POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio (físico ou digital) e local em que ela esteja armazenada, com base na legislação vigente, órgãos reguladores e nas boas práticas de segurança da informação.

2. RESPONSABILIDADE

Esta Política é de reponsabilidade do Departamento de Tecnologia da ABC SISTEMA DE TRANSPORTE SPE S.A – Quaisquer mudanças nesta Política devem ser aprovadas pelo Departamento de Tecnologia.

A alta gestão tem o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação.

Essa política se aplica a todos os colaboradores, fornecedores e prestadores de serviços que utilizem ou forneçam serviços tecnológicos relevantes.

3. PÚBLICO ALVO

Esta Política se aplica a ABC SISTEMA DE TRANSPORTE SPE S.A

4. DIRETRIZES GERAIS

A. Tratamento da Informação

A informação sob custódia da ABC SISTEMA DE TRANSPORTE SPE S.A, mesmo que pertencente a clientes, colaboradores ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas.

O acesso, geração, utilização, classificação, modificação, distribuição, transferência, armazenamento e eliminação da informação devem ser feitas de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados. A ABC SISTEMA DE TRANSPORTE SPE S.A –, reservam-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais.

Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

A informação deve ser armazenada, pelo tempo determinado pela empresa, legislação ou regulação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

B. Acesso à Informação

O uso de redes externas de comunicação (Internet, VPN, etc.) deve ser controlado através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

O acesso externo aos sistemas da organização, quando realizado pelo pessoal da Área de Suporte Técnico ou por prestadores de serviço, deve ser controlado e restrito aos serviços

necessários, mantendo trilhas de utilização e restringindo–se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada.

A remessa de dados da empresa, seja para atender requisitos de negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

C. Sistemas/Aplicativos

Sistemas e aplicativos desenvolvidos dentro da organização devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito a guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

Sistemas e aplicativos desenvolvidos fora da organização, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes etc.) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do software. Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de produção.

O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de atividades críticas do sistema. Onde for impraticável implantar a segregação, outros controles como monitoração das atividades, trilhas de auditoria e acompanhamento gerencial devem ser considerados.

Para minimizar o risco de falhas nos sistemas, deve-se fazer um planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos. Para novos sistemas os requisitos operacionais devem ser documentados e testados antes da sua aceitação e uso. Para sistemas já em uso devem ser feitas projeções da demanda de recursos e da carga da máquina futura a fim de reduzir o risco de indisponibilidade por sobrecarga (Capacity Planning).

5. SEGURANÇA QUANTO ÀS PESSOAS

Este tópico trata da segurança quanto às pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos da empresa.

A. Identificação das pessoas

Todas as pessoas com acesso aos sistemas e informações, pertencentes a empresa, deverão ter uma única identificação (login). As exceções deverão ser devidamente documentadas e aprovadas pela direção, a qual informará o Gerente de TI para a criação de novo acesso.

B. Declaração de Responsabilidade

É um compromisso de responsabilidade direta do colaborador para com as informações, equipamentos e outras propriedades da empresa a ele confiadas, devendo ser lida e assinada quando de sua admissão.

A declaração de responsabilidade deve ser lida e assinada, dentro dos formatos aceitos e homologados em meio físico ou eletrônico, por todos os colaboradores antes de ser arquivada na respectiva pasta funcional. O Departamento de Recursos Humanos deve

garantir que todos os colaboradores tenham sua declaração de responsabilidade assinada.

6. SEGURANÇA LÓGICA DE COMPUTADORES, REDES E SISTEMAS APLICATIVOS

Este item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse da empresa.

Todo sistema de aplicativo define um conjunto de operações aplicáveis às informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão etc.

Um perfil de acesso define que operações podem ser executadas por certa classe de usuários, usando um determinado tipo de informação.

Caso as operações e suas respectivas informações envolvam quantias, poderão ser criadas alçadas, que definem a quantia máxima envolvida em operações executadas por cada classe de usuários.

As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis, alçadas e classe de usuários, bem como os processos operacionais a serem utilizados para sua administração e controle.

A. Normas para segurança lógica de computadores e redes:

Os acessos aos serviços e dados devem ser controlados com base nos requisitos de cada área, devem estar claramente definidos e documentados e todos os sistemas aplicativos devem estar direcionados para a implementação e manutenção desses controles.

Cada gestor da informação é responsável por definir e manter atualizados os perfis de acesso aos seus aplicativos visando o acesso mínimo necessário para a execução das atividades bem como evitar conflitos de interesse.

B. Administração do acesso aos sistemas e aplicativos:

As informações devem ser analisadas pelos respectivos gestores da informação, de forma a permitir que sejam definidas as regras de acesso, através de perfis e alçadas.

Os sistemas e aplicativos devem possuir recursos que possibilitem a administração dos acessos, através dos perfis e alçadas definidos pelos respectivos gestores da informação.

C. Administração do acesso de usuários:

Devem existir procedimentos formais que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários.

D. Controle de acesso a computadores e redes:

Deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto.

O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados.

Os ambientes de produção, homologação e desenvolvimento devem estar segregados entre si, de forma a impedir acessos indevidos.

E. Normas para controle de acesso a computadores, redes, sistemas e aplicativos:

Um sistema efetivo de controle de acesso deve ser utilizado para autenticar os usuários. As principais características desse controle são:

- O acesso a computadores e redes deve ser protegido por senha;

- As senhas poderão ser alteradas pelos usuários em qualquer ambiente (operacional ou aplicativo);

- Os sistemas devem ser programados para nunca exibir a senha na tela;

- As senhas devem ser individuais e intransferíveis. A senha é de uso exclusivo, pessoal e intransferível, sendo o compartilhamento proibido em quaisquer circunstâncias;

- As senhas não devem ser triviais e previsíveis;

- Os tipos de caracteres utilizados para a formação da senha devem ser:

a. Letras maiúsculas;
b. Letras minúsculas;
c. Números;
d. Sinais ou símbolos especiais (Ex: @ # $ % & * - + = “ ´ ` ^ ~ { } [ ] / | \ ? !).

- As senhas deverão ter um tamanho mínimo de 08 (oito) caracteres, sendo obrigatória a utilização de no mínimo três dos quatro tipos de caracteres acima definidos, sendo mandatário o uso de no mínimo um sinal ou símbolo especial;

- Os sistemas devem prever um prazo para a expiração de senhas de no máximo 30 (trinta) dias;

- Caso algum sistema defina uma senha inicial, deverá obrigar o usuário a alterá-la no primeiro acesso;

- As senhas trocadas ou expiradas devem ser cadastradas para efeito de bloqueio de reutilização (mínimo de vinte e quatro senhas);

- Os arquivos de senhas devem ser criptografados e gravados separadamente dos arquivos de dados, em ambiente de acesso restrito;

- Após um máximo de cinco tentativas consecutivas sem sucesso, os acessos devem ser bloqueados até que seja solicitado o desbloqueio do usuário; e

- Uma vez aprovada, a senha deve garantir acesso exclusivo do usuário na estação de trabalho. Portanto, um mesmo usuário não deverá utilizar simultaneamente mais de uma estação de trabalho.

F. Monitoramento de uso e acesso aos sistemas e aplicativos:

Todos os sistemas e aplicativos deverão:

- Detectar tentativas de acesso não autorizado;

- Registrar eventos de entrada no sistema (login);

- Sempre que houver riscos que afetem o negócio devem ser gravadas trilhas de auditoria para futuras investigações, registrando os dados dos acessos, tais como: identificação do usuário, localidade, identificação do terminal ou estação de rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas; e

- Emitir relatórios gerenciais de acessos (por usuário, módulo do aplicativo e funções).

G. Processo de desenvolvimento de sistemas:

Os sistemas desenvolvidos deverão observar e seguir as boas práticas de mercado sobre desenvolvimento seguro a fim de mitigar riscos e vulnerabilidades comumente exploradas nos sistemas.

A aderência do processo deve ser realizada através de adequação de processos e/ou uso de tecnologias específicas para esse tipo de finalidade.

Adicionalmente, cabe à Segurança da Informação avaliar a necessidade de testes de segurança sobre qualquer sistema, seja interno, exposto na internet, hospedado fora da infraestrutura tecnológica da empresa, desenvolvido internamente ou externamente.

7. MELHORIA CONTINUA DA SEGURANÇA DA INFORMAÇÃO

A política da ABC SISTEMA DE TRANSPORTE SPE S.A, em relação à melhoria contínua é:

A. Melhorar continuamente a eficácia dos controles de segurança da informação;

B. Aprimorar os processos atuais para adequá-los às boas práticas, conforme definido;

C. Aumentar o nível de proatividade (e a percepção da proatividade das partes interessadas) em relação à segurança da informação;

D. Tornar os processos e controles de segurança da informação mais mensuráveis, para fornecer uma base sólida para decisões.;

E. Revisar métricas relevantes anualmente para avaliar se é apropriado alterá-las, com base nos dados históricos coletados;

F. Obter ideias para melhoria por meio de reuniões regulares e outras formas de comunicação com as partes interessadas;

G. Analisar ideias para melhoria nas reuniões regulares de gestão, a fim de priorizar e avaliar prazos e benefícios;

Ideias para melhorias podem ser obtidas de qualquer fonte, incluindo colaboradores, clientes, fornecedores, equipe de TI, avaliações de risco e relatórios de serviço. Uma vez identificados, elas serão registradas e avaliadas em revisões administrativas.

8. CONJUNTOS DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

ABC SISTEMA DE TRANSPORTE SPE S.A, define a política em uma ampla variedade de áreas relacionadas à segurança da informação, descritas em detalhes em um conjunto abrangente de políticas que acompanha este documento.

Cada uma dessas políticas é definida e acordada por uma ou mais pessoas com competência na área específica e, uma vez formalmente aprovada, é comunica ao público alvo, dentro e fora da organização.

A tabela abaixo mostra as políticas individuais, resume o conteúdo de cada política e o público-alvo das partes interessadas.

Título da política	Áreas endereçadas	Público-alvo
Política de Computação em Nuvem	Diligências, configuração, gerenciamento e remoção de serviços de computação em nuvem.	Colaboradors envolvidos na aquisição e gerenciamento de serviços em nuvem
Política de Dispositivos Móveis	Segurança de dispositivos móveis, como laptops, tablets e smartphones, fornecidos pela empresa ou pelo indivíduo para uso comercial.	Usuários de dispositivos móveis fornecidos pela empresa ou próprio dispositivo do colaborador
Política de Controle de Acesso	Registro de usuário e cancelamento de registro, fornecimento de direitos de acesso, acesso externo,	Colaboradors envolvidos na configuração e gerenciamento do controle de acesso

	revisões de acesso, política de senha, responsabilidades do usuário e controle de acesso ao sistema e ao aplicativo.	
Política Criptográfica	Avaliação de risco, seleção de técnica, implantação, teste e revisão de criptografia e gerenciamento de chaves	Colaboradores envolvidos na criação e gestão do uso de tecnologia e técnicas criptográficas
Política de Segurança Física	Áreas de segurança local, segurança de papel e equipamento e gerenciamento do ciclo de vida de equipamentos	Todos os colaboradors
Política Antimalware	Firewalls, antivírus, filtragem de spam, instalação e verificação de software, gerenciamento de vulnerabilidades, treinamento de conscientização do usuário, monitoramento e alertas de ameaças, revisões técnicas e gerenciamento de incidentes de malware.	Colaboradors responsáveis por proteger a infraestrutura da organização contra malware
Política de Segurança de Rede	Projeto de segurança de rede, incluindo segregação de rede, segurança de perímetro, redes sem fio e acesso remoto; gerenciamento de segurança de rede, incluindo funções e	Colaboradors responsáveis por projetar, implementar e gerenciar redes

	responsabilidades, registro e monitoramento e alterações.	
Política de Mensagens Eletrônicas	Envio e recebimento de mensagens eletrônicas, monitoramento de facilidades de mensagens eletrônicas e uso de e-mail.	Usuários de facilidades de mensagens eletrônicas
Política de Retenção e Proteção de Registros	Período de retenção para tipos de registro específicos, uso de criptografia, seleção de mídia, recuperação de registros, destruição e revisão.	Empregados responsáveis pela criação e gestão de registros
Política de Proteção de Dados	Legislação, definições e requisitos de proteção de dados aplicáveis.	Colaboradors responsáveis por projetar e gerenciar sistemas usando dados pessoais

** Tabela 1*

9. POLÍTICA DA MESA/TELA LIMPA.

A política de mesa limpa e tela limpa se refere a práticas relacionadas a assegurar que informações (ISSO 27.001), tanto em formato digital quanto físico, não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia.

Uma vez que informações em uma área de trabalho estão em um de seus lugares mais vulneráveis, a adoção de uma política de mesa limpa e tela limpa é uma das principais

estratégias a se utilizar na tentativa de reduzir os riscos de brechas de segurança. Sendo métodos da mesa/tela limpa.

Áreas com trancas: gavetas com trancas, armários de pastas, cofres e salas de arquivo estão disponíveis para armazenar mídias de informação (ex: documentos em papel, pendrives, cartões de memória, etc.) ou dispositivos facilmente transportáveis (ex: celulares, tablets e notebooks) quando não em uso, ou quando não houver ninguém tomando conta deles. Além da proteção contra acesso não autorizado, esta medida também pode proteger a informação e ativos contra desastres tais como incêndios, descarga elétrica, entre outros.

Informações sensíveis ou críticas para o negócio da organização devem ser trancadas em local separado e seguro.

Proteção de dispositivos e sistemas de informação: computadores e dispositivos similares devem estar posicionados de tal forma a evitar que transeuntes tenham a chance de olhar as telas, e configurados para usar protetores de tela ativados por tempo e protegidos por senha, para minimizar as chances de que alguém tire vantagem de equipamentos desacompanhados. Adicionalmente, sistemas de informação devem ter sessões encerradas quando não em uso. Ao final do dia os dispositivos devem ser desligados, especialmente aqueles conectados em rede (quanto menos tempo o dispositivo permanecer ligado, menos tempo haverá para alguém tentar acessá-lo).

Restrições ao uso de tecnologias de cópia e impressão: o uso de impressoras, fotocopiadoras, scanners e câmeras, devem ser controlado, pela redução de sua quantidade ou pelo uso de funções de código que permitam que somente pessoas autorizadas tenham acesso ao material enviado a elas. E, qualquer informação enviada a impressoras deve ser recolhida tão rapidamente quanto possível.

Adoção de uma cultura sem papel: documentos não devem ser impressos desnecessariamente, e lembretes não devem ser deixados em monitores ou sob teclados. Pequenos pedaços de informação pode ser o suficiente para pessoa mal-

intencionadas descobrirem aspectos de pessoais, ou dos processos da organização, que possa ajudá-los a comprometer informações.

Descarte de informações em salas de reunião: todas as informações em quadros brancos devem ser apagadas e todos os pedaços de papel usados durante a reunião devem estar sujeitos a um descarte apropriado (ex: pelo uso de picotadora).

Ainda, com base na Política de Mesa/Tela limpa, deve-se:

A. Anotações, recados e lembretes não devem ser deixados amostra sobre a mesa ou colados em paredes, divisórias ou monitor do computador;

B. Não anotar informações sensíveis em quadros brancos;

C. Não guardar pastas com documentos pessoais/sensíveis em prateleira de fácil acesso;

D. Destruir os documentos impressos antes de jogá-los fora. Sempre que possível utilizar máquinas desfragmentadoras;

E. Não imprimir documentos apenas para lê-los. Leia-os na tela do computador, se possível;

F. Fotocopiadoras devem ser protegidas contra uso não autorizado;

G. Devolver, o quanto antes possível, todos os documentos obtidos por empréstimos de outros departamentos, quando eles não são mais necessários;

H. Computadores pessoais e terminais de computador e impressoras não devem ser deixados "logados", caso o usuário responsável não esteja presente;

I. Guardar agendas e cadernos de anotações numa gaveta trancada;

J. Manter os pertences pessoais em gavetas ou armários trancados;

K. Nunca deixar crachá de identificação ou chaves em qualquer lugar; mantenha-as junto a você;

L. Notificar o pessoal da segurança imediatamente se seu crachá ou chaves sumirem;

M. Nunca escrever senhas em lembretes e nem tente esconde-las no local de trabalho;

N. Não deixe mídias, como CDs ou disquetes nos drives;

O. Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários, e desligar computador;

P. Manter as gavetas e armários fechados e trancados e não deixar as chaves na fechadura.

Q. Não colocar copos de água, suco, refrigerante ou café sobre a mesa;

R. Sempre limpar sua área de trabalho antes de ir para casa, garantindo adequada organização dos itens/objetos manipulados;

S. Trancar o local de trabalho ao deixá-la, não deixar o local de trabalho aberto sem que haja um colaborador que trabalhe no local presente.

10. APLICAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As declarações de políticas feitas neste documento e no conjunto de políticas de suporte listadas na Tabela 1 foram revisadas e aprovadas pela alta direção da ABC SISTEMA DE TRANSPORTE SPE S.A, e devem ser cumpridas. A falha de um colaborador em cumprir essas políticas pode resultar na tomada de medidas disciplinares de acordo com o processo interno da empresa.

Perguntas relacionadas a qualquer política da ABC SISTEMA DE TRANSPORTE SPE S.A , devem ser abordadas, em primeira instância, ao supervisor imediato do colaborador.