Política de Segurança Cibernética e da Informação e Plano de Contingência e Continuidade de Negócios

Edição	Datas			Aprovação	Página
2ª	1ª versão	Última atualização	Próxima atualização	Comitê Executivo	1
	Fev/2020	Fev/2021	Fev/2022		

QUELUZ
Asset Management

Índice:

1. Política de Segurança Cibernética e da Informação:

1.1. Objetivo:

Este capítulo do Manual de Normas e Procedimentos Operacionais tem como objetivo atender ao disposto nos Artigos 16º e 17º do Capítulo V – Regras e Procedimentos, Seção V – Segurança Cibernética" do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros" de 20 de Julho de 2020 e estabelecer os princípios, conceitos, valores e práticas que devem ser adotados pelos administradores, funcionários e/ou colaboradores da Queluz na sua atuação interna e com o mercado.

1.2. Atribuições:

A Queluz incorpora em seus valores corporativos a convicção de que o exercício de suas atividades e a expansão de seus negócios devem se basear em princípios éticos, os quais devem ser compartilhados por todos os seus colaboradores.

Na constante busca do seu desenvolvimento e da satisfação dos clientes, a Queluz busca transparência e cumprimento da legislação aplicável às atividades de gestão de recursos de terceiros.

A publicação desta Política de Segurança Cibernética e da Informação representa o compromisso de todos os que trabalham na Queluz com os valores e as práticas fundamentadas na integridade, confiança e lealdade. Portanto, a constante busca do desenvolvimento e a defesa dos interesses dos clientes estarão sempre pautadas nas diretrizes aqui expostas.

O Departamento de *Compliance* & Risco é responsável pela implementação de um sistema de supervisão que demonstre que os controles de segurança da informação estão sendo devidamente executados e alinhados com os níveis adotados pela Queluz e a legislação vigente.

1.3. Princípios da Segurança da Informação:

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos. (ISSO 27002 A.5.1.1).

Confidencialidade: Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

Integridade: Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

Disponibilidade: Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

Acesso controlado: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

1.4. Regras do Uso de Tecnologia:

Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na Queluz ou para outras situações formalmente permitidas. (ISO A.6.1.3)

Quando o usuário se comunicar através de recursos de tecnologia da Queluz, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da empresa. (ISO A.7.1.3)

Os conteúdos acessados e transmitidos através dos recursos de tecnologia da Queluz devem ser legais, de acordo com o "Código de Ética", e devem contribuir para as atividades profissionais do usuário. (ISO A.15.1.5)

O uso dos recursos de tecnologia da Queluz pode ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente. (ISO A.10.10.1)

Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados. (ISO A.6.1.3)

Os recursos de tecnologia da Queluz, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização. (ISO A.6.1.3)

Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente ao Departamento de *Compliance* & Risco. (ISO A.13.1.1)

1.5. Direito à Propriedade:

Os programas homologados e instalados nos computadores e nos servidores de rede são propriedades exclusivas da Queluz, sendo vetada sua cópia parcial ou integral.

1.6. Usuários de Informática:

O recurso computador disponibilizado para o usuário é de propriedade da Queluz. (ISO A.7.1)

São reconhecidos como usuários de informática:

(i) Todos os colaboradores da Queluz;
(ii) Profissionais autônomos, temporários ou de empresas prestadoras de serviço que obtiverem a aprovação, por escrito, do Diretor de *Compliance* & Risco para prescrição de senhas de acesso aos recursos computacionais;
(iii) Estagiários (com a devida autorização da chefia).

1.7. Disponibilização e Uso:

Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela área de TI para uso na Queluz. (ISO A.10.3)

A Queluz pode a qualquer momento retirar ou substituir o computador disponibilizado para o usuário. (ISO A.10.3)

Cada computador tem o seu gestor/usuário, que é responsável por esse equipamento. O controle e manutenção das máquinas é de responsabilidade da área de TI. (ISO A.7.1)

A identificação do usuário ao computador é feita através do login e senha disponibilizado pela área de TI, portanto ela é sua assinatura eletrônica.

1.8. Programas utilizados no computador:

Os programas aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de TI. (ISO A.7.1)

É desabilitado aos usuários implantar novos programas ou alterar configurações sem permissão formalizada da área de TI.

É desabilitado ao usuário implantar ou alterar componentes físicos no computador.

1.9. Verificação do computador e acessos:

A Queluz mantém os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados pelas áreas de TI e *Compliance* & Risco.

Os acessos a equipamentos, softwares e respectivas permissões serão testados pela área de TI com validação do Departamento de *Compliance* & Risco semestralmente.

1.10. Atribuições do Usuário:

(i) Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
(ii) Responder pelo uso exclusivo e intransferível de suas senhas de acesso. Em caso de dúvidas, solicitar orientação a área de TI;
(iii) Adquirir conhecimento técnico necessário para a correta utilização dos recursos;
(iv) Relatar prontamente ao Representante da área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas / diretórios de rede, acesso indevido à Internet, programas instalados sem conhecimento da área de TI, etc;
(v) Não tentar obter acesso não autorizado a sistemas ou recursos de redes de computadores internas ou externas;
(vi) Assegurar que as informações e dados de propriedade da Queluz não sejam disponibilizados a terceiros, a não ser com autorização por escrito do Diretor de *Compliance* & Risco;
(vii) Relatar ao representante da área de TI a possibilidade de instalação de um novo software ou aquisição de novo Hardware para a melhoria dos serviços prestados.

1.11. Termo de Compromisso:

Para ter acesso à informação da Queluz, o usuário deverá assinar (manual ou eletronicamente) um Termo de Compromisso (modelo conforme Anexo xx). Os casos de exceção serão definidos pelo Departamento de *Compliance* & Risco da Queluz. (ISO A.8.1.3)

O Departamento de *Compliance* & Risco da Queluz alerta a todos os usuários que a instalação ou utilização de software não autorizados constitui em crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa.

A Queluz não se responsabiliza por qualquer ação individual que esteja em desacordo com a Lei mencionada acima. Todas as práticas que representam uma

ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares, conforme previsto no Código de Ética e Conduta (vide Capítulo 6 deste Manual).

1.12. Salvaguarda de Arquivos:

Compete a área de TI criar e manter cópias de segurança (backups) dos dados de softwares críticos, armazenados nos servidores de redes.

Os usuários devem manter, obrigatoriamente, os dados críticos da empresa nos servidores de redes.

São de responsabilidade exclusiva do usuário a cópia e a guarda dos dados gravados na estação local de trabalho.

Os backups devem ser guardados em local seguro, separados dos equipamentos, para viabilizar a recuperação dos dados.

1.13. Regras para utilização da Rede Coorporativa:

(i) Todos os recursos de rede de computadores deverão ser utilizados exclusivamente para fins profissionais, que envolvam atividades relacionadas ao bom andamento dos serviços e processos da Queluz;
(ii) Todos os arquivos que não tenham fins profissionais devem ser apagados dos equipamentos para evitar problemas futuros com auditorias;
(iii) Todos os computadores da Queluz devem ter antivírus instalado e atualizado periodicamente, é proibido desinstalar e utilizar computadores sem antivírus instalado;
(iv) Em caso de dúvidas, solicitar orientação a área de TI;
(v) É expressamente vedado aos usuários a instalação ou remoção de programas de computador, componente e periféricos;
(vi) É proibido aos usuários conectar computadores pessoais ou de terceiros à rede coorporativa da Queluz, exceto a utilização de *Notebooks* e outros equipamentos portáteis através da rede sem fio *WiFi*;
(vii) É proibido realizar conexões *Dial-Up* a partir de computadores conectados à rede da Queluz, exceto com expressa autorização da área de TI.

1.14. Regras para utilização do Correio Eletrônico (e-mail):

A Queluz fornecerá, a seu critério, contas de correio eletrônico aos seus colaboradores seguindo obrigatoriamente o padrão:

"nome"."sobrenome"@qlzasset.com.br

As Mensagens de correio eletrônico (*emails*) internos e externos devem ser exclusivamente de caráter profissional, sendo proibido qualquer tipo de utilização particular. O mesmo é válido para arquivos anexos.

Todas as mensagens recebidas de origem desconhecida deverão ser eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos. Quaisquer tipos de comunicados e informativos coorporativos deverão ser previamente aprovados e posteriormente divulgados pelo Departamento de *Compliance* & Risco.

É proibido configurar e/ou manter configuradas contas de correio eletrônico de servidores externos, isto é, diferentes de (@qlzasset.com.br), nos programas gerenciadores e correio eletrônico instalados em computadores da Queluz. Em caso de dúvidas solicitar orientação a área de TI.

O correio eletrônico poderá ser utilizado a partir de qualquer computador conectado à Internet, utilizando-se o site do Google. Este site poderá ser acessado através do endereço:

http://www.gmail.com

As caixas postais de contas de correio eletrônico da Queluz (@qlzasset.com.br) não tem limite de tamanho e para envio e recebimento de mensagens enviadas/recebidas poderão conter arquivos com até 25MB (25 Mega Byte) por anexo.

É proibida a utilização do e-mail para fins ilegais, transmissão de material de qualquer forma censurável, que viole direitos de terceiros e leis aplicáveis.

É proibida a utilização de e-mail para transmitir mensagens conhecidas como *Spam*, *JunkMail*, correntes ou a distribuição de mensagens em massa não solicitadas.

A troca da senha para acesso a caixas postais e envio de mensagens poderá ser efetuada através do site *http://www.gmail.com* e é de inteira responsabilidade do usuário.

É terminantemente proibido aos representantes da área de TI, administradores de rede e/ou correio eletrônico, ler mensagens de correio eletrônico de qualquer usuário quando estiver realizando serviços de manutenção e suporte, exceto quando em cumprimento de determinações do Departamento de *Compliance* & Risco da Queluz para efeitos de auditoria.

Reserva-se a Queluz o direito de auditar a utilização de suas contas de correio eletrônico (@qlzasset.com.br) fornecidas aos usuários, sem se caracterizar invasão de privacidade.

1.15. Regras para utilização da Internet na Rede Corporativa:

O acesso à Internet foi disponibilizado na Queluz para viabilizar a busca de informações ou agilizar determinados processos da empresa.

Todo o acesso à Internet através da rede coorporativa Queluz será controlado com a realização de auditorias nas páginas consultadas. Serão desenvolvidos relatórios com nomes, páginas consultadas, tempo de consulta. Estes relatórios serão enviados aos gerentes de cada área e ao Diretor de *Compliance* & Risco da Queluz, para acompanhamento.

Os usuários são responsáveis por toda a utilização da Internet em computadores iniciados com seu login e senha. Quando o usuário se afastar do computador deverá encerrar a sessão através do *logoff*, reiniciar ou desligar o sistema.

É proibido aos usuários configurar ou alterar as configurações de rede e de acesso à Internet dos computadores da Queluz, incluindo as seguintes configurações de rede: IP, DNS, WINS, Gateway, Proxy e a instalação ou reconfiguração de clientes Proxy.

Não é permitido enviar, baixar (download) ou manter arquivos de imagens, músicas, vídeo, arquivos executáveis em geral ou quaisquer outros de caráter pessoal.

Não é permitido o acesso a sites de Internet com conteúdo pornográfico, jogos, bate-papo, chat, blogger, cartoon, relacionamento, música, hacker ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança.

É proibido o acesso a sites, a instalação e a utilização de programas de troca de mensagens instantâneas ou arquivos do tipo: ICQ, Yahoo Messenger, Bittorrent, Imesh, AudioGalaxy, AIM, Morpheus, Kaaza, Emule, Napster e outros, excetuando-se sistema autorizado pelo Departamento de *Compliance* & Risco da Queluz.

A utilização de sites do tipo *Proxy* é proibida e será considerada falta grave.

Sempre que os usuários, utilizando a Internet, tiverem acesso a materiais criminosos como pornografia infantil (arte, textos, figuras, cenas, imagens) e outros, mesmo que de maneira esporádica e involuntária, deverão entrar em contato imediatamente com o Departamento de *Compliance* & Risco da Queluz.

1.16. Regras para utilização de programas de troca de mensagens e conferências:

A utilização do programa MSN Messenger e SYPE, Google Meetings, ZOOM de troca de mensagens e de conferências, está autorizada para uso exclusivo de caráter profissional. Todos os funcionários da empresa ficam cientes de que todas

as mensagens trocadas pelo programa serão gravadas e analisadas periodicamente, visando o controle da forma de utilização dos mesmos.

1.17. Regras para Utilização da Rede Sem Fio (*WiFi*):

Usuários autorizados pelo Departamento de *Compliance* & Risco poderão conectar computadores ou outros equipamentos portáteis e pessoais á Internet, utilizando a rede sem fio *WiFi* da Queluz.

Estes equipamentos deverão, obrigatoriamente, ser enviados previamente a área de TI para checagem e reconfiguração.

Todo o acesso à Internet através da rede *WiFi* da Queluz será controlado com a realização de auditorias nas páginas consultadas.

Os usuários são responsáveis por toda a utilização da Internet através da rede *WiFi* da Queluz, e serão identificados e responsabilizados em caso de acesso indevido.

1.18. Penalidades & Considerações Finais:

As áreas de TI e de *Compliance* & Risco alertam todos os usuários que a instalação ou utilização de software não autorizados constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa.

Todos os usuários são responsáveis pelo uso correto das ferramentas eletrônicas de propriedade da Queluz.

Todas as práticas que representam uma ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares.

Portanto, na ocorrência de infrações a este Manual, ou às determinações constantes de comunicações externas ou internas, ou mesmo às ordens de superiores hierárquicos, quando for o caso, ficam os infratores sujeitos às seguintes penalidades: advertência verbal, advertência por escrito, suspensão, demissão sem ou com justa causa e/ou outras medidas judiciais cabíveis.

Todos os usuários de informática passam a receber uma cópia deste Manual, dando ciência de seu conteúdo. Os novos colaboradores / usuários receberão o mesmo material por ocasião de sua admissão na Queluz.

A Queluz se reserva o direito de atualizar, alterar, anular toda ou em parte as normas aqui contidas, a qualquer momento e sem aviso.

Este Capítulo do Manual de Normas e Procedimentos da Queluz foi reeditado e aprovado pelo Departamento de *Compliance* & Risco e sua aplicação é imediata.

2. Plano de Contingência e Continuidade de Negócios:

2.1. Objetivo:

Este Capítulo do "Manual de Normas e Procedimentos Operacionais" contém o Plano de Contingência, e tem como objetivo definir os procedimentos que deverão ser seguidos pela Queluz no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da Queluz sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

O Plano de Contingência prevê ações que durem até o retorno à situação normal de funcionamento da Queluz dentro do contexto de seu negócio.

O Plano de Contingência da Queluz identifica duas variáveis para o funcionamento adequado da empresa: Infraestrutura e Processos.

A Infraestrutura engloba todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática e sistemas internos. Para cada um dos itens que compõem a infraestrutura existe uma ação a ser tomada.

Já os processos são as atividades realizadas para operar os negócios da Queluz. Os processos dependem da infraestrutura toda ou de parte da estrutura em funcionamento. Somente com os processos em andamento pode-se definir que o plano de ação foi bem executado.

2.2. Política e Procedimentos para Back-up:

(i) O backup dos servidores e sistemas serão feitos usando o método mais adequado e atual;

(ii) Os meios de armazenamento poderão variar entre Drive externo, on-line pela Internet ou espelhamento em servidores. Backups serão realizados utilizando um software de backup dedicado apropriado para o sistema operacional utilizado;

(iii) Procedimentos de *backup* & *restore*: o backup dos servidores e sistemas será realizado utilizando-se as instalações padrões disponíveis dentro do software de backup. O sistema é operado por uma empresa terceirizada de TI e pelo Diretor *Compliance* & Risco;

(iv) Status do backup: o software de backup é configurado para alertar automaticamente o administrador para o status de qualquer backup realizado. O status do backup será analisado em uma base diária e quaisquer falhas identificadas serão corrigidas;

(v) Verificação e teste de restauração: sempre que possível o software de backup será configurado para verificar automaticamente o backup. A verificação será realizada por meio da comparação do conteúdo da cópia de segurança com os dados no disco;

(vi) A restauração de informações a partir do backup será testada periodicamente;

(vii) Ciclos de *backup*:

i. *Repositório de Dados* - O *backup* completo dos sistemas importantes será realizado mensalmente, com backups incrementais todos os dias;

ii. *Esquema de rotação* - Será utilizado o método simples de rotação diária, sendo que, no mínimo, 10 (dez) *backups* serão mantidos;

iii. *Backups diários* - O *backup* será feito todos os dias, como parte de uma rotação diária simples. Um *backup* diário será composto de um *backup* completo em Drive externo e um espelhamento dos dados do servidor em outro Drive interno;

(viii) Armazenamento de *backup*: As mídias de *backup* serão armazenadas de forma segura quando não estiverem em uso. Para resiliência, várias mídias removíveis serão armazenadas fora do ambiente da Queluz. No mínimo, duas cópias do mais atualizado *backup* de dados serão armazenadas fora do local;

(ix) Backup de aplicativos: Técnicas de *backup* on-line serão utilizadas para minimizar o tempo de inatividade. *Backups off-line* completos serão utilizados onde os backups online não estão disponíveis.

2.3. Efetiva Contingência:

(i) Na impossibilidade de se utilizar o espaço físico do escritório, a Queluz poderá continuar a funcionar em escritório compartilhado, tipo Régus, localizado na cidade de São Paulo. Caso não haja disponibilidade para locação no escritório compartilhado, os colaboradores da Queluz deverão se dirigir ao *meeting point* conforme a seguir definido;

(ii) O serviço de e-mail da Queluz é fornecido pela Google, com suporte 24/7, serviço de antisspam, recuperação de informação e site de recuperação de desastre. A Queluz utiliza ainda o Exchange da Microsoft que possibilita, via webmail, o acesso remoto de todas as mensagens pelos colaboradores;

(iii) A Queluz conta com uma central de telefone própria e linhas de celulares em caso de contingência. Em caso extremo de falhas nas linhas telefônicas, os colaboradores da Queluz possuem celulares que podem substituir a telefonia fixa;

(iv) As informações dos portfólios e fundos além de estarem nos sistemas internos da Queluz, são disponibilizadas diariamente pelo administrador dos fundos, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos fundos;

(v) 3.5. Em caso de falha de fornecimento de energia, a Queluz possui *nobreaks* para suportar o funcionamento de seus servidores, rede corporativa, telefonia e estações chave de trabalho.

2.4. Estrutura de Suporte:

(i) Além dos mecanismos convencionais para garantir a integridade das informações, como back-up em servidores com hardware redundante, a Queluz replica todos os seus sistemas operacionais (Banco de Dados, Arquivos, E-mails, *Softwares*...) em notebooks guardados dentro e fora da empresa;

(ii) Tais hardwares estão à disposição para substituição, assim que o original apresentar qualquer problema. No caso de ocorrer uma falha, o monitoramento (através de sistemas e da empresa terceirizada de TI) detecta o problema e alerta os diretores da Queluz. A detecção de falhas em hardware permite a recuperação de todo o hardware.

(iii) Em caso de efetiva necessidade de utilização da estrutura de contingência, deverão ser encaminhadas para o local de contingência as pessoas responsáveis pelas funções de *boletagem* e conferência das operações junto ao administrador, os principais gestores das carteiras e o Diretor de *Compliance* & Risco;

(iv) Com os procedimentos descritos acima, a Queluz pode continuar a funcionar mesmo que não possa ter acesso físico ao escritório.

2.5. Lista de Informações:

Deverá ser mantida no local de contingência uma lista com as informações de todos os colaboradores da Queluz, das corretoras com as quais se realizam negócios, dos clientes e dos prestadores de serviço contratados, além de um *back-up* contendo Banco de Dados, Arquivos e *Softwares*.

2.6. Procedimentos de contingência:

(i) Na impossibilidade de se utilizar o espaço físico da Queluz e caso não haja disponibilidade para locação no escritório compartilhado, os colaboradores envolvidos no processo de contingência deverão comparecer ao *meeting point* deste plano de contingência;

(ii) O *meeting point* do plano de contingência da Queluz é a residência do Diretor de *Compliance* & Risco, (residência localizada cerca de 2 km do escritório);

(iii) Se a impossibilidade de se utilizar o espaço físico da Queluz ocorrer quando os colaboradores estiverem no escritório, eles irão se dirigir primeiro ao escritório compartilhado e caso não haja disponibilidade de locação, ao *meeting point* portando os notebooks da empresa, que estão preparados com todas as ferramentas necessárias para o processo de contingência (*Bloomberg*, *Phibra* e *Microsoft Office*);

(iv) Já se a impossibilidade de se utilizar o espaço físico da Queluz ocorrer quando os colaboradores não estiverem no escritório, eles irão se dirigir primeiro ao escritório compartilhado e caso não haja disponibilidade de locação, eles deverão se dirigir ao *meeting point* portando seus notebooks pessoais, que estão preparados com todas as ferramentas necessárias para o processo de contingência e instalação dos respectivos Banco de dados e acessos;

(v) No escritório compartilhado ou no *meeting point*, o Gestor CVM da Queluz, e na sua ausência o Diretor de *Compliance* & Risco, deverá contatar os colaboradores da Queluz em São Paulo, e efetuar os devidos procedimentos de contingência ou realocação dos colaboradores;

(vi) Chegando ao escritório compartilhado ou no meeting point, o Diretor de *Compliance* & Risco conjuntamente com o responsável pela área de TI, serão responsáveis por recuperar os arquivos no back-up diário;

(vii) Além do processo de recuperação dos arquivos, o Diretor de *Compliance* & Risco em conjunto com o responsável pela área de TI, irão providenciar junto a seus prestadores de serviço os devidos acessos para que os colaboradores possam executar suas funções.

2.7. Considerações Finais:

Este plano de contingência será atualizado anualmente e, em seguida, deverá ser testado, corrigido e divulgado antes de uma necessidade real de utilização, de modo que as pessoas estejam familiarizadas com o formato, conceitos, padrões e estratégias de atuação.

Este Capítulo do Manual de Normas e Procedimentos da Queluz foi reeditado e aprovado pelo Departamento de *Compliance* & Risco e sua aplicação é imediata.