www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

Política de Segurança da Informação

Última atualização em outubro de 2022

ÍNDICE

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

I. INTRODUÇÃO

A segurança das informações e dados de propriedade ou sob guarda da Recuperi é fundamental e faz parte dos valores que nortearam a fundação e que continuam a guiar o crescimento da Recuperi.

A Recuperi entende que seus serviços e atividades dependem da constante evolução e aprimoramento de sua Política de Segurança da Informação ("PSI"), bem como procedimentos e práticas associadas à segurança da informação e proteção de dados.

A PSI da Recuperi está sob constante revisão, expansão e melhoria, sendo obrigatório o cumprimento de suas obrigações conforme definido na sua versão mais recente por todos os seus colaboradores e fornecedores.

II. OBJETIVO

A PSI tem como principal objetivo a proteção das informações e dados da Recuperi ou que estão sob a sua guarda, garantindo a manutenção da confidencialidade, integridade e disponibilidade destas informações.

Para atingir seus objetivos, a PSI deve ser utilizada para prevenção, detecção e redução de vulnerabilidades na Recuperi, bem como para estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação.

III. ESCOPO

A PSI faz parte das políticas institucionais da Recuperi, e deve ser cumprida pela Recuperi, bem como por todos os seus colaboradores, fornecedores e parceiros que tenham acesso, armazenem, processem e/ou transmitam informações e dados da Recuperi ou fornecidas por seus clientes e parceiros.

Todos os colaboradores e fornecedores da Recuperi declaram aceitar e cumprir a PSI e demais políticas institucionais da Recuperi (**Anexo 1**).

IV. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A Recuperi e seus colaboradores se comprometem com a manutenção de tratamento adequado das informações e dados de sua propriedade ou sob sua guarda. Para tanto, a presente PSI e demais políticas e procedimentos relacionados à segurança da informação na Recuperi devem ser interpretados conforme os princípios gerais de segurança da informação:

- **confidencialidade**: apenas indivíduos ou entidades autorizados podem acessar informações;
- **disponibilidade**: quando necessário, deve ser garantido aos indivíduos ou entidades autorizados o acesso às informações solicitadas;
- **integridade e autenticidade**: dever de manutenção da precisão e completude das informações, com registro de eventuais modificações e acessos.

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

A Recuperi e seus colaboradores devem atender aos padrões de boas práticas, definidos pela PSI e conforme exigido por lei.

V. DIRETRIZES

As diretrizes da presente PSI devem ser aplicadas por meio de medidas e mecanismos específicos de segurança da informação, contemplando os fatores de risco, tecnologia e custo, quando cabíveis.

Destaca-se que todas as políticas, regras e procedimentos de segurança da informação devem sempre ser disponibilizados aos colaboradores e demais parceiros da Recuperi, de acordo com o escopo da PSI.

A PSI e demais políticas, regras e procedimentos de segurança da informação estão sob contínua revisão e aprimoramento. Quaisquer alterações são comunicadas aos colaboradores, fornecedores e demais parceiros da Recuperi.

São diretrizes da PSI:

I. Tratar todas as informações conforme as diretrizes definidas na Política de Privacidade, Código de Ética e Termos e Condições de uso da Recuperi, bem como de acordo com a legislação aplicável;

II. As informações e dados deverão contar com medidas adequadas de proteção contra acesso e/ou divulgação não autorizada, modificação ou destruição;

III. Deve sempre ser utilizado o devido cuidado na forma de tratamento das informações, tendo em vista as obrigações éticas e de confidencialidades adotadas pela Recuperi;

IV. As informações de propriedade ou sob guarda da Recuperi somente poderão ser utilizadas para a finalidade para as quais foram coletadas, conforme definido na Política de Privacidade da Recuperi;

V. Apenas indivíduos ou entidades autorizadas terão acesso a informações, sendo devida a identificação de acessos, e mantendo o critério de menor privilégio;

VI. Os acessos serão protegidos por senha única, pessoal e intransferível, secreta, qualificando o usuário responsável pelas ações realizadas com as informações acessadas;

VII. A identificação de riscos às informações de propriedade ou sob guarda da Recuperi devem ser reportados ao Comitê de Segurança da Informação;

VIII. As informações devem ser tratadas e armazenadas de forma segura, com o uso de métodos de criptografia e segurança avançadas, quando necessário;

IX. As obrigações da PSI e as responsabilidades atribuídas à segurança da informação devem ser continuamente divulgadas com todos os colaboradores e parceiros Recuperi, assegurando seu cumprimento.

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

O cumprimento das diretrizes da PSI é fundamental para a efetivar com segurança as parcerias da Recuperi e atender seus clientes com níveis apropriados de proteção à informação.

VI. PROCESSOS E CONTROLES

A aplicação das diretrizes de segurança da informação deverá seguir os processos e controles definidos pela PSI e demais políticas e processos associados à segurança da informação.

Todos os sistemas utilizados pela Recuperi e seus colaboradores devem ser estruturados de forma a proteger as informações de propriedade ou sob guarda da Recuperi. Devem ser avaliadas medidas de proteção dos dados presentes nos sistemas, especialmente contra acessos não autorizados, incidentes, destruição ou alteração de dados, tratamento inadequado ou atividade ilícita.

Em caso do desenvolvimento ou contratação de novos sistemas, os mesmos deverão ser homologados.

A. CONTROLE E GESTÃO DE ACESSOS

Os acessos e credenciais fornecidos aos clientes e colaboradores são de uso pessoal, intransferível, e não é permitido seu compartilhamento e uso não autorizado. Os acessos devem ser rastreáveis e permitir a identificação do executor.

Haverá a gravação de logs do ambiente computacional, contendo as informações de quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado. Os logs serão protegidos contra modificações e acessos não autorizados.

Todos os acessos seguem o critério de menor privilégio, limitando o acesso somente às informações imprescindíveis para a execução legítima e plena dos serviços contratados com a Recuperi.

O acesso a qualquer informação da Recuperi ou sob sua guarda, ou aos sistemas da Recuperi, atribui responsabilidade ao usuário por suas ações e implica no aceite da presente PSI, bem como os Termos e Condições de Uso, Política de Privacidade e Código de Ética da Recuperi.

Os clientes da Recuperi poderão solicitar concessões, revisões e exclusões nos seus acessos.

B. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação deve ser tratada conforme sua classificação definida pela Política de Classificação de Informação (**Anexo 2**) e receber a proteção adequada em todo o seu ciclo de vida.

C. GESTÃO DE RISCOS

A gestão dos riscos de segurança da informação deve ter como objetivo a redução dos riscos à níveis aceitáveis para os serviços, produtos, processos e tecnologias da Recuperi.

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

O desenvolvimento de sistemas na Recuperi é baseado nas diretrizes da PSI e melhores práticas de segurança de informação. A Recuperi constantemente avalia a necessidade de testes periódicos de continuidade, segurança e desempenho de seus sistemas.

Os softwares e tecnologias utilizados pela Recuperi e seus colaboradores deverão estar devidamente licenciados, e nas versões atualizadas definidas pelos seus fabricantes (Anexo 1).

O monitoramento de riscos deve ser constante, sendo obrigatório o devido tratamento das ameaças e vulnerabilidades identificadas. As recomendações referentes à gestão de riscos deverão ser apresentadas oportunamente ao Comitê de Segurança da Informação para revisão, planejamento e implementação das medidas necessárias.

Todos os prestadores de serviços contratados pela Recuperi devem seguir a presente PSI e a Política de Privacidade, Código de Ética e Termos e Condições de Uso da Recuperi e estão sujeitos à avaliação de riscos pelas equipes de tecnologia da informação e jurídica da Recuperi.

A identificação ou alteração de risco à segurança da informação em eventual contratação de fornecedor ou manutenção de vínculo com terceiro deverá ser comunicada imediatamente às equipes de tecnologia da informação e jurídica/compliance para adoção das medidas cabíveis.

D. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os incidentes deverão ser analisados e classificados em relação ao risco e impacto potencial aos clientes e à segurança das informações e dos dados de propriedade ou sob guarda da Recuperi. O monitoramento de segurança da informação deve ser constante, com o objetivo de identificar nos eventos e alertas analisados possíveis incidentes.

É obrigação de todos os colaboradores da Recuperi a comunicação de suspeita de incidentes. Os prestadores de serviços e terceiros contratados pela Recuperi têm o dever de comunicar imediatamente a suspeita de quaisquer incidentes relevantes relacionados às informações de propriedade ou sob guarda da Recuperi, e cumprir todas as determinações legais e contratuais na mitigação de eventuais danos causados pelo incidente.

Incidentes identificados como relevantes ou potencialmente relevantes devem ser comunicados ao Comitê de Segurança da Informação da Recuperi, e preparado relatório técnico a ser apresentado pelo gestor/responsável pela equipe de tecnologia da informação.

A análise, definição e execução de plano resposta a incidente de segurança de informação será tratado em pauta prioritária pela Gestão da Recuperi, em reunião extraordinária de seu Comitê de Segurança da Informação.

O cliente deverá ser notificado da ocorrência de incidente relevante, independentemente das medidas técnicas e jurídicas adotadas.

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

Os procedimentos de gestão de incidentes de segurança da informação são detalhados no **Anexo 3**.

E. COMUNICAÇÃO E TREINAMENTO

A presente PSI deverá ser apresentada e conhecida por todos os colaboradores da Recuperi, e poderão ser agendados treinamentos, workshops, palestras e envio de materiais para reforço da cultura de segurança da informação da Recuperi.

Igualmente, os fornecedores e terceiros contratados pela Recuperi deverão ter acesso à versão mais atualizada da PSI, e poderão ser agendados treinamentos, workshops, palestras e envio de materiais para reforçar a cultura de segurança da informação no relacionamento com a Recuperi e seus clientes.

As iniciativas e projetos das equipes comerciais, operacionais e jurídicas devem estar alinhadas com as orientações da equipe de tecnologia da informação e seguir nos seus procedimentos os princípios e diretrizes definidos na PSI.

VII. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Cabe à Gestão da Recuperi, por meio de suas atribuições como Comitê de Segurança da Informação, realizar a supervisão e revisão das políticas, estratégias e processos relativos à aplicação da PSI e segurança da informação.

A revisão de temas de segurança da informação fará pauta das reuniões de planejamento do Comitê de Segurança da Informação, bem como em fóruns apropriados, com a participação de pelo menos 1 (um) dos seguintes gestores designados: CEO, CFO e/ou CTO.

São responsabilidades do Comitê de Segurança da Informação:

a) Definição das políticas e procedimentos de segurança da informação a serem aplicados nos processos e serviços prestados pela Recuperi;
b) Planejamento dos investimentos em medidas de segurança da informação, conforme as recomendações apresentadas pela equipe de tecnologia da informação;
c) Implementar medidas de proteção contra ameaças e para a preservação da continuidade do negócio;
d) Responder adequadamente a eventuais incidentes de segurança da informação;
e) Promover a cultura de segurança da informação e as diretrizes definidas na PSI.

VIII. MEDIDAS DISCIPLINARES

São consideradas violações à PSI quaisquer ações ou omissões que possam expor a Recuperi, seus colaboradores, fornecedores e clientes a dano financeiro, reputacional ou que comprometa a segurança da informação e dados.

A não observância e violação dos princípios e disposições da PSI sujeita os colaboradores da Recuperi às sanções disciplinares previstas na legislação, bem como às seguintes medidas disciplinares:

- carta de advertência reservada;
- advertência pública;
- suspensão;
- demissão ou exclusão do quadro societário;
- rescisão contratual em caso de fornecedores/terceiros.

A aplicação das medidas disciplinares levará em consideração o grau e a potencialidade do dano causado pela violação, bem como as atitudes concretas do colaborador e/ou fornecedor visando a reparar, minorar ou compensar o dano causado.

IX. CANAIS DE COMUNICAÇÃO DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação é de responsabilidade compartilhada de todos os colaboradores e fornecedores da Recuperi.

Faz parte da cultura a abertura e manutenção de canais de comunicação para envio de sugestões, críticas e avisos sobre a PSI e segurança da informação diretamente com a gestão da Recuperi:

Suspeitas de incidentes de segurança da informação	tecnologia@recuperi.com.br dartanghan.vani@recuperi.com.br
Canal de contato com o DPO, esclarecimento de dúvidas ou solicitações relativas à temas de privacidade e proteção de dados	privacidade@recuperi.com.br
Dúvidas relacionadas às Políticas da Recuperi	jurídico@recuperi.com.br
Contato com o CEO	felipe.krausz@recuperi.com.br

X. DOCUMENTOS RELACIONADOS

A PSI faz parte das políticas institucionais da Recuperi, cujo cumprimento é obrigatório por todos os colaboradores e fornecedores contratados.

Deverão ser considerados na aplicação da PSI as seguintes políticas institucionais da Recuperi:

- Código de Ética
- Política de Privacidade
- Termos e Condições de Uso

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

ANEXO 1 – DECLARAÇÃO DE RESPONSABILIDADE

[Qualificação]declara que todas as ações e atividades conduzidas por si ou sob sua responsabilidade serão realizadas em conformidade com a Política de Segurança da Informação da Recuperi, especialmente em relação às suas diretrizes e princípios, bem como de acordo com demais obrigações e medidas de segurança da informação.

Destaca-se que não é permitido o uso de software não autorizado, bem como qualquer acesso não-autorizado aos sistemas da Recuperi ou as informações contidas nos seus bancos de dados.

As obrigações definidas na Política de Segurança da Informação da Recuperi devem ser cumpridas por todos, desde o início da relação de colaborador/fornecedor até o encerramento da relação jurídica.

São consideradas violações à PSI a exploração ou mesmo a não divulgação imediata de falhas ou vulnerabilidades, por meio de quaisquer ações ou omissões por colaboradores e fornecedores que possam expor a Recuperi, e seus demais colaboradores, fornecedores e clientes a dano financeiro, reputacional ou que comprometa a segurança da informação.

As obrigações de confidencialidade permanecem de acordo com as definições legais e conforme as obrigações contratuais com a Recuperi e seus clientes.

Local [...], Data [...]

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

ANEXO 2 – POLÍTICA DE CLASSIFICAÇÃO DE INFORMAÇÃO

As informações e dados de propriedade ou sob guarda da Recuperi somente poderão ser compartilhados com terceiros que estejam relacionados aos serviços prestados pela Recuperi, ou com autoridades, conforme definido pela legislação aplicável.

As informações serão classificadas de acordo com a presente Política e conforme sua natureza, e poderão estar sujeitas à restrições específicas de confidencialidade e acesso quando necessário para a sua proteção. Independentemente da classificação, todas as informações e dados de propriedade ou sob guarda da Recuperi somente podem ser utilizados para fins legítimos.

Poderão ser adotadas as seguintes classificações:

- **Confidencial**: informações somente disponíveis via acesso específico. Poderão ser consideradas confidenciais as informações que contenham dados sensíveis, sigilosos e estratégicos da Recuperi, de seus colaboradores, parceiros, clientes e terceiros.

- **Restrito**: informações que somente podem ser acessadas para cumprimento do contrato com o cliente ou fornecedor, para a prestação dos serviços da Recuperi ou para cumprimento de obrigação legal ou regulatória (ex. dados pessoais para fins de cobrança e protesto).

- **Sem restrição**: acesso amplo, aplicável para informações públicas ou tornadas públicas pelo titular da informação.

A classificação das informações será baseada nas necessidades da Recuperi e de seus colaboradores, bem como de fornecedores e parceiros para permitir o uso legítimo e seguro das informações, de acordo com a legislação aplicável. Caberá a equipe de tecnologia da informação a adoção de medidas de limitação de acesso e proteção de informações confidenciais ou restritas.

As medidas de proteção às informações e restrições de acesso devem ser aplicadas durante todo o ciclo de vida da informação sob guarda da Recuperi, incluindo os processos desde sua geração e posterior manuseio, transporte e armazenamento, até o seu eventual descarte.

Todas as informações, independentemente da classificação de acesso, deverão ser tratadas como sigilosas. Mesmo informações públicas poderão estar sujeitas à medida de restrição de acesso e compartilhamento, e devem ser tratadas como sigilosas, à luz da proteção oferecida pela legislação aplicável e nos princípios estabelecidos na PSI e na Política Privacidade da Recuperi.

É responsabilidade da equipe de tecnologia da informação apresentar para o Comitê de Segurança da Informação as recomendações para classificação de informações e dados, bem como adotar as medidas necessárias para executar a presente Política.

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

ANEXO 3 – PROCEDIMENTOS DE GESTÃO DE INCIDENTES

I. Detecção

Um novo ou possível incidente é notificado por colaborador, fornecedor ou terceiro externo à Recuperi ou o incidente foi identificado pela própria equipe de tecnologia da informação da Recuperi durante suas atividades de monitoramento.

Possíveis incidentes de segurança da informação:

- Uso indevido ou acesso não autorizado;
- Código malicioso, como vírus, *trojan*, *worm*, *spyware*, *scripts*, etc.;
- Prospecção de informações, inclusive varredura, *sniffing* e engenharia social;
- Tentativa de intrusão, exploração de vulnerabilidades, e acesso lógico;
- Comportamento inesperado das ferramentas.

A equipe de tecnologia da informação deverá registrar a notificação ou identificação do incidente ou possível incidente e iniciar procedimentos de triagem.

II. Triagem

Caberá à equipe de tecnologia da informação a avaliação preliminar para descartar eventuais notificações ou suspeitas de incidentes indevidos.

A avaliação preliminar deve compreender análise dos procedimentos e sistemas afetados, a criticidade do incidente, possíveis danos e riscos à segurança das informações e dados da Recuperi ou sob sua responsabilidade.

O resultado da avaliação preliminar deverá ser notificado imediatamente ao Comitê de Segurança da Informação, para definição das medidas apropriadas e aprovação de ações ou investimentos necessários.

Em caso de incidentes que exigem resposta imediata da Recuperi, a equipe de tecnologia poderá atuar em coordenação com o CTO antes da finalização da avaliação pelo Comitê de Segurança da Informação. Nessa hipótese, o Comitê de Segurança da Informação será notificado tempestivamente.

Por fim, caso um possível incidente de segurança possa afetar dados pessoais, informações confidenciais ou de acesso restrito, o DPO e a equipe jurídica deverão ser notificados imediatamente.

III. Avaliação

Caberá ao Comitê de Segurança da Informação determinar a criticidade do incidente com base nas informações colhidas na avaliação preliminar.

A criticidade dos incidentes de segurança da informação poderá ser classificada em:

- **Alta**: incidente com potencial de dano grave. Compromete a segurança de informações críticas ou confidenciais da Recuperi ou de seus colaboradores e clientes.

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

- **Média**: incidente com potencial de dano significativo. Compromete a segurança de informações de acesso restrito não-críticas da Recuperi ou de seus colaboradores e clientes.
- **Baixa**: incidente ainda não confirmado ou potencial de dano mínimo. Poderá comprometer informações e dados de natureza pública.

Independente da classificação da criticidade do incidente, as equipes envolvidas e o Comitê de Segurança da Informação deverão verificar a causa do incidente, vulnerabilidades exploradas, e possíveis responsáveis para definição das medidas legais cabíveis.

Em caso de vários incidentes, deverá ser definida a ordem de atendimento de acordo com a urgência na adoção de medidas de contenção e o potencial impacto da demora na atuação das equipes responsáveis.

IV. Contenção e Erradicação

Dentro de prazo razoável, tendo em vista a criticidade do incidente, o Comitê de Segurança da Informação determinará quais serão as medidas de contenção a serem adotadas para limitar e remediar os possíveis danos causados pelo incidente.

Poderão ser autorizadas medidas de contenção e erradicação, que incluem o desligamento de sistemas ou de funcionalidades específicas, e até indisponibilidade de sistemas para manutenção.

A adoção de medidas de contenção e erradicação deve considerar a preservação de evidências que possam identificar autoria, origem, vulnerabilidade e método utilizado no incidente.

V. Recuperação

O Comitê de Segurança da Informação deverá adotar as medidas necessárias para a pronta restauração dos sistemas e serviços afetados pelo incidente, formando um plano de recuperação a ser executado em prazo razoável.

O Comitê de Segurança da Informação possui competência para aprovar a contratação de fornecedores e terceiros, inclusive em caráter emergencial, para apoio na condução do plano recuperação e de ação

As medidas a serem implementadas poderão incluir reinstalação de sistemas, restauração via backups e mesmo o desenvolvimento e atualizações dos sistemas, aplicações e código-fonte.

VI. Prevenção e Documentação

Finalizada a execução do plano de recuperação, a equipe de tecnologia da informação deverá formalizar recomendações de medidas para o Comitê de Segurança da Informação com o objetivo de prevenir futuros incidentes semelhantes.

www.recuperi.com.br
R. Arquiteto Olavo Redig de Campos,
105 - 24° Andar, Torre B - Brooklin
São Paulo, Brasil - CEP:04711-904

As recomendações adotadas pelo Comitê de Segurança da Informação deverão ser implementadas em dentro de prazo razoável, a ser definido de acordo com a criticidade do incidente e das vulnerabilidades identificadas.

As disposições da Política de Segurança da Informação da Recuperi poderão ser alteradas para refletir as modificações realizadas nos sistemas, procedimentos e demais políticas internas.

A equipe de tecnologia da informação deverá formalizar em documentação as ações e medidas adotadas para conter, erradicar e prevenir o incidente, bem como as informações obtidas sobre o incidente, sua evolução no tempo e evidências.

Por fim, poderão ser adotadas medidas jurídicas para responsabilização dos atores responsáveis pelo incidente e comunicação para as autoridades policiais competentes das evidências obtidas com o incidente.

VII. Comunicações

Em caso de incidente que comprometeu dados pessoais, o Comitê de Segurança da Informação deverá avaliar juntamente com o DPO se houve risco ou dano relevante aos titulares dos dados impactados.

Verificado a ocorrência de dano ou risco de dano relevante, e sendo a Recuperi o controlador dos dados e informações comprometidas com o incidente, é obrigatória a sua comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular impactado.

Ainda que haja dúvida sobre a relevância dos riscos e danos envolvidos, o Comitê de Segurança da Informação poderá mesmo assim proceder com a comunicação apropriada.

Caso a Recuperi seja apenas a operadora das informações e dados, os clientes afetados deverão ser comunicados imediatamente, e eventual comunicação individual da Recuperi à ANPD e ao titular impactado poderá ser avaliada.