LESTE

Política de Cyber Segurança

Elaboração: Fabiano Silva
Responsável: LFS – Departamento de TI
Aprovação: Comitê de Segurança da Informação
Classificação do Documento: INTERNO

Código:
Vigente Desde: 18/02/2019
Última Versão: 22/05/2025
Versão: 01

ÍNDICE

1. Objetivo

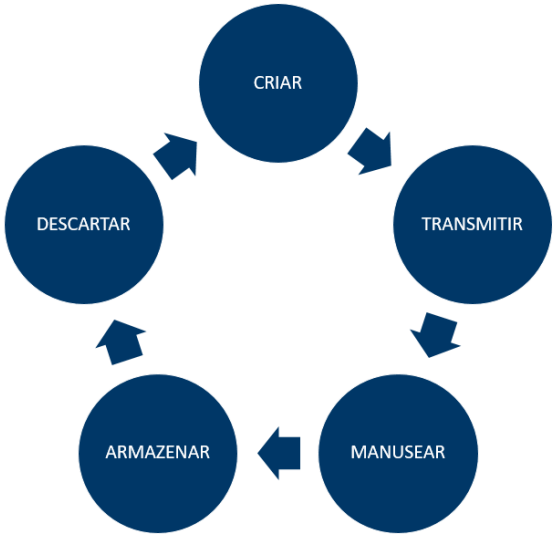
O objetivo da presente política de cyber segurança (“Política”) é definir as diretrizes referentes à segurança das informações do Grupo Leste, através de orientações sobre o manuseio, trato, controle e proteção das informações durante todo o seu ciclo de vida contra destruição, modificação ou divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

Além das informações propriamente ditas, esta Política também se aplica a todo e qualquer meio utilizado em qualquer uma das fases do ciclo de vida das informações, seja ele um ativo tecnológico ou não.

2. Abrangência

As diretrizes definidas a seguir são aplicadas a todos os sócios, diretores, empregados, estagiários, jovens aprendizes e prestadores de serviços do Grupo Leste (“Colaboradores”) e será regularmente atualizada e divulgada pelo Comitê de Segurança da Informação.

A abrangência das regras e controles aqui dispostos refere-se ao ciclo de vida, físico e lógico das informações, conforme ilustrado e detalhado abaixo:

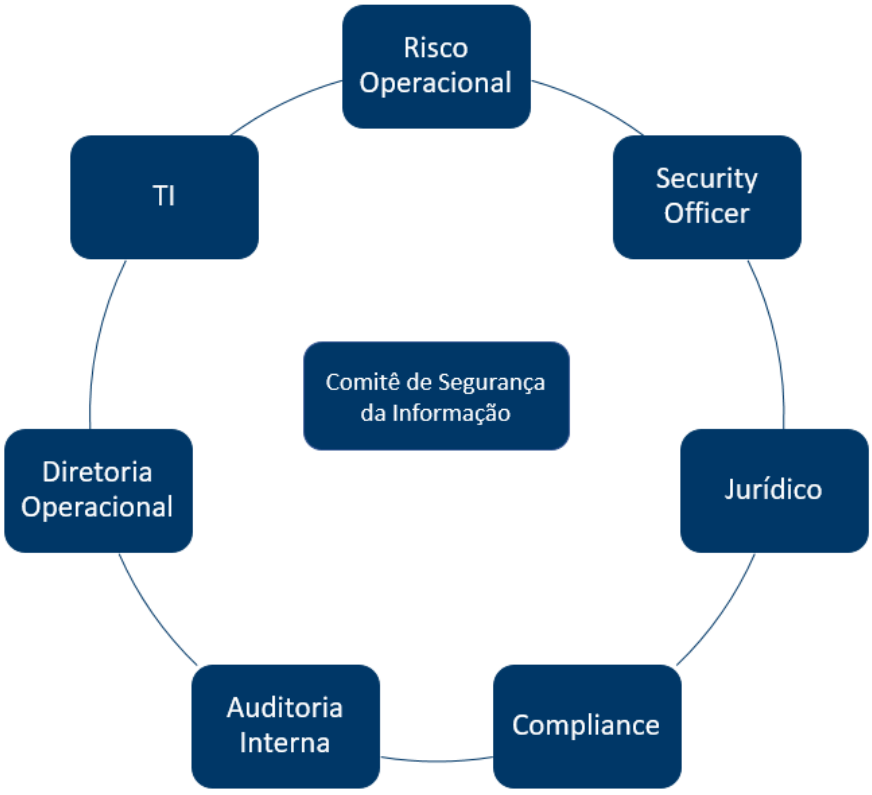


Fase/Meio	Meio Físico	Meio Lógico
Criar	*Documentos gerados e disponibilizados pelo Grupo Leste.*	*Base de Dados e informações geradas e disponibilizadas pelo Grupo Leste.*
Transmitir	*Documentos (inclusive mídias móveis) que circulam internamente ou aqueles recebidos e enviados (externamente)*	*Transmissão ou recebimento de arquivos e informações eletronicamente (ou por telefonia)*
Manusear	*Uso e acesso a informações e dados físicos (inclusive mídias móveis).*	*Uso e acesso a informações e dados lógicos (inclusive mídias móveis).*
Armazenar	*Forma de acesso e organização do armazenamento de documentos e mídias em locais físicos internos ou externos.*	*Arquivos de dados de documentos e informações eletrônicas.*
Descartar	*Fragmentação de documentos físicos e mídias.*	*Exclusão de dados e informações lógicas.*

3. Estrutura Organizacional em Segurança da Informação

O Grupo Leste acredita que a melhor prática para se gerir a segurança das informações é utilizando-se de uma estrutura descentralizada, a fim de assegurar isenção de efetivos ou potenciais conflitos de interesses, bem como minimizar vulnerabilidades existentes e nossa exposição às ameaças referentes ao tema.

Ilustrando o acima exposto, a seguir pode ser observada a organização estrutural e a composição do Comitê de Segurança da Informação, responsável por todas as deliberações no tocante à Segurança da Informação no Grupo Leste:



4. O Conceito

O que é cyber security?

Segurança cibernética, também conhecido como segurança da tecnologia da informação, é um sistema de proteção de computadores, redes, programas e dados contra acesso não intencional ou não autorizado, alteração ou destruição dos mesmos

Os três objetivos da segurança da informação são:

- Confidencialidade;
- Integridade;
- Disponibilidade;

Confidencialidade - refere-se à proteção de informações contra acesso não autorizado ou divulgação. Assegurar a confidencialidade é garantir que aqueles que estão autorizados para acessar informações são capazes de fazê-lo e aqueles que não estão autorizados são impedido de o fazer.

Integridade - refere-se à proteção de informações contra modificações não autorizadas ou destruição. Garantir a integridade é garantir que as informações e os sistemas são precisos, completos e não corrompidos.

Disponibilidade - refere-se à proteção de sistemas de informação e informação de interrupção não autorizada. Garantir a disponibilidade é garantir a pontualidade e confiabilidade de acesso e uso de sistemas de informação.

5. Resumo das Principais Vedações

É proibido aos usuários da rede:

- ✓ Acessar, copiar ou armazenar programas de computador ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais, bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, homofóbico, racista, de apologia a crimes, dentre outros;

- ✓ Passar-se por outra pessoa ou esconder, por qualquer meio, a própria identidade quando utilizar os recursos computacionais ou quaisquer outros de propriedade do Grupo Leste, colocados à disposição do Colaborador em razão do exercício de sua função;

- ✓ Usar ou divulgar informações confidenciais obtidas para benefícios pessoais (oportunidades de emprego, investimentos, dentre outros) mesmo após o término de seu vínculo com o Grupo Leste;

- ✓ Alterar os sistemas padrões, sem autorização;

- ✓ Divulgar quaisquer informações confidenciais para concorrentes e/ou qualquer pessoa não ligada às atividades do Grupo Leste;

- ✓ A senha deve respeitar, no mínimo, 8 (oito) caracteres e atender, no mínimo, a 3 (três) dos 4 (quatro) grupos de caracteres abaixo citados:

    - Letras maiúsculas (de “A” a “Z”);
    - Letras minúsculas (de “a” a “z”);
    - Algarismos (de “0” a “9”); e
    - Caracteres não-alfabéticos (Ex. !, #, @, #, %).

- ✓ Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes ao Grupo Leste;

- ✓ Violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas, sistemas de alarme e demais mecanismos de segurança e restrição de acesso;

- ✓ Utilizar acesso através de modem, ou qualquer outra forma de conexão não autorizada, quando conectado às redes instaladas nas dependências do Grupo Leste;

- ✓ Acessar *e-mail* pessoal e serviços de mensagens instantâneas não autorizados formalmente pelo Comitê de Segurança da Informação;

- ✓ Criar *blogs* ou comunidades na *internet*, ou veicular em redes sociais ou qualquer ambiente virtual semelhante, fazendo uso, sem autorização expressa, da logomarca, nome ou informações confidenciais, restritas ou internas do Grupo Leste;

- ✓ Fazer uso do telefone celular e outros meios de comunicação e gravação particulares dentro das dependências do Grupo Leste nos locais não autorizados;

- ✓ Usar ou instalar softwares não licenciados e sem autorização do Departamento de TI.

- ✓ Efetuar ligações telefônicas para serviços de Tele-Sexo e afins, campanhas de doações de valores para débitos em conta telefônica em nome ou titularidade do Grupo Leste e envio de mensagens (Tele-Mensagens);

- ✓ Utilizar dentro das dependências do Grupo Leste recurso da informação de procedência pessoal, mesmo que para fins profissionais, à exceção de recursos previamente autorizados pela Diretoria, devidamente auditados e monitorados;

- ✓ Fornecer credenciais pessoais de acesso lógico ou físico para o uso de outras pessoas, mesmo que se trate de Colaboradores do Grupo Leste;

*** Para maiores informações vide a Política de Segurança da Informação.*

6. Tratamento e Proteção das Informações

A seguir, estão dispostas regras e diretrizes não exaustivas quanto à proteção e tratamento das informações do Grupo Leste, sendo que quaisquer dúvidas ou esclarecimentos devem ser imediatamente direcionados aos membros do Comitê de Segurança da Informação.

6.1 Proteção de Perímetro

O Grupo Leste conta com appliances de segurança Firewall Fortinet como primeira linha de defesa contra os ataques cibernéticos.

O módulo de **Intrusion Prevention** se encarrega de monitorar a tentativa de acesso indevido contra a Rede de computadores.

A função **Web Filtering** efetua o bloqueio a sites maliciosos e não permitidos pela Política de Segurança de Informação pré-estabelecida.

O módulo **Applications** se encarrega de bloquear acesso a aplicações provenientes da internet utilizando-se de proxy anônimo ou outros artifícios.

Com a função **Advanced Threat Protection** ativada, é criada uma barreira contra os ataques do tipo ransomware.

6.2 Antivírus

O Grupo Leste utiliza um dos mais conceituados antivírus disponíveis no mercado, o Trend Micro.

Devido a sua confiabilidade, robustez, e facilidade de configuração, adotamos a ferramenta como responsável pela segurança de nossas Estações de Trabalho e Servidores de arquivos e aplicações.

As atualizações são efetuadas diariamente e o usuário não tem acesso às configurações, que são protegidas por senha de conhecimento apenas da área de tecnologia.

A verificação de integridade e de áreas críticas do computador é efetuada diariamente em horário preestabelecido.

A varredura semanal está agendada e com ela podemos analisar todos os arquivos da máquina, também em horário preestabelecido.

Existem funções ativadas para impedir que os usuários acessem dispositivos de mídia como USB, para pen drives e também leitores de CD/DVD.

Servidores de Desktops são configurados de forma diferenciada conforme suas características operacionais.

Alertas de dispositivos não atualizados, base de dados corrompida, detecção de intrusão ou ataque, firewall do antivírus ativado/desativado, objetos infectados, objetos em quarentena e outros avisos, são enviados por e-mail à área de tecnologia para tomada de ação imediata.

6.3 WI-FI Guest

O Projeto de Lei 2126/11, mais conhecido como Marco Civil tem sido assunto de debate no país desde 2009. Sendo chamado também de Constituição da Internet Brasileira, o projeto ganhou força, quando foram descobertas as práticas de espionagem usadas pelo governo americano contra o Brasil e outros países.

UPDATE: No decreto nº 8.771, de 11 de maio de 2016, a Presidente Dilma assinou as seguintes atualizações sobre a Neutralidade de Rede:

Ficam obrigadas as operadoras a prestar um serviço adequado com objetivo de manter a estabilidade, segurança, integridade e funcionalidade da rede, observando alguns requisitos como a restrição de Spam, controle de navegação e ataques; Se a rede principal sofre congestionamento, deve-se oferecer uma rota alternativa para manter a estabilidade; A Anatel deve fiscalizar com afinco eventuais infrações das diretrizes estabelecidas pelo Comitê Gestor da Internet - CGIbr

Fica permitido - para preservar a estabilidade e segurança da rede - que as operadoras façam o gerenciamento das redes utilizando as medidas técnicas estabelecidas pelo padrão internacional.

O Grupo Leste conta com serviço de Wi-Fi distribuído aos seus colaboradores e visitantes, devidamente cadastrados e identificados.

Os equipamentos instalados nas dependências da empresa possibilitam além do alto grau de confiabilidade e segurança, que também haja registro de acesso individualizado para cada dispositivo através de vouchers com validades específicas para cada caso. Seja visitante ou colaborador interno, todos possuem registro e rastreabilidade com intuito de proteção tanto a usuários quanto para a empresa.

6.4 Email - Office 365

O acesso a e-mail pelos colaboradores é feito através do Office365, módulo Outlook.

Contamos com a segurança da nuvem da Microsoft para oferecer o serviço aos nossos colaboradores.

O **Microsoft Multifactor Autentication** (MFA) possibilita adicionar uma camada a mais de proteção contra acessos indevidos as contas de e-mail dos colaboradores.

Modulo de Conformidade e Segurança permitem rastreabilidade total para fins de auditoria.

6.5 Assessment de Vulnerabilidade

O Grupo Leste utiliza o OpenVas como um gerenciador central que consolida as varreduras de vulnerabilidades e outras informações pertinentes à cyber segurança.

O OpenVas é um framework de vários serviços e scripts para pentest com foco em verificação e vulnerabilidades de segurança, no qual ele é composto por um servidor interno encarregado para realizar o scan na rede do Grupo Leste.

7. Considerações Finais

Os sistemas e os ativos de informação intrínsecos e necessários ao funcionamento e controle dos serviços essenciais à sociedade, públicos ou privados, tornam-se cada vez mais automatizados e dependentes tecnologicamente. À medida que esses sistemas se tornam interligados a uma rede de comunicação de dados e podem ser acessados remotamente, aumenta a insegurança e amplia-se o rol de ameaças e de vulnerabilidades, particularmente quando conectados à Internet. O gerenciamento da preservação da Informação digital remete a estratégias diversificadas que se estendem a processos, hardware, software, redes de dados, ambientes heterogêneos de armazenamento e produção, entre outros, envolvendo atividades complexas de segurança. Não obstante, almeja-se ampliar a capacidade de assegurar o funcionamento adequado dos sistemas e dos ativos de informação, em instituições financeiras de áreas diversificadas e níveis administrativos distintos, assim como nas infraestruturas críticas estratégicas nacionais a cargo da iniciativa privada.

Nós da área de tecnologia do Grupo Leste, procuramos estar sempre atentos as mais novas tecnologias e tendências de segurança para aplicá-las dentro do padrão adequado as nossas necessidades, respeitando sempre a decisão da alta direção quanto a seu plano de negócios.