à equipe de TI, apresentado cópia do boletim de ocorrência lavrado.

Todos os acessos remotos serão registrados pela equipe de TI, e tais registros ficarão disponíveis para consulta em caso de auditoria.

14. AUTENTICAÇÃO, IDENTIFICAÇÃO E SENHAS

Todos os Colaboradores têm determinados privilégios de acesso a Informações Protegidas, de acordo com seu cargo e as suas atribuições. Alguns exemplos de privilégio são acesso externo ao e-mail, liberações no acesso à Internet e no acesso lógico, utilização externa de determinados equipamentos da Empresa, liberação de espaço em disco rígido, utilização de dispositivos móveis, entre outros.

O Colaborador receberá um login e uma senha, de acordo com o perfil que lhe for atribuído, que lhe permitirá ser identificado quando do acesso à infraestrutura da Empresa. Assim, o Colaborador somente terá acesso às áreas da infraestrutura da Empresa que forem autorizadas considerando o seu perfil. A Empresa reserva-se o direito de revisar, a qualquer momento e sem aviso prévio, por meio dos Departamentos competentes, os privilégios de qualquer Colaborador, a fim de resguardar os níveis de segurança da informação da Empresa.

O login e a senha do Colaborador são pessoais e, consequentemente, o Colaborador é o responsável pelo sigilo e pela manutenção segura da sua senha vinculada ao login, sendo proibido o compartilhamento de login e senha com terceiros, inclusive outros Colaboradores, sob pena de arcar com as sanções não só previstas nesta Política, mas também as penalidades civis, criminais e trabalhistas, respondendo, inclusive, por todo e qualquer dano que causar à Empresa.

Além do login do Colaborador, ele também receberá uma identificação física que lhe concederá acesso a determinadas áreas físicas da Empresa. Tal identificação será feita por meio de senha pessoal e/ou biometria, cujo uso é exclusivo, e terá por finalidade registrar a entrada e saída das dependências da Empresa.

15. DISPOSITIVOS

Os dispositivos físicos capazes de armazenar Informações Protegidas, como computadores, celulares, notebooks, tablets e outros, disponibilizados aos Colaboradores para a execução de suas atividades, são de propriedade da UY3, 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 pelo Departamento de TI.

Os equipamentos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos. Os computadores devem ter o recurso de

atualizações automáticas do sistema operacional habilitada por padrão e software antivírus instalado, ativado e atualizado frequentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Departamento de TI.

Arquivos pessoais e/ou não pertinentes ao negócio da **UY3** (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento no disco do computador. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos Colaboradores da instituição deverão ser salvos em diretório sincronizado com nosso serviço de Cloud Microsoft OneDrive garantindo o backup e a disponibilidade por meio de qualquer computador. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio Colaborador.

O Colaborador entende que é o responsável por todo e qualquer dano que causar nos equipamentos, por dolo ou culpa, e está ciente e concorda em observar às seguintes regras:

- O Colaborador é responsável pelos equipamentos e se compromete a empregar todos os cuidados necessários, como se o dispositivo fosse seu;
- Os dispositivos devem estar sempre em seu alcance e não podem ser deixados em locais públicos, em veículos ou em qualquer outro local fora das dependências da Empresa em que possa haver acesso do equipamento por pessoas não autorizadas, a fim de evitar o furto e/ou roubo destes equipamentos, bem como o vazamento das Informações Protegidas nele contidas;
- Os Colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
- 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 de TI da **UY3** ou por terceiros devidamente contratados para o serviço;
- O Colaborador deverá manter a configuração do equipamento disponibilizado pela **UY3**, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- É expressamente proibido o fumo na mesa de trabalho e próximo aos equipamentos;

- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pela **UY3** devem ter imediatamente suas senhas padrões (*default*) alteradas;
- Quando o Colaborador usar um dispositivo em um local público, deve utilizar película protetora em tal dispositivo, a fim de impedir a visualização de conteúdo por terceiros;
- Todos os dispositivos devem ser protegidos por senha e não devem ficar logados quando o Colaborador não estiver presente;
- Se, no decorrer do uso do dispositivo, o Colaborador tiver dúvidas sobre o seu manuseio ou constatar falhas que impliquem na necessidade de sua substituição ou manutenção, o Colaborador deverá abrir um chamado junto ao Departamento de TI que, por sua vez, além de fornecer os esclarecimentos necessários, deverá orientá-lo a entregar o equipamento no local indicado para sua substituição ou conserto;
- Caso o uso de um dispositivo seja esporádico, o Colaborador deverá devolvê-lo ao Departamento de TI em perfeitas condições de uso, juntamente com eventuais acessórios lhe tenham sido entregues, como bolsas, *cases*, películas etc., tão logo termine o período necessário para o uso. Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à Empresa, sem prejuízo de outras medidas legais e administrativas a serem tomadas pela Empresa; e
- No caso de perda, furto, roubo ou dano ao equipamento, o Colaborador deve comunicar imediatamente o Departamento de TI, que procederá com a remoção do conteúdo corporativo contido no dispositivo. O Colaborador também deverá procurar as autoridades policiais e realizar um boletim de ocorrência, que deverá ser apresentado ao Departamento de TI quando da comunicação do incidente.

O uso indevido dos dispositivos da Empresa sujeitará o Colaborador às sanções aplicáveis, a depender da gravidade da conduta praticada. São algumas hipóteses de uso indevido:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (*sniffers*);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- 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;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública; e
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

É proibida a utilização, pelo Colaborador, de dispositivos móveis particulares ou de terceiros (tais como celulares, smartphones, notebook, tablets, entre outros) para o desenvolvimento das atividades profissionais vinculadas à Empresa. Excepcionalmente, a **UY3** poderá permitir que determinados Colaboradores possam configurar sua conta de e-mail corporativa em dispositivos pessoais móveis, o que deverá ser previamente aprovado pela Empresa e feito com o auxílio deste.

16. DATACENTER E CLOUD

A Empresa utiliza diversos softwares próprios ou de terceiros no curso de suas operações e o Colaborador não poderá:

(i) utilizar tais softwares para fins pessoais ou de qualquer forma que comprometa a segurança da infraestrutura da Empresa;

(ii) excluir, modificar, copiar, transferir, realizar engenharia reversa ou ceder o acesso de tais software a terceiros, ou praticar qualquer ato que esteja em desacordo com a legislação aplicável; e

(iii) instalar na rede ou nos dispositivos da Empresa qualquer software pirata, não licenciado ou não autorizado pela área TI, sendo que qualquer software não autorizado que seja baixado pelo Colaborador, será excluído pela equipe de TI.

É proibido a utilização pelo Colaborador de serviços de armazenamento na nuvem não disponibilizados por meio da infraestrutura tecnológica da Empresa, como por exemplo, OneDrive.

Ainda, a contratação de serviços de Datacenter e Cloud (*outsourcing*) deverá exigir certificações de segurança, como exemplo SSAE 16, ISAE 3402, ISO 27001 e PCI DSS, de acordo com o tipo de serviço que será hospedado ou conforme novos padrões de certificações que surgirem no mercado.

Os relatórios das certificações devem ser apresentados anualmente, contendo os detalhes sobre o nível de implementação dos controles. Os relatórios das certificações SSAE 16 e ISAE 3402, por exemplo, devem ser apresentados nos formatos SOC2 e SOC3.

Oportunamente, a UY3 ao realizar contratações de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar se de que a empresa contratada atende as seguintes exigências:

a) Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, como por exemplo.
   - Se mantém Política de Segurança da Informação;
   - Se possui Plano de Continuidade Operacional;
   - Se as mudanças ou alterações de serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças);
   - Se mantém Gestão de Incidentes.

b) Verificação da capacidade do potencial Prestador de Serviços de forma a assegurar os seguintes requisitos:
   - Cumprimento da legislação e da regulamentação em vigor;
   - Permissão de acesso da UY3 aos dados e as informações a serem processadas ou armazenadas pelo Prestador de serviços;
   - Confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas ou armazenadas pelo Prestador de serviços;
   - Aderência a certificações que a UY3 possa exigir para a prestação do serviço a ser contratado;
   - Acesso da UY3 aos relatórios elaborados por empresa de Auditoria especializada independente contratada pelo Prestador de serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;
   - Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados;
   - Identificação e segregação dos dados dos clientes UY3 por meio de controles físicos ou lógicos.

17. DESLIGAMENTO OU MOVIMENTAÇÃO DO COLABORADOR

Ao término do vínculo do Colaborador com a Empresa, o seu acesso à infraestrutura tecnológica da Empresa será revogado de forma imediata. O Colaborador deverá devolver todos e quaisquer dispositivos de propriedade da Empresa que estejam em sua posse, em perfeitas condições de uso, juntamente com eventuais acessórios lhe tenham sido entregues. As obrigações de sigilo e não reprodução das Informações Protegidas, assumidas pelo Colaborador nessa PSC, permanecerão em vigor mesmo após o desligamento do Colaborador.

Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à Empresa. Em caso de perda, furto ou roubo de equipamentos, as regras previstas no item 15 - *Dispositivos* - serão aplicadas.

Caso o Colaborador tenha acesso à conta de e-mail corporativa ou a qualquer outro software instalado em um dispositivo pessoal, deverá apresentar esse dispositivo para o Departamento de TI, que procederá a sua desinstalação.

Caso o Colaborador mude de departamento ou de função dentro da **UY3**, este também deverá ter seus acessos revistos, passando a visualizar apenas os sistemas e pastas de rede necessários ao desempenho de sua nova função.

18. REPORTE DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Para evitar a exposição indevida das Informações Protegidas, a Empresa emprega medidas de segurança, tanto internas quanto externas, as quais atendem as obrigações legais vigentes. Porém, essas medidas somente serão eficazes se o Colaborador cumprir com as obrigações de segurança assumidas nesta Política, uma vez que tais incidentes podem ocorrer em razão de falhas humanas, tecnológicas ou sistêmicas.

Caso o Colaborador tome conhecimento ou suspeite de qualquer acontecimento que viole as regras desta Política ou coloque em risco a segurança das informações da Empresa, ele deverá imediatamente comunicar o CSC da **UY3**.

A **UY3**, por meio do CSC, irá apurar as causas e os efeitos do incidente ocorrido, para então tomar as medidas de contenção, avaliação de impacto e necessidade de comunicação sobre o incidente ao órgão competente e/ou aos titulares das Informações Protegidas, conforme o Plano de Resposta a Incidentes de Segurança da Informação da Empresa.

Para que seja realizada uma auditoria sobre o incidente, a Empresa analisará toda e qualquer informação, bem como as evidências disponíveis que possam identificar a causa do problema. As informações e evidências serão compiladas e anexadas a um relatório para formalização do ocorrido.

19. SANÇÕES

Caso o Colaborador não cumpra as regras desta Política, ele estará sujeito à aplicação de sanções que serão determinadas pela direção da Empresa de acordo com o grau de gravidade da conduta praticada pelo Colaborador, podendo variar entre:

(i) **advertência;**
(ii) **suspensão;** ou
(iii) **encerramento do contrato**.

Os Colaboradores que cometerem infração às regras desta PSC serão comunicados por escrito. Tal comunicação conterá a regra violada, a conduta praticada pelo Colaborador e a sanção aplicada pela Empresa, sem prejuízo de eventual indenização paga pelo Colaborador a ser apurada judicialmente.

20. MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

Todos os Colaboradores devem obrigatoriamente cumprir as disposições expressas nesta PSC, independentemente de seu cargo, função, área de atuação ou localidade na qual exerça suas atividades profissionais vinculadas à Empresa.

Todos os Colaboradores, no ato de sua contratação, receberão uma cópia da Política de Segurança da Informação vigente, em formato impresso ou digital, conforme estabelecido pela Empresa, bem como eventual documentação suporte aplicável (por exemplo, acordo de confidencialidade), que estabeleça, além dos procedimentos de segurança a serem seguidos pelo Colaborador, regras sobre o correto uso das ferramentas e Informações Protegidas.

Uma vez que o Colaborador concorde com os termos descritos na Política e na documentação suporte, deverá assinar um Termo de Responsabilidade (por meio de assinatura física ou de software de assinatura eletrônica, conforme estabelecido pela Empresa) para formalizar o seu comprometimento em cumprir as disposições vigentes e suplementares.

Eventuais alterações introduzidas na Política e nos documentos suporte serão comunicadas por escrito ao Colaborador, sendo responsabilidade do Colaborador ler atentamente as atualizações enviadas. A manifestação de aceite, pelo Colaborador, às alterações apresentadas será realizada conforme oportunamente definido pela Companhia, mediante a assinatura do Colaborador, física ou digital, ou por meio de mecanismo de consentimento digital.

21. DISPOSIÇÕES FINAIS

As exceções às regras estabelecidas por esta norma específica para atender alguma demanda específica devem ser apresentadas ao CSC para avaliação e aprovação.

Essa Política poderá ser revista, atualizada e alterada anualmente ou a qualquer tempo, a exclusivo critério da Empresa, sempre que algum fato relevante ou evento motive sua revisão antecipada.

***

Histórico:

Versão	Data	Descrição da Alteração	Páginas Afetadas	Revisado por	Aprovado por
1	21/01/2022	Versão Preliminar	-	Tatiana - Jurídico	Carace – Diretor
2	13/06/2022	Complementar Seção 16 - Datecenter e Cloud - Capítulo III da Circular BCB nº 3.909	18 e 19	Tatiana – Jurídico e Lucas Tourinho _ Head TI	Carace – Diretor