GL Asset Management

Política de Segurança da Informação

Atualizado em: Setembro, 2022

Índice

Introdução

Com objetivo de aprimorar os controles de proteção da informação e zelar pela integridade e sigilo dos dados corporativos, a **GL Asset Gestão de Ativos Ltda.** ("GL Asset") implementou a presente Política de Segurança da Informação ("Política") a ser observada por todos os sócios, diretores, empregados, funcionários e estagiários da GL Asset ("Colaboradores" e, no singular, "Colaborador").

A informação é um dos bens mais valiosos da GL Asset, independentemente do formato em que se apresente: eletrônico, linguagem falada ou escrita. Dessa forma, é importante protegê-la sempre. Você, como usuário, tem um papel fundamental, pois a segurança da informação acontece através das pessoas.

A GL Asset deverá dar às informações e dados pessoais e financeiros recebidos em decorrência do exercício de suas atividades a proteção e o tratamento previsto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

A GL Asset contrata os serviços da **Itrading Comercio e Serviços em Tecnolia de Informação – EIRELI** (CNPJ nº 16.712.290/0001-36) ("Itrading") para a prestação de serviços de tecnologia de informação e segurança de dados. Todas as referências feitas neste documento ao "departamento de informática" da GL Asset deverão ser entendidas como referências à Itrading.

O envolvimento de todos os Colaboradores é essencial na consolidação e representatividade da nossa Política de Segurança da Informação.

Sugerimos que você leia este material por inteiro e que as orientações aqui repassadas façam parte do seu cotidiano.

Atenciosamente,

Diretor de *Compliance*
GL Asset Gestão de Ativos Ltda.

A Importância da Segurança da Informação

Os pilares da segurança da informação nos dão subsídios para proteger as informações da GL Asset. Portanto, quando mencionamos “segurança da informação” estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que, juntas, formam uma proteção adequada para qualquer empresa.

O que é Política de Segurança da Informação?

É o conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os Colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos Colaboradores em relação à segurança dos recursos com os quais trabalham, e prevê o que pode ser feito e o que será considerado inaceitável.

A informação é só o que está nos sistemas?

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Assim, além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo é repassada através de conversas nos ambientes interno e externo.

Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a empresa em locais públicos ou com pessoas estranhas ao nosso meio.

Os 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 podem comprometer esses princípios básicos.

- ***Confidencialidade:*** É a proteção da informação compartilhada contra acessos não autorizados. Ameaça à confidencialidade acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostos, voluntária ou involuntariamente, dados restritos que deveriam estar acessíveis apenas a um determinado grupo de Colaboradores.
- ***Integridade:*** É a garantia da veracidade da informação; ou seja, de que a informação não foi alterada enquanto estava sendo transferida ou armazenada. Ameaça à integridade acontece quando uma determinada informação fica exposta ao manuseio de um

Colaborador não autorizado, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

- ***Disponibilidade:*** Prevenção contra as interrupções das operações da GL Asset 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 disponibilidade acontecem quando a informação deixa de estar acessível para os Colaboradores que necessitam dela.
- ***Autenticação***: Todas as entidades do sistema são autênticas ou genuínas; em outras palavras, os dados associados a essas entidades são verdadeiros e correspondem às informações do mundo real que elas representam, como as identidades dos usuários, a origem dos dados de um arquivo etc.
- ***Irrefutabilidade:*** Todas as ações realizadas no sistema são conhecidas e não podem ser escondidas ou negadas por seus autores.
- ***Acesso controlado:*** O acesso dos Colaboradores à informação é restrito e controlado, o que significa que somente os Colaboradores que devem ter acesso a uma determinada informação tenham esse acesso. Ameaça ao acesso controlado acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede e aos documentos.

Uso dos Recursos de Tecnologia

- Os recursos tecnológicos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o Colaborador desempenhar suas funções na GL Asset, ou para outras situações específicas formalmente permitidas pelo Diretor de *Compliance*.
- O sistema da GL Asset só pode ser acessado por meio de *login* e senha, e permite identificar os usuários que acessaram determinada informação, de modo a permitir identificar os indivíduos que tiveram acesso a ela, inclusive para fins de responsabilização em caso de vazamento de informações confidenciais.
- Quando o Colaborador se comunicar utilizando recursos de tecnologia da GL Asset, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da GL Asset.
- Os conteúdos acessados e transmitidos através dos recursos de tecnologia da GL Asset devem ser legalmente permitidos, e devem seguir as diretrizes do Código de Ética, Regras, Políticas e Controles Internos da GL Asset.
- O uso dos recursos de tecnologia da GL Asset pode ser examinado, auditado ou verificado pelo Diretor de *Compliance*, sem necessidade de autorização dos Colaboradores, respeitada a legislação vigente.

- Cada Colaborador é responsável pelo uso dos recursos tecnológicos que lhe foram fisicamente entregues e estão sob sua custódia, devendo garantir a conservação, guarda e legalidade dos programas (*softwares*) instalados.
- Os recursos de tecnologia da GL Asset, disponibilizados para os Colaboradores, não podem ser repassados para outro Colaborador ou qualquer pessoa externa à GL Asset.
- Ao identificar qualquer irregularidade no uso dos recursos de tecnologia da GL Asset, o Colaborador deve comunicar imediatamente o Diretor de *Compliance*.

Uso do Computador

a. Propriedade do computador e acesso via *login* e senha

- O computador disponibilizado para o Colaborador é de propriedade da GL Asset.
- O computador disponibilizado para o Colaborador tem por objetivo exclusivo o desempenho das atividades profissionais desse Colaborador na GL Asset.
- Todos os equipamentos, *hardwares* e *softwares* devem ser testados, homologados e autorizados pelo departamento de informática da GL Asset, antes de serem instalados nos computadores da empresa.
- A GL Asset pode, a qualquer momento, retirar ou substituir o computador disponibilizado para o Colaborador.
- Cada computador tem o seu usuário, que é o responsável pelo equipamento. O controle das máquinas é de responsabilidade do departamento de informática da GL Asset, sob a supervisão da diretoria da sociedade.
- A autenticação do Colaborador, usuário do computador, é feita através de *login* e senha, disponibilizados pelo departamento de informática, devendo a senha ser alterada pelo usuário no primeiro acesso. Será apenas permitido o uso de senha forte, com no mínimo 8 (oito) caracteres alfanuméricos, devendo conter caracteres maiúsculos, minúsculos e especiais.
- Após 3 (três) tentativas malsucedidas de autenticação de *login* e senha, será bloqueado o acesso ao computador. O acesso ao usuário somente poderá ser restabelecido pelo departamento de informática, mediante autorização do Diretor de *Compliance*.
- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da expiração desse prazo.

b. Programas utilizados no computador

- *Hardwares*, *softwares* e aplicativos somente poderão ser baixados, instalados e configurados pelo departamento de informática.
- As funções de instalar novos programas ou alterar configurações não poderão ser executadas pelos Colaboradores.

- A GL Asset utiliza servidores *on premisses* com *cloud servers*, permitindo que sejam acessados de qualquer local desde que se disponha de um computador com um link de internet.

c. Verificação do computador

- A GL Asset verificará, regularmente e sem aviso prévio, quaisquer desvios de padrão de todos os computadores e arquivos em rede, sejam *softwares*, *hardwares* ou acessos que não sejam autorizados pelo departamento de informática e/ou pelo Diretor de *Compliance*.

d. Responsabilidades dos Colaboradores

- Cuidar adequadamente do equipamento. O Colaborador é responsável pela custódia deste recurso.
- Garantir a integridade física e o perfeito funcionamento do equipamento, seguindo as regras e orientações fornecidas pelo departamento de informática.

e. Informações contidas no computador

- A GL Asset desabilitou dos computadores a função de gravação de arquivos em áreas sensíveis dos discos rígidos, pois há um servidor designado e próprio para a consolidação de todas as informações nesse sentido. A partir do conteúdo desse servidor, inclusive, são feitas cópias de segurança e implementados os procedimentos de auditoria e redundância operacional de todas as informações.

f. Outras proteções

- Foi implantada a proteção de tela nos computadores da GL Asset e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia automaticamente o sistema, exigindo *login* e senha para ser usado novamente).
- Foi implantado o modo de “suspensão” automático por inatividade durante o período de 24 (vinte e quatro) horas, para a hipótese, por exemplo, de o Colaborador esquecer a estação de trabalho ligada.
- Foi implantado o bloqueio do acesso às portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos na rede local da GL Asset.
- Foi implantado o bloqueio do acesso a *sites* de armazenamento de dados em nuvem (*cloud*), que não aquele utilizado pela própria GL Asset no OneDrive.
- Foi implantado bloqueio de sistemas que permitem o gerenciamento do computador à distância.

g. Termo de compromisso

- Para acessarem as informações e o sistema da GL Asset, todos os Colaboradores devem assinar um Termo de Adesão, cujo modelo está anexo ao Código de Ética, Regras, Políticas e Controles Internos da GL Asset.
- O Diretor de *Compliance* da GL Asset alerta todos os Colaboradores que a instalação ou utilização de *softwares* não autorizados constitui crime contra a propriedade intelectual, de acordo com a Lei nº 9.609/1998, sujeitando os infratores à pena de detenção e multa, sem prejuízo das penalidades descritas no Código de Ética, Regras, Políticas e Controles Internos da GL Asset. A GL Asset não se responsabiliza por qualquer ação individual dos Colaboradores em desacordo com a lei mencionada acima.
- Todas as práticas que representem ameaças à segurança da informação serão tratadas com a aplicação de ações disciplinares previstas no Código de Ética, Regras, Políticas e Controles Internos da GL Asset.

Uso da Internet

a. Responsabilidade e forma de uso

- O Colaborador é responsável por todo acesso à internet realizado através da infraestrutura disponibilizada pela GL Asset com seu *login* e senha.
- O Colaborador é proibido de acessar endereços de internet (*sites*) que:
  - ✓ Possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes;
  - ✓ Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
  - ✓ Contenham informações que não colaborem para o alcance dos objetivos da GL Asset;
  - ✓ Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito.
- O Colaborador deve garantir que está cumprindo a legislação relativa ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pelo seu supervisor direto.

b. Uso de serviço de mensagem instantânea

- É proibido o uso de serviços de mensagem instantânea (Skype, Zoom, WhatsApp, Teams, etc.), através dos computadores da GL Asset, exceto em situações de uso profissional autorizado pelo Diretor de *Compliance*.

c. Uso de serviço de rádio, TV, *download* de vídeos, filmes e músicas

- É proibido o uso de serviços de rádio, TV, *download* de vídeos, filmes e músicas, através dos computadores da GL Asset, exceto em eventuais situações de uso profissional autorizado pelo Diretor de *Compliance*.

d. Bloqueio de endereços de internet

- Periodicamente, o departamento de informática revisará e bloqueará o acesso aos endereços da internet que não estejam alinhados com esta Política e com o Código de Ética, Regras, Políticas e Controles Internos da GL Asset.

e. Uso de e-mail particular

- É proibido o acesso pelos Colaboradores aos seus e-mails particulares, através dos computadores da GL Asset.

Uso do E-mail Profissional

a. Endereço eletrônico do usuário

- A GL Asset disponibiliza endereços de e-mail para utilização dos Colaboradores no desempenho de suas funções profissionais, com o domínio @glasset.com.br.
- O endereço de e-mail disponibilizado para cada Colaborador é individual, intransferível e pertence à GL Asset.
- O endereço de e-mail cedido para o Colaborador deve ser o mesmo durante todo o seu período de vínculo com a GL Asset.
- Se houver necessidade de troca de endereço de e-mail, a alteração deverá ser promovida pelo departamento de informática, com a autorização do Diretor de *Compliance*, e registrada para possibilitar uma posterior autenticação (verificação de autoria).

b. Criação, manutenção e exclusão do endereço de e-mail

- A liberação do endereço de e-mail será feita pelo departamento de informática de maneira controlada e segura, com o objetivo de garantir que apenas o usuário tenha possibilidade de utilizar o referido endereço.
- Quando acontecer desligamento do usuário com a GL Asset, o supervisor do referido Colaborador deve comunicar o fato ao departamento de informática, para que o endereço de e-mail seja desativado e uma mensagem de ausência automática seja habilitada.
- As caixas de e-mail da GL Asset têm limite de tamanho e armazenamento pré-definido, aplicável também às mensagens enviadas e recebidas.

c. Uso do e-mail em *sites* e programas e na comunicação interna

- Não é permitido o uso do endereço de e-mail da GL Asset em *sites*, programas e *softwares*, sem a prévia autorização do departamento de informática.
- É permitido o uso do endereço de e-mail da GL Asset para envio de mensagens, exclusivamente, no *software* adotado pela GL Asset para comunicação interna instantânea.

d. Acesso à distância

- O Colaborador pode acessar seu e-mail da GL Asset mesmo quando estiver fora do ambiente da empresa, através do serviço de e-mail via internet (*webmail*).
- O acesso ao e-mail da GL Asset na internet deve ser autenticado via *login* e senha do usuário.
- A GL Asset utiliza um serviço de e-mail em *cloud* (nuvem) na modalidade de Software as a Service (SaaS) oferecido pela Microsoft (Exchange Online Office 365). O serviço de e-mail pode ser acessado diretamente pela web através de senha. O Exchange Online protege as informações das caixas de correio utilizando recursos avançados, tais como: filtros *antimalware* e *antispam*, assim como a prevenção contra perda de dados. Os servidores possuem redundância global e recursos avançados de recuperação em caso de desastres. Além disso, para garantir o funcionamento ininterrupto do serviço de e-mail, a Microsoft oferece uma disponibilidade de 99,9%.

e. Propriedade do endereço de e-mail

- O endereço de e-mail da GL Asset disponibilizado para o Colaborador e as mensagens associadas a esse endereço são de propriedade da GL Asset.
- Em situações excepcionais e quando autorizado pelo Diretor de *Compliance*, as mensagens do e-mail de um Colaborador poderão ser acessadas pela GL Asset ou por pessoas/entidades por ele indicada. Não deve ser mantida, portanto, expectativa de privacidade pessoal no e-mail corporativo.

f. Responsabilidades e forma de uso

O Colaborador que utiliza um endereço de e-mail da GL Asset:

- É responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail;
- Deve enviar apenas mensagens necessárias e relacionadas ao desempenho de suas atividades na GL Asset;
- É proibido de criar, copiar ou encaminhar mensagens ou imagens que:
  - ✓ contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
  - ✓ façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;

- ✓ repassem propagandas ou mensagens de alerta sobre qualquer assunto (havendo situações em que o Colaborador ache benéfico divulgar o assunto para a GL Asset, a sugestão deve ser encaminhada para o Diretor de *Compliance*, que decidirá pela sua divulgação aos demais Colaboradores ou não);
- ✓ menosprezem, depreciem ou incitem o preconceito;
- ✓ possuam conteúdo pornográfico, obsceno ou impróprio para um ambiente profissional;
- ✓ sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- ✓ defendam ou possibilitem a realização de atividades ilegais;
- ✓ sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- ✓ possam prejudicar a imagem da GL Asset; e
- ✓ sejam incoerentes com o Código de Ética, Regras, Políticas e Controles Internos da GL Asset;

- É proibido de reproduzir qualquer material recebido pelo e-mail ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização;
- Deve estar ciente que uma mensagem de e-mail da GL Asset é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional emitido em papel timbrado da entidade;
- Exceto quando especificamente autorizado para tal, é proibido de emitir opinião pessoal, colocando-a em nome da GL Asset;
- Deve observar se o endereço do destinatário de suas mensagens eletrônicas corresponde realmente ao destinatário desejado;
- Deve ser diligente em relação:
  - ✓ aos Colaboradores que receberão a mensagem (Destinatário/*To*, Copiado/*Cc* e Copiado Oculto/*Bcc*);
  - ✓ ao nível de sigilo da informação contida na mensagem;
  - ✓ aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos; e
  - ✓ ao uso da opção “Encaminhar” (*forward*) das mensagens, verificando se há realmente a necessidade de manter as diversas mensagens anteriores que estão na cadeia de e-mails;
- Deve deixar mensagem de ausência quando for passar um período maior do que 48 (quarenta e oito) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do Colaborador substituto para quem deve ser enviada a mensagem.

g. Cópias de segurança

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria:

- A cópia de segurança dos e-mails da GL Asset é feita de forma centralizada, através de um *backup* completo com salvamento automático, armazenado em servidores da Microsoft Corporation, e que fica disponível por até 2 (dois) anos.
- O departamento de informática da GL Asset fornece o serviço de recuperação de e-mails, a partir de arquivos de cópia de segurança, mantidos em nuvem, cumprindo parâmetros de nível de serviço previamente estabelecidos, mediante solicitação do Diretor de *Compliance*.

Uso do Telefone

a. Número do telefone do Colaborador

- A GL Asset disponibiliza telefones fixos para utilização dos Colaboradores no desempenho de suas funções profissionais.
- Se houver necessidade de troca de número de telefone, a alteração deverá ser autorizada pelo Diretor de *Compliance* e realizada pelo departamento de informática.

b. Propriedade do número do telefone

- Os telefones disponibilizados para os Colaboradores e as conversas associadas a esses números são de propriedade da GL Asset.
- Todos os telefonemas feitos a partir dos telefones da GL Asset são gravados e monitorados regularmente, e, em situações especiais autorizadas pelo Diretor de *Compliance*, as conversas de um Colaborador poderão ser acessadas pela GL Asset ou por pessoas/entidades por ela indicada. Não deve ser mantida, portanto, expectativa de privacidade pessoal.

c. Responsabilidades e forma de uso

O Colaborador que utiliza um telefone da GL Asset:

- É responsável por todo conteúdo da conversa;
- Deve utilizar o telefone apenas para o desempenho de suas atividades na GL Asset;
- É proibido de utilizar o telefone da GL Asset para conversas que:
  - ✓ contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
  - ✓ menosprezem, depreciem ou incitem o preconceito;
  - ✓ possuam conteúdo pornográfico, obsceno ou impróprio para um ambiente profissional;

- ✓ defendam ou possibilitem a realização de atividades ilegais;
- ✓ possam prejudicar a imagem da GL Asset; e
- ✓ sejam incoerentes com o Código de Ética, Regras, Políticas e Controles Internos da GL Asset.

d. Cópias de segurança

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria:

- A cópia de segurança dos telefonemas realizados a partir dos telefones da GL Asset será feita de forma centralizada, no ambiente dos equipamentos e servidores corporativos, sob a responsabilidade do departamento de informática.
- O departamento de informática da GL Asset fornecerá a recuperação do conteúdo gravado de telefonemas, a partir de arquivos de cópia de segurança, mediante solicitação do Diretor de *Compliance*.

Monitoramento e Testes Periódicos

Para confiabilidade de informações e segurança dos próprios Colaboradores, os sistemas de informações da GL Asset são periodicamente auditados e monitorados. Para tanto, a área de *compliance*, juntamente com os responsáveis pela área de tecnologia da informação, realiza semestralmente testes de segurança no servidor e nos computadores da GL Asset, a fim de verificar a eficácia do sistema de segurança implementado, e evitar, assim, eventuais problemas com o acesso indevido de pessoas não autorizadas a informações confidenciais.

Tais testes deverão, por exemplo, verificar: (i) o uso da capacidade instalada da rede e dos equipamentos; (ii) o tempo de resposta no acesso à Internet e aos sistemas críticos da GL Asset; (iii) a ocorrência de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da GL Asset; (iv) a ocorrência de incidentes de segurança (vírus, *trojans*, furtos, acessos indevidos, e assim por diante); e (v) a ocorrência de acessos indevidos às áreas de acesso restrito do escritório da GL Asset.

Linhas Gerais de Comportamento

a. Controle de acesso e câmeras de gravação

O controle de acesso ao escritório da GL Asset é parte central da segurança da empresa. Por isso, é fundamental que, ao entrar nas dependências da GL Asset, os Colaboradores utilizem o acesso biométrico e registrem suas senhas.

Câmeras de gravação de vídeo foram instaladas no *hall* de entrada das dependências da GL Asset para garantir a sua segurança e o monitoramento do acesso ao escritório.

b. No ambiente externo, é melhor ficar atento

Falar sobre informações confidenciais ou segredos profissionais em um lugar público ou por telefone merece cuidado especial e deve ser evitado. Frequentemente, as pessoas são o elo mais fraco na segurança da informação de uma empresa.

Quando seu equipamento viajar com você, evite deixá-lo por muito tempo sozinho em uma sala ou mesa. Qualquer *pendrive* ou conexão de rede pode conter dados valiosos.

c. Cuidado com o lixo que você produz

O lixo pode ser uma fonte de informações para pessoas mal-intencionadas.

Em linha com a Política de Confidencialidade e Segregação de Atividades, antes de descartar, destrua os documentos que contenham informações confidenciais de investidores, fundos de investimentos geridos e/ou ativos-alvo de fundos de investimento. Se o papel que vai ser jogado no lixo contém informações que não devem ser lidas por estranhos, triture-o antes de jogá-lo fora.

d. Cuidados com senhas e acessos ao sistema

Cada tarefa desenvolvida na GL Asset precisa ter um responsável.

A única forma de saber o responsável por cada atividade é através da autenticação (identificação do usuário) via *login* e senha. Tudo que é feito com a sua senha é de sua responsabilidade. Portanto, cuidado com seus dados, seja na rede ou nos sistemas, pois sua identificação serve para garantir que você é realmente quem está acessando.

Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você, porém, a responsabilidade por tudo que ela fizer será sua.

Alguns exemplos de ações que podem ser atribuídas a você, são:

- liberação de ações indevidas;
- envio de e-mails com informações inadequadas; e
- acesso a páginas da internet proibidas.

Compartilhar sua senha é como assinar um cheque em branco. Não anote a sua senha em local público ou de fácil acesso.

e. Adote um comportamento seguro

- Não compartilhe nem divulgue sua senha a terceiros;
- Não transporte informações confidenciais da GL Asset em qualquer meio (HD externo, CD, discos, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abra mensagens de origem desconhecida;
- Armazene e proteja adequadamente documentos impressos e arquivos eletrônicos que contêm informações confidenciais;
- Siga corretamente a política para uso de internet e correio eletrônico estabelecida pela GL Asset.