SEGTRUCK

Boas práticas de Segurança da Informação para usuários

Nunca a afirmativa de que novos tempos são sempre desafiadores foi tão verdadeira como agora. Basta que pensemos no grande avanço das comunicações, por exemplo, das últimas décadas.

De repente, temos o mundo dentro do nosso computador ou do nosso smartphone!
Nada é mais fascinante do que essa possibilidade de aproximação. Literalmente, temos o mundo ao alcance das mãos e as pessoas muito próximas, embora distantes, umas das outras.

Atenta e preocupada em garantir a segurança de nossos funcionários e usuários, elaboramos essa cartilha que especifica quais as políticas desenvolvidas pela SEGTRUCK nessa área. Por meio de ferramentas de segurança especializadas, buscamos fornecer condições básicas e seguras de uso de informações e dos recursos de tecnologia da informação.

As informações produzidas na SEGTRUCK, ou por ela adquiridas, são consideradas de sua propriedade, sendo parte de seu patrimônio, não importando a forma de apresentação ou de armazenamento.

Por entender a responsabilidade que temos em proteger adequadamente todos esses dados, oferecemos esse manual com o intuito de orientação quanto a privacidade, proteção de dados e segurança da informação. Leia com atenção!

1- INTRODUÇÃO

Todas as informações produzidas na SEGTRUCK, ou por ela adquiridas, são consideradas de sua propriedade, sendo parte de seu patrimônio, não importando a forma de apresentação ou armazenamento. Essas informações, bem como as de terceiros, sob a sua responsabilidade, devem ser adequadamente protegidas.

As informações devem ser utilizadas exclusivamente para fins relacionados diretamente às atividades-fins e meio da SEGTRUCK, observando as orientações contidas nas diretrizes éticas, normas e políticas da empresa.

As informações pertencentes à SEGTRUCK só podem ser usadas no seu interesse. Seu uso ou divulgação externa somente poderão ocorrer mediante autorização do responsável. A SEGTRUCK garante a segurança da rede através da inspeção automática dos dados trafegados, respeitando o sigilo e a privacidade dos seus funcionários.

Aplicação da Política de Segurança da Informação

CCPD - Comitê de Privacidade e Proteção de Dados
Cabe a este Comitê atuar como fórum de discussão sobre Privacidade e Proteção de dados.

CSI - Comitê de Segurança da Informação
Cabe a este Comitê manter a Política de Segurança da Informação atualizada e alinhada às diretrizes éticas e à cultura da SEGTRUCK; tratar dúvidas e questões não contempladas pela Política de Segurança da Informação; e informar o CPPD - Comitê de Privacidade e Proteção de Dados sobre decisões relacionadas à segurança da informação.

Funcionários da SEGTRUCK

Cabe aos funcionários da SEGTRUCK de todos os escalões garantirem a aplicação adequada da Política de Proteção de Dados Pessoais e Segurança da Informação.

Usuários e demais envolvidos

Cabe a cada pessoa envolvida com atividades-fim e atividades-meio da SEGTRUCK zelar pela utilização adequada das informações e pelos recursos computacionais disponibilizados.

Divulgação

Cabe à SEGTRUCK efetuar ações de divulgação para conscientização dos usuários sobre a importância e a necessidade de seguir a Política de Segurança da Informação.

Tecnologia da Informação

O termo tecnologia da informação (TI) pode ser definido como o conjunto de recursos tecnológicos e computacionais para geração e uso da informação, abrangendo todas as atividades desenvolvidas na sociedade pelos recursos da informática.

Recursos relacionados à TI, como Internet, correio eletrônico, redes sem fio, entre outros, são atualmente ferramentas de trabalho indispensáveis no desempenho das mais diversas atividades. Porém, tais recursos podem ser explorados para fins ilícitos, como roubo de informações, disseminação de vírus, envio de spam, etc.

Diante deste cenário, este manual foi elaborado visando orientar diretores e funcionários para uma utilização segura dos recursos de tecnologia da informação disponibilizados pela SEGTRUCK.

Nos próximos tópicos, serão apresentadas orientações sobre:

- Senhas;
- Certificado digital;
- Internet;
- Correio eletrônico;
- Estações de trabalho;
- Rede local.

2- SENHAS

Via de regra, o acesso aos diversos serviços de informática, como sistemas, e-mail, rede local, entre outros, ocorre mediante autenticação do usuário através de seu *nome de usuário* (login) e *senha* (password). Tal processo visa garantir que o acesso à informação seja obtido apenas por pessoas autorizadas (garantia de confidencialidade).

Cada usuário é responsável pela escolha de suas senhas pessoais. Algumas recomendações importantes:

Selecione senhas de boa qualidade.

Uma senha bem elaborada reduz as chances de ser comprometida. Algumas recomendações para elaboração de senhas:

- Utilize senhas com o mínimo de: 8 caracteres, 2 letras maiúsculas, 1 letra minúscula, 1 número, 2 símbolos: @#$%.
- Não elabore senhas baseadas em informações pessoais, como nomes, sobrenomes, número de documentos, placas de carros, telefones e datas;
- Não elabore senhas baseadas em palavras que constem no dicionário de qualquer idioma;
- Não elabore senhas com caracteres repetidos ou seqüenciais. Ex.: aa22, abcde, ab123;
- Não elabore senhas com caracteres seguidos no teclado do computador. Ex.: qwer, zxcv;

Nunca divulgue ou compartilhe senhas pessoais.

As senhas são utilizadas no processo de identificação do usuário perante os acessos à sistemas e serviços de informática. Sua confidencialidade é importante, de forma a evitar que terceiros acessem informações sensíveis, como e-mails e arquivos pessoais, documentos sigilosos, etc.

Cada usuário possui logins e senhas individuais, sendo proibida a divulgação ou compartilhamento de tais dados;

Altere periodicamente as senhas

Com o objetivo de assegurar a confidencialidade das mesmas. É recomendável que as senhas sejam alteradas a cada dois ou três meses no máximo;

Quando possível, não utilize senhas iguais para serviços diferentes.

Ex.: Utilize senhas distintas para cada sistema e e-mail;

Evite registrar senhas em locais inseguros

Como anotações em papel, embaixo do teclado, adesivos colados no monitor, etc.

O recomendável é apenas memorizar a senha;

Sempre altere as senhas temporárias no primeiro acesso.

Ex.: Alterar no primeiro acesso, as senhas iniciais fornecida pela TI;

Não digite senhas quando observado

Evite que outras pessoas descubram suas senhas;

Sempre altere uma senha quando suspeitar que a mesma foi descoberta.

3- CERTIFICADO DIGITAL

Certificado digital é um documento eletrônico que identifica pessoas e instituições, provando sua identidade e permitindo acessar serviços informatizados com a garantia de autenticidade, integridade e não-repúdio, assim como assinar digitalmente documentos.

Cada usuário é responsável pela guarda e utilização de seu certificado digital. Algumas recomendações importantes:

- **Nunca forneça o certificado digital a terceiros.**

O certificado digital é um documento pessoal e intransferível. Assim como outros documentos pessoais, como CPF, RG e passaporte, não deve ser fornecido a terceiros por questões de segurança;

- **Aplique as recomendações descritas no item *2. Senhas* para as senhas do certificado digital.** Um certificado digital possui duas senhas: PIN e PUK.

  O PIN (Personal Identification Number) é fornecido pelo usuário na utilização do certificado, como por exemplo para assinar um documento eletrônico.
  O PUK (Personal Unblocking Key) é utilizado pelo usuário para alterar o seu PIN em caso de necessidade.

4- INTERNET

A internet é uma ferramenta de trabalho utilizada pelos funcionários como apoio ao desenvolvimento de suas competências e à realização de atividades profissionais. A SEGTRUCK pode monitorar seu uso para eventuais perícias, identificando os usuários e quais as páginas visitadas.

O funcionário pode usar a Internet como um recurso pessoal, desde que não interfira na execução de suas atividades profissionais, em observância às políticas e normas vigentes. O acesso à Internet deve ser feito respeitando a legislação, as políticas e normas vigentes e preservando a imagem da SEGTRUCK.

Não é permitido efetuar ações que possam ser caracterizadas como violação da segurança da informação, tais como capturar ou quebrar senhas de outros usuários, efetuar varreduras na rede, invadir sites, entre outras.

O uso da rede e da Internet deve ser feito de forma a não prejudicar os serviços de rede ou as atividades de outros funcionários, dentro ou fora da rede da SEGTRUCK. Se necessário, poderão ser configurados filtros de bloqueio.

Não é permitido acessar computadores, softwares, informações ou outros recursos, sem a devida autorização ou, intencionalmente, habilitar terceiros a fazerem isso. É dever dos funcionários o respeito à propriedade intelectual e aos direitos autorais.

O acesso à Internet na SEGTRUCK está disponível para funcionários a partir das estações de trabalho conectadas à rede local da empresa. Algumas recomendações quanto à utilização da Internet:

Na SEGTRUCK, utilize somente os meios de acesso à internet homologados pela TI, que são a rede local e a rede sem fio da instituição. Demais formas de acesso, como modem (acesso discado), acesso sem fio fornecido por empresas (Ex.: Oi, TIM, Claro), entre outras, não devem ser utilizadas no âmbito da instituição, pois podem comprometer a segurança da rede e das informações institucionais;

Não acesse sites e serviços Internet suspeitos, como os relacionados à pornografia, software ilegal, spam, etc. Tais sites costumam ser utilizados para disseminação de vírus e roubo de informações pessoais;

Não acesse sites e serviços da internet sem relação com as atividades desempenhadas pela instituição, como sites de jogos, fóruns não profissionais, comunidades de relacionamento pessoal, bate-papo, áudio e vídeo, dentre outros,

evitando assim que o desempenho do acesso Internet e serviços relacionados sejam afetados;

Não utilize softwares e serviços Internet não homologados pela TI, como aqueles relacionados a compartilhamento de arquivos (Ex.: Torrent), troca de mensagens em tempo real (Ex.: Telegram), transmissão de áudio e vídeo (Ex.: YouTube), telefonia Internet (Ex.: Skype), evitando assim que a segurança e o desempenho da rede institucional sejam afetados;

Somente envie informações pessoais através de sites seguros. Informações pessoais, como senhas e números de cartões de crédito, devem ser fornecidas somente em sites considerados seguros. Para identificar se um site é seguro, verifique se o endereço do mesmo (URL) é iniciado por https:// e se o navegador (Ex.: Internet Explorer, Firefox) exibe a figura de um cadeado fechado;

Somente acesse sites de instituições financeiras e públicas digitando o endereço diretamente no navegador, nunca clicando em outro site ou em um e-mail recebido, evitando assim que dados pessoais sejam furtados através de sites fraudulentos;

Não utilize computadores públicos ou compartilhados, como terminais em aeroportos, cafés e shopping centers, para acessar serviços disponibilizados no site da SEGTRUCK, webmail, etc. Computadores compartilhados são ambientes inseguros, onde informações sigilosas podem ser obtidas por terceiros.

5- CORREIO ELETRÔNICO

O serviço de correio eletrônico institucional está disponível para funcionários a partir de qualquer estação com acesso à Internet. Algumas recomendações quanto à utilização do serviço de correio eletrônico:

Não abra e-mails e anexos considerados suspeitos, como os relacionados à pornografia, propagandas, correntes, arquivos executáveis, remetentes desconhecidos, dentre outros. Tais e-mails e anexos costumam ser utilizados para disseminação de vírus e roubo de informações pessoais. Caso considere um e-mail ou anexo suspeito, apague o mesmo de sua caixa postal;

Limpe periodicamente sua caixa postal, apagando e-mails antigos, spams, etc.
Tal procedimento previne o não recebimento de e-mails, devido ao limite da caixa postal;

Evite enviar e-mails para um grande número de destinatários, pois tal atitude compromete o desempenho da rede local e do serviço de correio eletrônico;

Utilize o serviço de correio eletrônico somente para fins profissionais, pois o envio de e-mails sem relação com as atividades desempenhadas pela instituição compromete o desempenho da rede local e do serviço de correio eletrônico;

Divulgue seu e-mail da SEGTRUCK somente para fins profissionais, evitando informar o mesmo em sites e serviços da internet não seguros. Tal procedimento reduz o recebimento de spams, mensagens indesejadas e roubo de credenciais;

6- ESTAÇÕES DE TRABALHO

Constituem estações de trabalho os computadores e notebooks registrados como patrimônio da SEGTRUCK e utilizados pelos funcionários no desempenho de suas atividades funcionais. Algumas recomendações quanto à utilização das estações de trabalho:

- **Não instale softwares sem a autorização da TI**
  Somente softwares devidamente licenciados para utilização na SEGTRUCK e homologados pela TI podem ser utilizados nas estações de trabalho. A utilização de software não licenciado ou considerado "pirata" constitui infração prevista na Lei nº 9.609/1998.

- **Não instale, remova ou modifique qualquer software ou hardware sem a autorização da TI .** Tal atitude pode comprometer a segurança e o desempenho da estação de trabalho;

- **Acesse a estação de trabalho somente com sua conta de usuário**
  Nunca utilize uma estação de trabalho através do nome de usuário (login) e senha (password) de outra pessoa. Tal procedimento visa garantir a confidencialidade das informações processadas;

- **Ao se afastar da estação de trabalho, efetue o bloqueio ou "logoff" da mesma**
  Evitando assim que outra pessoa acesse a estação de trabalho através do seu nome de usuário (login) e senha (password);

- **Utilize a estação de trabalho somente para fins profissionais.**

7- REDE LOCAL

O acesso à rede local da SEGTRUCK está disponível para funcionários a partir das estações de trabalho. Algumas recomendações importantes:

- **Não utilize computadores pessoais na rede local da SEGTRUCK**
  Somente acesse a rede local através de computadores e notebooks registrados como patrimônio da instituição. Computadores pessoais conectados à rede da SEGTRUCK representam uma das principais portas de entrada de vírus e outras ameaças à segurança da informação;

- **Armazene na rede somente arquivos relacionados com suas atividades funcionais**
  Não utilize a rede para armazenar arquivos pessoais, como fotos, músicas, vídeos ou qualquer tipo de arquivo sem relação com as atividades da SEGTRUCK. A má utilização do espaço disponível para armazenamento de arquivos afeta a performance de serviços essenciais;

- **Nas dependências da SEGTRUCK, nunca utilize redes sem fio de terceiros.**
  Caso seja necessário acesso sem fio, utilize somente a rede local sem fio disponibilizada pela instituição, evitando assim que informações sensíveis sejam interceptadas por terceiros.

8- ZELO COM AS INFORMAÇÕES

Informações de acesso restrito não podem ser deixadas expostas, devendo ser sempre protegidas em um local seguro. Quando houver informações de acesso restrito na tela, deve-se tomar todo o cuidado para evitar sua visualização por pessoas não autorizadas.

Informações pessoais, tais como nome, endereço, telefone, e-mail, entre outras são consideradas de acesso restrito e devem ser protegidas. Quando algum documento for impresso, deve-se buscá-lo imediatamente na impressora.

Não permita que pessoas desconhecidas utilizem seu computador. Quando não forem mais necessárias, as informações de acesso restrito devem ser descartadas de forma adequada. Por exemplo: papéis e CD/DVDs devem ser triturados e pendrives e HDs devem ser apagados, utilizando um software de destruição de dados (Solicite auxilio da TI). A simples formatação da mídia não impede que os dados sejam recuperados.

9- ALTERAÇÕES DE CONFIGURAÇÃO

A SEGTRUCK possui ferramentas de monitoramento de hardware instaladas em cada novo computador para fins de inventário e gestão da configuração e monitoramento de possíveis vulnerabilidades. Toda alteração à configuração deve ser solicitada ao responsável de TI por meio de abertura de chamado via help-desk. As configurações de equipamentos de infraestrutura de rede, tais como roteadores, switches e APs, entre outros, só poderão ser modificadas mediante autorização do responsável de TI.

10- PONTOS DE ATENÇÃO

Os 10 pontos fundamentais na segurança da informação para a comunidade da SEGTRUCK

1. Proteção de dados pessoais;
2. Cuidados com suas senhas;
3. Proteção contra software malicioso;
4. Navegação na Internet;
5. Correio eletrônico;
6. Instalação de software;
7. Realização de backups;
8. Dispositivos móveis;
9. Sintomas de contaminação;
10. Atividades maliciosas ou de espionagem na navegação de sites;

11- CUIDADOS COM SUAS SENHAS

1. Sua senha é pessoal e intransferível;
2. Suas credenciais (conta e senha) representam a sua identidade na SEGTRUCK. Cuide bem delas;
3. Você é responsável por todas as ações realizadas utilizando a sua senha;
4. Não divulgue e nem compartilhe – a senha é sua e de mais ninguém;
5. Não escreva sua senha em local público ou de fácil acesso, em papéis, no computador ou em outro tipo de mídia;
6. Não deixe sua senha visível ao digitá-la, muito menos na presença de desconhecidos;

7. Nunca use palavras de dicionários ou dados pessoais como senha;

12- DISPOSITIVOS MÓVEIS

1. Todas as instruções acima aplicam-se também a dispositivos móveis;
2. Proteja fisicamente os dispositivos móveis de forma a reduzir o risco de perda e roubo;
3. No caso de dispositivos institucionais, mantenha sempre ativo o software de rastreamento e gerenciamento remoto;
4. No caso de perda ou roubo de dispositivo institucional, comunique imediatamente o responsável patrimonial;
5. Instale aplicativos apenas de fontes confiáveis;
6. Habilite bluetooth e wi-fi só quando for utilizá-los;
7. Faça as atualizações no dispositivo móvel;
8. Faça backup de dados na nuvem ou no computador;
9. Instale e habilite software antivírus;
10. Não aceite e não execute qualquer arquivo enviado para o dispositivo móvel que não tenha sido solicitado;

Violações da Política de Segurança da Informação da SEGTRUCK estão sujeitas a sanções disciplinares, observadas a natureza e a gravidade da infração.

Ao identificar ou suspeitar de possível violação das diretrizes, normas e procedimentos estabelecidos, busque orientação com CSI - Comitê de Segurança da Informação.

SEGTRUCK

CSI - Comitê de Segurança da Informação

CPPD - Comitê de Privacidade e Proteção de Dados