



CAPITAL

RUBY

POLÍTICA DE SEGURANÇA CIBERNÉTICA

ÍNDICE

1.	OBJETIVO	2
2.	ABRANGÊNCIA.....	2
3.	VIGÊNCIA E ATUALIZAÇÕES.....	2
4.	DIRETRIZES	2
4.1.	DIRETRIZES FUNDAMENTAIS DESTA POLÍTICA	3
5.	CYBER SEGURANÇA.....	6
5.1.	Estrutura de TI.....	6
5.2.	Acesso da equipe de TI.....	7
5.3.	Trilhas de auditoria.....	7
5.4.	Logins e usuários	8
5.5.	Riscos fundamentais identificados e controlados	8
5.6.	Gateway	9
6.	RTM.....	10
7.	SEGREGAÇÃO DE OPERAÇÕES.....	10
8.	BACKUP E REDUNDÂNCIAS	13
9.	DILIGÊNCIAS E CONTROLES	14
10.	PENALIDADES	17
11.	MANUTENÇÃO DOS ARQUIVOS.....	17
12.	DOCUMENTOS RELACIONADOS	17
13.	CONTROLE E REVISÃO.....	17
	ANEXO – TERMO DE CONFIDENCIALIDADE	19

1. OBJETIVO

A Política de Segurança Cibernética (“Política”) assegura a preservação das informações geradas, adquiridas, processadas, armazenadas, transmitidas e descartadas; devendo ser prioridade constante da Ruby, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos, e devem ser protegidas adequadamente; seguindo em conformidade com a Resolução CMN nº 4.893/2021.

2. ABRANGÊNCIA

O público-alvo desta Política são todos diretores e colaboradores da Ruby, bem como estagiários e os prestadores de serviços, clientes e usuários dos produtos e serviços oferecidos pela instituição, a comunidade interna à sua organização e as demais pessoas que, conforme avaliação da instituição, sejam impactadas por suas atividades.

3. VIGÊNCIA E ATUALIZAÇÕES

As diretrizes contidas nesta Política entram em vigor na data de sua publicação e permanecem vigentes por prazo indeterminado, devendo ser revisada anualmente ou em prazo inferior, sempre que solicitado pelo órgão regulador, em casos de alteração de legislação aplicável, ou ainda, se houver alteração no modelo de negócios, previamente validado pelo Compliance.

4. DIRETRIZES

Esta Política visa estabelecer as diretrizes a serem seguidas pela da Ruby se estendem da preservação das propriedades da informação, notadamente sua confidencialidade, integridade, disponibilidade e privacidade dos seus dados permitindo o uso e o compartilhamento da informação de forma controlada em nossos sistemas e informações prestadas, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

As diretrizes têm por principais objetivos:

- Tratamento confidencial: Informações Confidenciais recebidas são tratadas e arquivadas de forma segura e íntegra, se necessário com métodos de criptografia. Estas apenas serão acessadas por pessoas autorizadas e capacitadas para seu uso

adequado; as informações somente serão fornecidas a terceiros, mediante autorização prévia do cliente ou para o atendimento de exigência legal ou regulamentar;

- Disponibilidade por necessidade: o uso de informações confidenciais será garantido apenas àqueles que tiverem acesso em vista de sua função ou que solicitarem sua divulgação por necessidade de trabalho, quando tal necessidade for concreta, sendo possível, desta maneira, identificar qual Colaborador detém cada tipo de informação (“as-needed”);
- Integridade da informação: salvaguarda da exatidão e completeza da informação e dos métodos de processamento e arquivamento, protegendo as informações contra acesso, modificação, destruição ou divulgação não-autorizada.
- Legalidade de uso a informação: garantia de que a informação está em conformidade com a legislação em vigor. Cumprindo as leis e as normas que regulamentam os aspectos de propriedade e assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pela empresa.
- Usuário: a política aplica-se a qualquer usuário da informação, incluindo qualquer Colaborador, incluindo empregados, contratados, estagiários, prestadores de serviços, parceiros que utilizam as informações da empresa.

4.1. DIRETRIZES FUNDAMENTAIS DESTA POLÍTICA

Proteção da Informação

As medidas de proteção da informação devem considerar:

- ✓ os níveis adequados de integridade, confidencialidade e disponibilidade;
- ✓ a legislação, as decisões judiciais, as diretrizes e as instruções e procedimentos em vigor;
- ✓ Manual de Compliance, em especial o Código de Ética;
- ✓ o alinhamento com as estratégias de cada área;
- ✓ as melhores práticas para a gestão da segurança da informação; e
- ✓ os aspectos comportamentais e tecnológicos.

Responsabilidade pela Segurança da Informação

As atividades de Segurança da Informação são exercidas por pessoas com sólidos conhecimentos em Segurança da Informação, inseridas na estrutura organizacional das áreas de Gestão de Riscos e Compliance.

Cada funcionário é responsável pela segurança da informação do grupo e deve cumprir as diretrizes, a declaração de princípios éticos e código de conduta e as instruções de procedimentos e restritos aplicáveis às suas funções zelando pela correta aplicação das medidas de proteção.

Acesso à informação

O acesso e o uso de qualquer informação da empresa, pelo usuário, devem se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da Ruby.

Para acessar informações nos sistemas da empresa deverão ser utilizadas somente ferramentas e tecnologias autorizadas pela empresa.

Senhas são pessoais e intransferíveis, não devem em hipótese alguma ser disponibilizadas a terceiros ou compartilhadas com outros colaboradores.

As Informações confidenciais poderão ser classificadas segundo seu grau de confidencialidade.

A segregação de acessos a informações confidenciais será estruturada a partir de grupos de perfil de acesso.

Regras fundamentais de segurança da informação

Dever de preservar. Os Colaboradores não devem transmitir nenhuma informação não-pública a terceiros. Todos os Colaboradores são responsáveis por preservar ativos de informação e devem estar comprometidos com a proteção adequada de informações e sistemas da empresa, considerando que a segurança da informação é um importante diferencial competitivo.

Autorização prévia. Toda e qualquer divulgação de informações estratégicas da empresa deve ser previamente autorizada.

Acesso privilegiado. Colaboradores da empresa deverão guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Operações em andamento. Colaboradores devem preservar a confidencialidade de informações relativas a operações em andamento, bem como informações recebidas de entidades/pessoas cuja publicidade ou posição possa influenciar o mercado.

Divulgação acidental. Colaboradores devem evitar manter em suas mesas papéis e documentos confidenciais, e manter sigilo sobre senhas do computador, rede e sistemas. Funcionários e sócios devem garantir que o acesso à área de trabalho seja feito somente por pessoal autorizado.

Propriedade da informação. Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional ou dentro da empresa pertence ou foi cedido à Ruby. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Propriedade de equipamentos. 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, visando assegurar o cumprimento desta Política.

Autorização para gravação e uso. Esta Política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Autorização para monitoramento de rede. O colaborador está ciente de que a Ruby pode e monitorará a rede interna para garantir a integridade dos dados e programas.

Autorização para monitoramento mensagens. O colaborador está ciente de que a Ruby pode e monitorará mensagens de e-mails ou qualquer outra forma de comunicação eletrônica a que o colaborador tiver acesso na empresa para garantir a integridade das informações e mensagens repassadas.

Usos inadequados. 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 instituição cooperará ativamente com as autoridades competentes.

Dever de informar. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Área de Tecnologia e ela, se julgar necessário, deverá encaminhar posteriormente à Diretoria de Compliance para análise.

Termo de confidencialidade

Todo Colaborador assinará o termo de confidencialidade de informações conforme o Anexo ao presente desta Política.

5. CYBER SEGURANÇA

5.1. Estrutura de TI

A Ruby adotará o servidor do OneDrive para armazenamento, leitura, criação e edição de documentos, email, agendas, administração de usuários a rede e segregação de acessos dos documentos por área e inclusive monitoramento equipamentos remotos atrelados aos usuários.

Com total controle e segurança do administrador da área utilizando o serviço em nuvem mais seguro do mundo hoje, atendendo com excelência todas normativas da Resolução nº 4.658 do BACEN, inclusive possuindo hoje servidores no Brasil e entre outras partes do mundo, garantindo assim ainda mais a segurança que veremos logo abaixo segundo a documentação da própria empresa.

O plano do G Suite da instituição contemplará:

- Painel de controle: verificação de insights relevantes sobre sua organização
- Usuários: Adicionar ou gerenciar usuários
- Grupos: Criar grupos e listas de e-mails
- Unidades organizacionais: Adiciona, remova, mova ou pesquise uma unidade organizacional
- Edifícios e recursos: Gerenciar e monitorar edifícios, salas e recursos
- Dispositivos: Proteger os dados corporativos em dispositivos
- Apps: Gerenciar os apps e as respectivas configurações
- Segurança: Definir configurações de segurança
- Relatórios: Monitorar o uso na sua organização
- Faturamento: Gerenciar as assinaturas e o faturamento
- Perfil da empresa: Atualizar informações sobre a empresa
- Funções do administrador: Gerenciar funções administrativas
- Domínios: Gerenciar seus domínios
- Migração de dados: Gerenciar a migração
- Suporte: Suporte (por telefone, chat ou e-mail)

Além disso, será utilizado um servidor interno para backup de todos os dados em nuvem que ficará em nossas dependências.

5.2. Acesso da equipe de TI

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 for 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.

5.3. Trilhas de auditoria

Os sistemas geram e mantêm trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em

meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

5.4. Logins e usuários

Cada usuário deverá ter uma única conta para acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física.

Nenhum usuário poderá usar a conta de outro.

As contas de usuários do G Suite são protegidas por arquitetura segura, que garante que um usuário não possa ver os dados de outro.

É possível acessar todos os dados dos serviços do Google através da página de Web amparada pelo *Https*, que utiliza o protocolo *SSL/TLS*. Este por sua vez oferece uma camada adicional de segurança e permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais.

O cliente de e-mail para dispositivos móveis também usa o acesso criptografado para garantir a privacidade das comunicações. Também exigimos criptografia para o acesso aos seus dados de e-mail por clientes de e-mail de terceiros.

5.5. Riscos fundamentais identificados e controlados

Os principais riscos levantados e cobertos pela atual política são os seguintes:

- Risco de perda de controle de acesso físico a ambientes protegidos;
- Risco de perda de informações por erro operacional;
- Risco de falha de dispositivos de armazenagem e processamento internos;
- Risco de falha de nuvem externa;
- Risco de invasões de terceiros;
- Risco de fraudes e agentes internos corrompidos;
- Risco de acesso a dados sensíveis por pessoa não autorizada (internos e terceiros); e
- Risco de envio das Informações confidenciais ou vírus por e-mails e outras

comunicações eletrônicas.

Acessos proibidos

A Ruby protege continuamente todos os ativos de informação da empresa contra código malicioso, e garante que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Software não-autorizado

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 não autorizado baixado será excluído pela área de Tecnologia de Informação. Os Colaboradores com acesso à internet não poderão fazer o download (baixar) de programas, mesmo que ligados diretamente às suas atividades na Ruby e deverão solicitar a área de Tecnologia da Informação a instalação e licenciamento desses programas, desde que autorizados pela diretoria.

Conteúdo proibido

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

O acesso a softwares *peer-to-peer* (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de *streaming* (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à área de Tecnologia de Informação.

Vírus

Os Colaboradores não poderão utilizar os recursos da Ruby para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

5.6. Gateway

Todas as estações de trabalho passarão por *firewall* de borda que é responsável por

filtrar as conexões de entrada e saída, bem como monitorar e “dropar” (descartar) pacotes não reconhecidos, assim tentativas de invasão bem como fará um monitoramento com antivírus gateway e AntiSpam na rede de computadores.

O Gateway da Ruby está composto por dois links de internet sendo um primário e outro secundário para redundância, são links dedicados simétrico de mídia fibra óptica com velocidades de 50 Mbps para download e 50 mbps para upload. Ambos farão parte da função de *Failover* configurado no Router em que ao identificar qualquer anomalia no link principal automaticamente o secundário (*backup*) será acionado ou vice-versa.

6. RTM

Contratamos com um link dedicado da empresa RTM, que acessará CETIP, Selic e SISBACEN e fará a sincronização de dados com nossas estações, dentro do prédio em outro endereço que servirá de contingência e acomodará o backup externo, lá teremos posições chaves físicas exclusivas que serão utilizadas pelos nossos funcionários em caso de emergência (incêndios a o prédio principal, falta de energia prolongada, ataques etc.).

7. SEGREGAÇÃO DE OPERAÇÕES

A Ruby mantém a devida segregação entre as suas diversas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

Controladoria

Para área de controladoria utilizaremos o sistema BRITECH, lembrando que este sistema é acessado por meio de site e não há instalação de software em máquina local, abaixo seguem a política de tecnologia do sistema BRITECH e a Política de Backup:

Área de Tecnologia da Informação:

Abaixo segue uma série de procedimentos utilizados para garantir a segurança da informação referente a Infraestrutura e instalações do Software.

Infraestrutura instalação:

Os acessos a console da AWS são realizados através de senha forte e token.

Servidores hospedados na rede privada dentro da rede AWS.

Os acessos a rede privada dentro da AWS são realizados pelo administrador através de uma VPN com senha forte e certificado de segurança.

Todas as informações de tráfego da rede e acesso aos serviços da AWS são logados.

Todos os comandos executados nos servidores são logados.

Criptografia em trânsito na rede com SSL em todos os dispositivos.

O acesso as aplicações são através de Certificado Digital (HTTPS).

Informações do Banco de Dados são criptografados.

Usamos o Oracle Flashback Technology, com essa tecnologia podemos voltar o banco de dados do momento atual para qualquer segundo até 30 dias.

Realizaremos backup da infraestrutura, vide política de backup.

Aplicação:

Senha login criptografada.

Controle de acesso e transações gerenciada pelo administrador do sistema designado pelo cliente.

Log auditoria informa situação anterior e atual do cadastro, com dados do usuário que fez a alteração, IP da máquina, data e hora da alteração.

Custódia

Na área de custódia de FIDC utilizaremos o sistema FROMTIS que terá acesso via site, sem instalação de software na máquina da estação, o sistema ficará em 2 servidores Fujitsu, no Brasil, com as seguintes especificações.

Servidor SQL.

Papel da Instância: Banco de Dados;

de 4 a 8 vCPUs 2.6 Ghz;

de 32 a 64 GB de RAM;

Disco - 500 GB de Disco SSD;

Sistema Operacional: Windows Server 2016 64 Bits;

Banco de Dados: MS SQL Server 2012 Standard ou superior (em inglês).

Servidor de aplicação.

Servidor Aplicação (para até 2 aplicações).

Papel da Instância: Aplicação;

2 vCPUs 2.1 Ghz;

8 GB de RAM;

Disco - 200 GB de Disco SSD;

Sistema Operacional: Windows Server 2016 64 Bits.

A Fujitsu possui um programa de treinamento anual obrigatório junto aos funcionários sobre segurança da informação. Trata-se de uma plataforma de treinamentos Global onde são abordados temas e conceitos, bem como ações a serem tomadas para garantir a segurança da informação da empresa e dos clientes, possui política e/ou procedimento de backup e redundância de informações, trabalha com os sistemas de proteção citados além de manter os sistemas operacionais e aplicações atualizados.

Sua contingência fica a mais de 20km de distância geográfica do datacenter principal, A Fujitsu realiza testes periódicos de verificação de segurança e integridade de sistemas.

Todo o tráfego entre a contratante e a contratada é criptografado utilizando VPN site-to-site. Além disso, o acesso ao ambiente da contratante é controlado através de ACL (regras de firewall).

Possuímos Firewall e mecanismo de detecção de atividade ilícita/suspeita (IDS) sendo que o mesmo é opcional e deve ser contratado a parte. Sim resposta ao cliente cadastrado na Fujitsu para este fim. Os SLAs de resposta e fluxo de comunicação são definidos junto aos clientes na contratação do serviço para atender a necessidade do negócio.

A Fujitsu oferece serviços de *Cloud Computing Privada*, onde todos os ambientes virtuais são logicamente segregados. Além de contar mecanismos de controle de tráfego de rede e acesso restrito aos equipamentos.

Existe sim restrição para a entrada física com fechadura biométrica. Para o acesso ao datacenter é necessário o cadastro de uma visita através de um sistema online, feita por um administrador do datacenter.

O backup é realizado por um servidor dedicado no mesmo site dos demais servidores, entretanto, este servidor é replicado para um segundo datacenter 20km de distância como contingência.

O plano de backup e retenção é definido pelo cliente de acordo com as necessidades do negócio. Incluindo o envio de evidências de backup e restore e destruição dos dados.

Caso haja a necessidade, os dados são restaurados de acordo com o SLA do contrato e o plano de backup. Este processo se inicia a partir da abertura de um ticket via e-mail por onde toda a comunicação é feita.

A Fujitsu possui os Certificados ISO 27001, ISSO 22301, ISO 9001, SOC1, SOC2, SAP Cloud Infrastructure Certificate.

A custódia de ativos financeiros de outros tipos de fundos será armazenada em nossos sistemas e registrados nos ambientes e órgãos competentes.

Liquidação

As liquidações financeiras serão feitas através dos sites dos maiores bancos do país que pressupomos que já atendam a resolução vigente do Bacen, através de token sempre em dois passos, com autorização apenas para lançamento pelo analista e aprovação via token pelo responsável pela área, assim será também para os ambientes CETIP e Selic.

8. BACKUP E REDUNDÂNCIAS

Elétrico

Em caso de queda ou instabilidade na rede elétrica, o parque de máquinas da Ruby conta com (1) nobreak de 1200 va por estação de trabalho e garante uma autonomia

média de 2h40m, o Data Center é servido por (2) nobreaks de 3 kva e oferece uma autonomia de até 8 horas para continuidade de sua operação.

Físico

De acordo com o que já foi mencionado, a Ruby contará com ambiente físico de contingência para a continuidade da operação, este por sua vez se assemelha ao mesmo ambiente de produção e está alocado na estrutura RTM no endereço: Rua Líbero Badaró 377 11º e 22º andares – Centro – São Paulo – SP.

Para qualquer incidente de força maior, não deverá ocorrer interrupção dos serviços já que automaticamente o ambiente externo será acionado, seja a contingência para estações de trabalho quanto servidores de arquivos e aplicações.

Lógica

Para a contingência lógica a [•] conta com o plano de DRP (Desastre Recovery) para as seguintes Ci's; redundância para o link de internet principal de forma transparente e controlado pelo *Firewall* de borda, utilizando o recurso de failover (quando identificado qualquer anomalia no link principal, e para garantir a continuidade de operação o sistema aciona o link secundário automaticamente), redundância para o ambiente de dados e aplicações do servidor de produção para o ambiente de dados alocados no site da RTM já supra mencionado, plano de backup e restore de dados (arquivos, pastas, arquivos de banco de dados) copiados regularmente em mídias externas gerenciado com o software de backup, para o planejamento de backup está previsto 3 fases de cópias. Na primeira fase a cópia será realizada em storage externa de 2 terabytes com a gestão de um backup completo mensal e outro incremental diário, na segunda fase será realizado uma vez por semana a cópia do primeiro disco para um disco externo secundário denominado "disco de transporte" em que será retirado por um funcionário autorizado das dependências da Ruby que levará para um site externo onde ficará até a próxima rotina de backup e sendo armazenado em cofre seguro. Já na terceira e última fase será realizada uma cópia em tempo real do *file server* para o sistema *Google Cloud* (nuvem).

9. DILIGÊNCIAS E CONTROLES

A Ruby controla os dados, sistemas e serviços, com o objetivo de proteger os ativos de informações e a privacidade de seus clientes contra a coleta, retenção, uso, divulgação, modificação ou destruição não autorizada. Isso é abordado através de normas, procedimentos e arquitetura de segurança com a adoção de controles técnicos apropriados.

A política e os controles de segurança da informação fornecem cobertura de áreas críticas de segurança da informação, incluindo:

Programa de Conscientização de Segurança da Informação e Riscos Cibernéticos – Periodicamente é feito um programa de conscientização de segurança aos funcionários e demais colaboradores para que conheçam os riscos e possam agir adequadamente. As políticas de segurança garantem os deveres e responsabilidades dos funcionários e demais colaboradores em relação à proteção dos ativos de informação.

Controle de acesso - O acesso é concedido com um mínimo de privilégio e necessidade de saber. Todo o acesso é concedido com base em perfis de usuários e com aprovação prévia adequada na plataforma de Gerenciamento de Acessos. Acesso a dispositivos moveis e serviços de armazenamento web são controlados.

Segmentação dos Ambientes – Os ambientes são segregados para que exista um controle de tráfego entre os eles, garantindo maior restrição nos ambientes que exigem mais integridade e confidencialidade.

Segurança de aplicações – Desde o processo de planejamento e criação da arquitetura, até o processo de implantação, as aplicações estão sujeitas a um processo de análise de segurança para confirmar que foram desenvolvidas de acordo com nossas normas e padrões de segurança de desenvolvimento de aplicativos.

Classificação das Informações – Todas as informações geradas ou sobre custódia pela Ruby, são classificadas de forma manual ou automática (quando possível) de acordo com as normas internas de classificação a informação, garantido o nível de proteção

adequado a informação.

Plano de Continuidade ao Negócio e Recuperação de Desastres – O ambiente Operacional da Ruby é digital, arquitetado para que os sistemas, processos e ativos críticos suportem eventos catastróficos utilizando de recursos em alta disponibilidade, garantindo contingência. Os sistemas que mantem essa disponibilidade são testados regularmente para garantir a eficácia do processo em casos reais de desastres. São feitas regularmente novas análises de impacto ao negócio e alterações no plano caso se façam necessário.

Gerenciamento de Fornecedores – O processo conduz análises de diligências em atividades relacionadas à Segurança da Informação e Compliance de terceiros, incluindo: avaliação de potenciais fornecedores para o cumprimento das políticas e controles da empresa; controles em relação a Privacidade dos Dados; revisões de devida diligência, incluindo a elaboração de classificações de risco e resultados; mitigação de riscos; Suporte na seleção de fornecedores.

Resposta a Incidentes – O departamento de Segurança da Informação detecta, controla e remedia incidentes relacionados a segurança de sistemas, processos e ativos de informação.

Em caso de alguma violação, a equipe de segurança da informação tomará medidas para manter as informações seguras e mitigar a violação. As notificações oportunas de clientes afetados são emitidas de acordo com os requisitos contratuais, regulamentares e legislativos.

Periodicamente são feitas novas análises deste processo (plano) para garantir máxima eficiência na detecção e controle dos incidentes.

Gestão de Vulnerabilidades – É feito regularmente processos de rotina que visem diminuir as falhas sistêmicas que possam ser exploradas por ataques. Todas as falhas detectadas são colocadas para acompanhamento e correção de acordo com o nível de criticidade do sistema.

Proteção de Recursos Computacionais – Todos os equipamentos computacionais da Ruby, possuem políticas de configuração segura, atualizações constantes de patches de segurança e proteções contra malwares. Todos os tráfegos de rede e mídias removíveis são controlados e monitorados para detecção de incidentes.

Termo de confidencialidade

Todo Colaborador assina termo de confidencialidade de informações conforme o Anexo à presente Política.

10. PENALIDADES

O não cumprimento desta Política implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho e/ou de serviços, outra ação disciplinar e/ou processo civil ou criminal.

11. MANUTENÇÃO DOS ARQUIVOS

A Ruby manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Conformidade (Compliance) desta Política pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

12. DOCUMENTOS RELACIONADOS

Esta Política é interpretada em conjunto com os seguintes documentos: Código de Ética e Conduta Profissional, Manual de Compliance e Controles Internos e Política de Segurança da Informação.

Todos os colaboradores e prestadores de serviços devem observar as seguintes leis, mas não se limitando somente a elas, que servem como suporte a esta Política.

Lei nº 9.609 de 19 fevereiro de 1998. Proteção da propriedade Intelectual

Lei nº 13.709 de 14 agosto de 2018. LGPD

13. CONTROLE E REVISÃO

Informações Gerais	
Título	POLÍTICA DE SEGURANÇA CIBERNÉTICA
Número da Versão	V1
Data da Última Aprovação	01/10/2022

ANEXO – TERMO DE CONFIDENCIALIDADE

Por meio deste Termo de Responsabilidade e Confidencialidade (“Termo”), _____, inscrito no CPF sob o no _____ (“Colaborador”), e Ruby, para fim de preservação de informações pessoais e profissionais dos clientes e da Ruby, e para o resguardo da propriedade intelectual da empresa, acordam e resolvem o que se segue:

São consideradas informações confidenciais (“Informações Confidenciais”), para os fins deste Termo:

- a) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos administrados ou geridos pela Ruby, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Ruby a seus sócios ou clientes, independente destas informações estarem contidas em discos, disquetes, pendrives, fitas, outros tipos de mídia ou em documentos físicos.
- b) Informações acessadas pelo colaborador em virtude do desempenho de suas atividades na Ruby, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Ruby ou de subsidiárias ou empresas coligadas, afiliadas ou controladas pela Ruby ou, ainda, junto a seus clientes, fornecedores e prestadores de serviços em geral.

Não são consideradas Informações Confidenciais:

Quaisquer informações que: (i) já forem de domínio público à época em que tiverem sido obtidas pelo Colaborador; (ii) passarem a ser de domínio público, após o conhecimento pelo Colaborador, sem que a divulgação seja efetuada em violação ao

disposto neste Termo; (iii) já forem legalmente do conhecimento do Colaborador antes de lhes terem sido reveladas e este não tenha recebido tais informações em confidencialidade; (iv) forem legalmente reveladas ao Colaborador por terceiros que não as tiverem recebido sob a vigência de uma obrigação de confidencialidade; (v) forem ou sejam divulgadas ou requisitadas por determinação judicial, Poder Público e/ou pela autoridade competente, devendo o Colaborador, neste último caso, informar imediatamente ao Compliance da Ruby para que as medidas legais cabíveis sejam tomadas, observado o disposto no item 5 deste Termo.

O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Ruby, comprometendo se, portanto, observadas as disposições do Código de Ética (“Código”) e dos manuais de Compliance da empresa (“Manuais”), a não divulgar tais Informações Confidenciais para quaisquer fins ou pessoas estranhas à Ruby, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Ruby.

As obrigações ora assumidas ainda persistirão no caso do colaborador ser transferido para qualquer subsidiária ou empresa coligada, afiliada, ou controlada pela Ruby.

A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita a apuração de responsabilidades nas esferas cível e criminal.

O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a Ruby ou terceiros, ficando desde já o Colaborador obrigado a indenizar a Ruby, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

O descumprimento acima estabelecido será considerado ilícito civil e criminal,

ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho, e desligamento ou exclusão por justa causa do Colaborador se este for sócio da Ruby, sem prejuízo do direito da Ruby de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

O Colaborador expressamente autoriza Ruby a deduzir de seus rendimentos, sejam eles remuneração, participação nos lucros ou dividendos observados, caso aplicáveis, eventuais limites máximos mensais previstos na legislação em vigor, quaisquer quantias necessárias para indenizar danos por ele dolosamente causados, no ato da não observância da confidencialidade das Informações Confidenciais, nos termos do parágrafo primeiro do artigo 462 da Consolidação das Leis do Trabalho, sem prejuízo do direito da Ruby' de exigir do Colaborador o restante da indenização, porventura não coberta pela dedução ora autorizada.

A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, mencionados nos itens supracitados.

O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

O Colaborador reconhece e está ciência de que:

a) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Ruby são e permanecerão sendo propriedade exclusiva da Ruby de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Ruby, devendo todos os documentos permanecer em poder e sob a custódia da Ruby, salvo se em virtude de interesses da Ruby for

necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Ruby;

b) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Ruby todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

c) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Ruby, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

d) É expressamente proibida a instalação pelo Colaborador, de softwares não homologados pela Ruby no equipamento do mesmo.

e) A senha que foi fornecida para acesso à rede de dados institucionais é pessoal e intransferível e não deverá, em nenhuma hipótese, ser revelada a outra pessoa.

f) O software antivírus, instalado no equipamento do Colaborador jamais deverá ser desabilitado, exceto com prévia anuência da área de informática e do Compliance.

Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Ruby, permitindo que a Ruby procure a

medida judicial cabível para atender ou evitar a revelação.

Caso a Ruby não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela a que o Colaborador esteja obrigado a divulgar.

A obrigação de notificar a Ruby subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a Ruby, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto supracitado será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelo Compliance, conforme descrito no Código Ética.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

São Paulo, ____ de _____ de 20__.