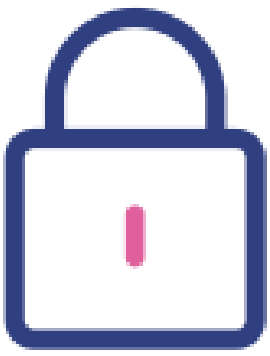
Política de Segurança da Informação

Versão 1.0



Conteúdo

01 Introdução

Esse documento de **Política de Segurança da Informação**, também referida como PSI, reforça o compromisso da Lecom com todos os aspectos relacionados à Segurança da Informação, nossa e de nossos clientes e parceiros.

As políticas aqui listadas se dirigem a diferentes grupos e reúnem as políticas e diretrizes gerais de segurança da informação, as normativas de acesso e os procedimentos associados à segurança dos sistemas de informação da Lecom.

1.1 Visão Geral

A Política de Segurança da Informação é o documento que orienta e estabelece as diretrizes corporativas da Lecom para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da nossa organização.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

A PSI deve ser de conhecimento e aplicação obrigatórios por todo o pessoal, próprio ou terceiros subcontratados, assim como por empregados de empresas provedoras e colaboradoras e todo usuário com direitos de acesso a qualquer sistema de informação da Lecom.

As normas se referem a todos os sistemas de informação, automáticos ou manuais, sobre os quais a Lecom tem responsabilidade administrativa, independente da tecnologia empregada. Elas afetam a todo tipo de informação, criada ou utilizada, como suporte do negócio da Lecom, independentemente de seu formato ou meio utilizado (físico ou eletrônico).

1.2 Objetivos

Estabelecer diretrizes que permitam aos colaboradores e clientes da Lecom seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da Lecom quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

1.3 Responsabilidade Geral

A segurança dos ativos de TI da Lecom é responsabilidade de todos, independentemente dos ativos de TI que lhes foram designados, quer façam uso deste ou não. Consequentemente, todos os usuários são parceiros responsáveis pela segurança, devendo desenvolver sua atividade no sentido de alcançar a segurança da informação adequada.

Para tal devem assumir e acatar as normas e procedimentos de segurança estabelecidos, estando obrigados a manter a confidencialidade dos dados utilizados em seu ambiente e devendo comunicar, com a maior brevidade possível, os possíveis incidentes ou problemas de segurança que porventura venham a detectar.

A Lecom é responsável por promover e apoiar o estabelecimento de medidas técnicas, organizacionais e de controle que garantam a integridade, disponibilidade e confidencialidade dos ativos de TI, de modo a evitar sua possível alteração, destruição, perda, roubo, cópia, falsificação e outras ameaças existentes, sejam estas acidentais ou não.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

02 Definições, Acrônimos e Abreviações

- **Segurança da Informação**: Consiste na preservação das características de confidencialidade, integridade e disponibilidade da informação.
- **TI (Tecnologia da Informação)**: Termo aplicável a todas as formas de tecnologia utilizadas para criar, compartilhar e utilizar informações.
- **Vulnerabilidade**: É uma fraqueza inerente de um ativo. Por si só não é prejudicial, é simplesmente uma condição, ou conjunto de condições, que aumentam a probabilidade de que o evento de uma ameaça se materialize.
- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Ativo**: É qualquer elemento ao qual é associado um valor e que, portanto, requer proteção. Os ativos podem ser de TI, documentos físicos, pessoas e ativos intangíveis.
- **Ameaça**: Qualquer evento ou ato potencial que pode ocasionar a revelação, destruição, remoção ou modificação de ativos.
- **SLA**: Service Level Agreement - Acordo de Nível de Serviços
- **Usuário**: Sujeito autorizado para acessar dados ou recursos do sistema de informação da Lecom.
- **Identificação**: Procedimento de reconhecimento da identidade de um usuário.
- **Autenticação**: Procedimento de comprovação da identidade de um usuário.
- **QA**: Quality Assurante
- **LGPD**: Lei Geral de Proteção de Dados

03 Políticas e Diretrizes

3.1 Políticas e diretrizes de segurança da informação

A Lecom, por meio de seus profissionais que atuam voltados para segurança da informação, utiliza meios e ferramentas centrados na proteção preventiva e estática de possíveis acessos indevidos por parte do pessoal próprio ou de terceiros, mas também possui um enfoque orientado a proteger de forma proativa acessos aos ativos de TI.

Para que o plano de segurança entre em vigor é necessário o envolvimento e colaboração de todas as unidades e seus funcionários.

3.2 Escopo e aplicação

As políticas e diretrizes de segurança da informação são de aplicação a todos ativos da Lecom, e dizem respeito a todos os sistemas de informação, automáticos ou manuais, sobre os quais tenha responsabilidade administrativa independentemente da tecnologia utilizada.

Afetam a todo tipo de informação, criada ou utilizada como suporte dos negócios a Lecom, independentemente de seu formato ou mídia.

Constituem uma declaração da postura da direção da Lecom em relação à segurança dos sistemas de informação e estabelecem os objetivos, responsabilidades e comportamentos necessários para gerir os ativos de TI em um ambiente seguro.

3.3 Políticas

A informação que é gerada, processada e armazenada nos sistemas de informação da Lecom é o elemento fundamental para conseguir uma boa gestão e controle sobre esta.

Para o correto desempenho de suas funções é indispensável que possamos gerir, em termos de integridade, disponibilidade e confidencialidade, a informação da qual necessitam para o bom desenvolvimento de suas atividades.

Também, é uma obrigação legal e ética da Lecom, garantir, nos mesmos termos a informação que compete aos seus clientes, entidades colaboradoras e aos órgãos oficiais competentes.

Os diferentes recursos de TI, utilizados para administrar e gerir a informação – basicamente hardware e software – propriedade da Lecom e aqueles alugados ou licenciados pelo mesmo, são também considerados como ativos a serem protegidos.

Consequentemente, é estabelecido como política de segurança que o acesso, a utilização e a guarda dos ativos de TI serão realizados garantindo sempre a integridade, disponibilidade e confidencialidade da informação, respeitando e cumprindo as diretrizes, procedimentos e normativas de acesso estabelecidas.

É de responsabilidade da Lecom promover e manter o estabelecimento das medidas técnicas, organizacionais e de controle necessárias com o objetivo de garantir a integridade, disponibilidade e confidencialidade da informação.

3.4 Diretrizes

As diretrizes de segurança da informação estabelecem um conjunto de conceitos básicos de segurança, considerados como indispensáveis para o desenvolvimento dessa política.

Consta, a seguir, a definição das diretrizes de segurança da informação que suportam a política

de segurança para a proteção dos ativos de TI da Lecom:

3.4.1 Propriedade da Informação

Estabelece-se como norma que todos os ativos de TI, de acordo com as definições estabelecidas neste documento, são propriedade da Lecom, com exceção dos softwares, propriedade de terceiros, que a Lecom tenha licenciado para seu uso, assim como os ativos de TI que sejam alugados.

Fica estabelecido que toda informação que se gera, processa e armazena nos sistemas de TI da Lecom é propriedade da mesma, com exceção das informações cedidas à Lecom e/ou informações de clientes das quais a Lecom se considera guardiã.

Para a definição e implantação das permissões de acesso à informação e o estabelecimento de responsabilidades na concessão de tais permissões aos usuários, será estabelecido um procedimento. Neste procedimento é considerada a intervenção do departamento responsável pela definição de perfis e concessão de acesso à informação.

Os usuários irão acessar as informações mediante perfis definidos em função das necessidades, dos papéis que desempenham e do nível de confidencialidade designado à informação. Os terceiros que acessem qualquer tipo de informação da Lecom, tais como provedores, empresas colaboradoras ou órgãos oficiais, devem ter acesso à informação estritamente necessária segundo o contrato que tenham assinado com a Lecom. Esses terceiros também deverão possuir um contrato de confidencialidade (também conhecido como NDA), assinado com a Lecom.

Os usuários são responsáveis por respeitar os controles implantados e utilizar a informação apenas para os fins autorizados. Esta autorização de acesso deve ser avaliada periodicamente. O fato de obter acesso à determinada informação, não lhes confere o direito de dar acesso a outras pessoas.

Os responsáveis pela informação, também são responsáveis, entre outros, por conhecer e utilizar todas as possibilidades técnicas para realizar a implantação de controles.

3.4.2 Acesso aos ativos de TI

O acesso aos recursos da Lecom deverá ser realizado mediante o uso de um identificador de usuário, pessoal e intransferível e de uma senha associada ao identificador, que deve permanecer em segredo.

Sob esta filosofia fica expressamente proibida a utilização de um identificador de usuário e de sua senha de acesso por outrem. É responsabilidade de cada usuário manter em segredo sua senha, já que qualquer acesso indevido com tal identificador será responsabilidade de seu proprietário.

A equipe de infraestrutura e segurança estabelecerá os procedimentos necessários para fornecer aos usuários a responsabilidade sobre a intransferibilidade e confidencialidade de seus identificadores (códigos de usuário) e senhas de acesso; também estabelecerá os procedimentos de controle para a prevenção e detecção de ações que podem originar um não cumprimento desta norma. Adicionalmente, implantará os mecanismos necessários para assegurar a qualidade das senhas utilizadas e seu armazenamento e transporte de forma segura.

Os usuários devem acessar, exclusivamente, a informação estritamente necessária para o desenvolvimento de sua atividade, independentemente se tem acesso físico a informações não relacionadas à mesma.

Devido à sua confidencialidade, deve-se prestar atenção especial às medidas a implantar para limitar o acesso a toda informação resultante da realização de auditorias ou revisões de segurança.

Consequentemente fica proibido qualquer tipo de acesso por parte de terceiros à informação e

recursos de TI, salvo nos casos em que se determine com o conhecimento e acordo da Lecom. Os usuários devem levar ao conhecimento de seus superiores, mediante os mecanismos necessários, qualquer não cumprimento conhecido desta norma.

Em termos gerais deve-se impossibilitar qualquer acesso que pode implicar em perigo de vazamento de informação. Entre elas temos:

- As redes que, devido às suas características, possibilitem a escuta por parte de terceiros, tais como as redes Wifi.
- As redes criadas desde qualquer dependência da Lecom até outro lugar qualquer (provedores de serviço, empresas colaboradoras, clientes, etc.).
- Acesso remoto aos Sistemas e Ativos de Informação internos, por empregados ou terceiros, desde terminais controlados pela Lecom.

É necessário estabelecer mecanismos tecnológicos para facilitar a monitoração, na medida do possível, tanto dos eventos de segurança ocorridos nos sistemas de informação da Lecom, como das ações realizadas pelos usuários nos mesmos.

Toda conexão externa deve ser certificada antes de seu estabelecimento, mediante a revisão do cumprimento das normas e procedimentos de segurança exigidos. As áreas ou departamentos encarregados de sua manutenção e administração serão os responsáveis por manter o nível de segurança acordado.

A conexão à Internet ou a qualquer outra rede pública, independente do meio utilizado para realizá-la, requer uma menção específica por parte da equipe de infraestrutura e segurança.

A conexão e uso da rede interna devem ser limitados aos usuários autorizados, mediante mecanismos necessários estabelecidos pela Lecom.

3.4.5 Sistemas e equipamentos

Todos os Sistemas de Informação, bem como as mídias armazenadas, devem estar situados em áreas protegidas por mecanismos de controle de acesso físico.

Também, os Sistemas de Informação devem estar adequadamente protegidos de ameaças físicas, ambientais ou de falta de fornecimento de materiais ou serviços, sejam devidos a causas fortuitas ou intencionais, que possam afetar negativamente os ativos da Lecom.

Todos os dispositivos de armazenamento de informação da Lecom devem ser acondicionados e protegidos frente a perdas, destruição, ou falsificação de forma que se cumpra a normativa vigente e as políticas de segurança.

A proteção dos dados de caráter pessoal de clientes, funcionários e empresas colaboradoras deve garantir a honra, a privacidade e o plano exercício de seus direitos.

04 Normas Gerais

4.1 Normas gerais de segurança

Essa seção estabelece as normas gerais de segurança da informação, aplicação comum e cumprimento por todos os usuários que acessam ou utilizam os sistemas, e/ou ativos de TI da Lecom.

As normas gerais de segurança da informação são de obrigatório conhecimento e aplicação por todo o pessoal, seja próprio ou terceiros subcontratados, assim como por empregados de empresas provedoras e colaboradoras, e todo usuário com direito de acesso a qualquer sistema de informação da Lecom.

As normas gerais de segurança da informação afetam a todos os tipos de informação criada ou utilizada como suporte aos negócios da Lecom e sobre os quais tem responsabilidade administrativa, independentemente de seu formato ou mídia.

4.2 Normas para uso dos recursos e ativos de TI

4.2.1 Uso ilícito dos recursos de TI

Fica proibida a utilização dos Sistemas de Informação de propriedade da Lecom com o fim de realizar ações que sejam contra a legislação e normas nacionais e internacionais, com a intenção de prejudicar ou obter benefícios. Estão incluídas entre estas ações:

- Provocar danos intencionalmente na rede ou outros sistemas;
- Prejudicar de forma intencional o tráfego da rede ou o acesso a recursos;

- Tentar ou conseguir acessar recursos conectados à rede os quais, o usuário não está autorizado;
- Exploração de potenciais falhas de segurança dos sistemas;
- Uso de materiais de TI para os quais não se disponha das licenças apropriadas;
- Uso não autorizado da informação protegida por leis de propriedade intelectual.

4.2.2 Uso pessoal dos recursos de TI

Fica vetado o uso, para fins pessoais, tanto de recursos de TI como de informações da Lecom, para finalidades distintas às estritamente profissionais e relacionadas com o desenvolvimento habitual das funções na Lecom que não tenham sido expressamente aprovadas pela direção. Esta proibição é também aplicável ao pessoal de empresas terceiras contratadas.

É vetada às empresas subcontratadas, a prestação de quaisquer serviços a terceiros utilizando ativos de TI da Lecom, sem a autorização expressa e por escrito da direção da Lecom.

4.2.3 Cuidados com a estação de trabalho

As estações de trabalho devem estar sempre protegidas por senha, de forma que seja necessário o fornecimento da mesma para a autenticação. Em conformidade com o que já foi dito antes, esta senha tem caráter confidencial e é pessoal e intransferível.

Se a pessoa sai de seu posto de trabalho, esta deverá bloquear o equipamento para impedir o acesso ao mesmo por terceiros.

Nas estações de trabalho o usuário deve manter habilitada a opção de proteção de tela com senha. O tempo máximo recomendado de ativação por inatividade deve ser estabelecido em 30 (trinta) minutos.

Os usuários devem desligar a estação após encerrar suas atividades.

Qualquer perda ou subtração de equipamentos, componentes ou periféricos deve ser comunicada por telefone, imediatamente, à equipe de infraestrutura e segurança Lecom.

Os usuários não são autorizados a modificar a configuração padrão das estações de trabalho e, em especial, as opções ou parâmetros que podem implicar em riscos pela alteração das medidas de segurança existentes.

Os usuários ficam proibidos de instalar softwares adicionais, não homologados pela Lecom, em suas estações de trabalho.

4.2.4 Informações impressas e cópias físicas

É recomendada a não utilização de material impresso e dispositivos móveis ou removíveis, para os quais se interpõem normas de segurança.

Nos casos em que, excepcionalmente, existem documentos com informações sensíveis, estes devem ser retirados imediatamente das impressoras e copiadoras.

Estes tipos de documentos e meios devem ser arquivados de forma segura.

4.2.5 Monitoramento e auditoria dos ambientes

Os usuários devem conhecer os sistemas aos quais se conectam e sua atividade nos mesmos está sujeita a acompanhamento e monitoramento permanente, relacionados exclusivamente com a segurança dos sistemas de informação e o respeito à dignidade das pessoas.

Para garantir as regras mencionadas nesta PSI, a Lecom poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou direção da empresa;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

4.2.6 Instalação e utilização de softwares

Fica proibida a utilização de software de qualquer tipo que não tenha sido licenciado pela Lecom e homologado para sua utilização, independente de se tratar de software de licença livre ou autorizada para uso pessoal (freeware e shareware).

Os usuários não estão autorizados a copiar ou utilizar softwares licenciados pela Lecom para uso doméstico pessoal ou para sessão a terceiros, sem o conhecimento e autorização prévios da gestão da Lecom.

4.2.7 Incidentes de segurança

Perante a detecção ou suspeita de qualquer situação que possa afetar a segurança da informação da Lecom, qualquer usuário deve levar o fato a conhecimento, de forma imediata, aos seus superiores.

Quando ocorrer a avaria de uma estação de trabalho que armazena informações confidenciais da Lecom, ou para as quais a Lecom tenha responsabilidade, e seu reparo se faça necessário fora das dependências da Lecom, o usuário, ao qual está associada a máquina, deve informar à equipe de infraestrutura e segurança sobre a situação.

Quando ocorrer a subtração de uma estação de trabalho que armazena informações confidenciais, o usuário deve notificar a subtração à equipe de infraestrutura e segurança. O objetivo é manter registrado quaisquer subtrações de informações confidenciais que podem ter ocorrido.

4.2.8 Acesso à terceiros

Antes de outorgar qualquer permissão de acesso à terceiro, deve-se identificar e classificar o tipo de acesso e o risco associado. Desta forma, é possível implementar as medidas de segurança necessárias para minimizar o risco associado a tais acessos. Também é importante assegurar-se de que todo o pessoal externo cumpra com a normativa de segurança da Lecom, empregando as medidas de segurança e confidencialidade.

Todos estes aspectos devem estar refletidos nos acordos de serviço constantes nos contratos estabelecidos com terceiros.

4.2.9 Utilização de correio eletrônico (e-mail)

O e-mail interno ou através da Internet constitui uma ferramenta para uso exclusivo de tarefas relacionadas à Lecom, consequentemente fica proibida a utilização do correio eletrônico da Lecom para uso pessoal ou qualquer outro que não esteja estritamente relacionado com o desempenho das atividades profissionais.

Toda mensagem eletrônica dentro dos sistemas de informação da Lecom será considerada propriedade da Lecom e poderá estar sujeita a revisão, arquivamento ou eliminação.

Assim como o resto dos sistemas de informação da Lecom, o acesso ao e-mail deve realizar-se com um identificador de usuário e senha, pessoais e intransferíveis. Consequentemente fica proibida a utilização coletiva de uma conta de e-mail, salvo os casos em que a atividade profissional justifique.

Não se devem transmitir, através de e-mail externo, informações relacionadas com identificadores de usuário, senhas, informações sobre a configuração da rede da Lecom, endereços ou nomes dos sistemas, nem qualquer outra informação que possa por em evidência a segurança dos sistemas de informação da Lecom.

4.2.10 Proteção contra vírus de computador

Os vírus de computador constituem uma ameaça contínua para os ativos de TI da Lecom em especial aqueles que afetam documentos de Microsoft Word e Excel (vírus de macro) ou os que se proliferam através de e-mail. É responsabilidade de todos os usuários adotarem as precauções apropriadas para prevenir a proliferação destes e outros tipos de vírus.

Todas as estações de trabalho devem dispor de uma cópia licenciada e sempre ativa da última versão disponível do software antivírus corporativo, homologado pela Lecom. Se a estação de um usuário não dispõe desta ferramenta, deve ser feita a solicitação à equipe de infraestrutura e segurança.

Em relação à navegação na Internet, todos os arquivos que sejam baixados de qualquer página web devem ser devidamente analisados, fazendo uso das ferramentas automáticas ou manuais de proteção antivírus homologadas pela Lecom.

Não se deve utilizar nenhuma mídia (CD, DVD, unidades USB, etc.) cuja procedência não seja conhecida.

4.2.11 Backup das informações das estações de trabalho

As informações armazenadas nos servidores da Lecom estão sujeitas a cópias periódicas de segurança, que permitem sua recuperação no caso de imprevistos.

As cópias de segurança serão realizadas utilizando softwares homologados pela Lecom.

4.3 Normas de controle de acesso

Quaisquer acessos aos Sistemas de Informação da Lecom devem ser realizados mediante a utilização de um identificador de usuário, devidamente autorizado, seguindo os padrões de nomenclatura estabelecidos e provido da respectiva senha.

4.3.1 Autenticação: usuário e senha

Para o acesso a qualquer sistema de informação, todo e qualquer usuário da Lecom deve dispor de uma senha secreta de autenticação, associada ao seu identificador de usuário.

O identificador de usuário e a senha de acesso aos sistemas são considerados pessoais e intransferíveis. Adicionalmente, a senha deve ser secreta e não deve ser comunicada a nenhuma outra pessoa.

O caráter secreto das senhas obriga a sua não exibição em nenhuma das seguintes maneiras:

- Não deve ser visualizada na tela enquanto é digitada no teclado para acessar a qualquer sistema de informação da Lecom.
- Não deve ser anotada ou mantida em lugares visíveis ou de fácil acesso como monitores, calendários de mesa, atrás de teclados, gavetas, etc.
- Não devem ser armazenadas em dicionários de senhas, arquivos ou macros que não estejam adequadamente protegidos por senhas.

Qualquer suspeita da quebra de confidencialidade de uma senha deve-se originar uma solicitação de mudança de senha, através dos procedimentos usuais.

A senha deve ser comunicada ao usuário através de meios seguros de comunicação, e nunca devem ser reveladas a outras pessoas, incluindo a gerência ou administradores de sistemas.

As senhas geradas pelo usuário não devem ser distribuídas por nenhum meio (oral, escrito, eletrônico, etc.). As chaves devem ser trocadas mediante qualquer indício de risco das mesmas ou do sistema, devendo-se também ser informado um incidente de segurança.

Por padrão, sempre que for tecnicamente possível, as aplicações e ferramentas utilizadas pela equipe da Lecom devem utilizar a autenticação pelo Microsoft AD (Active Directory), garantindo uma administração centralizada dos usuários.

4.3.1.1 Composição da senha

As senhas de usuário devem ser de fácil memorização por parte do usuário, porém não devem ser triviais para evitar que possam ser adivinhadas por um potencial transgressor. Por este motivo devem cumprir os seguintes requisitos:

- O comprimento da senha deve ser, no mínimo, de 8 caracteres;
- A senha deve conter ao menos um caractere alfabético em maiúscula e um em minúscula;
- A senha deve conter ao menos um caractere especial;
- A senha não deve ser relacionada com dados pessoais (por ex., data de nascimento, residência, nome de um familiar, etc.);
- A senha deve ser alterada a cada 3 meses;
- A senha, quando do primeiro acesso ao sistema, deve ser alterada;
- As chaves não devem ser armazenadas em um sistema de armazenamento automatizado (por ex., macros ou navegadores de internet);
- Não será permitida a reutilização de senhas, ou seja, não se deve utilizar senhas que já tenham sido utilizadas pelo usuário recentemente, para isto um histórico de senhas deve ser mantido.

4.3.1.2 Alterações de senhas

Todos os usuários são obrigados a alterar periodicamente sua senha. O período de expiração de senha será definido em cada sistema, mas como boa prática a Lecom sugere que todos os usuários devem alterar sua senha a cada três meses.

Quando se acessa o sistema pela primeira vez ou quando solicitado, através dos procedimentos estabelecidos, o desbloqueio da senha, o usuário deve alterar tal senha.

4.3.1.3 Bloqueio automático de usuário e senha

O processo de identificação e autenticação de usuários através do identificador de usuário e senha, em quaisquer sistemas da Lecom, deve estar dotado de controles pra o bloqueio automático do usuário e sua inativação temporária para o acesso ao sistema no caso de haver um Número de tentativas de acesso incorretas de usuário ou a senha por 3 vezes consecutivas.

Nestas situações e em qualquer outra originada pelo bloqueio manual de um identificador de usuário, a pessoa deverá solicitar, pelos procedimentos estabelecidos, o desbloqueio de seu identificador de usuário.

4.3.2 Desligamento de colaborador

No caso do desligamento de um colaborador ou de um terceiro que preste serviço nas plataformas e ambientes da Lecom, esse desligamento deve ser comunicado imediatamente, seguindo os procedimentos a seguir:

- Abertura do Processo Desligamento, dentro da Plataforma Lecom. Esse processo garante o aviso automático de todas as áreas e pessoas responsáveis pelas revogações de acesso;
- Envio de e-mail para o líder da equipe de infraestrutura e segurança. Essa medida é uma redundância de segurança, tendo em vista que a medida anterior já fará os avisos necessários. Porém, pela criticidade dessa ação, foi definido o procedimento de segurança;
- A pessoa responsável pela comunicação do desligamento será sempre o chefe imediato daquela pessoa que foi desligada.

4.4 Normas de segurança física

Considera-se área de acesso restrito qualquer instalação ou dependência da Lecom que tenha servidores, roteadores, computadores departamentais de uso compartilhado. Consequentemente é proibido o acesso físico aos usuários que não estejam convenientemente autorizados.

O acesso de visitantes as áreas de acesso restrito devem ser realizadas sempre em companhia de uma pessoa autorizada.

Proíbe-se a realização de qualquer tipo de atividade que possa significar um risco para a disponibilidade dos equipamentos e periféricos localizados nas dependências de acesso restrito. Não é autorizado o consumo de alimentos, bebidas ou tabaco nas dependências de acesso restrito.

Os usuários não devem utilizar as dependências de acesso restrito para o armazenamento de documentação, itens de consumo, caixas, móveis ou qualquer outro objeto que não esteja diretamente relacionado com os dispositivos ali localizados.

05 Gestão de Mudanças

As alterações no código fonte das aplicações ou nos próprios sistemas base podem impactar negativamente os Sistemas de Informação, motivo pelo qual é necessário controlar todas as alterações realizadas em aplicações e sistemas. A Lecom deve definir os mecanismos pertinentes de Gestão de Mudanças para poder controlar os processos de alterações de aplicações e sistemas instalados no ambiente de Produção. Tais mecanismos devem estabelecer que toda documentação relacionada com as aplicações sujeitas a alterações deverá ser atualizada.

Todas as alterações realizadas nas aplicações devem estar adequadamente identificadas, registradas e autorizadas, de forma a assegurar o controle de todas as modificações realizadas no ambiente de Produção.

Antes de implantar as mudanças no ambiente de Produção, é necessário testar tais mudanças nos ambientes de Testes e Desenvolvimento. Toda documentação dos sistemas e aplicações deverão ser atualizadas após a implantação de alterações significativas.

Antes da realização de mudanças nos Sistemas Operacionais, Banco de Dados, e demais Sistemas dos Servidores, é necessário verificar que as aplicações não são impactadas com nenhuma falta de funcionalidade ou mau funcionamento.

06 Incidentes de Segurança

6.1 Gestão de incidentes

É necessário estabelecer mecanismos adequados para o tratamento de incidentes que permitam tomar ações corretivas para solucionar os problemas com um tempo de resposta reduzido.

Todos os usuários e administradores da Lecom devem seguir os mecanismos estabelecidos para a gestão de incidentes, e para isso seguem abaixo os principais pontos que devem ser implantados:

- A Lecom deve desenvolver os mecanismos necessários para que os usuários dos Sistemas de Informação possam reportar os incidentes relacionados a estes.
- Todos os procedimentos devem estar oportunamente definidos e documentados e disponíveis para todo o pessoal da Lecom.
- Todos os incidentes de segurança detectados nos Sistemas de Informação da Lecom devem ser geridos de acordo com os procedimentos estabelecidos.
- É encorajada a análise dos eventos, com o objetivo de reduzir o tempo de resposta ante aos eventos futuros relacionados com incidentes ocorridos no passado.
- No caso da ocorrência de um incidente de segurança grave, deve-se comunicar ao aos superiores e responsáveis o mais rápido possível.

O corpo normativo indica que a segurança dos ativos de informação da Lecom é de responsabilidade de todos os usuários. Consequentemente todos são corresponsáveis pela segurança, devendo contribuir para a adequada segurança da informação.

Um dos aspectos fundamentais no qual é necessária a colaboração de todos os usuários é a comunicação dos incidentes de segurança que porventura sejam identificados.

Este procedimento estabelece o método de comunicação destes incidentes. Seu objetivo é abrir uma via de comunicação que permita gerir os incidentes de uma forma ágil e controlada para

que o impacto na segurança dos sistemas seja o menor possível e a análise das causas destes incidentes reduza o número de incidentes no futuro.

Este procedimento é aplicável sempre que seja detectada uma situação que possa diminuir, de qualquer forma, o esquema de segurança existente sobre os ativos de informação da Lecom, por exemplo:

- Qualquer tipo de erro ou furo na segurança dos sistemas de informação;
- Uso inadequado (intencional ou não) dos sistemas de informação;
- Não cumprimento das normas de segurança;
- Falta de acompanhamento dos procedimentos de segurança;
- Possíveis acessos a informações confidenciais quando não se esteja expressamente autorizado a tal.

6.2 Notificação de incidentes de segurança

Caso qualquer incidente de segurança detectado, se deve enviar imediatamente um e-mail ao coordenado da equipe de infraestrutura e segurança da Lecom, com cópia para seu líder imediato, indicando em seu título “URGENTE: Incidente de Segurança”.

Este e-mail deve conter toda informação disponível sobre o incidente, as causas que motivaram sua ocorrência e suas consequências:

- Data e hora de ocorrência do incidente;
- Usuário que identificou o incidente;
- Departamento, área e unidade a qual pertence o usuário;
- Descrição do incidente de segurança identificado, incluindo tudo que se conheça relativo às causas e consequências do mesmo;
- Medidas adotadas, caso tenham sido tomadas;
- Em caso de se tratar de um erro ou uso mal-intencionado, todos os dados disponíveis sobre o causador do incidente.

07 Normas de Gestão de Ambientes e Plataformas

Essa seção regula atividades relacionadas a nossos ativos de tecnologia, ambientes e plataformas, tanto no que se refere ao uso interno da Lecom, quando plataformas que são disponibilizadas a nossos clientes.

7.1 Datacenter

A Lecom se utiliza de datacenters de classe mundial para hospedar suas aplicações e plataformas com dados dos nossos clientes e parceiros.

Para isso, possuímos algumas normativas que definem nosso uso de tais provedores:

- O provedor de host da Lecom deve possuir as principais certificações mundiais de segurança, entre elas, ISO 27001;
- O provedor deve atender as principais normal proteção de dados mundiais, incluindo a lei brasileira (LGPD);
- A administração e acesso aos servidores hospedados sob guarda da Lecom será feito apenas por profissionais autorizados pela Lecom. Esse acesso somente será concedido a parceiros e clientes mediante necessidade inequívoca e após consentimento das partes interessadas.
- Acesso a datacenters e servidores que possuem informações confidenciais, ou cujo potencial acesso indevido ou incidente acarreta em um impacto muito significativo, devem utilizar prioritariamente fatores de autenticação duplo, como por exemplo, no acesso aos datacenters de terceiros utilizados pela Lecom;
- São estabelecidos acordos de nível de serviço com os provedores contratados e seu posterior acompanhamento pela Lecom, garantindo que os provedores ofereçam pelo menos nível igual ao que a Lecom oferece aos seus clientes e parceiros.

7.2 Ambientes e Servidores

A seguir são descritas normas e boas práticas utilizadas na implantação dos ambientes e plataformas geridas pela Lecom:

- Separação de ambientes de Desenvolvimento, QA (Quality Assurance), e Produção, quando aplicável. Esta separação será realizada através da utilização de servidores distintos, na falta destes, através de diferentes partições lógicas no servidor;
- Os ambientes de clientes são segregados e estão em redes independes, de forma que os servidores não são compartilhados, e não há ligação entre eles;
- Não é autorizado o acesso direto ao ambiente de produção. Os administradores de segurança devem estabelecer os controles e definições de acesso necessárias;
- Não é permitida a realização de testes no ambiente de desenvolvimento com dados reais ou cópias dos mesmos que não tenham sido devidamente tratadas.

7.3 Backups

Todas as informações da Lecom, ou informações sob nossa guarda estão sujeitas às políticas de backup da Lecom. A seguir listamos as principais definições dessa política:

- A informação mantida nos servidores centrais, servidores de rede, roteadores, sistemas de e-mail, etc. está sujeita a cópias periódicas de segurança que permitam sua recuperação ante uma perda imprevista, causada por erros, falhas do sistema, desastre naturais, sabotagem, roubo, etc.;
- Deve-se realizar uma cópia de segurança completa antes e depois da instalação de um novo sistema e antes de qualquer atualização relevante, com o objetivo de manter uma cópia total da configuração das instalações homologadas da Lecom;
- As cópias periódicas totais devem complementar-se com as cópias incrementais as quais concentram as mudanças introduzidas nos dados a partir das cópias totais. No mínimo devem-se realizar cópias mensais totais e semanais incrementais. A periodicidade das cópias de segurança deve ser diretamente proporcional à relevância ou sensibilidade da informação armazenada, à frequência de modificações ou atualizações e ao risco de que o sistema falhe ou se corrompa;
- As cópias são retidas durante um período suficiente para restaurar os dados e serviços críticos. As cópias diárias devem ser mantidas, ao menos, por uma semana, as semanais, no mínimo, um mês e as mensais devem ser guardadas ao menos 6 meses;

- As cópias de segurança devem ser realizadas utilizando ferramentas de software homologadas pela Lecom. Não são realizadas cópias físicas de backup em mídias como: CDs, Fitas, Cartuchos, Discos Rígidos, etc. Todos os backups são armazenados de forma cruzada em datacenters diferentes.
- Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

7.4 Senhas de administração

É necessário definir e implementar medidas de segurança complementares para proteger as senhas de usuários administradores:

- Implementar mecanismos que assegurem a continuidade operacional dos Sistemas de Informação no caso em que não seja possível acessá-los com contas de administração;
- O comprimento da senha deve ser de, no mínimo, 8 caracteres;
- A senha deve conter ao menos um caractere numérico;
- A senha deve conter ao menos um caractere alfabético em maiúsculo e um em minúsculo;
- A senha deve conter ao menos um caractere especial;
- A senha não deve ser uma palavra que se encontre no dicionário, em um dialeto ou gíria de qualquer idioma, nem nenhuma destas palavras escritas de trás para frente;
- A senha não deve ser relacionada com dados pessoais (por ex., data de nascimento, residência, nome de um familiar, etc.);
- A senha deve ser alterada a cada 3 meses;
- A senha, quando do primeiro acesso ao sistema, deve ser alterada;
- As chaves não devem ser armazenadas em um sistema de armazenamento automatizado (por ex., macros ou navegadores de internet).

Se as senhas se encontrarem armazenadas em uma caixa de segurança, devem-se especificar as medidas de segurança física que permita proteger a localização de tal caixa.

7.5 Registro (log) das atividades nos sistemas

Os sistemas, aplicações e a atividade dos usuários nos ambientes administrativos devem estar sujeitos a um acompanhamento e monitoramento permanente, relacionados exclusivamente com a segurança dos sistemas de informação e o respeito à dignidade das pessoas.

Para que os registros sejam úteis, é necessário conhecer o momento temporal exato no qual foram produzidos. Portanto devem-se estabelecer medidas técnicas necessárias que permitam a sincronização temporal dos diferentes sistemas de informação.

Devido às necessidades de integridade dos registros dos sistemas obtidos, é necessária a implantação de mecanismos que garantam a exatidão dos mesmos, de forma que seja possível a detecção de tentativas de modificação.

7.6 Testes de intrusão

A Lecom tem como boa prática a realização periódica de testes de intrusão. Esses testes podem ser contratados por ela ou por meio de terceiros (cliente, parceiros, etc.), para assegurar a adequada proteção dos sistemas de informação da Lecom, mediante a comprovação da confiabilidade dos controles de acesso e confiabilidade da plataforma.

Em cada um dos testes que forem realizados se devem tomar o máximo de precaução, já que se o acesso for conseguido, pode-se causar a falha no sistema de produção.

Os testes a serem realizados devem ser ao menos, os seguintes:

- Tentativa de adivinhação de senhas com ferramentas de descodificação ou crackeadores de senhas que geram senhas com base em dicionários, frases comuns, combinações de letras e números, etc.;
- Buscar os possíveis backdoors nas aplicações;
- Tentativa de sobrecarga nas comunicações, realizando ataques de DoS por diversos pontos de redes públicas ao mesmo tempo;
- Tentativa de utilização de diferentes métodos de exploração em aplicações, roteadores, switches, firewalls e bases de dados.

No caso de encontrar vulnerabilidades, deve-se executar um plano de ação que contemple as ações corretivas que minimizem ou eliminem as vulnerabilidades identificadas, com o objetivo de alcançar um nível de segurança adequado aos padrões da Lecom.

O sentido da transformação