POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

1. INTRODUÇÃO

Esta Política de Segurança da Informação demonstra a preocupação da Empresa RODA com as informações que trafegam por seus ambientes, sejam físicos ou digitais, bem como informações de seus colaboradores e seus clientes, e tem como finalidade estabelecer as diretrizes para a Segurança da Informação da Empresa RODA**,** de acordo com os requisitos do negócio, com as leis e regulamentações vigentes.

Assim, todos os colaboradores, inclusive terceiros e prestadores de serviços, independentemente do cargo ou atividade exercida, são responsáveis pela proteção das informações, físicas ou digitais da RODA e devem cumprir diariamente as diretrizes estabelecidas por esta Política de Segurança da Informação.

1. OBJETIVO

Esta Política de Segurança da Informação (PSI) tem por finalidade:

- Declarar formalmente o comprometimento da direção da Empresa RODA na proteção de seus ativos tangíveis e intangíveis de acordo com as necessidades de negócio e em conformidade legal;
- Preservar e proteger as informações da Empresa RODA e os Recursos de Tecnologia da Informação (TI) que as contêm, ou que estejam sob sua responsabilidade, dos diversos tipos de ameaça e em todo o seu ciclo de vida, contidas em qualquer suporte ou formato;
- Definir as melhores práticas, padrões e recomendações de uso aplicáveis aos ativos da Instituição por meio de diretrizes e procedimentos, resguardando a segurança das informações de propriedade ou sob a responsabilidade da Empresa RODA;
- Estabelecer as responsabilidades e limites de atuação dos colaboradores da Instituição em relação à segurança da informação, reforçando a cultura interna e priorizando as ações necessárias;
- Garantir a sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações e promover credibilidade às atividades prestadas pela Empresa RODA**,** tendo como missão promover o respeito aos princípios da Segurança da Informação;
- Prevenir e reduzir impactos gerados por incidentes de segurança da informação, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade no desenvolvimento das atividades da Instituição;
- Orientar sobre o uso seguro de Recursos de TI, da Instituição ou de seus colaboradores e clientes, bem como sobre medidas de traga seu próprio dispositivo (*BYOD*) e de trabalho remoto (*Home Office,*) se houver;

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- Zelar por relações transparentes e éticas de seus colaboradores e prestadores de serviços;
- Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados à prestação das atividades da Instituição, no que diz respeito à segurança da informação e aos objetivos corporativos, morais e éticos da Empresa RODA.

1. APLICAÇÃO

Esta **PSI** possui valor jurídico e tem abrangência nacional, envolvendo a responsabilidade de todos os colaboradores e/ou prestadores de serviços.

Esta **PSI** envolve a responsabilidade direta e imediata das seguintes áreas:

- **Diretoria**
  - Analisar, aprovar e declarar formalmente o seu comprometimento com esta PSI.

- **Tecnologia da Informação**
  - Analisar, aprovar, cumprir e fazer cumprir esta PSI e demais Procedimentos Complementares por todos os colaboradores e prestadores de serviços da Empresa RODA;
  - Garantir que a Comissão de segurança da informação tenha atuação permanente, reunindo-se periodicamente;
  - Promover e realizar a gestão do Sistema de Gestão em Segurança da Informação, garantindo a implementação de controles, modelos, padrões e recursos necessários para a proteção da informação;
  - Orientar para que as atividades desempenhadas pela Área de Segurança da Informação estejam adequadas à prestação de serviços pela Empresa RODA;
  - Aprovar os investimentos em segurança da informação da Empresa RODA, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio;
  - Analisar procedimento disciplinar para apuração de responsabilidades dos envolvidos em Incidentes de segurança da informação e recomendar as penalidades em conjunto com a comissão de segurança da informação, quando necessário;
  - Autorizar, ou não, a utilização de dispositivos móveis particulares conforme as necessidades do negócio e nos termos desta PSI e dos documentos que a complementam;
  - Analisar e aprovar, ou não, em conjunto com a comissão de segurança da informação, os pedidos de exceções à esta PSI.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- **Segurança da Informação**
  - Manter esta PSI atualizada e submetê-la para aprovação da Diretoria de Segurança da Informação e Comissão de Segurança da Informação;
  - Elaborar e manter atualizado os documentos que compõem o Sistema de Gestão de Segurança da Informação (SGSI);
  - Encaminhar para avaliação da Segurança da Informação e Comissão de Segurança da Informação as exceções deste documento;
  - Identificar e avaliar os riscos relacionados à segurança da informação e propor melhorias;
  - Auxiliar a Área de Recursos Humanos na publicidade e disponibilidade desta PSI da Empresa RODA;
  - Receber, analisar e tratar os incidentes de segurança da informação reportados e submeter relatório para deliberação da Comissão, sempre que necessário;
  - Realizar a definição de controles para a gestão das identidades digitais de acesso ao ambiente lógico da Empresa RODA**;**
  - Aprovar os repositórios digitais e os dispositivos removíveis de armazenamento de informações para serem utilizados pelos colaboradores da Empresa RODA de acordo com a necessidade para a prestação de serviços da Instituição e os procedimentos de segurança da informação;
  - Avaliar a liberação da atividade relacionada a gravação de áudio, vídeo ou foto dentro das dependências, inclusive salas de reuniões, da Empresa RODA.

- **Tecnologia da Informação**
  - Registrar, armazenar e atualizar o inventário de hardwares e softwares;
  - Realizar a gestão e manutenção dos Recursos de TI de propriedade da Empresa RODA ou que estão sob sua responsabilidade;
  - Garantir que todos os Recursos de TI utilizados pela Empresa RODA atendam as recomendações de seus fabricantes ou desenvolvedores;
  -
  - Disponibilizar e realizar a gestão das identidades digitais de acesso ao ambiente lógico da Empresa RODA;
  - Realizar o registro e o monitoramento dos acessos aos ambientes lógicos da Empresa RODA;
  - Elaborar e manter procedimentos de salvaguarda das informações e dos dados necessários para recuperação dos sistemas da Empresa RODA;
  - Avaliar se os requisitos de segurança da informação e controles de acesso estão presentes antes da aquisição, manutenção ou desenvolvimento de softwares;
  - Garantir que o andamento e o resultado de uma mudança preservem os controles relacionados à disponibilidade, integridade, confidencialidade e autenticidade das informações;

- Apoiar para que os procedimentos de gestão da Continuidade de Negócios sejam executados em conformidade com os requisitos de segurança da informação;
- Aplicar no ambiente os controles de segurança definidos por procedimentos complementares;
- Definir, analisar e priorizar ações necessárias, balanceando custo e benefício.

- **Área de Recursos Humanos**
  - Garantir a publicidade e disponibilidade desta PSI da Empresa RODA;
  - Apoiar a área de segurança da informação na realização de campanhas de capacitação e divulgação da segurança da informação da Empresa RODA;
  - Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores;
  - Disponibilizar os documentos relacionados à Segurança da Informação aos colaboradores, além de custodiar e colher assinatura do "Termo de Ciência e Responsabilidade" na admissão de novos colaboradores;
  - Aplicar medidas disciplinares quando identificado responsabilidades dos envolvidos em Incidentes de segurança da informação.

- **Área Jurídica**
  - Validar previamente as minutas de contratos de trabalho e de prestação de serviços, a fim de atender aos controles de segurança da informação aplicáveis;
  - Validar contratos sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras da Empresa RODA;
  - Garantir que contratos possuem cláusulas que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade;
  - Apoiar o Departamento de Marketing, de Tecnologia da Informação e demais Departamentos com relação ao uso de obras intelectuais, softwares, desenhos industriais, marcas, identidade visual ou qualquer outro sinal distintivo atual ou futuro de propriedade da Empresa RODA;
  - Avaliar e publicar a política de segurança da informação e procedimentos complementares.

- **Departamento de Segurança Patrimonial**
  - Realizar o registro e o monitoramento dos acessos aos ambientes físicos da Empresa RODA;
  - Estabelecer perímetros de segurança para proteção de ativos tangíveis da Empresa RODA e implementar os controles necessários;
  - Realizar o controle de entrada e saída de equipamentos de acordo com o procedimento de segurança física da Empresa RODA.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- **Colaborador**
  - Estar ciente e manter-se atualizado com esta PSI e demais Procedimentos Complementares;
  - Conhecer e assinar os documentos disponibilizados pela Área de Recursos Humanos no momento da contratação e demais documentos disponibilizados pela empresa durante o período da prestação dos serviços;
  - Utilizar os ativos de propriedade da Empresa RODA ou sob sua responsabilidade de acordo com as orientações do fabricante, do desenvolvedor e da empresa, com cuidado e zelo, inclusive para resguardar o sigilo e a confidencialidade de informações, bem como a proteção de dados pessoais;
  - Utilizar os ativos e informações da Empresa RODA somente para fins profissionais e de forma ética e legal, respeitando os direitos e as permissões de uso concedidas, ainda que se valendo de provisão de conexão à internet e de dispositivos de TI próprios;
  - Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações acessadas ou manipuladas;
  - Zelar pela segurança da sua identidade digital, não compartilhando, divulgando ou transferindo a terceiros quaisquer de seus componentes;
  - Preservar a privacidade e a proteção de dados pessoais dos titulares de dados pessoais cujas informações são objetos de atividades de tratamento, nos termos da Lei;
  - Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais;

- **Gestor do Colaborador**
  - Garantir e gerenciar o cumprimento desta PSI e demais Procedimentos Complementares pelos seus colaboradores;
  - Identificar e medir as vulnerabilidades e ameaças nos processos e atividades de sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir os impactos ao negócio;
  - Garantir que os ativos de propriedade ou sob a responsabilidade da Empresa RODA sejam utilizados com cuidado e de acordo com as orientações do fabricante e da empresa;
  - Identificar incidentes de segurança de informação ou qualquer ação duvidosa praticada por seus colaboradores, comunicando-o para o DPO, imediatamente.

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

1. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade**: garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.
- **Integridade**: garantia de que as informações estejam fidedignas em relação à última alteração desejada durante o seu ciclo de vida.
  Disponibilidade: garantia de que as informações e os Recursos de Tecnologia da Informação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.
- **Autenticidade**: garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

1. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

- **Interpretação:** Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, as atividades que não estão tratadas nos normativos só devem ser realizadas após prévia e formal autorização da área de segurança da informação, podendo ser solicitado aprovação da Comissão de segurança da informação e do Diretor do Departamento, de acordo com a criticidade para o negócio.
- **Publicidade:** Esta PSI e seus documentos complementares devem ser divulgados aos colaboradores pela Área de Recursos Humanos com o apoio da área de segurança da informação, visando dar sua publicidade para todos que se relacionam profissionalmente com a Empresa RODA, de acordo com o Procedimento de Treinamento e Conscientização em Segurança da Informação da Empresa RODA.
- **Propriedade:** As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade ou estão sob a responsabilidade e direito de uso exclusivo da Empresa RODA**,** devendo ser empregadas unicamente para fins profissionais.
- **Propriedade Intelectual:** A utilização de obras intelectuais, softwares, desenhos industriais, marcas, identidade visual ou qualquer outro sinal distintivo atual ou futuro de propriedade da Empresa RODA em qualquer suporte, inclusive na Internet e mídias sociais, deve ser formal e previamente autorizada e vinculada as atividades profissionais.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- **Vedação à Pirataria:** É proibido ao colaborador instalar, utilizar, copiar, reproduzir, transmitir ou compartilhar software ou quaisquer conteúdos protegidos por Lei pelos Recursos de TI, devendo somente fazê-lo quando houver licença e esteja autorizado pelo departamento de Tecnologia da Informação e a área de segurança da informação.
    - É proibido o armazenamento ou reprodução de músicas, em formato MP3 ou similar, pelos Recursos de TI da Empresa RODA, sem a devida licença de uso.
- **Classificação da Informação:** Todas as informações de propriedade ou sob a responsabilidade da Empresa RODA devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida, de acordo com o Procedimento de Classificação da Informação.
- **Sigilo:** É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade da Empresa RODA, sem a prévia e formal autorização do Gestor da Informação, excetuando-se a hipótese de que a informação seja pública.
- **Preservação da Privacidade**: Em atendimento ao constante na legislação vigente, notadamente a Constituição Federal, o Código Civil (Lei Federal nº 10.406/2002), o Marco Civil da Internet (Lei Federal nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018) e o Decreto Federal nº 8.771/2016, a vida privada se mostra inviolável e a preservação da privacidade, como princípio na disciplina da internet no Brasil, a Empresa RODA e seus colaboradores devem assegurar e concorrer para sedimentar tais preceitos.
- **Proteção de Dados Pessoais**: Ao identificar a existência ou tratamento de Dados pessoais em novas atividades, demandas ou projetos da Empresa RODA, deve-se buscar a aderência dos deveres e respectivos princípios da Lei Federal nº 13.709/2018 (LGPD). Para cumprimento desta diretriz, deverão ser acionados os departamentos Jurídico, Segurança da Informação e respectivo ocupante do cargo de Encarregado de assuntos LGPD nomeado pela Empresa RODA. Ademais, a Empresa RODA deve garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte.
- **Uso dos Ativos:** Os ativos de propriedade ou sob a responsabilidade da Empresa RODA devem ser utilizados somente para fins profissionais e autorizados pelo Gestor do colaborador ou Diretor do Departamento, de acordo com a criticidade do ativo para o negócio.
- **Manutenção dos Ativos:** A gestão dos ativos na RODA deve atender às recomendações dos fabricantes ou desenvolvedores, sendo que qualquer necessidade de manutenção, atualização ou correção de falhas técnicas somente pode ser realizada pelas Áreas específicas da Empresa RODA, de acordo com o tipo de ativo.
    - **Inventário dos Ativos:** O Departamento de Tecnologia da Informação é responsável pelo registro, armazenamento e atualização do inventário de hardwares e softwares.
- **Uso dos Recursos de Tecnologia da Informação (Recursos de TI):** Os Recursos de TI de propriedade ou sob a responsabilidade da Empresa RODA devem ser utilizados apenas para fins profissionais, de modo lícito, ético e moral.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	Alterado e Revisado por:	Revisado por:	Total de Páginas:
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- **Dispositivos Móveis:** Os dispositivos móveis devem ser utilizados de acordo com as diretrizes:
    - **Dispositivos Móveis Corporativos:** Somente serão fornecidos pela Empresa RODA em razão da atividade ou função do colaborador para a Empresa RODA;
        - Aos colaboradores autorizados a utilizar dispositivos móveis particulares para uso corporativo, é permitida a troca de informações corporativas desde que atendidas as condições previstas no Procedimento de Classificação da Informação.
    - **Dispositivos Móveis Particulares para uso Corporativo:** Somente quando prévia e expressamente autorizado pelo Diretor do colaborador e pela área de segurança da informação, conforme as necessidades do negócio.

Aplicativos de Comunicação Instantânea: Somente é permitido o uso de aplicativos de comunicação instantânea homologados pelo Departamento de Tecnologia da Informação para troca de informações corporativas.

Repositórios Digitais e Dispositivos Removíveis: É vedado aos colaboradores o uso de repositórios digitais ou dispositivos removíveis não aprovados pela área de segurança da informação para armazenar ou transmitir informações de propriedade ou sob a responsabilidade da Empresa RODA.

Ambientes Lógicos: Os sistemas e Recursos de TI que suportam os processos e as informações da Empresa RODA devem ser confiáveis, íntegros, seguros e disponíveis a quem deles necessitem para execução de suas atividades profissionais.

- Para garantir a segurança acima estabelecida, o Departamento de Tecnologia da Informação deve contar com sistemas de proteção, sempre ativos e atualizados:
    i. Contra programas maliciosos e acessos indevidos, como antivírus e firewall;
    ii. Para indicar tentativas de intrusão realizada aos ambientes lógicos, como Sistemas de Detecção a Intrusão IPS (Intrusion Protection Systems);
    iii. Contra mensagens eletrônicas indesejadas ou não autorizadas, como *AntiSpam;*
    iv. Filtro de conteúdo para controle de acesso a páginas indevidas, como Proxy ou URL *Filtering.*
- Em situações de trabalho remoto e de utilização de infraestrutura que não da Empresa RODA (dos próprios colaboradores ou de terceiros), o Departamento de Tecnologia da Informação deverá disponibilizar uma Rede Virtual Privada (“VPN”) e/ou nuvem (“Cloud”), dotadas dos meios técnicos hábeis a garantir uma maior segurança apta a manter a confidencialidade, integridade e sigilo das informações comerciais, principalmente para cenários de trabalho remoto, a fim de que os colaboradores se conectem à rede interna.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- **Ambientes Físicos:** O Departamento de Segurança Patrimonial deve estabelecer perímetros de segurança para proteção de seus ativos tangíveis, além de:
  i. Implementar controles de identificação e registro antes do acesso aos seus ambientes físicos, constando data, hora e área onde será realizado o acesso;
  ii. Manter portas, janelas, gavetas e armários trancados;
  iii. Implementar segurança patrimonial, câmeras, alarmes e fechaduras;
  iv. Garantir que instalações críticas sejam localizadas de modo mais restrito.
- **Aquisição, Desenvolvimento e Manutenção de Software:** O desenvolvimento interno e/ou externo de softwares, assim como a sua aquisição no mercado, devem garantir o cumprimento dos requisitos de segurança da informação e controles de acesso, além de serem realizadas somente pelas Áreas do Departamento de Tecnologia da Informação responsáveis por sistemas e infraestrutura com o apoio da área de segurança da informação.
- **Salvaguarda (*backup*):** O Departamento de Tecnologia da Informação deve manter um processo de salvaguarda das informações e dos dados necessários para completa recuperação dos seus sistemas (backup), além de testes periódicos de recuperação, nos termos do Procedimento de *Backup* e *Restore*, a fim de atender os requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes, ou sua recuperação o mais rápido possível.
- **Documentação: a Empresa** RODA deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam seus Recursos de TI, com periodicidade mínima de revisão de seus procedimentos.
- **Gestão de Mudança:** Toda mudança que impactar o ambiente deve ser realizada somente após aprovação da área de segurança da informação para preservação dos controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações.
- **Comitê de Mudanças Emergenciais**: a Empresa RODA deve estabelecer o Comitê para Execução de Mudanças Emergenciais, sendo responsável pela avaliação de riscos e autorização das mudanças emergenciais que, se não implementadas a curto prazo, podem incorrer em risco para a Empresa RODA.
- **Análise dos Processos e Recursos de TI:** Os Gestores de Áreas e Departamentos da Empresa RODA devem analisar seus processos e ativos em intervalos regulares, zelando para que estejam devidamente inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança mapeadas.
- **Gestão de Risco:** A área de segurança da informação deve identificar e avaliar os riscos relacionados à Segurança da informação e adotar as melhores práticas para o seu gerenciamento de acordo com o procedimento de gestão de riscos.
- **Continuidade do Negócio:** Os procedimentos de gestão da Continuidade de Negócios devem ser executados em conformidade com os requisitos de segurança da informação. Sua execução deve ser realizada pelo Departamento de Tecnologia da Informação e com o apoio da área de segurança da informação, para garantir a proteção das informações e dos ativos críticos da Empresa RODA.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	Alterado e Revisado por:	Revisado por:	Total de Páginas:
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- **Contratação de Colaboradores e Terceiros (Fornecedores de Bens e Prestadores de Serviços):** As contratações em que ocorra o compartilhamento de informações de propriedade ou sob a responsabilidade da Empresa RODA ou a concessão de acesso aos seus ambientes ou ativos, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à segurança da informação, além de preverem a realização de auditorias eventuais ou periódicas para certificar a conformidade com a PSI e seus documentos complementares.
- **Comunicação de Incidentes: a Empresa** RODA possui um canal de comunicação divulgado aos seus colaboradores para reportar imediatamente os possíveis casos de incidentes de segurança da informação.
- **Dúvidas:** Qualquer dúvida relativa a esta PSI deve ser encaminhada à área de Segurança da Informação.
- **Monitoramento:** Os ambientes físicos e lógicos da Empresa RODA devem ser monitorados visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.
- **Auditoria e Inspeção:** Os Recursos de TI que estiverem nas dependências da Empresa RODA ou que interajam com seus ambientes podem ser auditados ou inspecionados sempre que necessário, atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores.
- **Capacitação**: A Área de segurança da informação, com o apoio da área Recursos Humanos deve estabelecer um plano anual de capacitação direcionado ao desenvolvimento e manutenção das habilidades dos colaboradores sobre segurança da informação, nos termos do Procedimento de Treinamento e Conscientização em Segurança da Informação.
- **Exceções:** As exceções que ocorram de forma exclusiva e excepcional a essa PSI e demais Procedimentos Complementares devem ser formalizadas e fundamentadas pelo Gestor da Área Solicitante, analisadas pela área de segurança da informação e aprovadas pela Comissão e pelo Diretor de Tecnologia da Informação, que poderá, a qualquer tempo, revogá-las.

1. Uso de Dispositivos pessoais

- O uso de um dispositivo próprio para o desenvolvimento das atividades laborais está sujeito aos termos e condições da presente Política de Segurança da Informação. Tal dispositivo deverá ser utilizado de maneira ética.
- Os colaboradores devem respeitar a confidencialidade das informações da Empresa RODA acessadas por meio de seu dispositivo pessoal, sendo de sua responsabilidade, protegê-las contra o comprometimento, acesso não autorizado etc., prezando-se sempre pela manutenção da autenticidade, confidencialidade, integridade e segurança de seus recursos de TIs.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

1. Dados Pessoais compartilhados e/ou armazenados nos dispositivos

- Dados e informações pessoais trocados entre os Colaboradores e a Empresa RODA, em decorrência do uso de dispositivos pessoais e para as finalidades aqui previstas, estão sujeitos às disposições da Lei Federal nº 13.709/2018 (“LGPD”), bem como as demais normativas concernentes à preservação da privacidade e à proteção de dados pessoais. Também, o tratamento de dados pessoais (nos termos do Art. 5º, inciso X, LGPD) deverá estar em conformidade com os princípios de proteção de dados e legitimado por uma base legal, dispostas nos artigos 7º e 11 da LGPD.
- a Empresa RODA cumpre e continuará a cumprir suas obrigações decorrentes das leis e normas aplicáveis versando sobre preservação da privacidade e proteção de dados pessoais, especialmente a LGPD, a Lei Federal nº 12.965/2014 (“Marco Civil da Internet”) e o Decreto Federal nº 8.771/2016.
- Os Colaboradores que, no exercício de suas funções, tenham acesso aos dados pessoais de clientes, funcionários e demais informações confidenciais no contexto das atividades da Empresa RODA, comprometem-se a não usá-los para fins diversos daquele para os quais o tratamento é expressamente autorizado.
    - Sempre que os Colaboradores utilizarem dados pessoais acessados por meio de seus dispositivos pessoais, estes se obrigam a respeitar todas as políticas da Empresa RODA, devendo se abster de extrair, copiar, compartilhar, transmitir ou publicar qualquer dado relativo a pessoas naturais, inclusive dados pessoais relacionados a outros colaboradores, fornecedores.
    - Os Colaboradores têm conhecimento acerca da obrigação de sigilo profissional referente a dados de clientes, colaboradores e demais informações confidenciais as quais tenham autorização de acesso no exercício de suas funções, assim como o dever de guarda e cumprimento de obrigações e deveres adotados pela Empresa RODA, quanto ao tratamento de dados pessoais, em razão de leis e normas aplicáveis.
    - Os Colaboradores reconhecem que, em caso de descumprimento culpável de sua parte, responderão por quaisquer perdas ou danos causados a Empresa RODA, no tocante a obrigações relativas à proteção de dados pessoais dispostas na presente Política – incluindo, mas não se limitando a casos em que houver eventual acesso não autorizado ou indevido, vazamento ou perda de dados.

1. MEDIDAS DISCIPLINARES

Os incidentes de segurança da informação identificados devem ser avaliados pela área de segurança da informação, que, após análise, poderá apurar as responsabilidades dos envolvidos em procedimento disciplinar, visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.
A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

1. DISPOSIÇÕES FINAIS

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com a Política e Procedimentos aplicáveis pela Empresa RODA.

Qualquer dúvida relativa a esta PSI deve ser encaminhada à área de segurança da informação da Empresa RODA**.**

Esta PSI entra em vigor na data de sua publicação.

1. REVISÃO E ATUALIZAÇÃO

Esta **Política** deve ser revista e atualizada em intervalos não superiores a 01 (um) ano ou sempre que as atividades previstas modificarem.

1. DEFINIÇÕES

- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano a Empresa RODA.
- **Aplicativos de Comunicação Instantânea:** conjunto de código e instruções compiladas, executadas ou interpretadas por um Recurso de Tecnologia da Informação, hospedadas em um dispositivo ou na nuvem, usada para troca rápida de mensagens, conteúdos e informações multimídia.
- **Ativo:** qualquer coisa que tenha valor para a Empresa RODA e precisa ser adequadamente protegido.
- **Ativo Intangível:** todo elemento que possui valor para a Empresa RODA e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à reputação, imagem, marca e conhecimento.
- **Autenticidade:** garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.
- ***Backup* ou Salvaguarda:** salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada da Empresa RODA.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- **Colaborador:** empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venham a ter relacionamento profissional, direta ou indiretamente, com a Empresa RODA.
- **Confidencialidade:** garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.
- **Dados Pessoais:** informação relacionada a pessoa natural identificada ou identificável. Exemplo: nome, CPF, endereço, dados de GPS, hábitos de consumo, identificadores eletrônicos, etc.;
- **Disponibilidade:** garantia de que as informações e os Recursos de Tecnologia da Informação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.
- **Dispositivos Móveis:** equipamentos que podem ser facilmente transportados devido a sua portabilidade, com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexões com a Internet e outros sistemas, redes ou qualquer dispositivo.
- **Dispositivos Removíveis de Armazenamento de Informação:** dispositivos capazes de armazenar informações que pode ser removida do equipamento, possibilitando a portabilidade dos dados, como CD, DVD e pen drive.

- **Encarregado (LGPD):** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- **Gestor da informação:** diretor ou gestor de Área/Departamento responsável pela criação, classificação, divulgação, compartilhamento e destruição da informação, tomando por base as premissas empresariais e importância dos dados em questão, assim como sua revisão periódica, validação, liberação e cancelamento dos acessos.
- **Identidade Digital:** é a identificação do colaborador em ambientes lógicos, sendo composta por seu login e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.
- **Informação:** é o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.
- **Integridade:** garantia de que as informações estejam fidedignas em relação à última alteração desejada durante o seu ciclo de vida.
- **Legalidade:** garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.
- **LGPD –** Lei Geral de Proteção de Dados Pessoais. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Data de Criação	Elaborado por:	Aprovado por:	Número da Revisão:
03/08/2022	**BRUNA LINS** Tecnologia da Informação	**TATI WONG** Diretora Executiva	**02**
Data da Última Revisão	**Alterado e Revisado por:**	**Revisado por:**	**Total de Páginas:**
08/03/2024	**ADEMAR COIMBRA** Tecnologia da Informação	**MARCOS FRIOL** Tecnologia da Informação	**14**

- **PSI:** Política de Segurança da Informação.
- **Recursos de Tecnologia da Informação (Recursos de TI):** hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.
- **Repositórios Digitais (*Cyberlockers*):** plataformas de armazenamento na Internet, a exemplo, mas não se limitando ao Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd.
- **Risco:** combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos;
- **Segurança da Informação:** é a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.
- **SGSI:** Sistema de Gestão de Segurança da Informação.
- **Tentativa de Burla:** fazer esforços para não respeitar ou tentar violar as diretrizes estabelecidas nos normativos da Empresa RODA.
- **Tratamento de dados pessoais:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- **Violação:** qualquer atividade que desrespeite as regras estabelecidas nos normativos da Empresa RODA.