Responsável:	Gabriel Machado

AUTORIA		
Elaborado por:	**Homologado por:**	**Aprovado por:**
Nome: Gabriel Machado	Nome: Adauto Junior	Nome: Jackson Nascimento
Data: 24/02/2021	Data: 18/02/2026	Data: 05/03/2026

HISTÓRICO DE REVISÕES		
Revisão:	**Data:**	**Descrição:**
01	24/02/2021	Reunião entre as áreas para definir criação do documento
02	25/02/2021	Iniciado criação do documento
03	03/03/2021	Revisão geral do documento. Informada área de desenvolvimento
04	29/03/2021	Revisão geral para envio a Lev
05	11/05/2021	Revisão geral do setor
06	15/07/2021	Revisão geral do setor
07	20/09/2021	Revisão geral do setor
08	17/11/2021	Revisão geral do setor
09	11/01/2022	Revisão geral do setor
10	07/03/2022	Revisão geral do setor
11	09/05/2022	Revisão geral do setor
12	08/09/2022	Revisão geral e alteração de identidade visual
13	29/05/2023	Revisão geral do setor
14	20/02/2024	Revisão geral do setor
15	17/04/2024	Revisão do documento (Projetos)
16	23/10/2024	Inclusão de Pentest
17	20/02/2025	Revisão geral do setor
18	18/02/2026	Revisão geral do setor
19	05/03/2026	Revisão do documento (Projetos)

OBJETIVO

A Política de Gestão de Incidentes de Segurança da Informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de

incidentes de segurança da Lev, visando orientar o funcionamento do processo de gestão de incidentes de segurança cibernética e da informação, de forma que estes sejam tratados adequadamente reduzindo, ao máximo, os impactos para o negócio.

APLICABILIDADE

Esta política se aplica a todos os colaboradores da Lev, quais sejam: funcionários, estagiários, menores aprendizes, terceirizados e indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura e as informações da Lev com qualquer tipo de interação física ou lógica com os ativos e espaços da organização. Todos esses colaboradores serão tratados nesta política como “usuários”.

1. INTRODUÇÃO

A área de Infraestrutura, Segurança da Informação e Comunicações terá como missão atuar na detecção, resolução, prevenção e redução da ocorrência de incidentes de segurança da informação na Lev, visando proporcionar um ambiente mais confiável, disponível e íntegro.

É fundamental que a gestão de incidentes seja feita de forma adequada, para que se garanta a eficiência da proteção das informações contra roubos, fraudes, espionagens, perda não intencional, acidentes e outras ameaças. Para tal, a área de Infraestrutura de TI e Segurança da Informação tem como objetivo promover ações para redução das ocorrências de incidentes de segurança da informação, mantendo o ambiente seguro e tecnologicamente saudável.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que o maior patrimônio da instituição, que é a informação, tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade adequado.

As regras gerais da Política de Gestão de Incidentes de Segurança da Informação da Lev obedecem ao disposto neste Documento e à legislação pertinente e estão alinhadas com os princípios e as diretrizes da Política de Segurança da Informação (LV-SGSI-PL-SI-04).

2. DIRETRIZES

Esta Política não será extinta ou cancelada. Será revisada em períodos não superior a um ano, quando será publicada uma nova versão, caso haja necessidade de ajustes, ocasião em que será, portanto, substituída por outra com mesmo objetivo e valor que a administração entender cabível ou necessário.

3. PAPÉIS E RESPONSABILIDADES

3.1. AS RESPONSABILIDADES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

- Condução do processo de Gestão de Incidentes de Segurança da Informação;

- Investigação de incidentes, levantamento, cadeia de custódia e segurança das evidências;

- Acompanhamentos dos planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;

- Comunicação aos Gestores responsáveis;

- Realização de análises pós-incidentes (post mortem) para identificação e tratamento de causas raiz e aprimoramento de processos da empresa e do próprio processo de gestão de incidentes de segurança da informação.

3.2. AS RESPONSABILIDADES DOS COLABORADORES

Devem informar imediatamente à área de Segurança da Informação todas as

violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento. Em caso de negligência, o colaborador poderá ser penalizado com o mesmo peso do autor.

3.3. AS RESPONSABILIDADES DA ÁREA DE INFRAESTRUTURA E DESENVOLVIMENTO

- Provimento dos acessos necessários para que a área de Segurança da Informação possa realizar a identificação e investigação dos incidentes de segurança;

- Responsável pelo provimento de trilhas de auditoria e evidencias para a investigação de incidentes;

- Suporte às investigações através do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área.

3.4. AS RESPONSABILIDADES DOS GESTORES

Ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência e SLA's pré-definidos pela área de Segurança da Informação.

3.5. AS RESPONSABILIDADES DA ÁREA JURÍDICA

Suporte às questões legais relacionados a incidentes de segurança da informação.

4. DOS CRITÉRIOS GERAIS SOBRE OS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

São considerados Incidentes de Segurança da Informação quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que

levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de segurança da informação, quais sejam: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em risco;

Todos os colaboradores devem estar em capacidade de identificar incidentes de segurança da informação quando forem testemunhados.

Todos os colaboradores devem notificar qualquer evento de segurança ou fragilidade observada que possam causar: prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas da empresa.

Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a política de segurança cibernética e da informação, bem como provocar danos aos serviços ou recursos tecnológicos.

A lista a seguir exemplifica, mas não esgota os possíveis incidentes de segurança da informação tratados nesta política:

- Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

- Indisponibilidade do ambiente tecnológico em virtude de ataques maliciosos interno e externo;

- Vazamento de informações confidenciais (informações de clientes, informações estratégicas, dentre outras);

- Tentativas interna ou externa de ganhar acesso não autorizado a sistemas, dados ou até mesmo comprometer o ambiente de TI;

- Ato de violar uma política de segurança, explícita ou implícita;

- Uso ou acesso não autorizado a um sistema;

- Modificações em um sistema, sem o conhecimento, instruções ou

consentimento prévio do dono do sistema;

- Compartilhamento de senhas.

O conteúdo da notificação precisa ser claro, em formato simples e deve incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida.

Os eventos de incidente de segurança da informação devem ser categorizados e classificados através de uma matriz de severidade com intuito de se ter uma melhor visibilidade, tratamento e prioridade quanto a sua gestão.

Os eventos abaixo não são considerados eventos de segurança da informação:

- Eventos acidentais (falhas de hardware ou sistêmicas) não intencionais;

- Eventos não maliciosos (erro humano ou descuido que não infrinja as regras de segurança da informação).

OBS: Todo e qualquer incidente que se caracterize como uma CRISE (extrema severidade) deve seguir o Plano de Crise da Lev.

Todos os eventos de incidente de segurança da informação devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento.

A Gestão de Incidentes de Segurança da Informação deve contemplar processos que atendam aos seguintes objetivos:

- Detecção: identificação de incidentes por meio de monitoração, relatórios, denúncias, informações obtidas de áreas parceiras ou qualquer outra análise de eventos adversos;

- Registro e Análise: registro dos incidentes, análise, classificação quanto ao tipo, severidade e priorização;

- Comunicação: comunicação do incidente às partes envolvidas e, se necessário, às entidades externas;

- Resposta: contenção do incidente, análises forenses, custódia de evidências,

tratamento do incidente e da causa raiz;

- Finalização: encerramento formal e análise pós mortem para identificação de possíveis melhorias em processos, controles e na própria Gestão de Incidentes.

É de extrema importância que o horário de servidores e equipamentos de redes estejam sincronizados com uma fonte confiável de tempo (ex: via protocolo NTP) para que não haja disparidades na correlação de eventos, logs e outros dados.

Violações ou tentativas de violação da Diretriz de Segurança da Informação, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

Incidentes de segurança podem ser identificados por processos de monitoração da área de infraestrutura, por Colaboradores que observem fragilidades, anomalias e violações que coloquem a segurança da empresa em risco.

Todos os incidentes de segurança da informação devem ser documentados, classificados, priorizados de acordo com a criticidade da Lev e comunicados aos gestores responsáveis no momento apropriado.

Deve ser definido um plano de comunicação de incidentes de segurança da informação que esteja de acordo com a classificação e o nível de criticidade do incidente. Em casos mais simples e de baixa criticidade apenas o gestor responsável pelo recurso ou informação deve ser comunicado. Em casos mais graves a Diretoria Executiva, a área Jurídica ou outros departamentos pertinentes devem ser comunicados.

A investigação de incidentes de Segurança da Informação deve ser realizada exclusivamente pelas áreas de Segurança da Informação e de Infraestrutura, de forma a garantir a privacidade e o sigilo das informações obtidas.

Sendo necessárias informações ou levantamentos, para os quais devam ser analisadas trilhas de auditoria (logs), acessos à Internet, fluxo de mensagens ou

conteúdo de caixas de correio, ou outras informações que coloquem em risco a privacidade de colaboradores e o sigilo das informações da Lev, deve ser aberto um incidente junto a área de Segurança da Informação para que este realize as investigações.

- As informações obtidas e arquivadas pelo processo de Gestão de Incidentes de Segurança da informação devem ser protegidas de forma a garantir a privacidade de colaboradores e o sigilo das informações, não podendo ser fornecidas a outros departamentos ou auditorias.

- A identificação de incidentes de segurança pode ocasionar o corte imediato dos acessos de colaboradores envolvidos ou a desconexão de sistemas, até que sejam concluídas as investigações necessárias.

- O acesso às evidências e relatório de incidentes de segurança da informação é permitido apenas a área de Segurança da Informação e aos Gestores diretamente envolvidos nos incidentes.

- A documentação de incidentes, resultados de investigações, evidências e suas soluções devem ser atualizadas logo após a conclusão do tratamento do incidente.

O contato para a notificação de incidentes de segurança da informação deve ser feito diretamente a área de Segurança da Informação através de canais previamente definidos.

5. DAS PENALIDADES

O Colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

6. DA REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A política de gestão de Incidentes de Segurança da Informação deverá ser revista e atualizada, ao menos anualmente, com vistas a se manter em sintonia com as regras de negócios, com as melhores práticas do mercado, leis, regulamentos e demais aspectos.

7. DAS DÚVIDAS

Em caso de dúvida solicitar esclarecimento a área de Segurança da Informação.

8. PENTEST

Para garantir a segurança e a proteção dos sistemas de informação da **Lev**, será realizado testes de invasão (Pentest) de forma semestral. O objetivo dos testes é identificar, avaliar e corrigir vulnerabilidades em nossas aplicações, redes e infraestrutura tecnológica, visando minimizar os riscos de segurança e proteger os dados corporativos e pessoais.

Objetivos dos Testes de Pentest:

1. **Identificar Vulnerabilidades**: Avaliar os sistemas e redes em busca de falhas de segurança que possam ser exploradas por agentes maliciosos.
2. **Avaliar a Efetividade das Medidas de Segurança**: Verificar a robustez das defesas existentes e identificar áreas que precisam de melhorias.
3. **Garantir a Conformidade**: Assegurar que as práticas de segurança da empresa estão em conformidade com normas e regulamentações aplicáveis.
4. **Prevenir Incidentes**: Antecipar possíveis ameaças e ataques,

implementando medidas preventivas para proteger os sistemas e dados.

Escopo dos Testes:

- Os testes de Pentest semestrais abrangem aplicações web, sistemas internos, redes, dispositivos móveis e infraestrutura de TI.
- Todos os sistemas críticos para as operações da empresa serão priorizados, conforme o plano de segurança definido pela equipe de segurança da informação.
- O escopo dos testes será revisado a cada ciclo semestral, com a possibilidade de inclusão de novos sistemas ou tecnologias que tenham sido implementados recentemente.

Responsabilidades:

1. **Equipe de Segurança da Informação**:
   - Planejar e coordenar a execução dos testes de Pentest.
   - Selecionar fornecedores e consultorias especializadas para a realização dos testes, quando necessário.
   - Garantir que os resultados dos testes sejam documentados e analisados.
   - Implementar correções e melhorias com base nas descobertas dos testes.
   - Reavaliar os sistemas após a aplicação de correções para verificar a efetividade das medidas implementadas.
   - Prazo para regularizar vulnerabilidade 06 meses, antes da próxima análise de vulnerabilidade.
2. **Gestores de TI**:
   - Fornecer as informações e o acesso necessário para a realização dos testes de Pentest.
   - Acompanhar a implementação das correções sugeridas pela equipe de segurança.

3. Fornecedores de Serviços de Pentest:

- Executar os testes conforme o escopo definido e de acordo com as melhores práticas.
- Elaborar relatórios detalhados com os achados de vulnerabilidade e recomendações para mitigação.
- Manter a confidencialidade de todas as informações a que tiverem acesso durante a execução dos testes.

Periodicidade:

- Os testes de Pentest serão realizados a cada seis meses. A data de execução dos testes será definida pela equipe de segurança da informação com antecedência, permitindo o planejamento das atividades.

Tratamento das Vulnerabilidades:

- As vulnerabilidades identificadas serão classificadas por gravidade (crítica, alta, média, baixa) e tratadas conforme seu nível não passando do prazo de seis meses.
- As correções para vulnerabilidades críticas e altas deverão ser priorizadas, com prazos específicos para implementação, conforme o nível de risco identificado.

Relatório e Documentação:

- Um relatório com os resultados do Pentest será elaborado após cada teste, detalhando as vulnerabilidades encontradas e as recomendações para mitigação.
- Os relatórios serão compartilhados com as partes interessadas relevantes, respeitando as diretrizes de confidencialidade.
- A documentação dos testes e das correções será armazenada e mantida para fins de auditoria e conformidade.

Conformidade e Auditoria:

- A realização dos testes de Pentest semestrais faz parte das práticas de

conformidade da empresa e será auditada periodicamente para assegurar que os testes sejam realizados conforme o planejado.

- Os resultados dos testes podem ser utilizados para melhorar continuamente o programa de segurança da informação.