POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Sumário

1. OBJETIVO E ABRANGÊNCIA

A Política de Segurança da Informação e Segurança Cibernética ("Política") da Lerosa Investimentos Ltda ("Lerosa") tem como objetivo estabelecer as regras e diretrizes de segurança da informação e segurança cibernética, visando no mínimo proteger as informações e ativos da Lerosa e dos clientes em geral, bem como reduzir o risco de ocorrência de acessos indevidos e modificações não autorizadas.

Todos os Colaboradores (funcionários, estagiários, prestadores de serviços, diretores e sócios) da Lerosa devem conhecer e seguir as regras definidas nesta política.

Os controles aqui estabelecidos devem ser implementados, monitorados, analisados e aprimorados para garantir que os objetivos do negócio e de segurança da Lerosa sejam sempre atendidos.

2. CONCEITO E CLASSIFICAÇÃO DE INFORMAÇÃO

2.1 CONCEITO DE INFORMAÇÃO

O conceito de informação pode ser definido como um conjunto de dados, neste caso processados ou não, que reunidos sejam capazes de gerar algum tipo de conhecimento sobre qualquer assunto ou pessoa. É elemento essencial para as unidades de negócio da Lerosa, portanto, podendo ser alvo de ameaças.

Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da Lerosa em todo o seu ciclo de vida, que compreende; geração, manuseio, armazenamento, transporte e descarte.

A informação pode ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, meio impresso, verbalmente, em mídias de áudio e vídeo etc.

As mídias que contenham informações da Lerosa e/ou seus clientes devem ser mantidas permanentemente em áreas de controle restrito e sua movimentação é autorizada somente sob rígido controle de pessoa designada.

2.2 CLASSIFICAÇÃO DA INFORMAÇÃO

Dada a sua importância, a informação deve ser classificada de acordo com o grau de confidencialidade e criticidade para os negócios da Lerosa. Além disso, essa classificação deve ficar evidente e de fácil reconhecimento pelo usuário ou Colaborador, para que este possa utilizar e compartilhar o recurso apenas com as áreas de negócio que tenham acesso.

Dessa forma, cabe ao Proprietário da Informação, com suporte das áreas de Tecnologia da Informação e Compliance, classificar a informação conforme abaixo, sendo certo, que todas as informações obtidas no exercício de suas atividades que não tiverem rótulo de classificação definido devem ser tratadas como confidenciais.

- **Confidencial Restrita:** corresponde a informações associadas ao interesse estratégico da Lerosa e outras informações sujeitas a alto grau de sigilo, em geral, restrita ao diretor presidente e demais diretores.
- **Confidencial:** corresponde a informações, que se divulgadas indevidamente, podem reduzir vantagens competitivas da Lerosa, violar privacidade de indivíduos, violar acordos de confidencialidade, prejudicar processos de negociação em andamento, dentre outras.
- **Restrita ou Interna:** corresponde a informações usadas rotineiramente pelos Colaboradores da Lerosa durante suas atividades, não se destinando, contudo ao público externo.
- **Pública:** corresponde a informações de livre divulgação e criadas para fins de distribuição pública, por meio de canais autorizados, que não necessitam de proteção efetiva ou tratamento específico.

3. CONCEITO DE SEGURANÇA DA INFORMAÇÃO

De forma resumida, a segurança da informação pode ser definida como conjunto de regras e parâmetros definidos com o objetivo de proteger dados de propriedade de organizações.

A segurança da informação, por princípio, é caracterizada pela preservação de três aspectos básicos:

- **Confidencialidade**: Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário.
- **Integridade**: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.
- **Disponibilidade**: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária.

4. ATRIBUIÇÕES DE RESPONSABILIDADES

DIRETORIA EXECUTIVA

- Aprovar a Política e suas revisões;
- Nomear Proprietários da Informação;
- Tomar decisões administrativas referentes aos casos de descumprimento da Política.

PROPRIETÁRIO DA INFORMAÇÃO

O Proprietário da Informação pode ser um Diretor ou um Gerente da Lerosa, acumulando as seguintes responsabilidades:

- Conceder, manter, revisar e cancelar as autorizações de acesso a determinado conjunto de informações sob sua guarda;
- Elaborar com apoio da diretoria responsável, a classificação das informações sob sua responsabilidade, com base em critérios de classificação;
- Elaborar matriz de segregação de funções sob sua responsabilidade;
- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções na Lerosa às autorizações de acesso concedidas, observada a matriz de segregação de funções;
- Autorizar a liberação do acesso a informação sob sua responsabilidade, observada a matriz de segregação de funções;
- Analisar os relatórios de controle de acesso, com o objetivo de identificar desvios em relação a Política e as normas em vigor;
- Participar de investigação de incidentes de segurança relacionados às informações sob sua responsabilidade;
- Quando convocado, participar das reuniões do Comitê de Gestão de Segurança da Informação.

TECNOLOGIA DA INFORMAÇÃO

- Disponibilizar, modificar e retirar acesso dos Usuários aos Recursos Tecnológicos conforme perfil de acesso definido;
- Disponibilizar, manter disponível e atualizar a infraestrutura necessária para suportar o funcionamento dos recursos tecnológicos;
- Definir Perfil de Acesso aos Recursos Tecnológicos de domínio da TI;
- Definir padrões de formação dos logins e senhas nos Recursos Tecnológicos;
- Quando convocado, participar das reuniões do Comitê de Gestão de Segurança da Informação.

COLABORADORES

- Cumprir fielmente a Política;
- Não compartilhar, em hipótese alguma, dispositivo de identificação pessoal e informações confidenciais de qualquer tipo;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.) incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Utilizar os recursos tecnológicos, as informações e sistemas a sua disposição exclusivamente para as finalidades aprovadas pela Lerosa;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual.

PRESTADORES DE SERVIÇOS

Os contratos entre a Lerosa e Empresas Prestadoras de Serviços com acesso às informações, aos sistemas e/ou ao ambiente tecnológico da Lerosa devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram esta Política.

5. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A Lerosa utiliza elevados padrões tecnológicos de segurança de rede, para evitar fraudes internas, invasões e garantir o sigilo de toda informação e comunicação interna e externa, incluindo testes anuais dos procedimentos descritos nesta politica.

É proibida a criação de usuário não nominal (genérico), exceto usuário *default* que é criado no momento da instalação para administração do banco de dados, e sua utilização é restrita à equipe de TI. Entretanto, eventual necessidade deverá ser formalizada, com indicação e atribuição do responsável, e submetida à aprovação da Diretoria.

É importante destacar que as informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da Lerosa não podendo ser interpretados como de uso pessoal.

Os servidores são protegidos contra acesso físico não autorizado, em sala de acesso restrito com dispositivo de controle de acesso eletrônico ou mecânico. Além disso, os servidores com acesso à Internet e e-mail possuem *firewalls* e ferramentas de segurança de rede.

Os *softwares* de sistema (operacionais de rede e de estações de trabalho, sistemas gerenciadores de bancos de dados, utilitários de rede e similares) devem ser testados antes da sua implantação, inclusive na troca de versões. Os testes de homologação devem ser aplicados pelos analistas em ambiente próprio de homologação, de forma a não gerar risco de instabilidade ou parada nos servidores de produção.

Equipamentos vitais para o processamento do sistema (servidores, no-breaks e afins) estarão segregados em locais específicos, com acesso restrito e com infra-estrutura mínima ambiental e de segurança (ar condicionado e extintores).

5.1 SIGILO DA INFORMAÇÃO

Todos os Colaboradores da Lerosa, durante o período de vigência dos respectivos contratos e, inclusive, após o término da relação empregatícia ou do contrato de serviços, se obrigam a manter total absoluto sigilo de todas as informações a que tiverem acesso, sejam estas relativas aos Clientes, às operações ativas ou passivas e aos serviços prestados ou aos documentos da Lerosa, obrigando-se a não revelar a terceiros, salvo nas hipóteses previstas em Lei, quaisquer fatos que possam ser caracterizados como violação do sigilo da Lerosa, nos termos do, art.154 do Código Penal e art. 18 da Lei nº 7.492/86.

Somente os Colaboradores, devidamente autorizados pela Diretoria, podem falar em nome da Lerosa para os meios de comunicação, seja por e-mail, entrevista on-line, podcast, documento físico, entre outros. Também apenas os Colaboradores autorizados poderão copiar, captar, imprimir e enviar informações de/para terceiros.

5.2 SEGURANÇA DE ACESSO LÓGICO

A Lerosa adota, em seus recursos tecnológicos, procedimentos de autenticação e identificação de usuários, de modo a prevenir e/ou obstruir ações de qualquer natureza que possam comprometer recursos computacionais, redes corporativas, aplicações e sistemas de informação.

5.2.1 CORREIO ELETRÔNICO

O acesso aos e-mails armazenados é restrito ao Supervisor de TI e a Diretoria, por meio do qual também é possível recuperar as mensagens apagadas acidentalmente da caixa de entrada dos Colaboradores.

5.3 *SOFTWARE ANTIVÍRUS*

A Lerosa utiliza a solução de antivírus para prevenção e combate a vírus nas estações de trabalho e servidores. O servidor de antivírus (repositório) busca a cada 01 hora atualizações no site do fornecedor. As estações de trabalho e os demais servidores buscam as atualizações no servidor local de antivírus a cada 02 dias.

O monitoramento do status de atualização da ferramenta e dos níveis de detecção e infecção de vírus é realizado diariamente pela área de TI, por meio da console de administração e e-mails encaminhados pela ferramenta. Caso sejam identificadas falhas na aplicação da atualização ou execução do antivírus, as correções devem ser realizadas manualmente pelo próprio analista.

6. ADMINISTRAÇÃO E CONCESSÃO DE ACESSOS

O acesso às informações e aos ambientes tecnológicos da Lerosa, necessário para execução de atividades dos Colaboradores, deve ser controlado de acordo com sua classificação, de forma a garantir acesso apenas às pessoas autorizadas, mediante aprovação formal.

Os Gerentes das áreas de Gestão, Distribuição, *Compliance e* Risco são responsáveis pela definição, manutenção e revisão dos perfis de acesso e estes devem ser concedidos em conformidade com a Matriz de segregação de função.

Cada Gerente é responsável por informar a equipe de TI sempre que ocorrerem inclusões, alterações, transferências e exclusões de usuários.

6.1 PARTES INTERNAS

O acesso a redes e sistemas é concedido pelos Gerentes de cada área, por meio da Ficha de Controle de Acesso, com base na função a ser desempenhada pelo Colaborador e/ou responsabilidade delegada. No caso de base de dados, o acesso é restrito aos Gerentes e equipe de TI.

6.1.1 DIRETRIZES PARA O USUÁRIO

O usuário deve seguir as seguintes diretrizes:

- Somente acessar outro computador conectado à rede se possuir autorização para tal ou se o serviço alvo permitir acesso público.
- Quando utilizar alguma rede de dados externa o usuário deve observar as suas normas.
- Não interceptar ou tentar interceptar a transmissão de dados através da rede, exceto quando autorizado explicitamente pelo superior hierárquico, com prévio conhecimento da área de TI.

- Não desenvolver, manter, usar ou divulgar meios que possibilitem a violação da rede de computadores da Lerosa.
- Não colocar um hub ou switch em um ponto de rede para ampliar o número de pontos de rede sem previa autorização.
- Não utilizar ou disponibilizar para fins particulares ou de recreação, serviços que sobrecarreguem as redes de computadores e ainda, que possam ir contra a ética, a moral e os bons costumes, tais como: escuta de rádio, páginas de animação, jogos, pedofilia, pornografia, músicas, vídeo, filmes, *software* comercial ou outro que comprometa a imagem da Lerosa.

6.1.2 DIRETRIZES PARA O ADMINISTRADOR

Cabe ao administrador zelar pelo bom funcionamento da rede observando o seguinte:

- Fazer uso de ferramentas para monitorar a rede, inclusive os links a ela agregados.
- Gerenciar adequadamente os privilégios de usuários, as senhas de usuários, os procedimentos de logon (shell scripts), de desconexão de usuários por inatividade e de política de troca de senha.
- Comunicar imediatamente ao Gerente de TI a ocorrência de invasões (*hackers*, *lammers*, *crackers* etc), tomando as medidas de desconexão da rede e correção das falhas.
- Proteger os serviços de rede utilizando ferramentas apropriadas, como *firewall*, *Proxy*, Sistemas de Detecção de Intrusão etc, desde que não seja no backbone, pois neste caso deve haver a prévia consulta ao Gerente de TI.
- Sugere-se que o administrador divida as redes muito grandes em subredes, cada uma protegida por um perímetro de segurança.
- Comunicar o uso de outras ferramentas como NAT (*Network Adress Translation*) para o Gerente de TI, cuidando do gerenciamento dos logs e responsabilizando-se pela identificação do usuário na eminência de alguma atividade tida como ilícita.
- Consultar o Gerente de TI sobre a criação de VPNs.
- Bloquear os serviços desnecessários que possam comprometer o desempenho ou ir contra o código de ética ou qualquer item desta política.
- Fazer a atualização de *patches* e erratas nos equipamentos de rede (*switches, hubs* e roteadores).
- Não fornecer a usuários ou fornecedores/instituições informações sobre número IP ou nome de usuários em caso de reclamação ou denúncia; a solicitação deve sempre ser feita por vias formais (ofícios, protocolados etc).
- Limitar ao máximo a divulgação de informações de roteamento, faixa de IP, servidores, equipamentos de rede, entre outros, a terceiros.
- Não desenvolver, manter, usar ou divulgar meios que possibilitem a violação de rede de computadores da Lerosa.

6.2 CONCESSÃO E PARAMETRIZAÇÃO DE SENHAS

Cada usuário recebe uma senha pessoal de acesso de acordo com a função a ser desempenhada.

Os padrões de formação de logins e senhas de acesso aos sistemas de informação devem seguir os mesmos padrões mínimos para acesso à rede Lerosa.

A senha de acesso deve seguir obrigatoriamente os seguintes parâmetros e diretrizes:

- Possuir no mínimo 7 caracteres;
- Possuir complexidade atividade (caracteres alfanuméricos, especiais (@, #, $, %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo), sempre que possível);
- Ser trocada no primeiro logon;
- Ser trocada novamente, no máximo, a cada 45 dias (não é permitida a reutilização das últimas 6 senhas);
- Ser armazenada com criptografia;
- Ser bloqueada, caso o usuário erre 3 vezes consecutivas;
- Ser desbloqueada somente pelo Administrador;
- Ser criada, no caso de administrador de rede, servidores e banco de dados, de acordo com as regras de conhecimento exclusivo da equipe de TI.

6.3 INSTALAÇÃO DE *SOFTWARE* E *HARDWARE*

Toda instalação de software deve ser feita somente pela equipe de TI por meio do usuário administrador, e todos os *softwares* e aplicativos devem ser licenciados e constar da lista de *softwares* homologados.

Para evitar instalações não aprovadas pelo administrador, em todas estações há bloqueio em *hardware*, impossibilitando qualquer tentativa.

Todo o sistema desenvolvido internamente ou comprado de terceiros deve possuir documentação que possibilite:

- Aprendizado dos usuários;
- Continuidade dos trabalhos, sem interrupção, na falta destes;
- Pronta identificação dos pontos a serem alterados numa manutenção, no caso de sistemas desenvolvidos internamente.

6.3.1 INVENTÁRIO DE *SOFTWARE E HARDWARE*

A área de TI mantém controle com a relação de licenças adquiridas e dos *softwares* homologados e aprovados para uso nas estações de trabalho e servidores. O confronto com os *softwares* instalados no parque é realizado sob demanda por meio de levantamento manual ou com o auxílio da ferramenta *OCS Inventory*, que permite identificar os *softwares* e *hardwares* instalados em cada estação de trabalho.

6.4 CORREIO ELETRÔNICO

É disponibilizado para cada colaborador um e-mail nominal e intrasferível, vinculado à Lerosa para uso profissional. O uso para demandas pessoais é permitido desde que pontualmente e sem prejuízo às atividades principais.
As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato: (i) nome do colaborador, (ii) área/departamento, (iii) nome da Lerosa e (iv) telefone.

É proibido aos Colaboradores a utilização do correio eletrônico para:

- Enviar qualquer mensagem que torne seu remetente e/ou a LEROSA vulneráveis a ações civis e criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Apagar mensagens pertinentes de correio eletrônico quando a LEROSA estiver sujeita a algum tipo de investigação;
- Enviar piadas, correntes, cartões virtuais, promoções pessoais e outros assuntos não relacionados às atividades profissionais;
- Produzir, transmitir ou divulgar mensagem que:
  a) Contenha ato ou forneça orientação que conflite ou contrarie os interesses da Lerosa;
  b) Contenha arquivos com código executável que represente risco à segurança;
  c) Vise interromper serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
  d) Vise burlar qualquer sistema de segurança;
  e) Vise acessar informações confidenciais sem explicita autorização do proprietário;
  f) Contenha conteúdo considerado impróprio, obsceno ou ilegal;
  g) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros.

6.5 INTERNET

As diretrizes estabelecidas nesta Política miram o uso profissional e ético da internet nas dependências da Lerosa. Qualquer tipo de atividade ilícita poderá acarretar sanções administrativas e/ou penalidades decorrentes de processos civil e criminal, com a LEROSA atuando ativamente em conjunto com as autoridades competentes. Para isso, são monitorados e registrados todos os acessos de seus colaboradores.

7. INSTRUMENTOS DE MONITORAMENTO E DE CONTROLE

- A utilização de *software* de acesso remoto é restrita à equipe de TI para manutenção nas estações dos usuários;
- Para Sistemas de informação com dados sensíveis utilizamos criptografia e certificados digitais;
- Os servidores e as estações dos usuários têm seus relógios sincronizados com servidor central para que não haja discrepâncias nas operações ou acessos aos sistemas;
- Para as empresas que tenham acesso a informações confidencias, utilizamos Acordos de Confidencialidade;
- Monitoramento da disponibilidade e capacidade de servidores, serviços, processos e links.

São utilizadas as seguintes ferramentas:

- ***Firewall*:** função de restringir acessos indevidos internos e externos.
- **Anti-vírus:** instalado e atualizado em todas as estações.
- **Antispam:** baseado em regras de reputação, também possui solução de antivírus e utiliza filtros de conteúdos.
- **Cacti:** administração de rede.
- **Nagios:** monitoramento de redes e sistemas.
- **OCS-Inventory:** realiza a auditoria e inventário de *hardwares* e *softwares* instalados.
- **Sensores:** de temperatura e umidade nas Salas de Servidores com alertas via e-mail e ligações telefônicas.
- **Desativação em *Hardware*:** em todas as estações de trabalho, que impossibilita quaisquer instalações.

8. VIGÊNCIA

Esta Política entra em vigor em Maio de 2024 e é válida por prazo indeterminado, podendo ser alterada ou substituída a qualquer momento de acordo com a regulamentação em vigor ou por determinação do Comitê de Compliance.