ROiT

CONHEÇA NOSSA POLÍTICA OPERACIONAL

de segurança da informação (PSI).

e contribua para construirmos uma empresa e uma sociedade mais seguras.

Considerando o aumento dos riscos e das ameaças que impactam a proteção de dados e ativos informacionais, a Segurança da Informação (SI) tornou-se de importância estratégica para o **Grupo ROIT.**

O compromisso da Alta Direção e de toda a liderança do **Grupo ROIT** com a Segurança da Informação é inegociável e constitui um pilar fundamental para a sustentabilidade e a integridade de nossos negócios.

Dessa forma, o **Grupo ROIT** elaborou este documento como expressão de seu compromisso com a transparência e o aprimoramento contínuo da cultura de segurança da informação, disponibilizando diretrizes objetivas que visam servir de referência para clientes, parceiros de negócios e o mercado em geral.

Lucas Ribeiro Fundador e CEO da **ROIT.**

VOCÊ SABE O QUE É

SEGURANÇA DA INFORMAÇÃO?

É a garantia da **CONFIDENCIALIDADE**, da **INTEGRIDADE** e da **DISPONIBILIDADE** das informações.

A **SEGURANÇA DA INFORMAÇÃO** é importante para proteger as informações de negócio e a nossa propriedade intelectual, que é tudo aquilo que criamos enquanto trabalhamos aqui.

As informações corporativas pertencem à empresa e aqui devem permanecer; isso é vital para preservar a nossa segurança, as nossas operações e à nossa competitividade.

Também é importante proteger a **SEGURANÇA** das informações que os nossos clientes e outras partes interessadas nos fornecem e arquivos que eles utilizam através nossos produtos e serviços.

ELEMENTOS DA **SEGURANÇA DA INFORMAÇÃO?**

CONFIDENCIALIDADE

Propriedade da informação não ser tornada disponível ou divulgada a indivíduos, entidades ou processos não autorizados.

INTEGRIDADE

Propriedade de acuracidade e completeza da informação.

DISPONIBILIDADE

Propriedade de a informação ser acessível e utilizável sob demanda de uma entidade autorizada.

Esta política define as REGRAS GERAIS e COMPORTAMENTOS DE SEGURANÇA esperados dos **ROITERS.**

TODOS devem seguir essas regras.

Esta Política faz parte do nosso **Sistema de Gestão de Segurança da Informação (SGSI)**

Esta Política deve ser divulgada a todos os colaboradores, prestadores de serviços, estagiários e demais públicos relacionados, bem como disponibilizada no site institucional.

ESTA POLÍTICA FOI CONSTRUÍDA COM BASE EM ALGUMAS PREMISSAS IMPORTANTES:

- **As necessidades de segurança da nossa empresa.**
- **A Norma ISO / IEC 27001:2022, que é um padrão internacional para gestão da segurança da informação.**
- **As boas práticas de segurança consagradas no mercado.**

VAMOS CONHECER
NOSSAS REGRAS?

CONTEÚDO DESSA POLÍTICA

- Responsabilidades
- Iniciando as atividades
- Uso das informações corporativas
- Cuidando dos dispositivos de trabalho
- Cuidando das credenciais de acesso
- Uso de mídias removíveis
- Uso de e-mail e aplicativos de mensagens
- Uso da internet e compartilhamento de conteúdo
- Segurança no trabalho remoto
- Uso seguro de redes e pastas de rede
- Mesa limpa, tela limpa e impressão segura
- Reportando eventos e incidentes de segurança
- Educação e conscientização em SI
- Medidas disciplinares
- Uso de Inteligência Artificial (IA)
- Uso Seguro de Softwares

RESPONSABILIDADES

Para que esta política seja eficaz, cada um tem um pedacinho de responsabilidades sobre ela:

ROITER (você mesmo!):
Cumprir as regras determinadas nesta e em outras políticas, procedimentos e normas estabelecidas pela **ROIT.**

Time de SI:
Cuida do ciclo de vida deste documento (publicação e controle de revisões).

Este time é composto pelo CTO, Analista Jurídico e Analista de Infraestrutura.

CEO Lucas Ribeiro:
é ele quem aprova essa política!

Comitê de Segurança da Informação (CSI):
Este comitê é responsável por criar, comunicar e zelar pelo cumprimento desta e de outras políticas, procedimentos e normas de SI (Segurança da Informação) na empresa. Ah, e se for constatada alguma violação de segurança, é ele quem analisa o caso e determina as medidas a serem tomadas!

O Comitê é formado pelo CTO, COO, Analista Jurídico, Analista de Infraestrutura e Gerente de Pessoas.

INICIANDO AS ATIVIDADES

Ao entrar aqui na ROIT, você recebe tudo o que você precisa para iniciar as suas atividades:

Dispositivos móveis de trabalho:

Laptop, desktop, telefone celular ou tablets, de acordo com a necessidade de sua função.
Os dispositivos possuem todas as configurações de segurança necessárias e você deve zelar pelo cuidado dos equipamentos sob sua guarda.

Você deve devolver os dispositivos sob sua guarda, caso encerre seu contrato de trabalho.

Credenciais de acesso: você recebeu uma identidade funcional, que inclui:

Credenciais de acesso físico: crachá ou identificação biométrica.

Endereço de e-mail: o básico para você acessar as informações e recursos necessários para o seu trabalho.

Senhas: informações secretas, individuais e intransferíveis que você utiliza para acessar as informações e recursos necessários para o seu trabalho.

Permissões de acesso: você terá acesso a um conjunto mínimo de permissões, necessárias para que você execute seu trabalho.

Onboarding: você recebeu um treinamento básico sobre a **ROIT** e as políticas, regras e procedimentos que você deve cumprir, incluindo esta Política de Segurança.

USO DAS INFORMAÇÕES CORPORATIVAS

Toda e qualquer informação pertencente à empresa deve ser tratada com cuidado.

Propriedade Intelectual: Toda informação, em meio físico ou digital criada, processada, armazenada, acessada, compartilhada ou descartada dentro do ambiente corporativo pertence à **ROIT** e deve ser utilizada apenas para fins profissionais. Isto se chama propriedade intelectual.

Praticamos o princípio do *need to know*, o que significa que você tem acesso somente às informações mínimas e necessárias para executar o seu trabalho. Também classificamos as informações como **públicas**, **internas** e **confidenciais**. Mas, na dúvida, trate a informação como **confidencial.**

O QUE VOCÊ DEVE FAZER

- Utilizar as informações corporativas apenas para executar seu trabalho.
- Zelar pela confidencialidade das informações, não as expondo sob qualquer circunstância.
- Trocar ou transferir informações somente com pessoas ou entidades autorizadas, de acordo com os relacionamentos esperados com outras partes interessadas (clientes, funcionários, fornecedores, etc).

O QUE NÃO É PERMITIDO

- Extrair informações corporativas para qualquer tipo de armazenamento externo, dispositivo pessoal, contas de e-mail pessoal, entre outras situações.

CUIDANDO DOS DISPOSITIVOS DE TRABALHO

Laptops, desktops, celulares, tablets, tokens, etc.

O QUE VOCÊ DEVE FAZER

- Utilizar os dispositivos para cumprir com suas atividades profissionais.
- Zelar pela preservação e guarda do dispositivo sob sua responsabilidade.
- Cuidar da segurança física do seu dispositivo, informando a ROIT em caso de dano, perda ou roubo.
- Assinar o termo de responsabilidade pelo dispositivo.

O QUE NÃO É PERMITIDO

- Extrair informações corporativas para qualquer tipo de armazenamento externo, dispositivo pessoal, contas de e-mail pessoal, entre outras situações.

SOBRE OS DISPOSITIVOS BYOD (BRING YOUR OWN DEVICE)

- Algumas pessoas utilizam laptop pessoal para trabalhar, mediante autorização prévia, em caráter de exceção. Para os **ROITERS** em geral, a **ROIT** fornece os equipamentos de trabalho de acordo com a necessidade de cada time. Você poderá utilizar seu celular pessoal apenas para aplicativos de colaboração corporativos e ferramentas de autenticação.
- A **ROIT** não se responsabiliza por qualquer dispositivo pessoal utilizado no trabalho.
- A **ROIT** se reserva o direito de instalar softwares de segurança em seu dispositivo, para sua própria proteção e proteção da **ROIT.**

CUIDANDO DAS CREDENCIAIS DE ACESSO

Nomes de usuário, senhas, tokens, etc.

O QUE VOCÊ DEVE FAZER

- Zelar pela preservação da confidencialidade das suas credenciais de acesso, incluindo dispositivos físicos de acesso (como tokens físicos).
- Utilizar suas credenciais apenas para realizar suas atividades profissionais e dentro dos horários de trabalho permitidos.
- Utilizar senhas fortes e múltiplo fator de autenticação, sempre que esses recursos forem disponibilizados pela ROIT e renovar suas credenciais sempre que isso for solicitado.
- Usar gerenciador de senha corporativo para consulta de logins e senhas de acessos compartilhados.

O QUE NÃO É PERMITIDO

- Escrever ou guardar lembretes de nomes de usuários e senhas, em nenhum lugar inseguro (físico ou digital).
- Compartilhar com qualquer pessoa, credenciais de acesso nominais, por qualquer meio.
- Compartilhar senhas não nominais em locais diferentes do nosso cofre de senhas corporativo.

Lembre-se: você é o único responsável pelas atividades realizadas através de suas credenciais.

USO DE MÍDIAS REMOVÍVEIS

Pen drives, armazenamento em celular, drives externos, etc.

O QUE VOCÊ DEVE FAZER

- Utilizar mídias removíveis de acordo com as necessidades de suas atividades profissionais.

O QUE NÃO É PERMITIDO

- Utilizar qualquer mídia removível para fazer cópias pessoas de arquivos e informações **ROIT**, independentemente de sua classificação.

USO SEGURO DE SOFTWARES

É expressamente **proibido** o uso de *Softwares* ou Sistemas não homologados pelo **Comitê de Segurança da Informação.**

O QUE VOCÊ DEVE FAZER

- Utilize apenas softwares ou sistemas homologados pelo Comitê de Segurança da Informação.
- Baixe arquivos e programas apenas de fontes oficiais e autorizadas pela **ROIT.**
- Solicite a homologação via canais oficiais caso precise de uma nova ferramenta.

O QUE NÃO É PERMITIDO

- Fazer *download* de softwares, executáveis ou extensões não homologados.
- Utilizar ferramentas não homologadas fora do ambiente de teste autorizado.
- Burlar o bloqueio padrão de *download* e instalação das máquinas.

USO DE E-MAIL E APLICATIVOS DE MENSAGENS

Permissões e restrições.

Dispositivos móveis de trabalho: laptop, desktop, telefone celular ou tablets, de acordo com a necessidade da sua função. Os dispositivos possuem todas as configurações de segurança necessárias e você deve zelar pelo cuidado dos equipamentos sob sua guarda. Você deve devolver os dispositivos sob sua guarda, caso encerre seu contrato de trabalho.

O QUE VOCÊ DEVE FAZER

- Enviar e-mails apenas para destinatários autorizados, dentro dos relacionamentos esperados no seu trabalho (colaboradores, clientes, fornecedores, etc)
- Estar atento às ameaças digitais que podem usar o e-mail e aplicativos de mensagens como porta de entrada, como ataques de engenharia social (*phishing*, envio de arquivos maliciosos, etc)
- Reportar situações suspeitas de pessoas usando ou tentando usar o e-mail corporativo ou pessoal.

O QUE NÃO É PERMITIDO

- Utilizar o e-mail corporativo para assuntos pessoais e o e-mail pessoal para assuntos corporativos.
- Encaminhar mensagens de e-mail corporativo para endereços de e-mails pessoais.
- Compartilhar quaisquer arquivos da **ROIT** e/ou informações confidenciais em aplicativos de mensagens (ex. whatsapp, telegram, entre outras).
- Compartilhar conteúdo impróprio (ilegal, de cunho sexual, discriminatório, racista, piratas, streaming de fins não profissionais, violência, jogos e outros).

USO DA INTERNET E COMPARTILHAMENTO DE CONTEÚDO

A internet deve ser usada com bom senso e não se deve acessar ou compartilhar conteúdo impróprio.

O uso da internet é permitido para fins profissionais e pessoais, respeitando-se o bom senso. A **ROIT** se reserva o direito de monitorar o acesso à internet.

A divulgação de informações da empresa ou sobre a empresa em sites públicos ou redes sociais não é permitida por padrão; a autorização é restrita ao **CEO**, à equipe de **Marketing** e ao **Employee Experience.** No caso dos **ROITERS**, é permitido apenas repostar/compartilhar o conteúdo oficial, sem realizar quaisquer alterações em seu teor original.

O QUE VOCÊ DEVE FAZER

- Caso necessário, os arquivos relevantes ao cliente ou terceiro devem ser compartilhados exclusivamente por meio de Drive Compartilhado (Google Drive).
- Acessar apenas os websites autorizados pela empresa.
- Caso precise acessar um site bloqueado pelos nossos filtros de conteúdo, solicitar este acesso através de chamado específico, justificando sua necessidade.
- Reportar situações suspeitas de pessoas usando ou tentando usar internet, sites públicos ou redes sociais.
- Certifique-se de que suas ações estejam em conformidade com os interesses da **ROIT**, evitando qualquer conduta que possa causar prejuízo ou expor a organização a riscos.

O QUE NÃO É PERMITIDO

- Acessar sistemas bancários; acessar ou compartilhar conteúdo impróprio (ilegal, de cunho sexual, discriminatório, racista, piratas, violência, mineração de criptomoedas, fake news, spam, malware, jogos de azar e atividades fraudulentas).
- Compartilhar qualquer informação interna ou confidencial da empresa em sites públicos ou redes sociais que não tenha sido expressamente autorizada. Isso inclui textos, imagens, vídeos ou áudios feitos dentro do ambiente de trabalho contendo imagens de telas de computador, por exemplo.

USO DE INTELIGÊNCIA ARTIFICIAL (IA)

Os **ROITERS** podem utilizar *insights* da **IA** em suas atividades, mas devem sempre avaliar criticamente as respostas antes de aplicá-las. A **ROIT** se reserva o direito de monitorar o uso de qualquer ferramenta em seu ambiente corporativo.

O uso de Inteligência Artificial (IA) deve ser restrito exclusivamente às ferramentas previamente **homologadas.** Qualquer ferramenta não homologada deve ser submetida para avaliação e somente poderá ser utilizada após aprovação formal do **CSI.**

Além disso, o uso de IA deve ser feito com bom senso e **nunca** deve envolver informações confidenciais ou sensíveis.

O QUE VOCÊ DEVE FAZER

- Validar e revisar as respostas da IA antes de aplicá-las em decisões ou documentos oficiais.
- Usar informações fictícias ou anonimizadas em exemplos e testes.
- Utilizar exclusivamente contas corporativas e ambientes previamente autorizados para o acesso à IA, conforme homologação do Time de SI. Consultar a lista atualizada de contas e ambientes permitidos.
- Reportar incidentes de segurança ou suspeitas de vazamento ao time de SI.

O QUE NÃO É PERMITIDO

- Compartilhar informações confidenciais (senhas, chaves de API, dados da ROIT ou de clientes, documentos sigilosos, etc.).
- Copiar e colar diretamente conteúdo sensível de sistemas internos em chats de IA.
- Confiar cegamente nas respostas da IA sem análise crítica ou validação.
- Usar contas pessoais para tratar informações relacionadas ao trabalho.
- Violar ou contornar políticas internas de SI para uso não autorizado de IA.

SEGURANÇA NO TRABALHO REMOTO

Orientações gerais e cuidados no acesso remoto a recursos computacionais.

O QUE VOCÊ DEVE FAZER

- Acessar os recursos de trabalho por meio de dispositivo autorizado.
- Conectar-se a redes, sistemas e aplicações por meio de canal seguro (VPN, conexões https, etc).
- Utilizar os processos de autenticação segura (múltiplo fator de autenticação - MFA) sempre que estiverem disponíveis.
- Atentar para a segurança do ambiente físico de trabalho remoto: lugar reservado, silencioso e bem iluminado; posição de trabalho que evite ou minimize o contato visual de terceiros com a tela do dispositivo; uso de fones de ouvido para preservar a confidencialidade das informações; essas mesmas regras valem para quando o trabalho remoto estiver sendo executado em lugares públicos.

Sempre que você estiver em trabalho remoto, deve zelar pela segurança da informação em seu ambiente de trabalho.

O QUE NÃO É PERMITIDO

- Acessar redes públicas suspeitas como meio de acesso a sistemas, aplicações e websites.
- Desabilitar os softwares de segurança de seus dispositivos, incluindo VPN, antivírus e outros.

USO SEGURO DE REDES E PASTAS DE REDE

Restrição de acesso a informações
Segregação de redes

As redes de dados utilizadas pela **ROIT** de qualquer natureza (incluindo wifi) são protegidas por mecanismos de segurança apropriados, como por exemplo, firewalls, software antivírus, EDR, IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems), DLP (Data Loss Preventions), entre outros.

Os ambientes de rede são segregados e o acesso às redes e pastas da rede são restritos de acordo com políticas de grupo. Cada colaborador acessa apenas as informações que precisa para realizar o seu trabalho.

A **ROIT** se reserva o direito de monitorar o acesso às redes e serviços de rede.

O QUE VOCÊ DEVE FAZER

- Acessar os recursos de rede apenas para fins profissionais.
- Armazenar os arquivos de trabalho nas pastas de rede liberadas para seu uso.

O QUE NÃO É PERMITIDO

- Armazenar arquivos de trabalho de forma permanente no disco de armazenamento, local do dispositivo (com exceção de código fonte desenvolvido em IDEs locais, antes do envio para o repositório de códigos-fontes).

MESA LIMPA, TELA LIMPA E IMPRESSÃO SEGURA

Cuidados para não expor informações confidenciais ou sensíveis.

Nos locais de trabalho presencial, alguns setores possuem armários e cofres para guarda de documentos impressos. Você não deve deixar documentos internos ou confidenciais expostos.

Quando imprimir um documento, o **ROITER** deve dirigir-se imediatamente ao local onde a impressão foi feita para retirá-la.

Por padrão, os dispositivos corporativos possuem configurações de **bloqueio automático de tela**, após tempo inativo.

O QUE VOCÊ DEVE FAZER

- Bloquear (Win + L) ou abaixar a tela de seu dispositivo sempre que se afastar dele.
- Descartar qualquer mídia impressa de forma segura (triturar, rasgar, cortar, tornar ilegível).
- Retirar imediatamente qualquer documento enviado para impressão.

O QUE NÃO É PERMITIDO

- Quando afastado de seu dispositivo, deixar a tela aberta ou com conteúdo exposto.
- Quando ausente, deixar mídias impressas contendo informações confidenciais / sensíveis expostas.
- Deixar com papel-rascunho qualquer mídia impressa contendo informação confidencial ou sensível.
- Desabilitar as configurações de bloqueio automático de tela (suspensão/desativar tela).

REPORTANDO EVENTOS E INCIDENTES DE SEGURANÇA

Nossa atenção plena ajuda a proteger a empresa e as pessoas.

Sempre que você notar um comportamento estranho de qualquer pessoa, que pareça ou esteja violando qualquer regra de segurança, deve reportar isso através de canais apropriados via sistema de abertura de chamados ou através do e-mail **csi@roit.com.br**.

O QUE VOCÊ DEVE FAZER

- Discretamente, observe o potencial incidente ou violação.
- Reporte o fato para o time de segurança da informação.
- Caso tenha recebido ou clicado em um arquivo malicioso, reporte imediatamente ao time de Infraestrutura / SI.
- Caso algum agente malicioso tente fazer contato com você, não faça nada e reporte o fato para o time de SI.
- Preserve qualquer informação que possa servir como evidência.

O QUE NÃO É PERMITIDO

- Ocultar potenciais incidentes ou ameaças.
- Omitir-se no caso de observar comportamentos suspeitos.
- Desfazer-se de qualquer potencial evidência de ameaça ou incidente de segurança.

EDUCAÇÃO E CONSCIENTIZAÇÃO EM SI

O elo mais forte da segurança precisa ser o humano.

A **ROIT** fornece treinamentos recorrentes em SI para seus colaboradores e partes interessadas relevantes, como apropriado.

Esses treinamentos incluem:

***Onboarding*:** treinamento inicial para novos colaboradores ou terceiros.

Treinamentos regulares: pílulas de conhecimento sobre temas relevantes em SI.

O QUE VOCÊ DEVE FAZER

- Participar de **todos** os treinamentos que forem atribuídos a você.
- Adotar os comportamentos seguros explicados nesta e em outras políticas de SI da **ROIT**.

O QUE NÃO É PERMITIDO

- Ignorar as campanhas de treinamento e conscientização.

MEDIDAS DISCIPLINARES

O que acontece caso alguma violação de segurança seja cometida?

A **ROIT** pode aplicar sanções disciplinares caso seja constatada a violação das regras estabelecidas nas políticas, procedimento e normas de SI. Estas sanções podem ser dos seguintes tipos, dependendo da gravidade ou reincidência:

- Orientação e Treinamentos
- Advertência por escrito
- Rescisão contratual
- Advertência verbal
- Suspensão disciplinar

A **ROIT** ainda se reserva o direito de monitorar as atividades dos **ROITERS** enquanto exercendo suas atividades profissionais; para isso, não há expectativa de privacidade por parte dos **ROITERS**.

Para não se sujeitar a uma sanção disciplinar, CONHEÇA e PRATIQUE todas as regras de segurança da **ROIT**!

CASOS OMISSOS

AQUILO QUE NÃO É EXPRESSAMENTE PERMITIDO É IMPLICITAMENTE PROIBIDO.

Caso você tenha dúvidas sobre qualquer regra expressa nesta política ou queira discutir situações descritas, procure o comitê de SI.

HISTÓRICO DE REVISÕES:

Versão	Data	Alteração	Elaborado por:	Aprovado por:
1.0	22/03/2024	Primeira Versão.	CSI	CEO
2.0	02/05/2025	Adequação da política: (i) Inclusão do Selo de Classificação e Versionamento; (ii) Alteração na política sobre uso da Internet e softwares; (iii) Inclusão da mensagem do CEO sobre política estratégica de SI; (iv) Ajuste de membros do Comitê de SI; (v) Definição sobre divulgação da política.	CSI	CEO
3.0	30/10/2025	Adequação da política: Uso de Inteligência Artificial.	CSI	CEO
4.0	11/05/2026	Adequação da política: (i) Uso Seguro de Software; (ii) Atualização das medidas disciplinares; (iii) Atualização membros do Comitê.	CSI	CEO