LVNT | Asset Management

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E CIBERNÉTICA

Histórico de Atualizações				
Versão	Data de publicação	Autor	Revisor	Motivo das Alterações
1	25/12/2021	Vitor Kawano Horibe	Alexandre Chiuratto Dias	Versão Inicial
2	15/06/2023	Alexandre Chiuratto Dias	Vitor Kawano Horibe	Atualização
3	28/10/2023	Alexandre Chiuratto Dias	Vitor Kawano Horibe	Atualização
4	16/06/2025	Leonardo Rocha de Faria	Ricardo Romero	Atualização

SUMÁRIO

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

INTRODUÇÃO

A Política de Segurança da Informação se aplica a (i) Levante Gestão de Recursos Ltda e (ii) Jatobá LVNT Ltda (em conjunto, "Grupo Levante"),, aplica-se a todos os sócios, colaboradores, prestadores de serviços, clientes e parceiros de negócio, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Levante, ou ainda que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados inseridos no ecossistema de negócios da nossa instituição, tem por responsabilidade zelar, proteger e reportar incidentes referente a segurança ou integridade das informações e dos equipamentos e plataformas de tecnologia da Levante.

OBJETIVOS

A Política de Segurança da Informação da Levante visa proteger as informações de propriedade e/ou sob guarda da Levante, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Levante, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais relacionadas a esta instituição.

Qualquer informação sobre a Levante, ou de qualquer natureza relativa às atividades da empresa e a seus sócios, prestadores de serviços, clientes e parceiros de negócio, obtida em decorrência do desempenho das atividades normais do colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pelo Diretor de Risco e *Compliance*, assim definido no Código de Ética da Levante.

SEGURANÇA DA INFORMAÇÃO

As medidas de segurança da informação utilizadas pela Levante têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa.

É terminantemente proibido que os colaboradores, clientes, prestadores de serviços ou parceiros de negócio façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Levante e circulem em ambientes externos à empresa com eles, sem prévia autorização do Diretor de Compliance. Isso porque tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Levante. Nestes casos, quem estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade. Ainda, nas dependências da Levante, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação, sendo recomendável o seu descarte total.

Adicionalmente, os colaboradores devem se abster de utilizar pen-drives, HD externo ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Levante.

É proibida a conexão de equipamentos na rede da Levante que não estejam previamente

autorizados.

Cada colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O acesso a sites e blogs, bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo também é terminantemente proibido, como também o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Levante.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia dos sócios. Não é permitida a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos.

Todo conteúdo que está na rede pode ser acessado pelo Diretor de *Compliance* caso haja necessidade, inclusive e-mails. Arquivos pessoais salvos em cada computador poderão ser acessados caso seja necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais ou administrativas.

SISTEMAS E *BACKUPS*

Todos os dados da Levante são protegidos por sistemas automatizados de *backup* realizados diariamente que garantem a recuperação rápida do ambiente dentro de *Data Center*.

De forma a preservar os sistemas e informações da Levante, acesso ao *Data Center* é realizado apenas por funcionários autorizados.

A Levante adota procedimentos internos que visam garantir a confidencialidade e integridade das informações corporativas. A rede da Levante não é acessada sem autorização do(s)

responsável(is) pela infra-estrutura de TI, os e-mails são guardados por 10 anos com estrutura na nuvem.

MONITORAMENTO E TESTES

O Diretor de Risco e *Compliance* adotará as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, anual.

Mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nesta Política ou aplicáveis às atividades da Levante que cheguem ao conhecimento do Diretor de Risco e *Compliance*, de acordo com os procedimentos estabelecidos nesta Política, o Diretor de Risco e *Compliance* poderá se utilizar dos registros e sistemas de monitoramento eletrônico e telefônico acima referidos para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede poderá ser acessado pelo Diretor de Risco e *Compliance*, caso haja necessidade. Arquivos pessoais salvos em cada computador poderão ser acessados caso o Diretor de Risco e *Compliance* julgue necessário.

A confidencialidade dessas informações deve ser respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

O Diretor de Risco e Compliance poderá utilizar as informações obtidas em tais sistemas para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos. A Levante se reserva ainda o direito de realizar inspeções periódicas com base nos seus sistemas de monitoramento eletrônico e telefônico.

O Diretor de Risco e *Compliance* deverá elaborar e manter arquivados relatórios descritivos dos resultados dos testes acima realizados. O Diretor de Risco e *Compliance* (ou pessoa por ele incumbida) adotará as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, anual: deverá verificar, por amostragem, as informações de acesso ao

espaço do escritório, a *desktops*, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

O Diretor de Risco e *Compliance* deverá elaborar e manter arquivados relatórios descritivos dos resultados dos testes acima realizados, caso seja encontrada qualquer inconsistência ou irregularidade. Ainda, ele poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Levante (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer informações confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Risco e *Compliance* prontamente. O Diretor de Risco e *Compliance* determinará quais membros da administração da Levante e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Risco e *Compliance* determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

O Diretor de Risco e *Compliance* responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Levante de acordo com os seguintes critérios: (i) avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda; (ii) identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados; (iii) determinação dos papéis e responsabilidades do pessoal apropriado; (iv) avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados; (v) avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública); (vi) avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo informações confidenciais de fundo de investimento sob gestão da Levante, a fim de garantir a ampla disseminação e tratamento equânime da informação confidencial); e (vii) determinação do responsável (ou seja, a Levante ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente.

A definição ficará a cargo do Comitê de Risco e *Compliance* e Risco, após a condução de

investigação e uma avaliação completa das circunstâncias do incidente.

VIGÊNCIA E ATUALIZAÇÃO

Esta política será revisada periodicamente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E CIBERNÉTICA

Histórico de Atualizações				
Versão	Data de publicação	Autor	Revisor	Motivo das Alterações
1	25/12/2021	Vitor Kawano Horibe	Alexandre Chiuratto Dias	Versão Inicial
2	15/06/2023	Alexandre Chiuratto Dias	Vitor Kawano Horibe	Atualização
3	30/04/2024	Alexandre Chiuratto Dias	Vitor Kawano Horibe	Atualização

INTRODUÇÃO

O objetivo desse documento é elaborar um processo que descreva como a Levante irá atuar em situações de emergência e exceção no que se refere a tratamento dos dados.

Esse plano contém um fluxo de trabalho rápido e com a devida rastreabilidade dos fatos geradores, bem como documenta todo o processo para evitar futuros incidentes da mesma natureza. Esse processo é aplicado e executado de modo contínuo e incremental.

Para que o processo funcione de forma confiável e bem definida, deve atender os seguintes tópicos:

I. Formação do Time de Resposta a Incidentes (TRI)

O TRI é um grupo de trabalho dentro da empresa, que deve ser designado através do Comitê Executivo da empresa, com o treinamento e ferramentas ideais para responder a diferentes tipos de incidentes. Esse grupo se reunirá na incidência de ocorrências para definir o plano de ação, bem como a frequência das reuniões de trabalho. O Responsável pelo tratamento de dados pessoais (DPO) da empresa e um representante da equipe de Segurança de informação fazem parte desse grupo.

Time: Gustavo Canettieri (DPO), Felipe Bevilacqua e Vitor Horibe.

Endereço de e-mail para notificações do time: *lgpd_tri@levante.com.br*

II. Instalação e divulgação dos mecanismos de comunicação de incidente.

Devem ser criadas, disponibilizadas e publicadas as formas de notificação à Companhia quando ocorrerem incidentes. O §1º, do Artigo 41, da Lei 13709/2018, a LGPD, estabelece: “A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.” Portanto, devem ser divulgados os e-mails: dpo@PROCEMPA.com.br e seguranca@PROCEMPA.com.br, bem como os contatos do Suporte. Deve haver indicação de quais mecanismos são considerados rápidos e seguros e se sugere o esclarecimento de quais as expectativas de anonimato que o notificador deve ter.

III. Definição do grupo de Acionadores do TRI.

Responsáveis por receberem as notificações e a realização do tratamento inicial. Para a cobertura 24 horas, este grupo deve incluir membros do Suporte e contatos qualificados para executar a triagem.

IV. Instalação, configuração e definição de ferramentas de monitoria e alarmes.

Devem informar diretamente o TRI através de mecanismos de comunicação direta como o Slack, WhatsApp ou SMS.

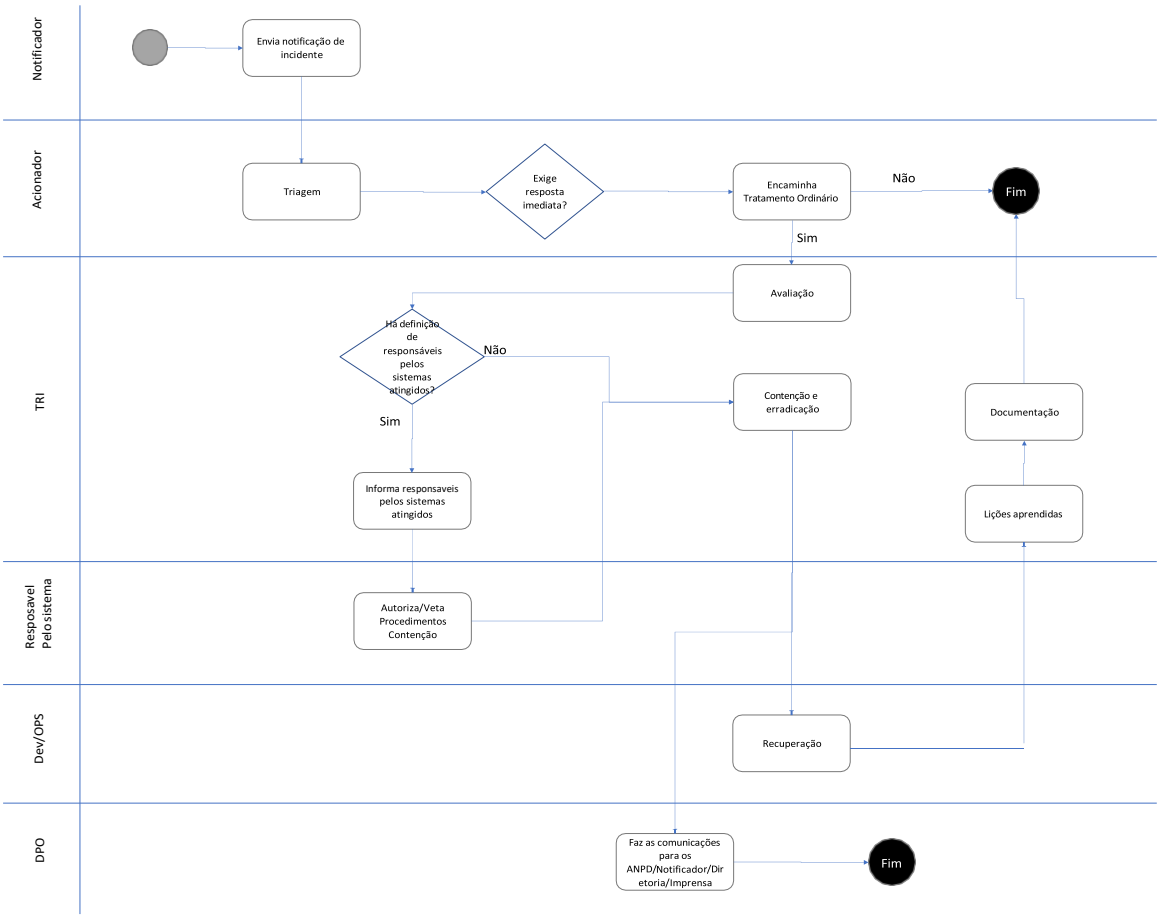
V. Preparo de um Plano de Comunicação de Incidentes.

Para facilitar a comunicação da Companhia deve ser criada uma biblioteca com modelos de documentos (templates) para comunicação formal do Encarregado pelo Tratamento de Dados Pessoais com a ANPD, titulares de dados, notificadores e imprensa. Link para a biblioteca LPGD https://www.dropbox.com/home/LGPD

PARTICIPANTES DO PLANO DE RESPOSTA A INCIDENTES ATORES

- Notificador: pessoa ou sistema de monitoração que notifica incidente.
- TRI: Time de Resposta a Incidentes, definido na preparação prévia.
- Acionadores do TRI: grupo que receberá notificações de incidentes em primeira mão para triagem, estruturado em níveis distintos para viabilizar a importante cobertura 24 horas.
- Responsável por Sistema ou Controlador de Sistema: indicado que deve ser contatado e pode autorizar ou vetar procedimentos de emergência. Deve estar documentado na CMDB, inclusive forma de contato para emergências
- Equipe de Segurança da Informação
- Encarregado pelo Tratamento de Dados Pessoais (DPO**)**: membro especial do TRI, responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais.
- Desenvolvedores/Operadores/Fornecedores dos sistemas: atuam no desenvolvimento de soluções e instalações deles.

DESENHO DO PROCESSO



INÍCIO

Um novo incidente é notificado, por pessoa externa ou não a Companhia ou por alarme da monitoração, usando um dos mecanismos de comunicação definidos. Notificação é recebida por Acionador do TRI.

TRIAGEM

Acionador do TRI deve fazer a avaliação preliminar ou contatar imediatamente outro Acionador em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se

agravarem se não houver resposta imediata.

Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para tramites regulares da Companhia pela Equipe de Segurança da Informação e Encarregado pelo Tratamento de Dados Pessoais, caso o incidente envolva dados pessoais.

Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o TRI deve ser acionado para às fases seguintes.

AVALIAÇÃO

Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos sistemas afetados para colaborar e isso deve ser feito a critério do TRI a qualquer momento que julgar adequado e viável.

CONTENÇÃO E ERRADICAÇÃO

Caso estejam identificados na CMDB, devem ser acionados os responsáveis pelos sistemas impactados, conforme indicado na documentação, que irão orientar e se manifestar sobre os procedimentos de contenção e erradicação.

Objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida será realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas, colocação de avisos de indisponibilidade para manutenção, sempre que possível tomando cuidados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot das mesmas para posterior análise.

RECUPERAÇÃO

Caso exista Plano de Continuidade de Negócio dos sistemas impactados, eles devem ser iniciados, conforme especificado.

A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema. O TRI tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação. Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas.

Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

LIÇÕES APRENDIDAS

Com o incidente contido e sua resolução encaminhada, o TRI deve agendar e conduzir uma formalização de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos - inclusive deste Plano de Resposta a Incidentes.

As melhorias sugeridas com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

DOCUMENTAÇÃO

TRI deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

COMUNICAÇÕES

Assim que possível, no caso de incidente com vazamento de dados pessoais, o Encarregado de Tratamento de Dados (DPO) deve avaliar e fazer as comunicações obrigatórias por Lei, se houver, bem como informar e subsidiar os Encarregados de Tratamento de Dados dos controladores do sistema. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a ANPD.