POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

OBJETIVO

Avaliar os elementos de segurança que compõem o Sistema de Gestão de Risco a fim de determinar as medidas protetivas. E estabelecer diretrizes e critérios que garantam a Segurança da Informação da Sigma Transportes e Logística Ltda, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e prevenção de responsabilidades. Deve ser adotada, cumprida e aplicada em todas as áreas da Sigma Transportes e Logística Ltda.

REFERÊNCIA NORMATIVA

LGPD Lei 13.709 de 14 de agosto de 2018.

APLICAÇÃO

Abrange toda e qualquer área diretamente envolvida no Sistema de Gestão de Risco, em especial a área de TI que providenciará as medidas necessárias.

ÁREAS ENVOLVIDAS

- Equipe de auditores internos;
- Equipe da tecnologia da informação;
- Gerência geral.

DEFINIÇÕES

Equipe de auditores internos

O desenvolvimento e postagem de arquivos serão executados, somente, por pessoas que tenham cadastro no sistema de Gestão de Risco e tenham responsabilidade direta nas evidências postadas.

Equipe da Tecnologia da Informação

A Equipe interna responsável pela Tecnologia da Informação deverá observar e cuidar do desenvolvimento, aprimoramento e segurança da informação da Sigma Transportes e Logística Ltda.

CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações são classificadas e identificadas por rótulos, considerando os seguintes níveis: pública, interna, confidencial e confidencial restrita.

- **Pública**

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.

- **Interna**

São informações disponíveis aos colaboradores da Sigma Transportes e Logística Ltda para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

- **Confidencial**

São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros.

- **Confidencial Restrita**

São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários dela, em geral, associadas ao interesse estratégico da empresa e restritas ao superintende, gerentes e colaboradores cujas funções requeiram conhecê-las.

RESPONSABILIDADES

Colaboradores

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação;
- Buscar o Setor de Gestão de Informação e Informática para esclarecimentos de dúvidas referentes à Política de Segurança da Informação;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pela Sigma Transportes e Logística Ltda;
- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Sigma Transportes e Logística Ltda;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Comunicar prontamente à chefia imediata qualquer violação a esta política, suas normas e procedimentos.

Gestores de RH - Recursos Humanos e/ou Processos

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da Política de Segurança da Informação do Sigma Transportes e Logística Ltda;
- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;
- Elaborar, com o apoio do Setor de Gestão de Processos e Tecnologia da Informação, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo os atualizados;

- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de colaboradores para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;
- Tomar as decisões administrativas referentes aos descumprimentos da Política de Segurança da Informação do Sigma Transportes e Logística Ltda.

Setor de Gestão de Processos e Tecnologia da Informação

- Definir as regras para instalação de software e hardware na Sigma Transportes e Logística Ltda;
- Homologar os equipamentos pessoais (smartphones e notebooks) para uso na rede da Sigma Transportes e Logística Ltda;
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;
- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades etc.;
- Promover, palestras de conscientização dos colaboradores em relação à importância da segurança da informação da Sigma Transportes e Logística Ltda;
- Analisar criticamente incidentes de segurança em conjunto com a gerência geral e gestores;
- Buscar alinhamento com as diretrizes da organização.

UTILIZAÇÃO DA REDE COMPARTILHADA E SISTEMAS INFORMATIVOS

A fim de monitorar, controlar e evitar os riscos de acessos ou o ingresso à rede compartilhada e sistemas informatizados da Sigma Transportes e Logística Ltda foram instauradas algumas regras, listadas a seguir:

- Todos os sistemas informativos da empresa exigirão autenticação por usuário e senha individual por colaborador assim como as pastas de redes compartilhadas será exigido a mesma autenticação, evitando acessos externos ou a colaboradores não autorizados;
- A concessão de acesso à rede sem fio para acesso apenas à Internet se dará através de solicitação junto ao Setor de Gestão de Processos e Tecnologia da Informação, devidamente autorizada pela Gerência Geral.
- O setor de RH ficará responsável por notificar formalmente ao Setor de Gestão de Processos e Tecnologia da Informação sobre desligamentos de colaboradores, para que os acessos deles sejam revogados;
- A Sigma Transportes e Logística Ltda reserva-se o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;
- Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade da Sigma Transportes e Logística Ltda, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação.
- Apenas a área de Comunicação Corporativa está autorizada a falar em nome da Sigma Transportes e Logística Ltda para meios de comunicação e/ou entidades externas poderão manifestar-se, seja por e-mail, entrevista on-line, documento físico, ligação telefônica etc.;
- É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a internet com via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;
- Os colaboradores com acesso à Internet só poderão fazer o download programas necessários às suas atividades da Sigma Transportes e Logística Ltda e deverão providenciar a licença e o registro necessário desses programas, desde que autorizados pelo Setor de Gestão de Processos e Tecnologia da Informação;

- O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo Setor de Gestão de Processos e Tecnologia da Informação;
- Os colaboradores não poderão em hipótese alguma utilizar os recursos da Sigma Transportes e Logística Ltda para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;
- Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.
- Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;
- Os colaboradores não poderão usar os recursos da Sigma Transportes e Logística Ltda para deliberada ou inadvertidamente propagar qualquer tipo vírus, malware, ransomware, spam, ou programas de controle remoto de outros computadores;
- Não serão permitidos os acessos a softwares peer-to-peer (Kazaa, BitTorrent, µtorrent e afins);
- Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de bypass de firewall;
- Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando o Setor de Gestão de Processos e Tecnologia da Informação deverá estar devidamente ciente e concedido autorização para tal;
- Os arquivos inerentes à Sigma Transportes e Logística Ltda, obrigatoriamente, deverão ser armazenados na plataforma OneDrive na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais;
- Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;

POLÍTICA DE SENHAS

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

- A senha para acesso ao sistema corporativo é liberada conforme as atribuições do colaborador e baseada em grupos de usuários;
- A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesmo ser imediatamente alterada no caso de suspeita de sua divulgação;
- A senha inicial só será fornecida ao próprio colaborador, pessoalmente. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador ou por intermédio do gestor imediato levando em consideração que o primeiro acesso deverá ser feito pelo colaborador para alteração das credenciais;
- A troca da senha deve ser realizada em até 90 dias, após este período, o usuário não conseguirá mais acessar o sistema sem fazer a mudança na senha;
- É proibido o compartilhamento de login para funções de administração de sistemas;
- As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor etc.);
- Os colaboradores serão instruídos a utilizar a senha com os seguintes critérios para maior segurança:
    - Tamanho mínimo de oito caracteres;
    - Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;
    - Não ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge etc.).

O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:

- Desligamento do colaborador;
- Mudança de função do colaborador;
- Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.
- Para os cancelamentos ou atualizações acima mencionadas, o RH ficará responsável por informar prontamente o Setor de Gestão de Processos e Tecnologia da Informação acerca dos desligamentos e mudança de função dos colaboradores.

E-MAIL

O e-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso:

- O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;
- Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;
- É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções;
- É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;
- É proibido enviar qualquer mensagem por meios eletrônicos que torne a Sigma Transportes e Logística Ltda vulnerável a ações civis ou criminais;
- É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- Produzir, transmitir ou divulgar mensagem que:
- Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;
- Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, cpl,.reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:

- Não contrariar as normas aqui estabelecidas;
- Não interferir, negativamente, nas atividades profissionais individuais ou de outros colaboradores;
- Não interferir, negativamente, na Sigma Transportes e Logística Ltda e na sua imagem.

USO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

- É de responsabilidade do colaborador do equipamento zelar por ele, mantendo-o em boas condições;
- Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;
- É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser realizado pelo responsável pelo setor de Tecnologia da Informação e Comunicação da Sigma;
- As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas;
- É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pelo responsável pelo setor de Tecnologia da Informação e Comunicação da Sigma;

- É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe do Setor de Gestão de Processos e Tecnologia da Informação;
- As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de ausência do colaborador;
- Os documentos e arquivos relativos à atividade desempenhada pelo colaborador sempre devem ser armazenados na plataforma OneDrive, o qual possui rotinas de backup e controle de acesso adequado;
- Documentos críticos e/ou confidenciais devem ser armazenados na plataforma OneDrive, nunca no disco local da máquina, somente quando ambos estiverem sincronizados;

É proibido o uso de estações de trabalho para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- O Setor de Gestão de Processos e Tecnologia da Informação não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da Sigma Transportes e Logística Ltda;
- As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do colaborador.

USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O objetivo da Sigma Transportes e Logística Ltda é maximizar a agilidade e eficiência da realização das tarefas dos colaboradores, contando com todos os recursos de equipamentos disponíveis, sempre considerando os requisitos de segurança da informação, por isso estabelece algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis.

Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade da Sigma Transportes e Logística Ltda ou particular com

prévia aprovação e permissão pelo Setor de Gestão de Processos e Tecnologia da Informação, como: notebooks, smartphones e pendrive.

Todas as regras de Uso das Estações de Trabalho se aplicam aos equipamentos particulares e dispositivos móveis, adicionalmente a:

- Fica autorizado o uso de notebooks e dispositivos móveis para acesso à rede interna da Sigma Transportes e Logística Ltda mediante autorização da coordenação do setor via e-mail e prévio cadastro e liberação do Setor de Gestão de Processos e Tecnologia da Informação;
- O Setor de Gestão de Processos e Tecnologia da Informação deverá verificar as configurações de rede, do aplicativo de antivírus e demais aplicativos instalados para que o acesso à rede interna seja concedido. Aplicativos peer-to-peer, farejadores de tráfego, softwares que possam gerar carga excessiva na rede, que não estejam de acordo com a legislação vigente ou que possam trazer prejuízos à infraestrutura ou à imagem da Sigma Transportes e Logística Ltda não serão permitidos. Caso o equipamento não obedeça aos requisitos mínimos de segurança, o acesso não será concedido;
- O Setor de Gestão de Processos e Tecnologia da Informação tem o direito de, periodicamente, auditar os equipamentos utilizados na Sigma Transportes e Logística Ltda, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo usados na Sigma Transportes e Logística Ltda;
- É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook, salvo exceções de aplicativos específicos autorizados pelo Setor de Gestão de Processos e Tecnologia da Informação;
- É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook;
- Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;
- É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam a Sigma Transportes e Logística Ltda não podem ser armazenados no disco rígido do notebook ou em dispositivos de armazenamento móvel (HD externos e pendrive), sem a autorização da área responsável pelos dados. Estes arquivos devem sempre ser armazenados na plataforma OneDrive;

- Mesmo nos computadores portáteis fornecidos pela Sigma Transportes e Logística Ltda, é proibido o armazenamento de informações confidenciais e confidenciais restritas no disco rígido do equipamento;

USO DE IMPRESSORAS

O uso de impressoras na Sigma Transportes e Logística Ltda deve seguir algumas regras:

- É proibida a impressão e xerox de documentos de cunho pessoal e/ou ilegal;
- A configuração e manutenção das impressoras só podem ser realizadas pela equipe técnica contrata pelo Setor de Gestão de Processos e Tecnologia da Informação;
- O gestor de cada setor / unidade será o responsável pela impressora localizada na sala, inclusive para responder a questionamentos como impressões e xerox excessivas;
- As impressoras devem estar ligadas na energia através dos seus transformadores;

BACKUP

Visando preservar a integridade das informações e funcionamento dos sistemas informatizados a adotado os seguintes itens referentes a backups.

- Todo sistema ou informação relevante para a operação dos negócios da Sigma Transportes e Logística Ltda deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição;
- As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e controlar seu fluxo, em eventuais percas, exclusão e afins, possuímos uma política de backup pré-estabelecida de controle e alteração estrita somente ao Setor de Gestão de Processos e Tecnologia da informação onde mantém os dados em contenção por 6 meses (180 dias) salvo arquivos onde os gestores solicitam a exclusão para otimizar armazenamentos;
- Todos os backups devem ser realizados diariamente ou semanal, dependendo de seu nível de criticidade e importância, preferencialmente, executados diariamente fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;

- Estes devem ser armazenados preferencialmente em Cloud, por mais segurança e controles de contingências obrigatórios e pré-estabelecido que estes ambientes possuem, como contingência os backups armazenados em mídias físicas devem ser acondicionados em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do Datacenter;
- Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;
- O Setor de Gestão de Processos e Tecnologia da Informação deve preparar semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;
- Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade.

SEGURANÇA DO AMBIENTE DE TI

Estrutura Física do Data Center

As máquinas (servidores) que armazenam sistemas da Sigma Transportes e Logística Ltda estão em área protegida – Data Centers;

- Todos os sistemas ou equipamentos classificados como críticos devem ser mantidos em áreas seguras do Data Center;
- A entrada aos Data Centers tem acesso devidamente controlado e monitorado. As permissões de acesso físico às áreas restritas do Data Center devem ser mensalmente revisadas;
- As áreas do Data Center devem ser protegidas com barreiras de segurança ou mecanismos de acesso, de forma a impedir o acesso não autorizado;
- A porta do Data Center deve permanecer fechada, com mecanismo de autenticação individual quando possível;

- O acesso às dependências dos Data Centers com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da Gerência de Risco e Segurança Patrimonial e mediante supervisão;
- O acesso ao Datacenter sem as devidas identificações só poderá ocorrer em emergências, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando;
- Caso haja necessidade do acesso não emergencial, o requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter;
- O Datacenter deverá ser mantido limpo e organizado;
- Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável;
- A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com a autorização da Gerência de Risco e Segurança Patrimonial via e-mail e a mesma deve ser acompanhada pelo Gestor de Segurança da Informação ou Gestor de Risco e Segurança Patrimonial.

Estrutura Lógica do Data Center

Na política de segurança da Informação estabelecida da Sigma Transportes e Logística Ltda, define-se que o Gestor de Segurança da Informação deve ser o único a ter permissão para ler/editar as informações, obedecendo as atribuições de sua área de atuação.

O objetivo da segurança lógica no Data Center é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados;

Somente o Gestor de Segurança da Informação e T.I da Sigma, podem ter acesso aos dados armazenados;

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS

Objetivo

A missão da Equipe de Tratamento à Incidentes em Redes Computacionais é zelar pela segurança das informações e comunicações da Sigma Transportes e Logística Ltda, prevenindo

e tratando incidentes de rede, em cumprimento à Política de Segurança da Informação da Sigma Transportes e Logística Ltda.

A Equipe de Tratamento à Incidentes em Redes Computacionais, será formada pelo Gestor de Segurança da Informação.

A atividade principal da Equipe de Tratamento à Incidentes em Redes Computacionais é o tratamento de incidentes de segurança em rede, que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de vulnerabilidades.

Diretrizes

Modelo de Implementação

O modelo de implementação a ser utilizado, inicialmente, pela Equipe de Tratamento à Incidentes em Redes Computacionais será o modelo centralizado.

O Gestor de Segurança da Informação será responsável por criar as estratégias, gerenciar as atividades e executar as tarefas, além de ser o responsável;

A atuação da Equipe de Tratamento à Incidentes em Redes Computacionais se dará por ações reativas e proativas;

As ações reativas incluem recebimento de notificações de incidentes, orientação no reparo a danos, e análise de sistemas comprometidos buscando causas, danos e responsáveis;

Estrutura Organizacional

O Gestor de Segurança da Informação será responsável por coordenar as atividades de tratamento e resposta a incidentes.

A execução das atividades de tratamento e resposta a incidentes poderá ser apoiada por colaboradores e prestadores de serviço, desde que supervisionadas pelo Gestor de Segurança da Informação.

A Equipe de Tratamento à Incidentes em Redes Computacionais terá como competências:

- Coordenar, executar e acompanhar as atividades de tratamento e resposta a incidentes na rede corporativa da Sigma Transportes e Logística Ltda;
- Coordenar, executar e acompanhar a análise dos sistemas comprometidos buscando, causas, danos e responsáveis;

- Coordenar, executar e acompanhar a avaliação, auditoria e testes das condições de segurança da rede corporativa da Sigma Transportes e Logística Ltda;
- Coordenar, executar e acompanhar a análise dos ativos de informação e estruturas constitutivas dos ambientes de tecnologia da informação, presentes no Setor de Gestão de Processos e Tecnologia da Informação;
- Desenvolver um Plano de Conscientização em segurança da informação e comunicações a fim de que todos os colaboradores no Setor de Gestão de Processos e Tecnologia da Informação tenham ciência do assunto;
- Manter em condições adequadas de segurança o acervo de informações relativas aos incidentes da rede corporativa da Sigma Transportes e Logística Ltda;
- Participar da definição e acompanhar os indicadores de incidentes na rede corporativa da Sigma Transportes e Logística Ltda;
- Prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicações;
- Participar na proposição de recursos necessários às ações de segurança da informação e comunicações;

Tratamento de Incidentes

Serviços Reativos:

- Informação sobre computacionais;
- Tratamento de Artefatos Maliciosos;
- Tratamento de Vulnerabilidades.

Serviços Proativo:

Detecção de Intrusão:

- Todo e qualquer colaborador deve estar ciente que o tratamento de incidentes visa minimizar os impactos de um incidente nos processos em curso na Sigma Transportes e Logística Ltda, sendo assim voltado à redução e contenção dos efeitos causados por eventos técnicos indesejáveis e seu monitoramento;
- Falhas, anomalias, ameaças ou vulnerabilidades observadas devem ser notificadas o mais rápido possível;
- Cabe a Equipe de Tratamento à Incidentes em Redes Computacionais obter informações quantitativas acerca dos incidentes ocorridos que descrevam: sua natureza, as causas, a data de ocorrência, a sua frequência e os custos resultantes.

Tais informações servem como indicadores da eficácia das políticas e da relação custo-benefício dos controles de segurança;

- Após o levantamento dos dados do incidente a Equipe de Tratamento à Incidentes em Redes Computacionais deverá tratá-lo e documentá-lo, visando manter um histórico dos incidentes e ainda uma cultura acerca deles;
- Os serviços proativos, reativos e de gerenciamento de qualidade prestados pela Equipe de Tratamento à Incidentes em Redes Computacionais serão detalhados e revisados pelo Gestor de Segurança da Informação.
- A Equipe de Tratamento à Incidentes em Redes Computacionais terá autonomia compartilhada, trabalhando em conjunto com a Gerência Geral e as outras unidades no processo de tomada de decisão sobre quais medidas devem ser adotadas quanto aos riscos e incidentes identificados.
- Em caso de conflito ou divergência no processo de tomada de decisão, a questão será encaminhada a Gerência Geral que poderá arbitrar perante o conflito.

ACESSO AOS SISTEMAS INFORMATIZADOS DE FORMA EXTERNA.

O acesso aos sistemas informativos internos da Sigma Transportes e Logística é expressamente proibido sem a devida autorização. O único meio permitido para acessar tais sistemas é através da Rede Privada Virtual (VPN), previamente configurada e fornecida pelo Departamento de TI. Qualquer tentativa de acesso por outros meios será considerada uma violação das políticas internas de segurança da informação, descritas a seguir.

DAS DISPOSIÇÕES INICIAIS

- Oferecer aos usuários meios de acesso remoto à rede interna da filia Alemoa, bem como o uso dos sistemas e arquivos disponibilizados.
- O uso da VPN possibilita o tráfego seguro e criptografado dos dados na rede de internet, entre o computador do servidor e as filiais, ampliando a segurança da informação.
- O uso da expressão “privada” tem conotação técnica, e em nenhuma hipótese significa que, no caso da VPN da Sigma Transportes de Logística LTDA, o usuário poderá fazer uso dela como se lhe pertencesse, portanto, não cabendo o uso de dita rede para finalidades não administrativas da empresa, nos termos e condições adiante apresentados.

DOS NÍVEIS DE SERVIÇO

- O Departamento de TI fica responsável por receber, registrar e solucionar ou encaminhar no GLPI (ti@sigmatransportes.com.br), todas as solicitações de atendimento.
- Serão empregados todos os recursos disponíveis no sentido de manter o serviço disponível 24 horas por dia, 7 dias por semana, ressalvadas as hipóteses de interrupção por força maior, caso fortuito, manutenções programadas, emergenciais (intempestivas) e similares.
- O Departamento de TI reserva o direito de reavaliar o serviço a qualquer momento em relação à sua continuidade, seus componentes e forma de distribuição, bem como outros detalhes que possam afetar a continuidade das operações e a disponibilidade de recursos.

DAS RESPONSABILIDADES DO DEPARTAMENTO DE TI

Cabe ao Departamento de TI:

- Manter disponível a infraestrutura fornecida ao usuário, conforme nível de serviço acordado.
- Comunicar ao usuário caso sejam identificadas falhas, vulnerabilidades ou incidentes que possam afetar a disponibilidade da solução ou afetar o serviço como um todo.

Não compreende responsabilidade do Departamento de TI:

- Prestar suporte aos usuários no que extrapole o escopo do uso do serviço, como questões relacionadas a sistema operacional, softwares instalados nas máquinas pessoais e virtuais, entre outros.
- Aplicar qualquer tipo de correção e melhoria na solução.
- Realizar a criação de acesso a VPN para os usuários que necessitarem de acesso externo somente se possuir autorização prévia pelo Coordenador de TI, setor de RH / DP e /ou Diretoria.

DAS RESPONSABILIDADES DOS USUÁRIO

- O usuário do serviço, deve conhecer, compreender e concordar expressamente através de declaração com o presente termo de uso, e cumprir com todas as suas condições, inclusive com regulamentos e leis que se apliquem ao uso do serviço.

São responsabilidades do usuário do serviço de VPN:

- Efetuar e manter a correta configuração do sistema operacional, dos softwares e demais componentes que componham a solução em uso.
- Manter atualizados os softwares e todos os componentes utilizados na solução.
  Tratar qualquer incidente de segurança que venha ser identificado com urgência e prioridade adequados, evitando toda e qualquer forma de postergação.

- Tomar as medidas necessárias em decorrência de manutenções programadas comunicadas pelo Departamento de TI.
- Não ceder, informar, emprestar, passar e/ ou o que o valha, a chave de acesso da VPN para terceiros em hipótese alguma;
- Em caso de extravio, furto, roubo ou reparo do equipamento o usuário deverá comunicar imediatamente o Departamento de TI através do email: ti@sigmatransportes.com.br relatando o caso e pedindo o cancelamento da chave de acesso da VPN;
- Usar o software e as informações obtidas única e exclusivamente para a finalidade determinada;
- Permanecer junto ao equipamento utilizado até que ele seja desativado ou seja bloqueada a sessão;
  Assegurar que nenhum relatório, tela ou listagem solicitado seja disponível sem sua presença e/ ou autorização;

- O usuário do serviço, ao concordar com o presente Termo de Uso, se compromete a acompanhar todas as atualizações deste Termo, a serem publicadas no e-mail.

Havendo discordância do usuário com o Termo de Uso, o mesmo deverá comunicar imediatamente o Departamento de TI e, ato contínuo, cessar o uso do serviço

DAS RESPONSABILIDADES DO SETOR DE RH / DP

Cabe o RH / DP:

- Informar ao Departamento de TI, por meio de e-mail para ti@sigmatransportes.com.br, sobre desligamentos de colaboradores, solicitando o bloqueio imediato dos acessos aos sistemas e à VPN.
- Solicitar ao Departamento de TI, por meio de e-mail, a criação e ativação de acessos à VPN para coordenadores e líderes que necessitem dessa funcionalidade, de acordo com os critérios estabelecidos pela empresa.
- Garantir que as informações referentes a admissões, desligamentos e mudanças de função sejam atualizadas e comunicadas ao TI de forma precisa e no tempo adequado.

DO USO ACEITÁVEL DO SERVIÇO

- O serviço da VPN deve ser utilizado apenas para executar conteúdo que seja de propriedade legal do signatário deste termo, ou que tenha sido legalmente licenciado para uso por essa pessoa.

1º. O signatário é responsável por avaliar as licenças de uso de todos os softwares e outros componentes protegidos por direitos autorais, a fim de garantir conformidade com os presentes termos.

2º. Sem prejuízo de outras hipóteses previstas em leis e/ ou normas, inclui-se neste caso a proteção aos direitos autorais, de imagem e outros correlatos, relacionados com produções audiovisuais, artísticas, científicas e congêneres.

3º. O Departamento de TI pode monitorar as interfaces de rede para certificar a conformidade com este termo de serviço, sendo vedado ao usuário bloquear ou interferir com o monitoramento, sem prejuízo do uso de tecnologias de criptografia e firewalls para ajudar a proteger seu conteúdo.

4º. Ao fazer uso da VPN o usuário concorda e autoriza, expressamente, o monitoramento das suas interfaces de rede.

- O signatário deverá cooperar ativamente para identificar a origem de qualquer problema com o serviço que o departamento de TI acreditar estar relacionado com o uso da infraestrutura fornecida a ele, sendo a omissão e/ ou a resistência passiva considerada(s) violação(ões) do presente Termo.
- O departamento de TI, ao encontrar ou ser informado sobre indícios de que a utilização do serviço por determinado usuário que viole os termos de uso estipulados neste documento ou outros regulamentos e leis que se apliquem, emitirá notificação ao usuário.

1º. A não correção de eventuais desvios, no prazo informado pelo departamento de TI, resultará na imediata suspensão do serviço, sem qualquer garantia ao usuário; a ausência de garantia inclui dados, backups e outros similares.

2º. Ao fazer uso da VPN, o usuário declara ciência que é seu dever providenciar e manter, às suas expensas e responsabilidade, backups dos seus dados, sendo que tais backups deverão ser externos à VPN, e não dependentes da mesma.

DO CONTROLE DE ACESSO

- O acesso ao serviço será concedido exclusivamente ao usuário signatário da declaração de concordância com o presente Termo de Uso.

1º. Cabe ao usuário avaliar e decidir sobre a transferência do acesso a terceiros, sob sua total responsabilidade, devendo adotar as medidas necessárias para o adequado gerenciamento e segurança.

2º. A concessão de acesso a terceiros não compreende a transferência da responsabilidade do usuário perante o serviço e a Sigma Transportes e Logística Ltda, permanecendo este o único responsável pelo cumprimento do presente Termo de Uso.

3º. O acesso aos recursos utilizados pelo usuário poderá ser concedido às autoridades se exigido, em razão de interesse público, por ordem judicial ou por detecção de indícios de irregularidade(s), crime(s) e/ ou turbação à ordem pública.

4º. Ao fazer uso da VPN o usuário concorda e autoriza, expressamente, o acesso aos seus recursos, nos termos do parágrafo acima.

- As instruções e credenciais de acesso ao serviço serão enviados diretamente ao e-mail do usuário após a entrega da declaração de concordância O Departamento de TI.

DAS DISPOSIÇÕES FINAIS

- Caso a utilização do serviço pelo usuário de alguma forma prejudique terceiros ao violar as leis e regulamentos vigentes, o usuário se compromete a responder diretamente a estes.

Parágrafo único. Sem prejuízo de outras hipóteses previstas em leis e/ ou normas, inclui-se neste caso a proteção aos direitos autorais, de imagem e outros correlatos, relacionados com produções audiovisuais, artísticas, científicas e congêneres.

- Os termos de uso apresentados neste documento serão atualizados quando houver necessidade e disponibilizados
- As providências administrativas eventualmente adotadas pelo Departamento de TI não excluem a instauração de Processo(s)
  Administrativo(s), além de notificação às autoridades cabíveis e ações judiciais.
- Os Caso omissos serão tratados pelo Departamento de TI.

SEGURANÇA DA INFORMAÇÃO

Objetivo:

Garantir a proteção dos sistemas de computadores da organização contra ameaças internas e externas, incluindo programas maliciosos (malware) e ataques baseados em engenharia social, por meio de medidas preventivas, uso de tecnologia adequada e educação contínua dos colaboradores.

Diretrizes:

1. **Proteção contra malware e intrusões:**
   - Soluções de software e hardware voltadas para a proteção contra programas maliciosos (malware) e tentativas de intrusão interna ou externa.
   - Firewalls, sistemas de detecção e prevenção de intrusão (IDS/IPS) e ferramentas de monitoramento contínuo.
   - Varreduras regulares nos sistemas para identificar e mitigar vulnerabilidades.

2. **Atualização de software de segurança:**
    - Garantir que todos os softwares de segurança utilizados, como antivírus, anti-malware e firewalls, estejam atualizados com as versões mais recentes, de forma a proteger contra novas ameaças cibernéticas.
    - Configurar atualizações automáticas sempre que possível e realizar verificações periódicas para confirmar a conformidade.
3. **Prevenção de ataques por engenharia social:**
    - Políticas e procedimentos claros para identificar e prevenir ataques baseados em engenharia social, como phishing, vishing e outras técnicas de manipulação psicológica.
    - Treinamentos regulares para os colaboradores sobre as práticas seguras de uso de sistemas e como reconhecer e reportar tentativas de engano.
    - Restringir o acesso a informações sensíveis apenas aos colaboradores autorizados, minimizando os riscos associados à exposição indevida de dados.

VIOLAÇÃO DA POLÍTICA E PENALIDADES

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança da Informação, o colaborador poderá sofrer as seguintes penalidades:

Advertência verbal

O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação da Sigma Transportes e Logística Ltda e será recomendado à leitura desta Norma;

A advertência verbal será anotada no prontuário do colaborador.

Advertência formal

A notificação será enviada ao gestor do colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida.

ASSINADO DIGITALMENTE
FERNANDA GOMES FERREIRA
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

Aprovador: Fernanda Ferreira

Diretora Executiva de Operações