Política de Segurança da Informação e de Segurança Cibernética

GTI Administração de Recursos Ltda.

Versão: Janeiro 2024

APRESENTAÇÃO

A Política de Segurança da Informação e de Segurança Cibernética da GTI Administração de Recursos ("GTI") é destinada a todos os sócios, colaboradores, prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da GTI, ou então que tenham acesso as suas informações. Todos os usuários de computadores na nossa organização têm a responsabilidade de proteger a segurança e a integridade de todas as informações e dos equipamentos de informática.

OBJETIVOS

A Política de Segurança da Informação e de Segurança Cibernética da GTI tem o objetivo de proteger as Informações Sigilosas (clientes e proprietárias), garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas conforme art. 4º, §8º, da Instrução CVM n.º 558/15.

Nenhuma informação de caráter confidencial deve ser divulgada a pessoas que não devam ter acesso a tais informações confidenciais para desempenho de suas atividades profissionais relacionadas à empresa.

Qualquer tipo de informação sobre a GTI ou de atividades da organização e de seus sócios, colaboradores ou clientes, obtida porventura por um Colaborador, só poderá ser pública, apresentada na mídia, redes sociais ou a demais órgãos caso seja consentido pelo Diretor de Riscos e Compliance.

SEGURANÇA DE INFORMAÇÕES

Colocar na Ata de Risco que foi feita uma atualização / reciclagem visando estar em conformidade com a política de segurança a informação com a participação de toda a equipe, referente. Foram abordados os seguintes tópicos, localizados na página XXX

Segurança da informação

Acesso as pastas

Descarte das informações:

Também foi revisado o acesso as diferentes pastas, assim como enfatizado que esse acesso é impessoal e intransferível, de forma a manter a segmentação do acesso à informação (informação compartimentada).

Operacional: Registramos a entrada da nova colaboradora Erika Feitoza na GTI para a área de operações.

Vulnerabilidades: mandamos novos exemplos de phishing.

As medidas de segurança de informações utilizadas pela GTI têm por finalidade de minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa.

É expressamente proibido que os Colaboradores façam cópias, imprimam, fotografem ou printem os arquivos utilizados, gerados ou disponíveis da GTI e fiquem disponíveis em ambientes externos à empresa

com os mesmos sem prévia autorização do Diretor de Riscos e Compliance.

Estes arquivos mencionados acima podem conter informações que são categorizadas como informações confidenciais ou sensíveis. Em relação as informações sensíveis e/ou confidenciais da empresa ou então de seus clientes, estas serão armazenados em diretórios de rede com acesso restrito e controlado pelo responsável de Riscos e Compliance da GTI.

Os Diretórios têm acesso definido pelos sócios e caberá ao Compliance coordenar com a empresa de TI terceirizada, a execução desta segregação. Também para o controle de acesso, temos UTM (Bloqueios por categorias) de saída e Microsoft 365 departamental para acessos a arquivos.

A GTI reforça que, embora invista os melhores esforços e recursos para o aprimoramento da proteção de dados e segurança da informação, ações tais como: print de tela, fotografia do

computador, uso de pen drive etc., são eventos difíceis de serem monitorados. Assim sendo, estas ações serão de inteira responsabilidade dos praticantes.

Este tipo de proibição não se aplica em caso das cópias ou a impressão dos arquivos forem para a execução e desenvolvimento dos negócios e dos interesses da GTI.

O Colaborador que porventura tiver alguma cópia ou impressão de arquivo que contenha alguma informação confidencial será o responsável por sua boa conservação, integridade e manutenção de sua confidencialidade. Também, qualquer impressão de arquivos ou documentos deve ser imediatamente retirada da máquina impressora, já que existe a probabilidade – mesmo que remota - de conter informações confidenciais, mesmo no ambiente interno da organização.

Data Mapping

As informações de acesso referente ao Data Mapping com o uso do SharePoint para a estruturação das pastas internas da GTI é realizado conforme solicitado pela GTI à empresa terceirizada de tecnologia.

Os acessos são liberados de acordo com as funções de cada colaborador, restringindo ao máximo informações, conforme demonstrado na fotografia abaixo.

DESCARTE DE INFORMAÇÕES

O descarte de quaisquer informações confidenciais em ambientes digitais deve ser executado de tal forma que seja impossível a sua recuperação. Através do Microsft 365 como padrão após 90 dias o dado é destruído. Existe o backup que contêm retenção de 7 anos, o dado não é deletado do mesmo. Em caso de necessidade de recuperação do backup, a informação será recuperada, no entanto será novamente excluída, de forma a garantir o descarte total da mesma.

Quanto ao descarte de documentos físicos que contenham informações confidenciais devem também ter algum procedimento de descarte imediatamente após seu uso, de maneira a impossibilitar a sua recuperação. Ainda vale destacar que os Colaboradores não devem fazer o uso de pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na GTI.

É expressamente proibida a conexão de equipamentos estranhos na rede da GTI que não estejam devidamente autorizados pelo responsável de Compliance. Novos equipamentos e sistemas deverão ter suas configurações feitas pela equipe de TI terceirizada. Todo Colaborador tem a responsabilidade de manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

Foi instituído um padrão de solicitação de alteração de senha sempre que exista a possibilidade de a mesma ter sido comprometida.

O acesso a sites diversos ou o envio e encaminhamento por e-mail de conteúdo ofensivo, pornográfico, obsceno, preconceituoso ou discriminatório também é expressamente proibido, como também o envio ou encaminhamento de materiais com comentários ou mensagens opinativas que possam de alguma maneira impactar negativamente na imagem com o fim de afetar a reputação da GTI.

Programas ou softwares instalados nos computadores, principalmente através de browser de internet (downloads) devem obter autorização prévia, além de avaliação de segurança pela empresa terceirizada para prover os serviços de TI. Existem proteções para a gestão de incidentes de segurança da informação como UTM (Firewall) e outros controles de segurança.

É proibida a instalação de qualquer software ilegal ou que detenham direitos autorais protegidos ou então, sem prévia autorização do responsável de Compliance.

Não é permitido também a instalação de softwares nos equipamentos sendo este procedimento restrito a empresa terceirizada de TI. Todo conteúdo que está na rede pode ser acessado pelos sócios ou pelo responsável de Compliance, caso haja necessidade.

Arquivos pessoais dos Colaboradores salvos nos diretórios da rede poderão ser acessados remotamente, caso seja necessário. A confidencialidade dessas informações deve ser respeitada, e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais, ou em atendimento a determinações judiciais ou administrativas. Por fim, é importante ressaltar que a GTI conta com um sistema e ferramentas contratadas para arquivamento (rede), firewall, antivírus, backup, prevenção de invasão e linha de contingência.

PREVENÇÃO DE VULNERABILIDADES

Diariamente um antivírus é rodado (remotamente pela empresa de TI) de forma a monitorar e proteger a rede de eventuais ameaças como: malaware, vírus, spyware, exploits. O antivírus é gerenciado remotamente e conta com detecção proativa, em tempo real, contra anomalias na rede através de sua

tecnologia comportamental identificando possíveis ataques de ransomware e barrando assim, o máximo possível a sua proliferação na rede de dados.

A GTI conta com o serviço oferecido pela empresa contratada de ti, SLTECH, de ARV (Análise de Riscos e Vulnerabilidades), onde contém o mapeamento de riscos e vulnerabilidades existentes a nível de rede e sistemas WEB, para que esteja em compliance com a LGPD, o processo de descoberta, detecção e identificação de vulnerabilidades é realizado mensalmente.

INSTALAÇÕES FISICAS TECNOLOGIA / ACESSO FISICO

Para garantir que o ambiente esteja em alta disponibilidade, foi implantado um sistema de nobreak individual em cada máquina de computador para assegurar o seu funcionamento na eventualidade de cortes de energia. Nestes casos os nobreaks deverão garantir energia por cerca de 15 min até a entrada do gerador do prédio.

O servidor de rede fica num rack segregado, tendo uma porta que eventualmente poderá ser trancada (cópia das chaves com o Diretor de Compliance e com um outro Sócio). O servidor conta com o ar-condicionado central do escritório, não contando com refrigeração específica.

Contamos também com a uma taxa de transferência de informações na rede de até 1 gigabit.

SERVIÇOS DE REDE

As redes de serviços são mantidas com o apoio de um serviço de TI terceirizado pela
GTI.

Contamos com dois provedores de banda larga de forma a garantir internet caso haja queda de um link.

Também está instalado na rede e nos equipamentos um sistema de prevenção de invasão para garantir a segurança das informações.

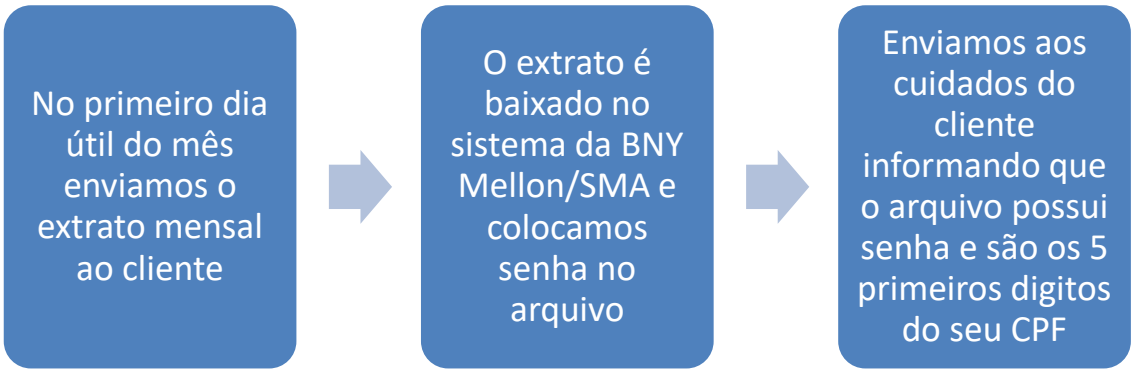
ARMAZENAMENTO DE DADOS

O armazenamento de dados é feito através de backup e realizado a cada dia através da ferramenta cloud e estando disponível para restauração. A GT conta também com inclusão de classificação de dados LGPD (data mapping), através do programa do Microsoft 365 Sharepoint.

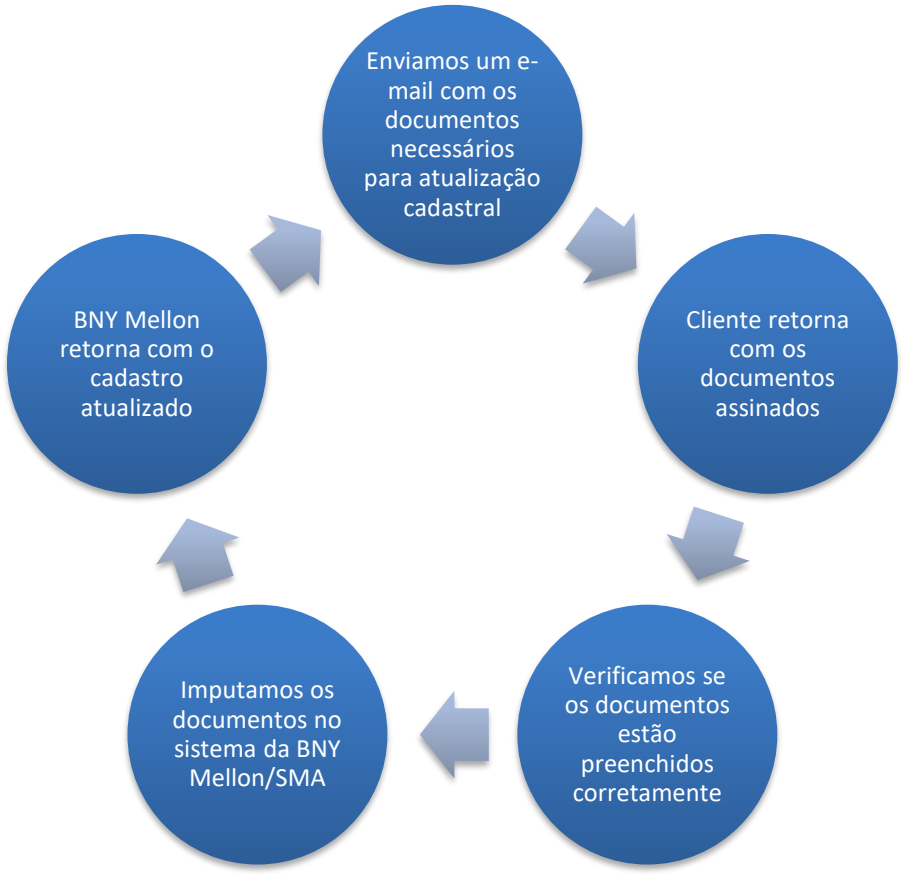
FLUXOGRAMA

A GTI lida com dados de cotistas em dois momentos (atualização cadastral quando necessário e envio de extratos mensais), conforme o fluxo descrito abaixo, com o respectivo inventário de quem tem acesso a informação em cada passo:

FLUXOGRAMA ENVIO DE EXTRATO



INVENTÁRIO/ FLUXOGRAMA – ATUALIZAÇÃO CADASTRAL



PLANO DE AÇÃO EM CASO DE INTERCORRÊNCIAS

Em caso de intercorrências, tais como possível vazamento de dados pessoas, ataque de hackers, ou outros eventos, a GTI montou um plano de ação de forma a dar uma pronta resposta. O plano de ação obedecerá aos seguintes passos:

- No caso de um possível vazamento de dados, a GTI entrará em contato com o cliente via contato telefônico e e-mail para comunicá-lo de todas as informações e ações cabíveis;
- Acionará imediatamente nosso prestador de serviços de TI para avaliação da situação e eventuais medidas cabíveis;
- Notificará a Agência Nacional de Proteção de Dados.

INDISPONIBILIDADE DE ACESSO A INFORMAÇÃO

Em caso de problemas que consista na indisponibilidade de acesso a dados ou informações registrados nos computadores, a empresa terceirizada de TI seria acionada para resolver a obstrução. Para rastreio do ambiente de rede e sistemas para registro de eventos indevidos, empresa terceirizada de TI atua através do Microsfot 365 e do monitoramento entregue pela por ela, sendo possível ratreabilizar eventos indevidos e/ou não autorizados.

TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES

O Departamento de Compliance repassa a todos os colaboradores as políticas e manuais da GTI de forma que todos tenham conhecimento das melhores práticas e condutas. A GTI incentiva que todos os colaboradores busquem atualizações em suas respectivas atividades de trabalho. Havendo necessidade, a GTI promove treinamentos abertos aos colaboradores a respeito das melhores práticas de mercado.

Atualização e Revisão

Esta política será revisada, no mínimo, uma vez por ano. Caso se faça necessário, poderá ser revista a qualquer momento.

Controle de Versões

Revisão: Jan/2024

Próxima Revisão: Jan/2025