ANEXO CÓDIGO DE ÉTICA DA ARAÚJO FONTES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Esta política tem por finalidade garantir a disponibilidade, a integridade, a confidencialidade, a legalidade, a autenticidade e a auditabilidade da informação necessária para a realização do negócio da Araújo Fontes.

2. Elegibilidade

Todos os colaboradores da Araújo Fontes devem cumprir os deveres estabelecidos nesta política. São considerados colaboradores todos os sócios, empregados e estagiários da Araújo Fontes.

3. Metodologia

3.1. Violações à Política de Segurança da Informação.

a) Considera-se violação a esta política qualquer ato que:

i. Exponha a Araújo Fontes a uma perda econômica efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou das informações ou ainda da perda de equipamento;

ii. Envolva a revelação de dados confidenciais da Araújo Fontes ou de terceiros; e

iii. Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

b) É dever do setor de tecnologia da informação (TI) cuidar do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

3.2. Responsabilidade pela Segurança da Informação

a) O Sr. Naylor Braga, inscrito no CPF sob o número 057.291.796-18, colaborador da Araújo Fontes, é o responsável chefe pelor setor de TI e quem, dentro do quadro de colaboradores da Araújo Fontes, responde por questões de segurança cibernética.

b) É dever de todos os colaboradores da Araújo Fontes considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a Araújo Fontes e deve sempre ser tratada profissionalmente.

c) É responsabilidade do Gerente/Supervisor de cada área estabelecer os critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a classificação abaixo:

i. Informação pública: é toda informação que está disponível, sem restrições, ao público em geral.

ii. Informação interna: é toda informação que só pode ser acessada por colaboradores da Araújo Fontes. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da instituição.

iii. Informação confidencial: é toda informação que pode ser acessada por colaboradores da Araújo Fontes e que sua divulgação não autorizada poderia causar impacto (econômico, de imagem ou operacional) ao negócio da Araújo Fontes ou seus parceiros. Toda informação de clientes da Araújo Fontes é considerada confidencial, a não ser que de outra forma definida pelo próprio cliente.

iv. Informação restrita: é toda informação que pode ser acessada somente por colaboradores da Araújo Fontes explicitamente indicados pelo nome ou pela área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos à Araújo Fontes e/ou comprometer a estratégia de negócio da organização.

d) Orientar os colaboradores subordinados é dever dos gerentes/supervisores, devendo estes definir que os subordinados:

i. Não circulem informações e/ou mídias consideradas confidenciais ou restritas;

ii. Não deixem relatórios nas impressoras e mídias em locais de fácil acesso; e

iii. Bloqueiem seus computadores de trabalho, de modo que somente será possível acessar novamente mediante colocação da senha pessoal.

3.3. Tratamento de Dados Pessoais.

a) O tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Araújo Fontes só será realizado nas seguintes hipóteses:

i. para o cumprimento de obrigação legal ou regulatória pela Sociedade;

ii. quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

iii. quando necessário para atender aos interesses legítimos da Araújo Fontes ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais e Dados Pessoais Sensíveis;

iv. mediante o fornecimento de consentimento pelo titular por escrito ou outro meio que demonstre a manifestação de vontade do titular; ou

v. para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

b) O legítimo interesse da Araújo Fontes indicado acima poderá ter fundamento, mas não se limita, às seguintes finalidades:

i. apoio e promoção de atividades da Araújo Fontes; e

ii. proteção, em relação ao titular, do exercício regular dos seus direitos ou prestação de serviços que o beneficie, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

c) O consentimento do titular deve observar as seguintes diretrizes:

i. se outorgado por escrito deverá constar de cláusula destacada das demais cláusulas contratuais;

ii. o Dado Pessoal obtido mediante consentimento do titular só poderá ser compartilhado com terceiros se houver expressa autorização do titular;

iii. o consentimento deve referir-se a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados. Caso alterada a finalidade, deverá ser coletado novo consentimento do titular;

iv. o consentimento poderá ser revogado a qualquer tempo por manifestação expressa do titular, por procedimento gratuito e facilitado, ratificado o tratamento realizado ao amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação dos dados.

d) A Araújo Fontes se compromete a não acumular ou manter dados pessoais de seus coloaboradores, salvo os de imprescindível relevância para o negócio.

i. Todos os dados pessoais de colaboradores da Araújo Fontes que porventura sejam armazenados são classificados como informação confidencial;

ii. Os dados pessoais dos colaboradores sob a responsabilidade da Araújo Fontes não serão tratados para fins diferentes daqueles para os quais foram coletados;

iii. Os dados pessoais dos colaboradores da Araújo Fontes não serão transferidos a terceiros, salvo quando exigido para a realização do negócio;

iv. Os dados pessoais dos colaboradores somente poderão ser transferidos a terceiros que mantenham a sua confidencialidade, incluindo-se, neste

caso, a lista de endereços eletrônicos (e-mails) usados pelos funcionários da Araújo Fontes; e

v. É dever dos colaboradores da Araújo Fontes não armazenar dados pessoais (próprios ou de terceiros) nas instalações da Araújo Fontes, salvo se expressamente necessário para o desenvolvimento dos negócios da Araújo Fontes.

e) A Araújo Fontes preza pelo zelo para com a privacidade dos titulares de dados pessoais, desta forma, somente fará negócios que envolvam compartilhamento de dados com parceiros que comprovem tratar a matéria com similar seriedade.

f) As atividades de tratamento de Dados Pessoais e Dados Pessoais Sensíveis deverão observar a boa-fé e os seguintes princípios:

i. finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

ii. adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

iii. necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

iv. livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais;

v. qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

vi. transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

vii. segurança: utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

viii. prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais;

ix. não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

x. responsabilização e prestação de contas: demonstração, pela Sociedade, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

3.4. Controles Internos de RH e de TI.

a) O setor de Recrutamento e Seleção de Pessoal (RH) da Araújo Fontes deverá informar ao TI acerca de qualquer alteração na condição dos colaboradores para que os cadastros dos mesmos possam ser atualizados nos sistemas da instituição. Isto inclui o fornecimento de sua senha e registro do seu nome como usuário no sistema pelo TI.

b) O RH deve comunicar ao TI sobre os diretórios a que qualquer novo colaborador terá acesso.

i. No caso de temporários e/ou estagiários, deverá também ser informado o tempo em que os mesmos prestarão serviços à Araújo Fontes para que, na data de seu desligamento, possam também ser encerradas as atividades relacionadas ao acesso ao sistema.

ii. No caso de desligamento, o RH deverá comunicar o fato ao TI para que o colaborador desligado seja excluído do sistema.

c) Compete ao RH obter as assinaturas de concordância dos novos colaboradores em relação à Política de Segurança da Informação da Araújo Fontes.

i. Consentir com esta política implica necessariamente em consentir com a coleta e o tratamento dos dados pessoais por parte da Araújo Fontes, implicando para esta todos os deveres de controlador de dados pessoais, descritos na Lei Geral de Proteção de Dados e nesta política.

ii. Nenhum colaborador poderá ser contratado sem ter expressamente concordado com esta política.

3.5. Programas Utilizados nos Computadores da Araújo Fontes.

a) A Araújo Fontes respeita os direitos de propriedade intelectual dos programas que usa e reconhece que deve pagar o valor justo por eles, não aceitando o uso de programas não licenciados nos computadores da instituição.

b) Somente a área de TI tem autorização para instalação de softwares nos equipamentos da Araújo Fontes.

i. Periodicamente a equipe de TI fará verificações nos dados dos servidores e/ou nos computadores de trabalho dos colaboradores visando a garantir a correta aplicação desta política.

ii. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores e os responsáveis estarão sujeitos às sanções previstas no Código de Ética da Araújo Fontes.

3.6. Equipamentos, Programas, Redes e Sistemas Internos da Araújo Fontes.

a) Para acesso aos dados da rede da Araújo Fontes, é necessária a utilização de login e senha previamente cadastrados pela equipe de TI.

b) Quando do ingresso de novo colaborador, a área de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha. Esta senha deverá ser alterada imediatamente após o primeiro login e, após isso, a cada 120 (cento e vinte) dias.

i. As senhas devem ter, no mínimo, 8 (oito) caracteres, contendo uma combinação de letras, números e caracteres alfanuméricos, de modo a não poderem ser repetidas;

ii. As senhas são privadas, apenas o seu titular deve ter ciência. É vedado a qualquer dos colaboradores compartilhar suas senhas, ficando estes responsáveis por eventuais prejuízos que decorram deste fato; e

iii. Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho. Havendo necessidade de novo acesso aos sistemas, o TI deverá liberá-lo novamente.

c) Todos os colaboradores responsáveis pela aprovação eletrônica de documentos deverão comunicar ao TI quem será o seu substituto quando de sua ausência da Araújo Fontes para que as permissões possam ser alteradas.

d) Não é permitido o compartilhamento de pastas e equipamentos da Araújo Fontes. Todos os dados deverão ser armazenados nos Servidores da rede e a autorização para acessá-los deverá ser fornecida pelo Servidor AD (*Active Directory*).

i. A equipe de TI, periodicamente, verificará todos os compartilhamentos existentes nas estações de trabalho e garantirá que os dados considerados confidenciais ou restritos não estejam armazenados nas máquinas locais;

ii. Os compartilhamentos de impressoras devem estar sujeitos às autorizações de acesso do AD; e

iii. É vedado o compartilhamento de dispositivos móveis de armazenamento dentro da Araújo Fontes.

e) Todos os dados da Araújo Fontes deverão ser protegidos através de rotinas sistemáticas de backup. Cópias de segurança do sistema integrado e de servidores de rede são de responsabilidade do TI.

f) Anualmente, o backup deverá ser testado pela equipe de TI, voltando-se parte ou todo o conteúdo do backup para um HD previamente definido para este fim.

Esta operação deverá ser acompanhada pelo gerente da Araújo Fontes responsável por supervisionar a área de TI.

g) Em caso de informações/programas que não permitam o armazenamento em rede, a equipe de TI alertará o colaborador sobre a necessidade de realização do backup.

i. É responsabilidade dos próprios colaboradores a elaboração de cópias de segurança de dados e arquivos, em suas estações de trabalho, que não sejam considerados de fundamental importância para a continuidade dos negócios da Araújo Fontes e que, portanto, não estejam incluídos na rotina de backup.

ii. No caso das informações consideradas de fundamental importância para a continuidade dos negócios da Araújo Fontes, o TI disponibilizará um espaço nos servidores no qual cada usuário deverá mantê-las. Estas informações serão incluídas na rotina diária de backup da informática.

h) O acesso à internet será autorizado aos colaboradores que necessitarem da mesma para o desempenho das suas atividades profissionais na Araújo Fontes, sendo a referida autorização conferida pelo TI.

i. O uso da Internet será monitorado pelo setor de informática, inclusive através de logs (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a internet e qual página acessou.

ii. Não é permitido instalar programas provenientes da internet nos computadores da Araújo Fontes sem a expressa anuência do TI, exceto os programas oferecidos por órgãos públicos necessários ao bom andamento dos serviços.

i) O correio eletrônico (e-mail) fornecido pela Araújo Fontes é instrumento de comunicação interna e externa para a realização dos negócios da instituição.

i. As mensagens devem ser escritas em linguagem formal, de acordo com as normas cultas da língua portuguesa, de forma a nunca prejudicar a imagem da Araújo Fontes.

ii. O uso do correio eletrônico é personalíssimo, não podendo o titular da conta permitir o seu uso por terceiros. O titular responde pelo uso de seu correio eletrônico.

iii. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis ou inúteis;
- Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas; e
- Sejam incoerentes com as políticas da Araújo Fontes.

iv. Não será permitido o uso de correios eletrônicos gratuitos nos computadores da Araújo Fontes. O Setor de Informática poderá, visando a evitar a entrada de vírus nos sistemas internos, bloquear o recebimento de mensagens provenientes de sites gratuitos.

v. As caixas de mensagens terão um limite de armazenamento, que poderá variar de acordo com o cargo do colaborador na Araújo Fontes.

- Fica estabelecido que até o maior cargo na empresa não poderá exceder o limite máximo estabelecido em reunião pelo TI.

j) O TI é responsável pela compra e/ou substituição de *software* e *hardware*. Qualquer necessidade de novos *softwares* ou de novos equipamentos de informática deverá ser discutida com o responsável pelo TI.

i. Salvo autorização da direção da Araújo Fontes, não é permitida a compra ou o desenvolvimento de *softwares* ou *hardwares* diretamente pelos usuários utilizando os equipamentos da Araújo Fontes.

k) Todos os dispositivos necessários para manter a estrutura tecnológica da Araújo Fontes funcionando, como servidores, armário de telecomunicações (*firewall,*

switch, modem, *router, wi-fi*, interface de celular) e o PABX estão equipados com *no-breaks*, que impedem os picos de energia, bem como sua falta, por até 30 minutos.

l) Os colaboradores que tiverem acesso a computadores ou qualquer outro equipamento computacional, de propriedade da Araújo Fontes, devem estar cientes que:

i. Os recursos de tecnologia da informação, disponibilizados aos colaboradores, têm por finalidade a realização das atividades profissionais da Araújo Fontes;

ii. A proteção do recurso computacional de uso individual é de responsabilidade do próprio colaborador;

iii. É de responsabilidade de cada colaborador assegurar a integridade do equipamento, bem como a confidencialidade e a disponibilidade das informações nele contidas, dentro dos limites da prudência em sua atuação; e

iv. Não devem alterar a configuração do equipamento recebido.

m) Se os equipamentos forem ser transportados para fora das instalações da Araújo Fontes, o colaborador deve ser diligente e cuidadoso da mesma forma que seria transportando seus próprios bens.

i. O colaborador deverá indenizar a Araújo Fontes sempre que, dolosa ou culposamente, danificar bens desta que estejam em sua posse; e

ii. Sempre que algum colaborador fique em posse de algum bem da Araújo Fontes, antes que este volte a ser comumente utilizado, o TI deverá avaliá-lo e, se necessário, submeter laudo de avaliação ao Comitê de Ética para que a possibilidade de indezinação seja deliberada.

n) Se o bem vier a ser perdido em face de atitude criminosa, deverá o colaborador, o mais rapidamente possível:

i. Registrar a ocorrência em alguma delegacia de polícia;

ii. Comunicar ao seu superior imediato e ao TI; e

iii. Enviar cópia da ocorrência ao TI.

o) Todos os acessos aos sistemas de informação da Araújo Fontes dependem de autenticação individual dos colaboradores usuários, de modo que todos os acessos e utilizações são rastreáveis.

i. O TI fará auditorias periódicas do acesso dos usuários às informações e, se encontradas irregularidades, reportará diretamente ao *Compliance* e à direção da Araújo Fontes, podendo o colaborador ser responsabilizado, conforme dispõe o Código de Ética.

ii. Ao concordar com esta política, o colaborador afirma estar ciente de que sua utilização da internet pode ser rastreada pela atuação fiscalizatória empregada pelo TI, de forma que o resultado desta fiscalização pode acarretar punições ao colaborador.

iii. É expressamente vedado ao TI divulgar o resultado da fiscalização mencionada acima a quaisquer terceiros, com exceção do *Compliance* da Araújo Fontes.

iv. Se da fiscalização resultar exclusão do colaborador do quadro de colaboradores, todo o histórico obtido pelo TI, por meio da fiscalização, deverá ser imediatamente apagado de qualquer fonte na qual tenha sido armazenado.

p) O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da Araújo Fontes, bem como o uso de eventuais ramais virtuais instalados nos computadores, é de responsabilidade do TI, de acordo com as definições desta política e da diretoria da Araújo Fontes.

i. Ao final de cada mês serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal.

q) Todo arquivo em mídia proveniente de entidade externa a Araújo Fontes deve ser verificado por programa antivírus, que está instalado em todos os computadores da instituição.

i. Todo arquivo recebido através do ambiente da internet deve também ser verificado por programa antivírus; e

ii. A atualização do antivírus será automática, agendada pelo TI, via rede.

iii. Aos colaboradores é expressamente vedado desabilitar o programa antivírus instalado nas estações de trabalho.

3.7. Testes de Segurança

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

ROTINAS OPERACIONAIS	PERIODICIDADE
Varredura de antivírus	Tempo real
Controle de conteúdo de Internet pelo Firewall e Antivírus	Tempo real
Varredura de memória pelo Antivírus	Tempo real
Monitoramento de Hosts e serviços	Tempo real
Autenticação de rede	Tempo real
Bloqueio de tela do Windows por Inatividade	A cada 15 min
Backup Online	Tempo real
Backup Firewall	A cada alteração
Notificação do consumo extra de link de Internet	A cada ocorrência
Verificar status dos logs do Backup	Semanal
Verificar sistema gráficos de consumo de link, visão diária, semanal e mensal	Diário
Teste de restore do backup	Anual
Reiniciar Servidores - Atualizações Microsoft	A cada atualização
Atualizar plano de ação	Mensal
Troca da senha dos usuários	45 dias

3.8. Propriedade Intelectual.

a) Durante o vínculo com a Araújo Fontes, todas as criações intelectuais dos seus colaboradores serão de propriedade desta se forem passíveis de registro como propriedade intelectual, desde que atendidos qualquer dos requisitos a seguir:

i. Se a criação for feita com a utilização de propriedades da Araújo Fontes; e

ii. Se a criação for desenvolvida por colaborador ou pessoa externa em contratação exclusiva para este fim.

4. Disposições Gerais

A presente política tem como anexo o Plano de Continuidade dos Negócios da Araújo Fontes.

Esta política é um anexo ao Código de Ética da Araújo Fontes. Em havendo qualquer contradição entre seus termos e os termos do Código de Ética, prevalecem os termos deste.

Esta política estará disponível a todos os colaboradores da Araújo Fontes, devendo qualquer dúvida acerca de seu conteúdo ser esclarecida junto ao *Compliance*.

Os colaboradores da Araújo Fontes, ao assinarem o Termo de Adesão ao Código de Ética, estarão manifestando sua total aceitação aos termos desta política.

PLANO DE CONTINUIDADE DOS NEGÓCIOS

(ANEXO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO)

O presente documento destina-se a estabelecer a metodologia de atuação da Araújo Fontes frente a determinadas situações que poderiam impedir a normal continuidade dos negócios.

1) Em caso de problemas envolvendo o abastecimento de energia elétrica nas instalações da Araújo Fontes, haverá queda nas atividades de processamento de informações. Para lidar com a referida situação, a Araújo Fontes possui nobreaks com autonomia de 30 minutos para segurar servidores, e rack e notebooks, que tem uma autonomia de ate duas horas, para assegurar a falta de energia dos equipamentos. Em casos extremos, os colaboradores essenciais poderão exercer suas funções de casa, tendo acesso aos sistemas de informações da Araújo Fontes de maneira remota.

2) Em caso de problemas envolvendo a conexão com a internet poderá haver queda no link principal de conexão, o que impediria grande parte das atividades da Araújo Fontes. Para lidar com a referida situação, a Araújo Fontes possui um Link principal da operadora Algar de 10MB (Full) e um link secundário de 240MB. Caso o link principal, que tem um SLA de 99,9% da Embratel, caia o link secundário assumirá imediatamente, com regra de prioridade para manter a Araújo Fontes em funcionamento.

3) Em caso de problemas envolvendo incêndios nas instalações da Araújo Fontes poderá haver perda completa de todos os equipamentos e impossibilidade de acesso ao local. Para lidar com a referida situação, o prédio no qual está inserida a Araújo Fontes possui sistema de detecção de fogo e placas de sinalizações para saída.

4) Em caso de problemas envolvendo o transporte dos colaboradores até as instalações da Araújo Fontes poderá haver impossibilidade de execução das tarefas em função da ausência dos mesmos. Para lidar com a referida situação, a Araújo Fontes autoriza o uso de transporte alternativo em casos de urgência.

5) Em caso de problemas envolvendo a perda total ou parcial de arquivos ou diretórios poderá haver impacto na execução das atividades diárias dos colaboradores da Araújo Fontes. Para lidar com a referida situação, os colaboradores da Araújo Fontes realizarão suas atividades através do sistema de backup, podendo variar, todavia, em face do tamanho do arquivo, o tempo de recuperação.

6) Em caso de problemas envolvendo falha de equipamentos computacionais, tais falhas poderão dificultar ou até impedir a execução diária das tarefas da Araújo Fontes. Para lidar com a referida situação, existe a possibilidade de reparo imediato do equipamento

com peças que podem ser substituídas. Caso contrário, solução será a troca imediata do equipamento utilizado por um reserva, p.ex.: (impressora ou CPU).

7) Em caso de problemas envolvendo falha no servidor geral poderá ocorrer paralisação de todo o acesso às informações. Para lidar com a referida situação, o backup das informações é gravado em nuvem e em HD externo, caso haja falha do servidor geral, tem-se a opção de acesso via nuvem ou acesso imediato através de um HD Externo.

8) Em caso de falha na rede local, esta poderá ficar paralisada e também, consequentemente, o acesso aos servidores e aos arquivos. Para lidar com a referida situação, a Araújo Fontes provê distintos meios de acesso à rede. Caso o acesso à rede local cabeada fique indisponível, o acesso poderá ser feito através do HD externo ligado a uma das maquinas do gerente da Araújo Fontes.

9) Em caso de impossibilidade física de acesso às instalações, causada por qualquer fator imprevisível, o impacto será na realização das atividades diárias. Para lidar com a referida situação, haverá a possibilidade de os colaboradores atuarem de suas casas.