MANUAL DA SEGURANÇA DA INFORMAÇÃO E TI

Sumário

Av. Santo Amaro, 48 - 6º andar - Itaim Bibi - São Paulo - SP - CEP: 04506-000

O Manual da Segurança da Informação, na TAG INVESTIMENTOS, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Companhia, ou acesso a informações pertencentes à TAG.

Todo e qualquer usuário de recursos computadorizados da Companhia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

A violação deste manual de segurança é qualquer ato que:

- Exponha a Companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

1 - Missão do Setor de Informática

Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

2 - Objetivo do Manual da Segurança da Informação

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da TAG.

3 - É Dever de todos dentro da TAG

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a TAG e deve sempre ser tratada profissionalmente.

4 - Classificação da Informação

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

1 – Pública
2 – Interna
3 – Confidencial
4 – Restrita

Av. Santo Amaro, 48 - 6º andar - Itaim Bibi - São Paulo - SP - CEP: 04506-000

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

5 - Dados Pessoais de Funcionários

A TAG se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais de Funcionários serão considerados dados confidenciais.

Dados Pessoais de Funcionários sob a responsabilidade da TAG não serão usados para fins diferentes daqueles para os quais foram coletados. Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da TAG.

6 - Programas Ilegais

É terminantemente proibido o uso de programas ilegais (PIRATAS) na TAG. Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da Companhia. Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

Av. Santo Amaro, 48 - 6º andar - Itaim Bibi - São Paulo - SP - CEP: 04506-000

7 - Permissões e Senhas

Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da Companhia, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática, por meio de formulário de requisição, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A Informática fará o cadastramento e informará ao novo usuário qual será a sua senha.

8 - Compartilhamento de Pastas e Dados

É de responsabilidade da Informática rever periodicamente todos os compartilhamentos existentes nas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos.

9 - Cópia de Segurança (Backup) do Sistema Integrado e Servidores de Rede

Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da Informática e deverão ser feitas diariamente.

10 - Segurança e Integridade do Banco de Dados

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de Informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

11 - Admissão/Demissão de Funcionários/Temporários/Estagiários

O setor de Recrutamento e Seleção de Pessoal da Companhia deverá informar ao setor de Informática, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da Companhia. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de Informática.

Cabe ao setor solicitante da contratação a comunicação ao setor de Informática sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço á Companhia, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.

No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação ao Manual da Segurança da Informação da TAG.

Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com este manual.

12 - Transferência de Funcionários

Quando um funcionário for promovido ou transferido de seção ou gerência, o setor de cargos e salários deverá comunicar o fato ao Setor de Informática, para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao sistema informatizado da Companhia.

13 - Propriedade Intelectual

É de propriedade da TAG, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a TAG.

14 - Uso do Ambiente Web (Internet)

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na TAG. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

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.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da Direção da Companhia, com base em recomendação do Supervisor de Informática.

Não é permitido instalar programas provenientes da Internet nos microcomputadores da TAG, sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;

- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da TAG;
- Que promovam discussão pública sobre os negócios da TAG, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Confidencial”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

15 - Uso do Correio Eletrônico – ("e-mail")

O correio eletrônico fornecido pela TAG é um instrumento de comunicação interna e externa para a realização do negócio da TAG.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da TAG, não podem ser contrárias à legislação vigente e nem aos princípios éticos da TAG.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as regras deste manual da TAG.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo.

A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado.

Em caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores da TAG.

O Setor de Informática poderá, visando evitar a entrada de vírus na TAG, bloquear o recebimento de e-mails provenientes de sites gratuitos.

16 - Necessidades de Novos Sistemas, Aplicativos e/ou Equipamentos

O Setor de Informática é responsável pela aplicação do Manual da TAG em relação a definição de compra e substituição de “software” e “hardware”.

Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.

Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

17 - Uso de Computadores Pessoais (Laptop) de Propriedade da TAG

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da TAG, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao Setor de Informática;
- Envie uma cópia da ocorrência para o Setor de Informática.

Nas dependências da TAG

- Os sistemas eletrônicos de telefonia móvel e outros equipamentos similares de envio e recebimento de mensagens deverão ser usados com discernimento em situações

particulares. Sugere-se que estes aparelhos permaneçam no modo vibratório durante o período comercial;
- Todos os equipamentos devem ser devidamente bloqueados, quando de ausência rápida da estação de trabalho.

18 - Responsabilidades dos Gerentes / Superiores

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da Companhia, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido neste manual.

O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina determinado usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

19 - Sistema de Telecomunicações

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da TAG, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de Informática, de acordo com as definições da Diretoria da TAG.

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

20 - Uso de Antivírus

Todo arquivo em mídia proveniente de entidade externa a TAG deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.

Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

21 - Identificação/avaliação de riscos (risk assessment)

Com a análise e identificação dos riscos, abaixo os equipamentos, serviços e dispositivos de maior impacto no ambiente:

- Acesso aos servidores locais e arquivos;
- Infecção de ransomware na rede;
- Pessoas não autorizadas ter acesso aos e-mails.

22 – Prevenção e proteção

- Acesso aos servidores locais e arquivos
    - Os acessos são feitos através de uso de VPN apenas para alguns usuários ou a equipe de TI acessa através de ferramentas de acesso remoto (Logmein), tudo registrado e autenticações dois fatores ativado ao celular corporativo do analista ou gestor;
    - Todo e qualquer dispositivo conhecido ou desconhecido que conecta na rede interna da Tag Investimentos é registrado um log de acesso;
    - Os servidores estão com antivírus ativo instalado e licenciado.
- Infecção de ransomware na rede
    - Todo e qualquer equipamento da Tag está instalado antivírus Kaspersky e tem uma funcionalidade já nativa de proteção de Ransomware;

- Pessoas não autorizadas ter acesso Acesso aos e-mails
    - Todos os e-mails estão ativos com autenticação baseado em dois fatores afim de solucionar esse problema que a pessoa mal-intencionada tente acessar os e-mails.

23 – Monitoramento e Testes

- Realizamos o monitoramento dos servidores, desktops com a solução do kaspersky a fim de coletarmos os logs e perfil de software padrão das maquinas e qualquer software fora do habitual o próprio antivírus não deixa instalar.
- Temos política dentro do ambiente para realizarmos a atualização periodicamente após o teste da atualização, caso seja válida aplicamos no ambiente de produção;
- Temos uma automatização de backups, caso tenhamos algum imprevisto é enviado um e-mail automaticamente para o setor de TI analisar o incidente e resolver dentro do SLA.

24 - Plano de resposta

- Para um plano resposta, dependendo da gravidade do incidente temos uma contingência no endereço Rua Tabapuã 81 que podemos ficar alocado para uma emergência, conforme nosso Plano de Continuidade de Negócios – Contingência.

25 - Penalidades

O não cumprimento deste Manual de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

26 – Parque Tecnológico – Anexo (Descrição)

REVISÃO	PERIODICIDADE	ÍNDICE
21. - Identificação/avaliação de riscos (risk assessment)	Anualmente – Dezembro/2018	Comitê de Sócios
22 – Prevenção e proteção	Anualmente – Dezembro/2018	Comitê de Sócios
23. Monitoramento e Testes	Anualmente – Dezembro/2018	Comitê de Sócios
24 - Plano de resposta	Anualmente – Dezembro/2018	Comitê de Sócios
25 - Penalidades	Anualmente – Dezembro/2018	Comitê de Sócios
26 – Parque Tecnológico – Anexo (Descrição)	Anualmente – Dezembro/2018	Comitê de Sócios