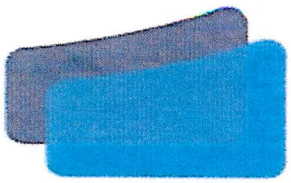

EXPERATO ASSET MANAGEMENT LTDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Capítulo I - Política de Segurança da Informação

Introdução

Este capítulo trata da Política de Segurança da Informação da EXPERATO ASSET MANAGEMENT LTDA. ("EXPERATO ASSET"). A informação é um ativo que possui grande valor para a EXPERATO ASSET, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante da empresa, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição.

A Política de Segurança da Informação da EXPERATO ASSET é uma declaração formal da empresa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda. Seu propósito é estabelecer as diretrizes a serem seguidas pela EXPERATO ASSET no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:
- Confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.
- Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.
- Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado

Objetivos

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

Abrangência

A Política de Segurança da Informação da EXPERATO ASSET deve estar disposta de maneira que seu conteúdo possa ser consultado a qualquer momento e aplica-se a todos os funcionários e prestadores de serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da EXPERATO ASSET, ou o acesso a informações pertencentes à EXPERATO ASSET. Todo e qualquer usuário de recursos computadorizados da EXPERATO ASSET tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:
- exponha a empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados, de informações ou ainda da perda de equipamento;
- envolva a revelação de dados confidenciais, incluindo negociações e uso não autorizado de dados corporativos, ou a violação de direitos autorais ou patentes; e
- envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

É dever de todos na empresa considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a EXPERATO ASSET e que deve sempre ser tratada de maneira profissional. Cabe ao colaborador buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à Segurança da Informação da EXPERATO ASSET e assinar o Termo de Responsabilidade, formalizando a ciência e o aceite da Política de Segurança da Informação da EXPERATO ASSET, bem como assumindo responsabilidade por seu cumprimento.

Aprovação e Revisão

A aprovação da Política de Segurança da Informação da EXPERATO ASSET é de responsabilidade da Diretoria, tendo periodicidade de revisão anual. Também é de competência da Diretoria tomar as decisões administrativas referentes aos casos de descumprimento da Política.

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:

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

b) 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.

c) 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.

d) 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.

Dados dos Funcionários

A EXPERATO ASSET 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 que porventura sejam armazenados serão considerados dados confidenciais e 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.

Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da empresa, sem prévia e expressa autorização por parte da diretoria. Mesmo que seja autorizado o armazenamento destes dados, a empresa não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos servidores de empresa, e jamais poderão fazer parte da rotina de *backup* da empresa. Ainda, os funcionários se comprometem a não realizar a instalação de *softwares* nos computadores da empresa sem que exista autorização prévia para tal.

Admissão e demissão de funcionários/temporários/estagiários

O setor de Recrutamento e Seleção de Pessoal da EXPERATO ASSET deverá informar ao setor de Informática e 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 empresa. 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 à autorização 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 à Política de Segurança da Informação da EXPERATO ASSET. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

Capítulo II - Política de Segurança Cibernética

Definições

A segurança cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger a rede, os computadores, os sistemas e os dados de ataques ou acessos não autorizados.

O risco de ataque cibernético ameaça os princípios da segurança das informações, tais como confidencialidade, integridade e disponibilidade.

Há diversas razões para que esses ataques ocorram e os principais motivos são:

(i) obter recursos financeiros;

(ii) roubar e manipular informações;

(iii) obter informações privilegiadas;

(iv) sabotagem à instituição;

(v) disseminar falsas notícias; e

(vi) disseminar o caos.

A segurança cibernética deve garantir:

(i) a segurança dos sistemas e dos bancos de dados;

(ii) o gerenciamento das pessoas autorizadas;

(iii) a segurança dos sistemas e informações que estão na nuvem;

(iv) a segurança para todos os dispositivos/equipamentos;

(v) o planejamento da continuidade do negócio; e

(vi) o treinamento constante do usuário final, com o objetivo de minimizar a vulnerabilidade da organização.

São exemplos de consequencias/danos que podem ser causados pela falha na segurança cibernética:

(i) risco de imagem;

(ii) risco de continuidade do negócio; e

(iii) prejuízos financeiros.

Programas Ilegais

A empresa respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não autorizando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de programas ilegais (sem licenciamento) na EXPERATO ASSET.

Os usuários não podem, em hipótese alguma, instalar qualquer "*software*" (programa) nos equipamentos da empresa sem autorização prévia e expressa. Periodicamente, o setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados se responsabilizam perante a companhia por quaisquer problemas ou prejuízos causados oriundos desta ação, estado sujeitos às sansões previstas neste documento.

Permissões e Senhas

Todo usuário para acessar os dados da rede da EXPERATO ASSET, deverá possuir um *login* e senha previamente cadastrados pelo pessoal de Informática. Quem deve fornecer os dados referentes aos direitos do usuário é o responsável direto pela sua chefia. Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da EXPERATO ASSET, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A área de Informática fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual se recomenda ser alterada imediatamente após o primeiro login e após isso a cada 180 (cento e oitenta) dias. Por segurança, a área de Informática recomenda que as senhas tenham: letra, número e caráter especial, critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc.) deverão comunicar ao seu superior imediato e ao setor de Informática qual será o seu substituto quando de sua ausência da empresa, para que as permissões possam ser alteradas (delegação de poderes).

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 e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo pessoal de Informática.

Compartilhamento de Dados

Não é permitido o compartilhamento de pastas nos computadores e desktops da empresa sem autorização prévia. Todos os dados deverão ser armazenados nos servidores da rede, e a autorização para acessá-los deverá ser fornecida pelo setor de Informática. Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso do setor de Informática. Não é permitido na empresa o compartilhamento de dispositivos móveis tais como pen-drivers e outros.

***Backup* (Cópia de Segurança dos Dados)**

Todos os dados da empresa deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade do setor de Informática e deverão ser feitas diariamente em um disco a parte e semanalmente em um servidor externo. O backup externo não tem risco de

vazamento porque é criptografado. Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, do Sistema Integrado.

Cópias de Segurança de Arquivos em *Desktops*

Não é política da EXPERATO ASSET o armazenamento de dados em desktops individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento em rede.

Nestes e em outros casos, o pessoal de Informática deverá alertar ao usuário que ele deve fazer backup dos dados de sua máquina periodicamente.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("*backups*") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da EXPERATO ASSET.
No caso das informações consideradas de fundamental importância para a continuidade dos negócios da EXPERATO ASSET, o setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de *backup* da Informática.

Segurança e Integridade dos 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.

Acesso a Internet

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na EXPERATO ASSET. 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 EXPERATO ASSET, com base em recomendação do Supervisor de Informática. Não é permitido instalar programas provenientes da Internet nos microcomputadores da EXPERATO ASSET, 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, licenças 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 conteúdo pornográfico ou relacionado 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 EXPERATO ASSET;
- que promovam discussão pública sobre os negócios da EXPERATO ASSET, a menos que autorizado pela Diretoria;
- que possibilitem a distribuição de informações de nível "Interno" ou "Confidencial"; e

- que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

Uso do Correio Eletrônico (e-mail)

O correio eletrônico fornecido pela EXPERATO ASSET é um instrumento de comunicação interna e externa para a realização do negócio da EXPERATO ASSET. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da EXPERATO ASSET, não podem ser contrárias à legislação vigente e nem aos princípios éticos da EXPERATO ASSET.

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 à qualquer "correntes" de *email*;
- possam prejudicar a imagem da organização;
- possam prejudicar a imagem de outras empresas ou de clientes; e
- sejam incoerentes com as políticas da EXPERATO ASSET.

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.

Sistemas de Telecomunicações

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da EXPERATO ASSET, assim como, o uso de eventuais ramais virtuais instalados nos computadores, são de responsabilidade do setor de Informática, de acordo com as definições da Diretoria da EXPERATO ASSET. Ao final de cada mês, para controle, serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal.

Uso de Antivírus

Todo arquivo em mídia não proveniente da EXPERATO ASSET deve ser verificado por programa antivírus. Todo arquivo recebido/obtido através do ambiente Internet deve ser verificado pelo setor de Informática e por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de informática, Atenção, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Proteção da Base de Dados e Procedimentos Internos para Tratar Casos de Vazamento de Informações Confidenciais

A proteção da base de dados no âmbito da EXPERATO ASSET estará lastreada nas bases legais da Lei de Proteção de Dados Pessoais, as quais, a saber estão descritas

a seguir: (i) fornecimento de consentimento pelo investidor; (ii) cumprimento de obrigação legal e/ou regulatória pela EXPERATO ASSET; (iii) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iv) o tratamento de dados se dará a pedido do próprio de titular dos dados para garantir a execução de um contrato ou de seus procedimentos preliminares; (v) o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (vi) o tratamento de dados para a tutela da saúde, desde que realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; e (vii) a proteção do crédito, em observância às regras especificas para este tema.

Riscos de vazamento de dados serão minimizados por meio da utilização de criptografia, certificados digitais e autenticações duplas. Os melhores meios de impedir violações de dados envolvem boas práticas e noções básicas de segurança bem conhecidas, tais como: A realização de testes contínuos de vulnerabilidade e penetração: (i) aplicação de proteções, que inclui processos e políticas de segurança; (ii) Uso de senhas fortes; (iii) uso de *hardware* de armazenamento seguro de chaves; (iv) uso de *hardware* para gerenciamento de chaves e proteção de dados; e (vi) aplicação consistente dos *patches* de *software* para todos os sistemas.

Vazamentos, mesmo que involuntários, serão penalizados mediante o afastamento/ demissão/desligamento imediato dos colaboradores responsáveis pelas áreas da EXPERATO ASSET nas quais se deram essas violações.

Santo Ângelo, 15 de junho de 2021.

Renan Schaefer Andrade

Diretor de *Compliance*