# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

**ALOCC GESTÃO FINANCEIRA LTDA.**
(“ALOCC”)

## 1. Objeto

O presente instrumento tem como principal objetivo a definição de regras e princípios das condutas dos Colaboradores da ALOCC no que se refere à segurança da informação e segurança cibernética.

Em caso de dúvidas ou necessidade de aconselhamento, o Colaborador deverá buscar auxílio junto ao Compliance que centralizará as questões de segurança cibernética e da informação para serem tratadas com o Responsável pela área de Tecnologia da Informação (“TI”).

## 2. Acesso Restrito

A troca de informações entre os Colaboradores da ALOCC deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação.

Os Colaboradores da ALOCC que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos sistemas, devendo salvaguardar as senhas e outros meios de acesso aos mesmos.

Os arquivos da ALOCC são armazenados em nuvem e servidores internos geridos pela área de TI.

O acesso controlado às pastas e arquivos se dá mediante a outorga de senhas de acesso individuais e intransferíveis que permitem a identificação do seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

Adicionalmente, todas as mensagens enviadas/recebidas dos computadores disponibilizados pela ALOCC permitem a identificação do seu remetente/receptor.

Em caso de acesso remoto concedido em caráter de exceção a colaboradores, este é protegido por criptografia, onde o sistema se baseia na identidade do usuário, solicitando uma identificação para acesso aos documentos da rede.

O armazenamento de informações em dispositivos portáteis deve restringir-se aqueles fornecidos pela ALOCC, mediante prévia autorização do Comitê Estratégico e ciência do Compliance.

A outorga de senhas é de responsabilidade do TI e deve ser realizada com a aprovação do Comitê Estratégico e o acompanhamento do Compliance, a fim de evitar a transgressão de barreiras de informação e potenciais conflitos de interesse. Este procedimento deverá ser observado ainda na hipótese de mudança de atividade/área de um determinado profissional dentro da ALOCC.

As senhas de acesso possuem prazo de validade e requisitos mínimos de segurança e são desabilitadas após um número máximo de tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação.

Após um tempo máximo de inatividade, os computadores bloqueiam e ficam protegidos por senha. Para reiniciar a sessão, o usuário terá que se autenticar novamente.

No caso do desligamento ou saída de algum Colaborador, o acesso aos arquivos será imediatamente bloqueado e a respectiva senha revogada pela equipe de TI. Para sistemas de terceiros, a ALOCC deverá submeter uma solicitação de revogação de acesso imediatamente e assegurar-se de que os acessos sejam revogados.

O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física do departamento interno de qualquer outra atividade no mercado de capitais que venha a ser desenvolvida pela ALOCC ou que, de alguma forma, possa vir a limitar a independência na tomada de decisões.

Quaisquer exceções aos parâmetros descritos neste manual devem ser submetidas ao Comitê Estratégico para avaliação de potenciais riscos.

## 3. Backup

O prestador de serviço de backup em nuvem do servidor de arquivos, armazena versões anteriores durante diferentes períodos, ou seja, se algum arquivo for apagado ou alterado de forma errônea, é possível recuperá-lo durante períodos pré-determinados.

Os backups são armazenados em Datacenters de empresas terceirizadas com ambiente controlado e contingenciado, sendo possível o acesso mediante autenticação, em caso de necessidade.

O serviço de e-mail é provido por sistema de nuvem e por empresa de alta reputação que possui Datacenters com ambientes controlados e contingenciados. Os computadores possuem cópia local dos e-mails gerados nos últimos 6 meses. Além disso, os e-mails excluídos são mantidos na Lixeira por até 2 anos.

## 4. Cópia de Arquivos e Instalações

Todos os sistemas utilizados pelos Colaboradores são instalados de forma padronizada pela área de TI. A instalação de novos programas necessita da autenticação com privilégios de administrador (TI) que deve submeter o pedido à aprovação de um membro do Comitê.

A cópia de arquivos e instalação de programas em computadores deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da ALOCC. Nestes casos, o Colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Qualquer impressão de documentos deve ser imediatamente retirada da impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da ALOCC. Para mitigar este risco, as áreas possuem impressoras segregadas em seus ambientes. É vedada, ainda, a manutenção destes documentos em mesas, máquinas de fax ou copiadoras.

## 5. Descarte de Informações

O descarte de informações confidenciais deve observar as seguintes diretrizes:

(i) o conteúdo descartado deverá ser apagado e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;
(ii) os documentos físicos que contenham informação protegida devem ser triturados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura;
(iii) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pela ALOCC devem ser apagados de modo que a informação seja irrecuperável.

## 6. Redundância

Além das cópias de segurança, os servidores de arquivos e base de autenticação de acesso são replicados em outros escritórios, tornando-se assim redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, as equipes chaves poderão acessar as informações em qualquer escritório. Caso necessário, a equipe de TI poderá disponibilizar acesso remoto mediante prévia autorização do Comitê.

No tocante ao acesso à internet, a ALOCC dispõe de dois links dedicados e um de banda larga, ligados simultaneamente pelo Firewall, que permite a automática comutação e a divisão do tráfego para o serviço secundário, sempre que houver interrupção do serviço principal. Adicionalmente, a ALOCC possui acesso à internet por sinal 4G garantindo a continuidade da conexão.

Para garantir o funcionamento da rede e a integridade dos dados, mesmo na eventual interrupção do fornecimento de energia elétrica, todas as estações de trabalho e o servidor estão conectados a um equipamento do tipo *no-break*, que permite a continuidade do funcionamento da rede por tempo suficiente para que os usuários salvem os arquivos recentes até a recuperação total do serviço.

## 7. Suporte e Monitoramento

Em caso de pane da rede ou em alguma estação de trabalho, a equipe de TI possui um sistema de monitoramento que busca identificar as ocorrências e assegurar o suporte interno ou providenciar que seja acionado o suporte externo, se necessário. Além disso, o usuário poderá comunicar outras ocorrências para tratamento da equipe de TI.

Todos os sistemas estão sujeitos à revisão e monitoramento a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

Nesse sentido, tendo em vista que a utilização do e-mail se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a ALOCC também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos Colaboradores.

Qualquer suspeita ou conhecimento de violação desta Política ou incidente de segurança da informação deve ser informado imediatamente ao Compliance e ao Comitê para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos.

Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

**Tratamento de casos de vazamento de informações confidenciais**

No caso de vazamento de informações confidenciais relacionadas aos clientes da ALOCC, ainda que oriundo de ação involuntária, o Compliance notificará imediatamente o Comitê Estratégico, que tomará as providências cabíveis sobre o ocorrido.

Sem prejuízo, a ALOCC acionará o seu Plano de Recuperação visando a identificação da causa que ensejou o vazamento e avaliação dos responsáveis. Ademais, será elaborado um relatório acerca dos danos ocorridos e atividades afetadas, estimativa de impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente.

Este relatório será elaborado pelo Compliance e será submetido ao Comitê da ALOCC que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

**Testes de Segurança**

São realizados os seguintes testes de segurança para monitoramento dos sistemas utilizados:

| ROTINAS OPERACIONAIS |
|---|
| Teste da Replicação do servidor de arquivos entre sites |
| Varredura de antivírus e Intrusion Prevent System pelo Firewall |
| Controle de conteúdo de Internet pelo Firewall e Antivírus |
| Varredura de memória pelo Antivírus |
| Sistema de Monitoramento de TI com alarme por e-mail |
| Bloqueio de tela do Windows por Inatividade |
| Backup Online |
| Suspender estações por inatividade |
| Backup do Firewall |
| Notificação do consumo extra de link de Internet |
| Verificar status dos logs do Backups Online |
| Backup local Diário |
| Analisar e-mails de Alertas dos firewalls |
| Verificar alarmes recebidos pelo Antivírus |
| Cópia de Sombra (Recurso de versões anteriores do Windows) |
| Backup Mensal Local |
| Atualizações Microsoft nas estações de trabalho |
| Varredura total de HDs por antivírus |
| Troca da senha dos usuários do AD/Office365 |
| Atualizar Software de backup Online |
| Atualizar do Firmware (Sistema Operacional) dos Firewalls |
| Teste de restore do backup |
| Teste de recuperação do Sistema de Gestão de Clientes no ambiente de homologação |
| Troca de bateria dos nobreaks |

As atividades acima são feitas pela área de TI e a área de Compliance é responsável por monitorar e fiscalizar essas atividades. Diariamente, é enviado um resumo das atividades realizadas por TI ao responsável de Compliance, onde reporta-se as evidências das rotinas.

## 8. Identificação e Avaliação de Riscos Cibernéticos

Considerando as atividades desempenhadas pela ALOCC, os recursos tecnológicos essenciais ao processo de análise, investimento e desinvestimento, são: (i) disponibilização de informações dos ativos financeiros e não financeiros dos clientes, (ii) boletagem de operações relacionada a seleção de veículos de acordo com a necessidade dos clientes, (iii) conferência e liberação das carteiras dos fundos sob gestão e (iv) acesso aos sistemas de informação.

Abaixo são descritos os riscos internos identificados e respectivas avaliações. Para tanto, considerou-se: (i) possíveis ameaças; (ii) grau de exposição dos ativos supramencionados às ameaças; (iii) impactos financeiros, operacionais e reputacionais; e (iv) a expectativa de que o evento de segurança se efetive:

| Risco Interno | Avaliação Inicial |
|---|---|
| Perda do Firewall | I – Possíveis ameaças: falha de eletricidade ou hardware. Imperícia na administração.<br>II – Grau de exposição: Baixo.<br>III – Impacto Operacional: Médio a Alto<br>IV – Expectativa: Baixa |
| Interrupção do serviço de autenticação de usuário | I – Possíveis ameaças: falha no serviço pelo Windows. Imperícia na administração.<br>II – Grau de exposição: Baixo.<br>III – Impacto Operacional: Baixo<br>IV – Expectativa: Baixa |
| Acesso a USB por pen drive/hd externo | I – Possíveis ameaças: Usuário mal intencionado ou pen drive/HD externo infectado.<br>II – Grau de exposição: Baixo.<br>III – Impacto Reputacional: Médio a Alto<br>IV – Expectativa: Baixo |
| Acesso não autorizado a rede wireless | I – Possíveis ameaças: Tentativa de invasão a rede ou quebra de senha.<br>II – Grau de exposição: Baixo.<br>III – Impacto Operacional: Baixo<br>IV - Expectativa: Baixo |
| Perda do equipamento Switch | I – Possíveis ameaças: falha de eletricidade ou hardware.<br>II – Grau de exposição: Baixo. |

| | |
|---|---|
| | III – Impacto Operacional: Baixo<br>IV - Expectativa: Baixa |
| Perda do servidor local | I – Possíveis ameaças: falha de eletricidade ou hardware. Falha de Sistema Operacional Windows. Imperícia na administração<br>II – Grau de exposição: Baixo.<br>III – Impacto Operacional: Baixo<br>IV - Expectativa: Baixa |
| Interrupção de um PC de usuário | I – Possíveis ameaças: falha de hardware. Falha de Sistema Operacional Windows.<br>II – Grau de exposição: Médio.<br>III – Impacto Operacional: Baixo<br>IV - Expectativa: Baixa |

| Risco Externo | Avaliação Inicial |
|---|---|
| Acesso remoto | I – Possíveis ameaças: Acesso indevido de informações confidenciais por acesso remoto.<br>II – Grau de exposição: Baixo.<br>III – Impacto Reputacional: Médio a Alto<br>IV – Expectativa: Baixa |
| Smartphones | I – Possíveis ameaças: perda do dispositivo, furto ou roubo.<br>II – Grau de exposição: Médio.<br>III – Impacto Reputacional: Médio a Alto<br>IV - Expectativa: Baixa |
| Webmail externo (terceiros) | I – Possíveis ameaças: Vazamento de informações ou exposição a vírus.<br>II – Grau de exposição: Baixo.<br>III – Impacto Operacional: Médio a Alto / Reputacional: Alto<br>IV - Expectativa: Baixa |
| Interrupção Energia elétrica | I – Possíveis ameaças: indisponibilidade do serviço.<br>II – Grau de exposição: Médio.<br>III – Impacto Operacional: Alto<br>IV - Expectativa: Baixa |
| Interrupção de Links de Internet | I – Possíveis ameaças: Indisponibilidade do serviço.<br>II – Grau de exposição: Médio. |

| | |
|---|---|
| | III – Impacto Operacional: Baixo<br>IV - Expectativa: Média |
| Vírus | I – Possíveis ameaças: Por meio de acesso web.<br>II – Grau de exposição: Médio.<br>III – Impactos Operacional: Médio a Alto / Reputacional: Alto<br>IV - Expectativa: Média |
| Interrupção do Sistema de Gestão de Clientes | I – Possíveis ameaças: perda do serviço por falha de software, e do sistema operacional.<br>II – Grau de exposição: Médio.<br>III – Impacto Operacional: Médio a Alto<br>IV - Expectativa: Baixa |
| Interrupção Servidor de arquivos | I – Possíveis ameaças: perda do serviço por falha de software, e do sistema operacional.<br>II – Grau de exposição: Médio.<br>III – Impacto Operacional: Baixo<br>IV - Expectativa: Baixa. |
| Interrupção VPN com Sistema de Processamento de Carteiras | I – Possíveis ameaças: interrupção no link de internet ou falha no firewall.<br>II – Grau de exposição: Médio.<br>III – Impacto Operacional: Médio<br>IV - Expectativa: Baixa |
| Interrupção VPN com Prestador de serviço em nuvem do Sistema de Gestão de Clientes | I – Possíveis ameaças: interrupção no link de internet ou falha no firewall.<br>II – Grau de exposição: Médio.<br>III – Impacto Operacional: Médio<br>IV - Expectativa: Baixa |
| Interrupção VPN com Prestador de serviço em nuvem do servidor de arquivos | I – Possíveis ameaças: interrupção no link de internet ou falha no firewall.<br>II – Grau de exposição: Médio.<br>III – Impacto Operacional: Baixo<br>IV - Expectativa: Baixa |
| Interrupção VPN com Prestador de desenvolvimento do Sistema de Gestão de Clientes | I – Possíveis ameaças: interrupção no link de internet ou falha no firewall.<br>II – Grau de exposição: Médio.<br>III – Impacto Operacional: Médio<br>IV - Expectativa: Baixa |
| Acesso a websites nocivos | I – Possíveis ameaças: Websites externos. |

| | |
|---|---|
| | II – Grau de exposição: Médio.<br>III – Impacto Reputacional: Baixo<br>IV - Expectativa: Baixa |
| Acesso a conteúdos web não autorizados | I – Possíveis ameaças: Websites externos.<br>II – Grau de exposição: Médio.<br>III – Impacto Reputacional: Baixo<br>IV - Expectativa: Baixa |

## 9. Ações de Proteção e Prevenção aos Riscos Cibernéticos

Os planos de ação e prevenção descritos neste Capítulo tem por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

Neste sentido, a ALOCC ratifica a adoção de controles de acesso físico e lógico implementados em linha com esta Política. Tais controles visam a identificação, autenticação e autorização de acesso pelos usuários a sistemas ou ativos da ALOCC, evitando o acesso por terceiros não autorizados.

Isto posto, todos os Colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede, bem como às barreiras da informação com relação a outras atividades desempenhadas pela ALOCC ou empresas do mesmo grupo econômico.

Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquer inconsistência ou inadequação com relação aos acessos recomendados pelo Compliance reportados imediatamente ao Comitê. Especial atenção deverá ser envidada aos casos de desligamento.

Todos os novos equipamentos e sistemas utilizados pela ALOCC devem passar pelas proteções descritas abaixo, sendo realizados testes antes do início da sua utilização. Além disso, são realizadas verificações automáticas diárias e ainda uma inspeção anual feita pela equipe de TI.

São adotadas as seguintes medidas preventivas para cada risco identificado:

| Risco Interno | Ação de Proteção/Prevenção |
|---|---|
| Perda do Firewall | Equipamento sobressalente e proteção elétrica por Nobreak. |
| Interrupção do serviço de autenticação de usuário | 2 servidores replicados acionados automaticamente |
| Acesso a USB por pen drive/HD externo | Acesso Bloqueado |
| Acesso não autorizado a rede wireless | Acesso por senha |
| Perda do equipamento Switch | Equipamento sobressalente e proteção elétrica por Nobreak |
| Perda do servidor local | Proteção elétrica por Nobreak, ambiente refrigerado e manutenção no sistema operacional. |
| Interrupção de um PC de usuário | Proteção elétrica por Nobreak e ambiente refrigerado durante o uso. Manutenção no sistema operacional Windows. |

| Risco Externo | Ação de Proteção/Prevenção |
|---|---|
| Acesso remoto | Restrição ao acesso com aprovação exclusiva do Comitê Estratégico e controle por firewall caso ele venha a ser solicitado e liberado. |
| Smartphones | Orientação por parte da equipe de TI. |
| Webmail de terceiros | Firewall e Antivírus |
| Interrupção Energia elétrica | Nobreaks |
| Interrupção de Links de Internet | Há 3 links cabeados e redundantes em cada escritório que são constantemente monitorados, além de 1 modem móvel 4G. |
| Vírus | Os PCs estão protegidos pelos antivírus e IPS (intrusion prevent system) do Firewall. Há restrições de acesso a páginas web por meio de reputações e conteúdo também no firewall |
| Interrupção do Serviço do Sistema de Gestão de Clientes | O servidor do Sistema de Gestão de Clientes está em um Datacenter em SP, com ambiente controlado e contingenciado. Em caso de perda deste serviço, usaremos o servidor local de homologação e o backup do Banco de Dados para restabelecer o serviço de |

| | |
|---|---|
| | contingência internamente, a previsão é de até 3h. |
| Interrupção Servidor de arquivos | O servidor de arquivos está em Datacenter na região Sul do país, com ambiente controlado e contingenciado. Em caso de perda desse serviço, há réplicas em tempo real do serviço nos escritórios de SP e Rio, cujos usuários serão direcionados manualmente com previsão de restabelecer o serviço de contingência em até 30 minutos. |
| Interrupção VPN com o Prestador do Sistema de Processamento de Carteira | Será acionado na TI do prestador o serviço de contingência por Internet do acesso remoto por RDP (Remote Desktop Protocol). |
| Interrupção VPN com Prestador de serviço em nuvem do Sistema de Gestão de Clientes | Há VPNs redundantes pré-configuradas que assumirão automaticamente ou manualmente esse serviço. |
| Interrupção VPN com Prestador de serviço em nuvem do servidor de arquivos | Há VPNs redundantes pré-configuradas que assumirão automaticamente ou manualmente esse serviço. |
| Interrupção VPN com Prestador de desenvolvimento do Sistema de Gestão de Clientes | Há VPNs redundantes pré-configuradas que assumirão automaticamente ou manualmente esse serviço. |
| Acesso a websites nocivos | Monitorados e controlados pelas políticas dos Firewalls e antivírus. |
| Acesso a conteúdos web não autorizados | Monitorados e controlados pelas políticas dos Firewalls e antivírus. |

## 10. Mecanismos de Supervisão da Segurança Cibernética

São realizados os seguintes testes de verificação para fins de identificação de anomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados:

| Rotina | Periodicidade |
|---|---|
| Teste de invasão externa e phishing | Executado através de consultoria terceirizada. |
| Teste de resposta a incidentes com simulação de cenários | De acordo com a ocorrência |
| Varredura de antivírus e Intrusion Prevent System pelo Firewall | Automático |
| Controle de conteúdo de Internet pelo Firewall e Antivírus | Automático |
| Log de tentativa de uso de drives externos ou de acessos a webmail externos | Automático |

São mantidos inventários atualizados de hardware e softwares licenciados utilizados pela ALOCC. Sempre que houver alteração relevante na estrutura tecnológica da ALOCC serão realizadas análises de vulnerabilidade.

## 11. Respostas a incidentes Cibernéticos

A ALOCC adota os seguintes planos de ação de resposta a incidentes em função das ameaças identificadas:

| Ameaça Interna | Severidade (Classificação) | Plano de Ação |
|---|---|---|
| Perda do Firewall | Alta | Em cada escritório, há um firewall de backup com ativação e restabelecimento dos principais serviços em até 02h. |
| Interrupção do serviço de autenticação | Média | Os outros escritórios assumirão a autenticação e autorização dos acessos automaticamente, até que possamos restabelecer o serviço local. |
| Acesso a USB por pen drive/HD externo | Média | Por conta da facilidade de cópia das informações por meio desses dispositivos, as estações estão com o acesso bloqueado pelo o antivírus. |
| Acesso não autorizado a rede wireless | Baixa | A rede wireless só tem acesso à Internet e é segregada da rede interna. |
| Perda do equipamento Switch | Alta | Há equipamento sobressalente no escritório que serão ativados manualmente com previsão de restabelecimento em até 01h. |
| Perda do servidor local | Baixa | O serviço de autenticação e DNS será |

| | | |
|---|---|---|
| | | atendido automaticamente por outro servidor de outro escritório. |
| Interrupção de um PC de usuário | Baixa | Há equipamentos reservas até que seja restabelecido o PC. |

| Ameaça Externa | Severidade (Classificação) | Plano de Ação |
|---|---|---|
| Acesso remoto | Alta | O acesso remoto é bloqueado à rede local e ao servidor de arquivos. |
| Smartphones | Média | Todos os aparelhos estão com proteção por senha. |
| Webmail de terceiros | Alta | O Acesso a webmails pessoais é bloqueado na rede interna pelo Firewall e antivírus. |
| Interrupção Energia elétrica | Alta | O CPD e as estações contam com nobreaks que darão autonomia de até 30 minutos. Caso não haja restabelecimento do serviço, o plano de contingência será acionado. |
| Interrupção de Links de Internet | Alta | Há links redundantes, em cada escritório há 3 links cabeados e 1 por 4G. |
| Vírus | Média | Os PCs estão protegidos pelos antivírus e IPS (intrusion prevent system) do Firewall e por antivírus nos PCs. Há restrições de acesso a páginas web por meio de reputações e conteúdo também no firewall |
| Interrupção do Serviço do Sistema de Gestão de Clientes | Alta | O servidor do Sistema de Gestão de Clientes está em um Datacenter de SP com ambiente controlado e contingenciado. Em caso de perda deste serviço, usaremos o servidor local de homologação e o backup do Banco de Dados para restabelecer o serviço de contingência, cuja previsão é de até 2h. |
| Interrupção Servidor de arquivos | Alta | O servidor de arquivos está em um Datacenter na região Sul do país com ambiente controlado e contingenciado. Em caso de perda desse serviço, há réplicas em tempo real do serviço no escritório de SP e Rio, cujos usuários serão direcionados manualmente e com |

| | | |
|---|---|---|
| | | previsão de restabelecer o serviço de contingência em até 30 minutos. |
| Interrupção VPN com o Prestador do Sistema de Processamento de Carteira | Alta | Será acionado na TI do prestador o serviço de contingência por Internet do acesso remoto por RDP (Remote Desktop Protocol). |
| Interrupção VPN com Prestador de serviço em nuvem do Sistema de Gestão de Clientes | Alta | Há VPNs redundantes pré-configuradas que assumirão automaticamente ou manualmente o serviço. |
| Interrupção VPN com Prestador de serviço em nuvem do servidor de arquivos | Alta | Há VPNs redundantes pré-configuradas que assumirão automaticamente ou manualmente o serviço. |
| Interrupção VPN com Prestador de desenvolvimento do Sistema de Gestão de Clientes | Alta | Há VPNs redundantes pré-configuradas que assumirão automaticamente ou manualmente o serviço. |
| Acesso a websites nocivos | Médio | Monitorados e controlados pelas políticas dos Firewalls e antivírus. |
| Acesso a conteúdos web não autorizados | Médio | Monitorados e controlados pelas políticas dos Firewalls e antivírus. |

Compete ao Compliance a comunicação da contingência aos demais colaboradores, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e severidade da contingência, em observância ao Plano de Continuidade de Negócios.

Cabe ao Compliance elaborar relatórios acerca dos danos ocorrido, atividades afetadas, estimativa de impacto financeiro, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente. Tais relatórios deverão ser submetidos ao Comitê que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade, a ALOCC estudará procedimentos preventivos a serem implementados e incluídos no plano de continuidade de negócios.