PLANO DE CONTINUIDADE DE NEGÓCIOS E DE SEGURANÇA CIBERNÉTICA

R2C Gestora de Investimentos Ltda.

CNPJ: 20.495.002/0001-06
NIRE: 35.228.0028402-8

Rua dos Pinheiros, nº 498, 14º andar, conjunto 141
São Paulo – SP
CEP 05422-000

www.r2cinvest.com.br

---

17 de fevereiro de 2023
(Versão 04)

ÍNDICE

1. Apresentação e objetivo

A R2C Gestora de Investimentos Ltda. ("**R2C**") atua de forma isolada e com equipes próprias na gestão de recursos de terceiros, por meio da gestão de veículos de investimento atuantes no mercado altamente específico de *distressed assets*, (e.g. créditos devidos por empresas em situação de insolvência, ativos sujeitos a discussões judiciais, dentre outros), na gestão de fundos de investimentos direcionados a aquisição de valores mobiliários negociados em mercados organizados e no oferecimento de acesso a estruturas não tradicionais de investimento voltadas à aceleração do crescimento (*growth*) de negócios que tenham atingido saturação na captação de recursos junto ao mercado de crédito.

Não obstante, a atividade de gestão de recursos exige a mais completa relação de credibilidade e confiança entre prestador de serviço e os investidores sendo que, para tanto, a existência de medidas de contingência para proteção das informações é imprescindível.

Sendo assim, o Plano de Continuidade de Negócios e de Segurança Cibernética ("**Plano**") tem por objetivo descrever as medidas adotadas pela R2C para garantir a segurança de todo conteúdo de informação e assegurar a continuidade da atividade caso ocorram falhas nos sistemas gerenciais ou nas instalações físicas da R2C.

Por meio de ações preventivas, o Plano confere à R2C determinados procedimentos, controles, responsabilidades e regras garantidoras da continuidade das operações e segurança das informações em caso de qualquer eventualidade.

2. Plano de continuidade de negócios e de Segurança Cibernética

A R2C possui todos os equipamentos necessários para armazenar e preservar as informações de seus clientes de maneira segura caso ocorram eventualidades que ameacem a integridade de tais informações ou da R2C, como se verá

2.1. Rede- Infraestrutura

(i) **Links de Internet:** A R2C possui dois links de internet operando no modo de FAILOVER (Tolerância a falhas), esses links pertencem a operadoras diferentes visando garantir uma separação física e logica no que compete a infraestrutura de cabeamento e roteadores para garantir que os Links fiquem operantes em caso de falha das operadoras.

LINK Claro NET – IP Dinâmico
Esse link opera como link secundário para navegação.

LINK VIVO – IP Estático
Esse link por possuir um IP Estático opera para conexões SSL-VPN e entre os colaboradores e a rede da R2C. Também atua como link primário de navegação.

(ii) **Firewall Watchguard em alta disponibilidade:** A R2C possui na borda das suas conexões de internet dois firewalls operando em Alta Disponibilidade. O Firewall primário chamamos de "FW-R2C-ACTIVE" está operando em modo Ativo atendendo a todas as requisições de entrada e saída da rede. O Firewall secundário chamamos de "FW-R2C-PASSIVE" e está operando em modo passivo, em standby monitorando o firewall para que, em caso de falha do primário, este assuma as requisições sem impactar os usuários.

(iii) **Recursos de Segurança:**

- FireCluster (Alta Disponibilidade)
  Dois equipamentos operando em alta disponibilidade de hardware em caso de falhas;

- WAN Failover
  Opera monitorando os links de internet e em caso de falha no link primário, alterna automaticamente para o link secundário;

- Intrusion Prevention Service (IPS)
  Efetua varredura de todas as portas e protocolos para proporcionar proteção em linha contra ataques;

- Application Control

Bloqueia aplicativos de risco, não autorizados e inapropriados, para dar segurança e produtividade;

- APT Blocker
  Usa tecnologia sandboxing premiada para detectar e bloquear malwares avançados e ataques de dia zero;

- Gateway AntiVirus (GAV)
  Usa tanto análise de assinaturas como heurística sofisticada para deter ameaças;

- DNSWatch
  Reduz a incidência de infecções por malware detectando e bloqueando solicitações de DNS mal-intencionadas e redirecionando usuários para uma página segura com informações para reforçar as melhores práticas de segurança;

- Reputation Enabled Defense (RED)
  Usa pontuação de reputação para garantir navegação de internet mais rápida e segura com funcionalidades especiais de botnet detection;

- WebBlocker (filtragem de conteúdo/URL)
  Proporciona filtragem de URL e conteúdo para bloquear materiais censuráveis e malwares.

(iv) **Switches e Distribuição e Wireless:** A R2C possui dois Switches, responsáveis por conectar os dispositivos com a rede, estes switches são gerenciáveis e estão cascateados para expandir o número de portas de rede, além de 2 Acess Points AC com gerenciamento centralizado.

(v) **Controles de Acesso e Monitoramento:** A R2C possui DVR com monitoramento e gravação de câmeras de circuito interno, além de controle de acesso de portas via cartão magnético.

2.2. Rede- Servidor e Armazenamento

(i) **Servidor Dell Poweredge R540:** A R2C possui dois servidores físicos Dell PowerEdge R540 responsáveis por hospedar três Máquinas Virtuais:

Máquina Virtual – R2CSP1VM001

- *Active Directory – Primary Domain Controller*

Gerenciamento de contas e senha de computadores e usuários assim como políticas de rede para as estações de trabalho;

- *DNS (Domaine Name System)*

Sistema de resolução de nomes da rede interna (essencial para o funcionamento da estrutura de controle de usuários e senhas, o AD);

- *DHCP (Dynamic Host Configuration Protocol)*

Habilita usuários para receber de forma dinâmica e transparente os endereços IP para os dispositivos da rede.

Máquina Virtual – R2CSP1VM002

- *Servidor de Arquivos*

Onde estão armazenados todas as pastas e arquivos da rede, com controle de acesso feito pelas permissões NTFS através dos usuários e grupos do *Active Dictory;*

- *Servidor de Impressão*

Destinado a controlar as tarefas de impressão enviadas para as impressoras locais e de rede, pelas diferentes estações de trabalho que compartilham entre si o uso destes equipamentos.

Máquina Virtual – R2CSP1VM003

- *Servidor Secundário de Active Directory, DNS e DHCP*

Este servidor assume o papel de *Active Directory*, DNS Server e DHCP primário caso ocorra falha do outro servidor, além de balancear a carga de trabalho destas funções.

2.3. Segurança de dados

(i) **Back Up:** Atualmente a R2C conta com duas soluções de backup de seus dados. Em caso de perda de dados, utiliza-se o Backup Local ou Off Site para restauração granular de arquivos e pastas.

Nos casos de perda de servidores físicos ou máquinas virtuais, pode-se restaurar para outro servidor a partir do Backup Local. Na hipótese de perda de servidores físicos e Backup Local, há possibilidade de restauração das máquinas virtuais a partir do Backup Off Site (nuvem).

- *Backup Local*

Backup completo das máquinas virtuais para HD externo;

- *Backup Off Site*

Backup dos arquivos da rede, banco de dados e estado do sistema, para nuvem da Solarwinds.

2.4. Antivírus

(i) **Kaspersky Endpoint Security for Business:** a R2C conta com a solução de antivírus com gerenciamento centralizado e instalado em todos os computadores e servidores da rede, com as seguintes funcionalidades:

- Segurança para computadores, Linux e Mac;
- Segurança para servidores;
- Segurança para dispositivos móveis;
- Controle de aplicativos para computadores;
- Controles de dispositivos e da Web;
- Proteção contra *ransomware*;
- Inteligência assistida por nuvem;
- Console de gerenciamento único.

2.5. Recuperação de Desastres

(i) **Hyper – V Réplica:** a R2C conta com uma solução para recuperação de desastres que replica suas três Máquina Virtuais (R2CSP1VM001, R2CSP1VM002 e R2CSP1VM003) para outro servidor físico (host). Em caso de falha crítica de hardware no servidor principal, as Máquinas Virtuais serão iniciadas no outro servidor físico, possibilitando continuidade da operação.