POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

ORRAM GESTÃO DE RECURSOS LTDA

Versão 4.0

(Março/2025)

SUMÁRIO

I. OBJETIVO

A informação é um dos principais ativos no mundo dos negócios. Assim, a ORRAM, estabelece a presente Política Corporativa de Segurança da Informação e Segurança Cibernética ("PSI"), a fim de proteger a informação sob sua responsabilidade de vários tipos de ameaças e garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual das empresas do grupo, dos clientes e do público em geral.

II. ABRANGÊNCIA

Esta Política se aplica a todos os sócios, colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da ORRAM, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da ORRAM.

A não aderência a PSI poderá implicar em advertência, suspensão ou demissão, a critério da empresa, após analisada a gravidade e impactos resultantes do descumprimento.

III. REGRAS GERAIS

Confidencialidade é um princípio fundamental. Aplica-se a quaisquer informações não-públicas referentes aos negócios da ORRAM, como também as informações recebidas de seus investidores, contrapartes ou fornecedores, durante o processo natural de condução de negócios. Os Colaboradores não devem transmitir nenhuma informação não-pública à terceiros.

Sob a supervisão do Diretor de Riscos e Compliance, os colaboradores, no exercício das suas atividades e funções, serão responsáveis por implementar e reforçar os procedimentos a fim de proteger a confidencialidade de informações privilegiadas reais ou potenciais. Muitas das atividades destes departamentos são consideradas confidenciais e podem ser usadas somente com aqueles fora do departamento com base na necessidade de

conhecimento.

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da ORRAM, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

Em atenção aos dispositivos da Resolução CVM n.º 21/2021 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, a ORRAM procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

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

A. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

A ORRAM deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de crimes cibernéticos são:

a) Malware (vírus, cavalo de troia, spyware e ransomware);

b) Engenharia Social;

c) Pharming;

d) Phishing scam;

e) Vishing;

f) Smishing;

g) Acesso pessoal;

h) Ataques de DDoS e botnets;

i) Invasões (advanced persistent threats).

Com a finalidade de manter a sua infraestrutura íntegra e resguardada contra estes e outros potenciais ataques, a ORRAM definiu todos os ativos relevantes, fundamentais ao seu funcionamento, criou regras para classificação das informações geradas e avalia continuamente a vulnerabilidade de cada um desses ativos.

A ORRAM levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

B. AÇÕES DE PREVENÇÃO

1. PROPRIEDADES DOS RECURSOS DE TI

Todos os recursos computacionais e de sistemas disponibilizados para os colaboradores são de propriedade da ORRAM. Não é permitida a utilização de notebooks, tablets ou outros hardwares para operações no âmbito da ORRAM, salvo expressa permissão do Diretor de Risco e Compliance.

Todos os computadores disponibilizados para os colaboradores da ORRAM têm por objetivo o desempenho das atividades profissionais na ORRAM, não devendo ser utilizado para quaisquer outros fins.

Como medida de proteção, serão definidos os sites e redes sociais que poderão ser acessados por esses equipamentos. As exceções serão tratadas pela Área de TI em conjunto com Risco e Compliance.

Caberá ao setor de infraestrutura o monitoramento de acesso não autorizado na rede, e a respectiva informação ao gestor responsável pelo colaborador, para que as devidas medidas sejam tomadas.

2. CORREIO ELETRÔNICO

É vedada a utilização de correio eletrônico particular ou qualquer outro meio de comunicação privado para fins de recepção e transmissão de ordens.

A ORRAM disponibiliza endereços de correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. O endereço eletrônico

disponibilizado para o usuário é individual, intransferível e pertence à.

O usuário pode acessar o seu correio eletrônico cedido pela ORRAM mesmo quando estiver fora do ambiente da empresa, por meio do serviço de correio eletrônico via Internet, sendo que deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da ORRAM.

Importante ressaltar que, por se tratar de uma ferramenta de trabalho de propriedade da ORRAM, a empresa se reserva ao direito de rastrear, monitorar, gravar e inspecionar, sem aviso prévio, quaisquer informações transmitidas, com o objetivo de evitar riscos decorrentes de ataques externos e do mau uso da ferramenta.

Por fim, recomenda-se que todos os e-mails sejam rotulados de acordo com a classificação da informação que lhe é inerente.

3. GRAVAÇÃO TELEFÔNICA

Em função da natureza das operações realizadas pela ORRAM, os ramais estão ligados a sistema de gravação de voz, cujo objetivo é proteger o colaborador nos eventuais conflitos que surjam nas negociações realizadas pela ORRAM e suas contrapartes, bem como possibilita a identificação de situações de não conformidades.

Estas gravações serão armazenadas em nuvem ou qualquer mídia para eventuais consultas posteriores, pelo tempo mínimo exigido pela regulamentação. Periodicamente, podem ser verificadas pelo Compliance e a escuta por qualquer funcionário só poderá ser realizada com a aprovação prévia desta área, mediante justificativa e condicionada ao acompanhamento.

4. USO DE TELEFONES CELULARES

É vedada a utilização de telefones celulares para fins de recepção e transmissão de ordens, salvo se utilizado em emergência ou contingência, ou seja, quando houver falha do sistema convencional de telefonia.

5. ESTAÇÕES DE TRABALHO

Ao se ausentar da estação de trabalho, o colaborador deverá desligar ou bloquear seus equipamentos, para que não haja utilização indevida dos recursos e/ou serviços disponíveis para ele, evitando a exposição de informações a pessoas não autorizadas.

A instituição tem os cadastros de seus clientes e seus documentos institucionais preservados em arquivo de imagem que ficam fora de sua sede, permitindo utilizá-los ou reconstruí-los de imediato em caso de uma ocorrência que danifique os originais que se encontram na sua sede.

Ademais, informações sensíveis e/ou sigilosas não devem ficar expostas nas mesas dos colaboradores. Quando não estiverem sendo utilizadas, essas devem ser armazenadas nas gavetas chaveadas de cada mesa, ou na ausência das gavetas, em locais individuais disponibilizados pela ORRAM. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

6. POLÍTICAS DE SENHA E DIREITOS DE ACESSO

A credencial de acesso a qualquer meio lógico ou físico é um importante mecanismo de controle e segurança dos ativos de informação. O Diretor de Tecnologia e de Compliance, devem realizar a revisão dos perfis e dos acessos físicos e lógicos periodicamente ou sempre que necessário, de acordo com o procedimento interno definido para tal e respeitando-se a segregação de funções. As não conformidades eventualmente detectadas durante esses processos poderão ser discutidas pela Diretoria de Compliance.

7. SENHAS DE ACESSO

Cada colaborador terá uma senha de acesso, de uso pessoal e intransferível, que permite o acesso à rede, intranet, internet, softwares ou quaisquer outros dispositivos mantidos pela ORRAM. A senha não pode ser compartilhada nem fornecida a terceiros e não deve ser anotada em arquivos físicos ou registradas em meios que permitam sua leitura por terceiros.

As senhas recebidas pelos colaboradores autorizados para acesso aos

ambientes e aplicativos devem ser alteradas no primeiro, sendo observadas as seguintes recomendações:

- Utilizar letras e números;
- Compor com caracteres maiúsculos e minúsculos;
- Não utilizar senhas com letras ou números repetidos ou em sequência;
- Não utilizar informações pessoais fáceis de serem obtidas, como data de nascimento, nomes e sobrenomes, números de telefone ou outros dados de fácil identificação;
- Não permitir o reuso da última senha cadastrada;
- Obrigatoriedade de reinserção da senha a cada 15 minutos de inatividade na estação de trabalho.

Caso o colaborador esqueça ou bloqueie sua senha, deve-se solicitar à TI o desbloqueio ou nova senha de acesso.

O Diretor de Tecnologia e de Compliance possuem uma senha de acesso master que permite monitorar se os colaboradores estão em conformidade com esta PSI.

8. ACESSO A SOFTWARES

Quando o colaborador for admitido ou transferido para outra área, cabe aos gestores providenciarem junto à TI os acessos necessários e eliminar os acessos desnecessários, garantindo a limitação de acesso às informações críticas. Contudo, é possível que por um período pré-determinado o colaborador utilize informações de ambas as áreas em função da necessidade delas. Caso isso seja necessário, o gestor da área originária do colaborador deve justificar a manutenção dos acessos antigos e a data prevista para sua migração.

9. ACESSO AO DIRETÓRIO DE REDE

Todos os colaboradores devem possuir um perfil de acesso que possibilita a realização de suas atividades, sendo necessária avaliação prévia para

alterações ou inclusões de novos acessos.

Os perfis de acessos aos diretórios da rede poderão ser sem restrições, só para leitura ou restrição total.

10. ACESSO À REDE POR CONEXÃO REMOTA

A ORRAM disponibiliza acesso interno à rede e softwares por meio de conexão remota segura para funcionários.

11. ACESSO À INTERNET

É vedado o download de arquivos e programas não autorizados ou sem revisão e aprovação da TI. A proibição tem por objetivo evitar que vírus e outros programas indevidos, não licenciados e nocivos apareçam no ambiente de computação da ORRAM, com possibilidades de perdas financeiras, de imagem e de confidencialidade das informações.

O eventual uso de e-mail particular para assuntos particulares é tolerado. Não obstante, é terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento à terceiros, bem como com conteúdo político ou outro que possa colocar a ORRAM em risco.

12. VÍRUS

A qualquer indício de existência de vírus, o colaborador deve interromper suas atividades e comunicar imediatamente à área de Tecnologia, por telefone, que executará os procedimentos para a erradicação de vírus no intuito de evitar a sua propagação em todo o ambiente lógico da ORRAM.

É terminantemente proibido os esforços individuais e isolados do colaborador para eliminar o vírus, pois podem contribuir para provocar danos ainda maiores, na medida em que, em geral, estes usuários não estão capacitados e/ou não possuem os softwares necessários para erradicação do vírus.

Todos os computadores da ORRAM possuem softwares de verificação de integridade (antivírus) com objetivo de proteger os arquivos, softwares e computadores. As práticas de desativação do antivírus, ou de download de

softwares de antivírus não homologados pela área de Tecnologia, estão proibidas e os colaboradores estão sujeitos às penalidades.

13. BACK-UP E RESTAURAÇÃO

O processo de backup nos servidores internos é realizado diariamente para todos os arquivos de dados salvos na rede (base de dados, planilhas, textos, etc.). O acesso ao servidor é restrito às pessoas autorizadas.

Servidores: Cópia de sombra realizada diariamente;

Cópia em disco físico local: realizada às em dois períodos diários (Contempla os dados dos Desktops);

Cópia na Nuvem: realizada diariamente (Contempla os dados dos Desktops); e

Desktops: Cópia local para o servidor diariamente.

14. ACESSO FÍSICO

A ORRAM, pela natureza de suas operações, deve garantir a segregação física das suas instalações, especialmente da área responsável pela gestão de carteiras de valores mobiliários, caso existam atividades conflitantes, com o objetivo de proteger as informações sobre operações, posições e estratégias que só podem ser de conhecimento da área responsável.

O controle de acesso físico tem por objetivo:

- impedir acesso não autorizado;
- identificar e checar permissão de acesso;
- liberar acesso autorizado;
- identificar e registrar as tentativas de acessos não autorizados; e
- e gerar relatórios sobre a movimentação de acessos ocorridos no local.

A presença de visitantes no interior das instalações da ORRAM deverá ser acompanhada por um colaborador.

15. ACESSO AO DATA CENTER

Acesso Físico: O controle de acesso ao Data Center é feito somente por funcionários autorizados, administradores ou prestadores de serviço acompanhado por tais funcionários.

Acesso Lógico: Todos os computadores possuem acesso limitado ao servidor com níveis de segurança diferenciados e senhas.

16. RETIRADA DE ACESSO

Quando um colaborador é desligado da ORRAM ou um contrato de prestação de serviços é encerrado, o a área contratante deve comunicar, imediatamente, a área de Tecnologia para bloquear os acessos físicos e lógicos concedidos.

C. TERMO DE USO E DE POSSE

A ORRAM poderá ceder notebook, tablet, modem ou aparelho de telefone celular para o colaborador desenvolver suas atividades profissionais, sendo necessário a assinatura do "Termo de Uso e Posse", no qual o colaborador assume toda a responsabilidade pelos mesmos e pelos softwares nele instalados. Os termos de uso e posse ficarão arquivados na área administrativa.
Quando do desligamento, o colaborador deverá devolver todos os equipamentos cedidos para realização de suas atividades profissionais.

D. NOTIFICAÇÃO DE INCIDENTES E ABUSOS

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Alguns exemplos de incidentes de segurança são:

a. tentativa de uso ou acesso não autorizado a sistemas, ambientes e dados;

b. tentativa de tornar serviços indisponíveis e modificação de sistemas

(sem o conhecimento ou consentimento prévio do TI); e

c. o descumprimento à PSI da ORRAM.

É muito importante que a área de Tecnologia e de Compliance sejam comunicadas sobre atitudes consideradas abusivas ou relacionadas à incidente de segurança. As notificações podem ser instrumentos eficazes na mitigação de incidentes e na contenção dos prejuízos como, por exemplo, em casos de fraudes.

Conforme as melhores práticas de mercado, a ORRAM desenvolveu um plano de resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto abaixo:

- Equipe de Tecnologia própria ou TI terceirizado (Sob supervisão do Compliance):

a) Verificação e Auditoria dos Logs;

b) Criação de laudo pericial contendo as informações que foram potencialmente vazadas;

c) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;

d) Desinstalação de software;

e) Execução de varreduras offline para descobrir quaisquer ameaças adicionais;

f) Formatação e reconstrução do sistema operacional;

g) Substituição física de dispositivos de armazenamento

h) Reconstrução de sistemas e redes;

i) Restauração de dados provenientes do backup realizado diariamente; e

j) Entre outros.

- Compliance ou Jurídico:

a) Criação de relatório baseado no laudo pericial elaborado pela Equipe de Tecnologia, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança; e

b) Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido.

- Administrativo/ Gestão:

a) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Companhia; e

b) Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos da ORRAM resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do plano de resposta, devem ser devidamente classificados por nível de severidade, arquivados e documentados pela Área de Compliance, bem como ser formalizado no Relatório de Controles Internos da ORRAM.

Caso o evento tenha sido causado por algum colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da ORRAM.

A ORRAM se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus colaboradores, podendo ser os registros e o conteúdo dos arquivos assim obtidos utilizados para detecção de violações aos documentos internos da ORRAM e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

E. PLANOS DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Os procedimentos para acessos físicos e lógicos nas emergências e contingências estão descritos no Plano de Continuidade de Negócios, no qual estão abrangidos os procedimentos a serem adotados nestas circunstâncias de forma a que todos os colaboradores estejam aptos a exercer suas atividades, sem descontinuidade.

F. DECLARAÇÃO DE RESPONSABILIDADE E MEDIDAS DISCIPLINARES

Os colaboradores devem aderir formalmente ao Termo de Confidencialidade e ao Termo de Ciência da Política Corporativa de Segurança da Informação, comprometendo-se a agir de acordo com a PSI e os demais normativos da ORRAM e de seus reguladores e autorreguladores.

As violações à PSI e demais normativos estão sujeitas às sanções disciplinares previstas no Código de Ética da ORRAM.

IV. POLÍTICA DE REVISÃO E CONTROLE DE VERSIONAMENTO

A. POLÍTICA DE REVISÃO

Neste documento, a ORRAM detalha os principais pontos de sua Política de Segurança da Informação que irão vigorar no período de 1 (um) ano, esta Política será submetida à revisão anual ou em períodos inferiores a este e sempre que ocorrerem alterações nos procedimentos ou legislação que afete a mesma.

B. CONTROLE DE VERSIONAMENTO

Esta Política será submetida à revisão periódica, sempre que necessário, com o intuito de preservar as condições das normas em vigentes e das melhores práticas do mercado.
Esta versão revoga todas as anteriores e passa a vigorar a partir da data de sua publicação.

Versão	Data	Modificações
01	Abril/2020	Original.
02	Dezembro/2021	Revisão geral, adequação de redação e nova formatação dos itens
03	Dezembro/2022	Revisão periódica e adequação para os processos atuais
04	Março/2025	Revisão periódica e adequação para os processos atuais