Plano de Continuidade de Negócios e Segurança da Informação

Resumo

Descreve as diretrizes e premissas básicas adotadas pela RIVIERA para estabelecer as medidas a serem tomadas para identificar, prevenir e contornar as possíveis contingências que poderão trazer um impacto negativo considerável sobre a condução das atividades da RIVIERA, bem como descrever a política de segurança da informação adotada.

Sumário

Plano de Continuidade de Negócios e Segurança da Informação

Plano de Continuidade de Negócios e Segurança da Informação

1. Objetivo

Tem por objetivo estabelecer as medidas a serem tomadas para identificar e prevenir as possíveis contingências que poderão trazer um impacto negativo considerável sobre a condução das atividades da RIVIERA. Dentre estas contingências se incluem, por exemplo, crises econômicas, falhas operacionais e/ou desastres naturais. Neste sentido, a política também inclui a estrutura física e lógica da RIVIERA, bem como seu o complexo de segurança da informação de que faz parte.

2. Público-alvo

2.1 Todos os colaboradores e diretores da RIVIERA.

3. Definições

3.1 Rede Riviera

3.1.1 Abrange todos os sistemas, diretórios e Intranet disponibilizados aos Colaboradores da RIVIERA, conforme perfil de acesso definido.

3.2 Software

3.2.1 São todos os programas instalados nos computadores, os quais são disponibilizados pela equipe de Tecnologia da Informação para o exercício de sua função.

3.3 Homologação

3.3.1 Verificação pela equipe de Tecnologia da Informação quanto à compatibilidade técnica do software e aplicativos em relação ao parque tecnológico. Confirmação pelo usuário final do sistema do adequado funcionamento das funcionalidades previstas no quando da implantação ou da atualização de versão do mesmo.

3.4 Informações Confidenciais

3.4.1 São consideradas informações confidenciais, para os fins desta Política, quaisquer informações consideradas não disponíveis ao público ou reservadas, dados, especificações técnicas, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, software e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela RIVIERA em decorrência do desempenho de suas atividades.

3.5 Colaboradores

3.5.1 São as pessoas naturais ou pessoas jurídicas contratadas pela RIVIERA para o desenvolvimento de suas atividades operacionais.

4. Recuperação do negócio e das atividades

4.1 Procedimento adotado em casos de contingência

Plano de Continuidade de Negócios e Segurança da Informação

4.1.1 A RIVIERA mantém a identificação atualizada de seus principais processos de negócios, de forma que em caso de ocorrência de contingências seja possível retomar as operações com os menores custos de transação e perdas de tempo e de recursos humanos, físicos e materiais possíveis.

4.1.2 Nesse sentido, para recuperar todos os procedimentos e atividades realizados diariamente, a RIVIERA se utiliza de tecnologia de última geração, com previsão de alternativas para cobertura em casos de falhas ou interrupções nas transações e consultas de dados, seja por pane de energia ou mesmo impossibilidade física (incêndio, roubo e etc).

4.1.3 Vale destacar que a RIVIERA está sediada no Edifício Plaza Iguatemi, dotado de alta tecnologia e que conta com avançados equipamentos de segurança, incêndio, telefonia e intercomunicação possuindo ainda sistema de cogeração de energia, além de geradores de emergência e demais itens necessários ao perfeito desenvolvimento das atividades da Sociedade.

4.1.4 Além disso, a RIVIERA possui sistema de contingência ao acesso de internet, com um provedor de internet e servidor “cloud” onde todas as informações são replicadas. Além da redundância de sistemas, a RIVIERA conta com local externo para início imediato das transações em caso da ocorrência de qualquer evento que acarrete na impossibilidade de utilização do escritório.

4.1.5 O servidor está instalado em sala com controle de acesso por senha. O equipamento é dotado de no-break e protegido por sistema de antivírus, hacker, e está em ambiente refrigerado por aparelho exclusivo para a função. É realizada online, em tempo real, uma cópia de segurança das informações para servidor espelho. Além disso, é realizado o backup em cloud, em link seguro, utilizando-se de sistema que ofereça acesso seguro via internet.

4.1.6 Desta forma, a salvaguarda dos dados brutos dos usuários, bem como imagens das estações de trabalho (planilhas, bancos de dados, etc.) e outras informações operacionais, permitem que a RIVIERA recomponha rapidamente o estado operacional em caso de falhas nos discos rígidos dos equipamentos.

4.1.7 Como resultado destes procedimentos, no caso da equipe da RIVIERA não ter acesso ao escritório, ela contará com todos os procedimentos e sistemas que a permitem voltar a operar sem maiores problemas, uma vez que todos os dados e informações operacionais, referentes aos deveres e procedimentos da RIVIERA estarão em segurança.

4.1.8 Na hipótese de uma contingência que inviabilize o uso do escritório por um longo período, a RIVIERA tem a possibilidade de voltar a operar no prazo estimado de 12h (doze horas) em um outro escritório, situado em sua sede, localizado no mesmo bairro.

4.1.9 Há, periodicamente, a realização de workshops internos entre colaboradores com diversas funções, para atender à hipótese de uma contingência que inviabilize a presença de algum colaborador, temporária ou permanentemente

4.1.10 A Riviera adota plano de contingência e continuidade de negócios estruturado na eventualidade da ausência temporária ou permanente de profissionais em sua estrutura hierárquica, seja para o nível de Diretoria como para os demais. Nos casos de ausência temporária ou de curto prazo, a sucessão é realizada naturalmente na linha vertical; Isto, em razão da RIVIERA Investimentos pressupor a existência das figuras do Gestor/co-gestor, de forma que sempre haja um *backup* profissional e que, dessa forma, o risco de ausência do gestor direto (titular) seja mitigado, por qualquer que seja o motivo.

4.1.11 Havendo ausência permanente ou a médio e longo prazo, a Diretoria responsável ou até mesmo os diretores em conjunto definirão como a lacuna será preenchida, podendo haver realocação de recursos internos ou até mesmo a contratação de profissional externo.

4.1.12 Por fim, para a retomada célere e eficaz das operações após uma contingência a RIVIERA pode se utilizar de alternativas internas ou externas para substituição de equipamentos danificados, através de fornecedores já conhecidos da gestora, bem como manter saldo financeiro e/ou acesso a crédito para qualquer despesa de contingência ou compra de equipamentos ou serviços que se fizerem necessários. Ainda, pode valore-se de outros procedimentos que visem a retomada das atividades.

5. Parque tecnológico

Plano de Continuidade de Negócios e Segurança da Informação

5.1 Link Principal:

5.1.1 Algar Telecom Plano: Link Dedicado 10 Mbps.

5.2 Link Secundário:

5.2.1 Americanet Plano: Link Dedicado 10 Mbps.

5.3 Modem:

5.3.1 Equipamentos Fornecidos Pelos Provedores De Links.

5.4 Firewall:

5.4.1 Fabricante: Fortinet Modelo: Fortigate 100d.

Access Point/ Wireless :No Ambiente, Existe 01 Roteador Wireless Ativo; Fabricante: Tp Link; Modelo: Tl-Wr840n; Ssid: Riviera.

5.5 Switch / Transiver:

5.5.1 No Rack Há 01 Switch: Fabricante: Hp Modelo: Hp V1410-24 – J9663a; Portas: 24 Portas; Velocidade:10 / 100 Mbps.

5.6 Nobreak:

5.6.1 No Rack, Há 01 No-Break Dedicado Para Os Equipamentos; Fabricante: Apc; Modelo: Apc 1400; Potência: 1400 Va; Input: 127 V / 220 V Output: 127 V

5.7 Servidores:

5.7.1 Ambiente Com 01 Servidor Ativo; Fabricante: Dell; Sistema Operacional: Windows Server 2012 Standard – X64

5.8 Servidor *Cloud*:

5.8.1 Funções Principais: -Active Directory (Dominio: Riviera.Local) -Dns -File Server.

5.9 Análise De Segurança Interna:

5.9.1 Apenas Porta Homologadas Estão Disponíveis Para Comunicação.

5.10 Unidade De Armazenamento:

5.10.1 No Rack Há 01 Disco Externo; Fabricante: Seagate; Nome: Backup (F:); Capacidade De Armazenamento: 931 Gb.

5.11 Desktops / Notebooks:

5.11.1 Computadores: 12 Unidades Modelo: Dell 3040m.

5.12 Impressora / Multfuncionais.

No Ambiente Há 02 Impressoras: Fabricante: Konica Modelo: C35p Conexão Via Tcp/Ip; Fabricante: Kyoscera Modelo: Fs 1135 Mfp Conexão Via Tcp/Ip.

5.13 Sistema De Telefonia:

5.13.1 Equipamento Voip /Ata; Pabx: O Ambiente Possui 01 Central Pabx; Fabricante: Panasonic; Modelo: Tde200.

5.14 Solução De Voz:

5.14.1 Algar Telecom Canal E1 Range De Ddrs: 11 4862-7500 à 11 4862-7599.

5.15 Solução de Backup:

5.15.1 “Srvriv01”; Método De Backup: Windows Server Backup; Rotina: Diária; Arquivos: Full Server; Destino: Hd Externo Usb Seagate; Status: Ok.

5.16 Antivírus:

5.16.1 O servidor, bem como todas as máquinas dos colaboradores, contam com solução antivírus para o sistema Windows. Servidor: Cla Win Antivirus; Máquinas: McAfee Antivirus.

5.17 Software:

5.17.1 As Aquisições Dos Equipamentos Já Contemplam O Licenciamento Do Windows.

5.18 Pacote Office:

5.18.1 Equipamentos Com Office 365 Licenciado.

5.19 E-Mail Corporativo:

5.19.1 Solução Google For Business.

5.20 Domínios:

5.20.1 Empresa Utiliza o Domínio “rivierainvestimentos.com.br”.

6. Diretrizes

6.1 Política de senhas

6.1.1 A senha é de uso pessoal e intransferível, sendo estritamente proibido o compartilhamento de senhas.

6.2 Acesso Físico

6.2.1 O acesso às dependências da RIVIERA para colaboradores é feito mediante autenticação via cartão magnético de segurança, que é fornecido individualmente. Este cartão é pessoal e intransferível, sendo vedado seu compartilhamento com terceiros;

6.2.2 Deste modo, fica vedada a entrada de quaisquer terceiros, salvo se autorizados e acompanhados por diretor da RIVIERA;

6.2.3 O acesso à sala de máquinas é restrito à empresa contratada para a manutenção da Rede RIVIERA, e controlado via senha. Colaboradores da RIVIERA e terceiros não tem acesso à senha;

6.3 Proteção e Integridade de dados

6.3.1 A RIVIERA seguirá as políticas relacionadas à Gestão de Tecnologia da Informação. O Officer de Risco da RIVIERA deverá monitorar ativamente o cumprimento dessas normas e comunicar imediatamente à Diretoria de *Compliance* da RIVIERA eventuais fragilidades e não conformidades identificadas. A RIVIERA se vale de mecanismos de *firewall*, *antivirus* e *antispam*. São realizadas cópias de segurança de sistemas e dados utilizando-se de software específico no "*Cloud*".

7. Informações de Controle

Responsáveis pelo Instrumento Normativo:

Etapa	Responsável	Contato	Unidade Organizacional
Elaboração	André Luís Bergamaschi	alb@bmbz.com.br	BMBZ Advogados
Revisão	Sabrina Molina	sabrina@rivierainvestimentos.com.br	Riviera Investimentos
Aprovação	Márcio Pinheiro Guimarães	marcio@rivierainvestimentos.com.br	Riviera Investimentos