Documento	**OT – 001 - Política de Segurança da Informação**	
Classificação	**Pública**	
Referência Normativa: ISO 27001 e ISO 27701		**Versão:** 16
Autor: Gerente de Segurança da informação	**Aprovação:** Diretoria de Segurança da Informação	**Efetivada em:** 03/05/2026

Política de segurança da informação da Ótima

Mensagem do Ceo,

Um dos pilares que alicerçam a Ótima é a confiança. Nossos clientes e parceiros confiam em nós, e a Ótima confia em você. Por isso vista essa camisa, e transmita confiança em suas atitudes. Sempre que uma decisão relacionada a compliance e privacidade de dados internos da Ótima, trate o assunto com a mais alta confiabilidade e profissionalismo.
Vamos juntos construir e manter uma imagem que inspire confiança.

Thiago Silva
CEO

1. Objetivo

Os objetivos de Segurança da Informação visam fortalecer continuamente o SGSI, reduzir a exposição aos riscos, aumentar a resiliência operacional, proteger os dados pessoais e apoiar os objetivos estratégicos da organização.

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade da informação necessária para a realização da continuidade de seus serviços e atividades em seus negócios traçando assim as diretrizes de segurança da informação, praticadas pela empresa e seus colaboradores. Compõem o número empresarial Ótima as seguintes empresas: Ótima digital ltda (cnpj: 34.753.151/0001-32) rua: benjamin constant,96 sala 09 jardim independência – Ituverava SP cep: 14500-00 - mt expert tecnologia da informacao ltda (cnpj:31.160.692/0001-69) rua: benjamin constant,96 sala 02 jardim independência – Ituverava - SP cep: 14500-00 - hash technology ltda (cnpj: 29.175.645/0001-47) rua: benjamin constant,96 sala 03 jardim independência – Ituverava SP cep: 14500-00 - Ótima tecnology ltda (cnpj:15.185.990/0001-57) rua: benjamin constant,96 jardim independência – Ituverava SP cep: 14500-00 - j.a.s - telecomunicações ltda (cnpj:12.850.879/0001-40) rua: benjamin constant,96 sala 01 jardim independência – Ituverava SP cep: 14500-00 e outras empresas que se vincularem expressamente ao número empresarial.

2. Introdução

A presente política de segurança da informação (PSI) está baseada nas recomendações da norma ABNT NBR ISO/IEC 27001:2022, reconhecida mundialmente como um código de prática para a gestão da segurança da informação. A informação é o ativo mais valioso da nossa empresa, por esse motivo necessita ser adequadamente protegido. Conforme conceito da norma: ‘segurança da informação é a proteção da informação de vários tipos de ameaças e seus vários níveis para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio’ (ABNT NBR ISO/IEC 17799:2005).

2.1 Princípios

A Ótima adota como princípios fundamentais de Segurança da Informação:

- ✓ Gestão baseada em riscos;
- ✓ Melhoria contínua;
- ✓ Menor privilégio;
- ✓ Need to Know;
- ✓ Security by Design;
- ✓ Privacy by Design;
- ✓ Defesa em profundidade;
- ✓ Conformidade legal e regulatória.

3. Abrangência

Este documento consiste na política de segurança da informação (PSI) da Ótima, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e definição de responsabilidades. Todo seu conteúdo deve ser adotado, cumprido e aplicado em todas as áreas da companhia em conjunto com nosso código de ética, que é também parte integrante desta política. Essa versão pode ser alterada a qualquer momento; suas alterações devem ser aprovadas pela diretoria e veiculada em nossos canais de comunicação. As informações desta política são revisadas e atualizadas no mínimo uma vez ao ano, ou conforme as demandas de negócio e/ou legais se tornem necessárias.

A Ótima reconhece que a segurança da informação depende de fatores internos e externos que influenciam sua operação. Para manter a conformidade com a norma ABNT NBR

ISO/IEC 27001:2022 e garantir a proteção adequada das informações, são considerados os seguintes aspectos:

3.1 Contexto interno

- ✓ Estrutura organizacional do grupo Ótima e suas empresas vinculadas.
- ✓ Processos de negócio e atividades essenciais da companhia.
- ✓ Recursos tecnológicos, humanos e financeiros disponíveis para apoiar o SGSI.
- ✓ Cultura organizacional voltada à ética, compliance, privacidade e inovação.

3.2 Contexto externo

- ✓ Exigências legais e regulatórias aplicáveis (ex.: LGPD, legislação trabalhista e fiscal, normas de telecomunicações).
- ✓ Expectativas de clientes, parceiros e órgãos reguladores quanto à confidencialidade, integridade e disponibilidade das informações.
- ✓ Ambiente competitivo e de mercado, que exige resiliência, agilidade e confiança nos serviços prestados.
- ✓ Evolução tecnológica e ameaças cibernéticas emergentes.

3.3 Partes interessadas e suas expectativas

- ✓ **Clientes:** proteção de dados, continuidade dos serviços, transparência.
- ✓ **Colaboradores e prestadores de serviço:** orientações claras de conduta, acesso seguro e capacitação.
- ✓ **Sócios e direção:** mitigação de riscos, conformidade legal e reputacional.
- ✓ **Órgãos reguladores:** atendimento às normas, leis e regulamentações.
- ✓ **Fornecedores e parceiros de negócio:** cláusulas contratuais de segurança, proteção de informações compartilhadas.
- ✓ **Sociedade em geral:** responsabilidade social, ética, proteção à privacidade.

4. Escopo da área de tecnologia e segurança da informação

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade da informação necessária para a realização do negócio da empresa, ser o gestor e o apoio do processo de segurança digital, protegendo as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações com o intuito de garantir a todos o entendimento da necessidade do compromisso da organização com este documento.

5. Papéis, Responsabilidades e Compromisso dos Colaboradores

A Segurança da Informação é uma responsabilidade compartilhada entre todos os colaboradores, administradores, estagiários, aprendizes, prestadores de serviços, terceiros, fornecedores e parceiros que atuem em nome da Ótima.

Toda informação tratada pela organização constitui um ativo estratégico para o negócio e deve ser protegida durante todo o seu ciclo de vida, preservando sua confidencialidade, integridade, disponibilidade, autenticidade e, quando aplicável, a privacidade dos dados pessoais.

Cada profissional é responsável por utilizar os ativos físicos, digitais e tecnológicos da organização de forma ética, segura e em conformidade com esta Política de Segurança da Informação, com o Código de Ética e Conduta, com a Política de Privacidade, com as demais normas internas e com a legislação vigente.

O compromisso individual de cada colaborador é essencial para preservar a confiança de clientes, parceiros, fornecedores, titulares de dados pessoais e demais partes interessadas, contribuindo para a continuidade dos negócios, a proteção das informações corporativas e a manutenção da reputação da Ótima.

Todo colaborador deverá conhecer, compreender e cumprir as diretrizes estabelecidas nesta Política de Segurança da Informação, assumindo, entre outras, as seguintes responsabilidades:

- ✓ Manter absoluto sigilo sobre as informações classificadas como Internas, Confidenciais ou Restritas às quais tenha acesso em razão de suas atividades.
- ✓ Cumprir integralmente esta Política de Segurança da Informação, o Código de Ética e Conduta, a Política de Privacidade de Dados e os demais normativos internos aplicáveis.
- ✓ Utilizar credenciais de acesso exclusivamente de forma individual, sendo expressamente proibido compartilhar senhas, certificados digitais, tokens, chaves de acesso ou qualquer outro mecanismo de autenticação.
- ✓ Zelar pela proteção de suas credenciais, comunicando imediatamente à área responsável qualquer suspeita de comprometimento, perda, roubo ou utilização indevida.
- ✓ Utilizar os recursos tecnológicos, equipamentos, sistemas, aplicações, serviços corporativos e ativos de informação exclusivamente para finalidades profissionais autorizadas.
- ✓ Proteger os ativos físicos e digitais sob sua responsabilidade, evitando perdas, danos, utilização inadequada ou divulgação não autorizada.
- ✓ Classificar corretamente as informações produzidas, armazenadas, processadas ou compartilhadas, observando os critérios estabelecidos nesta Política.
- ✓ Cumprir os princípios da Política de Mesa Limpa e Tela Limpa, garantindo que documentos, equipamentos e informações sensíveis permaneçam protegidos contra acessos não autorizados.
- ✓ Utilizar exclusivamente os canais corporativos aprovados para o compartilhamento de informações relacionadas às atividades da empresa.
- ✓ Não discutir, transmitir ou divulgar informações corporativas, estratégicas, técnicas, comerciais ou de clientes em ambientes públicos ou por meios de comunicação não autorizados.
- ✓ Participar obrigatoriamente dos treinamentos, campanhas de conscientização e reciclagens promovidos pela Ótima sobre Segurança da Informação, Privacidade, Proteção de Dados e demais temas relacionados.
- ✓ Reportar imediatamente à área de Segurança da Informação ou ao seu gestor qualquer incidente, vulnerabilidade, comportamento suspeito, tentativa de fraude, perda de equipamentos, vazamento de informações ou qualquer situação que possa comprometer a segurança das informações da organização.
- ✓ Cooperar com auditorias internas e externas, avaliações de conformidade, processos de gestão de riscos e demais atividades relacionadas ao Sistema de Gestão de Segurança da Informação (SGSI).
- ✓ Cumprir as diretrizes relacionadas à proteção de dados pessoais, observando os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD) e demais legislações aplicáveis.
- ✓ Contribuir continuamente para a melhoria do Sistema de Gestão de Segurança da Informação (SGSI), comunicando oportunidades de melhoria, riscos identificados e apoiando a implementação de novos controles de segurança.

A Ótima mantém um programa contínuo de conscientização em Segurança da Informação, Privacidade e Proteção de Dados, destinado a fortalecer a cultura organizacional, reduzir riscos operacionais, aumentar a maturidade em segurança e promover o uso seguro das informações e dos ativos tecnológicos.
O Comitê Gestor de Segurança da Informação (CGSI), em conjunto com a Diretoria de Segurança da Informação e a Alta Direção, é responsável por estabelecer as diretrizes estratégicas do Sistema de Gestão de Segurança da Informação (SGSI), aprovar políticas corporativas, acompanhar indicadores de desempenho, supervisionar a gestão de riscos, deliberar sobre incidentes relevantes e apoiar a melhoria contínua dos controles de segurança adotados pela organização.
O descumprimento das responsabilidades estabelecidas nesta Política poderá resultar na aplicação das medidas disciplinares previstas nas normas internas da Ótima, sem prejuízo das responsabilidades civis, administrativas e criminais cabíveis.
As obrigações de confidencialidade e proteção das informações permanecem válidas durante todo o vínculo profissional com a Ótima e continuarão produzindo efeitos após seu encerramento, sempre que houver obrigações legais, regulatórias, contratuais ou compromissos de confidencialidade relacionados às informações acessadas durante a prestação dos serviços.

6. Classificação da informação

É de responsabilidade do gestor de cada área estabelecer a rotulagem da informação que o seu setor manipula, orientar os colaboradores sob sua responsabilidade quanto as melhores práticas de rotulagem da informação, conforme descrito nesta política. Observando critérios relativos ao nível de confidencialidade da informação, seja ela física ou digital gerada por sua área, com os seguintes rótulos:

- ✓ Informação pública.
- ✓ Informação interna.
- ✓ Informação confidencial.
- ✓ Informação restrita.

Pública: Toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral, cuja divulgação externa não compromete a empresa. Exemplos de informação pública: agenda de negócios, participação em eventos, política de segurança da informação.

Interna: São as informações disponíveis aos colaboradores da Ótima, para a execução de suas tarefas rotineiras, não se destinando ao público externo, pois seu grau de confidencialidade assim o define. Exemplos de informação interna: memorandos, políticas internas, avisos e campanhas internas.

Confidencial: Informações que podem ser acessadas por um número mais restrito de colaboradores e parceiros da organização. Sua publicação não autorizada pode violar leis vigentes (ex.: LGPD – Lei Geral de Proteção de dados), acordos de confidencialidade, podendo causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro. Exemplos de informação confidencial: dados de funcionários ou pessoas físicas identificáveis, processos judiciais e todas as informações de contratantes e dos respectivos clientes destes. Toda a informação que não for declarada pública ou interna é considerada confidencial.

Restrita: Toda informação que pode ser acessada somente por usuários da organização explicitamente indicados pelo nome ou área a que pertencem, em geral, associada ao interesse estratégico da empresa. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo gerente deve orientar seus subordinados que tenham acesso a esse tipo de informação, por necessidade da função exercida, a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras e mídias em locais de fácil acesso, tendo sempre em mente o conceito de "mesa limpa", ou seja, ao terminar o trabalho, não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.
Exemplo de informação restrita: atas de reuniões da governança, análise, avaliação e gestão de risco, indicadores e estatísticas dos processos de negócio, resultados de auditorias internas.
Todo documento, informação ou dado físico ou digital, não classificado(rotulado) será considerado **confidencial**.

6.1 Tratamento das Informações

As informações classificadas como Internas, Confidenciais e Restritas deverão ser tratadas de acordo com seu nível de criticidade, observando, quando aplicável:

- ✓ restrição de acesso baseada no menor privilégio;
- ✓ criptografia em trânsito e em repouso;
- ✓ utilização exclusiva de canais corporativos autorizados;
- ✓ registro e rastreabilidade dos acessos;
- ✓ retenção conforme requisitos legais, regulatórios e contratuais;
- ✓ descarte seguro ao final do ciclo de vida da informação.

7. Sistema de Gestão da segurança da informação

A gestão de segurança da informação tem como uma das primeiras iniciativas a criação e implementação de uma política de segurança da informação. Visando proteger seus ativos tangíveis e intangíveis, a Ótima construiu essa política orientada na legislação vigente do País, nós órgãos reguladores em que se aplica e nas melhores práticas de mercado pautadas pelos princípios da ética e transparência.
Sendo a informação o ativo mais valioso da corporação, cabe a esta promover orientações aos seus colaboradores, treinamentos em segurança da informação, pois, as informações precisam transitar no cotidiano das atividades da empresa. Pois só os controles digitais não são suficientes para manter um ambiente seguro; todos os colaboradores precisam estar envolvidos e participativos nos temas de segurança da informação em suas atividades rotineiras.

- ✓ Criar comitê gestor de segurança da informação (CGSI), pautado nos pilares da segurança da informação, envolvendo lideranças da empresa conforme estratégia.
- ✓ Propor melhorias e ajustes nas políticas de segurança da informação.
- ✓ Analisar os investimentos em Segurança da Informação e Tecnologia da Informação para além da otimização do ambiente, minimizar os riscos operacionais.
- ✓ Apurar, analisar e exercer toda a governança dos incidentes em segurança da informação.
- ✓ Apoiar a direção na aplicação e criação de processo de análise e avaliação de riscos de segurança da informação.
- ✓ Apoiar a gestão dos processos em tecnologia da informação.
- ✓ Garantir apoio as áreas jurídica e de compliance.

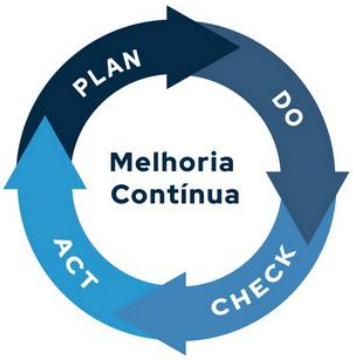
- ✓ Conduzir auditorias internas.

O Sistema de Gestão de Segurança da Informação da Ótima é continuamente melhorado com base nos resultados de auditorias, monitoramento de indicadores, gestão de riscos, tratamento de incidentes e análise crítica da direção, assegurando sua evolução contínua e alinhamento ao negócio.

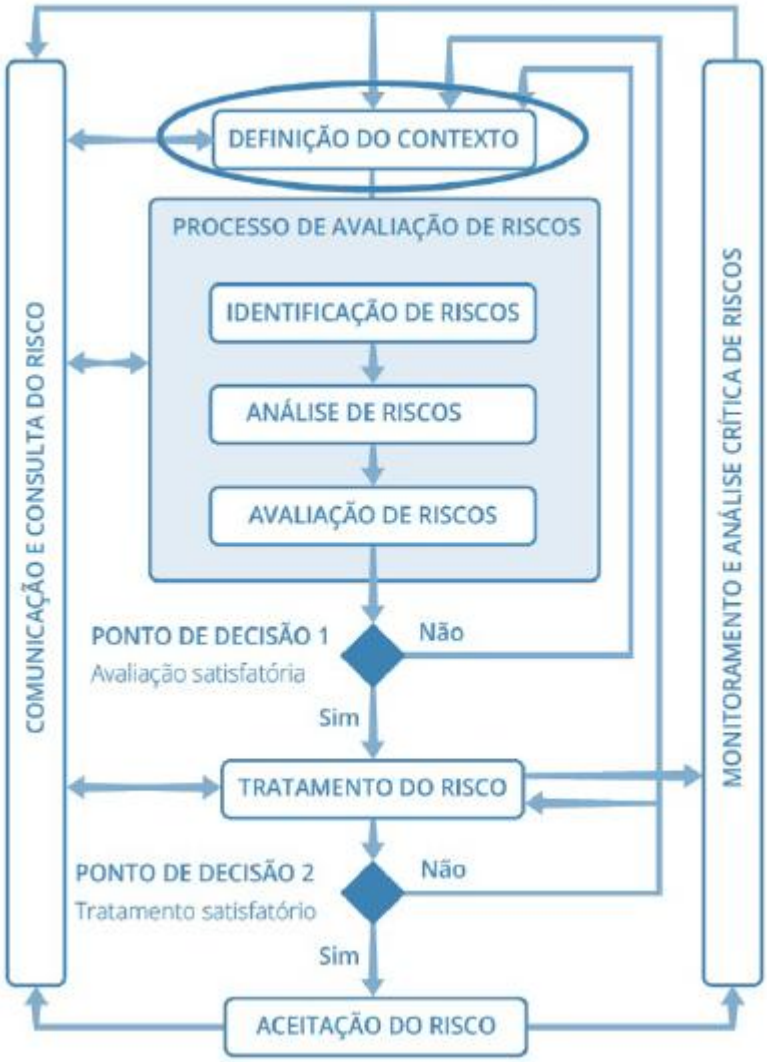
7.1 Gestão de Riscos

A gestão de riscos de segurança da informação na Ótima busca uma abordagem baseada na ISO 27005 com o objetivo de identificar as necessidades de segurança da informação servindo como base do sistema de gestão de segurança da informação.
A gestão de riscos, tal qual a segurança da informação são processos contínuos que utilizam como base o ciclo PDCA resumido:
Ciclo **PDCA** (Plan-Do-Check-Act)

1. **Plan (Planejar)**: Definir políticas, objetivos, processos e análise de riscos.
2. **Do (Executar)**: Implementar os controles e processos planejados.
3. **Check (Verificar)**: Validar, monitorar, auditar.
4. **Act (Agir)**: Corrigir falhas, lições aprendidas, melhoria contínua.



O processo de gestão de risco na Ótima, tem o seguinte fluxo:



Iniciada na gestão de contexto, onde fica estabelecido o ambiente ao qual a empresa está inserida, definindo limites, abrangência e critérios. Devem ser considerados os objetivos e políticas da organização, estrutura e funcionamento da empresa, processos de negócio, ativos, expectativas e restrições.

Critérios de avaliação de riscos

Definição	**Probabilidade**	**→ % de ocorrência**	**Valor Risco**	**Ação Proposta**
O risco seguramente se manifestará com frequência	Quase certa	81 → 99	**60**	**Atuar**
O risco poderá se manifestar com frequência	Provável	51 → 80	**50**	**Atuar**
O risco se manifestará em algum momento	Alta	30 → 50	**40**	**Atuar**
O risco poderá se manifestar em algum momento	Intermediária	16 → 29	**30**	**Atuar monitorar**
O risco raramente se manifestará	Baixa	6 → 15	**20**	**Atuar monitorar**
O risco poderá se manifestar em circunstânc excepcionais	Rara	1 → 5	**10**	**Monitorar**

A metodologia de avaliação de riscos é documentada e aplicada de forma consistente em todo o SGSI conforme política de gestão de riscos cibernéticos da Ótima.

Convém que esse processo análise e avalie os itens mapeados, a fim de extinguir ou reduzir os riscos a um nível aceitável. Espera-se da gestão de riscos, mas não se resumindo as seguintes ações:

- ✓ Identificação de riscos.
- ✓ Implementar um processo contínuo de análise e avaliação de riscos.
- ✓ Medir as consequências dos riscos ao negócio e as probabilidades de ocorrência.
- ✓ Estabelecer comunicação interna e a partes interessadas a respeito do tratamento conformo escopo a que se aplica.
- ✓ Priorizar ordem de tratamento dos riscos.
- ✓ Medir eficácia das ações e monitoramento do tratamento.
- ✓ Treinamento interno quanto a ações a diminuição de riscos.
- ✓ Melhoria contínua na gestão de segurança das informações.

7.2 Conscientização e treinamento

O departamento de segurança da informação em conjunto com a área de recursos humanos, são responsáveis em aplicar treinamentos e ou campanhas mensais a respeito da segurança da informação, boas práticas e diretrizes da Ótima, tanto abordadas em nossas políticas como no manual do usuário. Esses treinamentos são registrados em ata de participação onde cada colaborador é mensurado.

7.3 Gestão de mudanças

A gestão de mudanças tem como finalidade assegurar que qualquer alteração em sistemas, infraestrutura, aplicações, processos ou serviços de tecnologia da informação seja conduzida de forma controlada, minimizando riscos e impactos adversos à confidencialidade, integridade, disponibilidade e legalidade das informações.
Para tanto, devem ser observados os seguintes princípios:

- ✓ **Planejamento:** todas as mudanças devem ser avaliadas previamente quanto aos riscos, benefícios, impactos e recursos necessários.

  Aprovação: nenhuma mudança poderá ser realizada sem aprovação formal da área responsável e, quando aplicável, do Comitê Gestor de Segurança da Informação (CGSI).
- ✓ **Registro e rastreabilidade:** toda mudança deve ser registrada em sistema ou documento apropriado, assegurando histórico, responsáveis e prazos.
- ✓ **Testes e validação:** sempre que possível, a mudança deve ser testada em ambiente controlado antes da implantação em produção.
- ✓ **Plano de reversão (rollback):** toda mudança crítica deverá possuir procedimento documentado para retorno ao estado anterior caso ocorram falhas.
- ✓ **Mudanças emergenciais:** mudanças realizadas em caráter emergencial deverão ser formalizadas e aprovadas posteriormente, sendo submetidas à análise crítica do processo.
- ✓ **Comunicação:** as áreas e partes interessadas devem ser informadas previamente sobre as mudanças que possam impactar suas atividades.

- ✓ **Revisão pós-implementação:** após a execução, deve ser realizada análise dos resultados, eventuais incidentes e lições aprendidas, promovendo melhoria contínua.

A implementação deste processo visa garantir que alterações no ambiente corporativo ocorram de forma segura, estruturada e alinhada às diretrizes de segurança da informação da Ótima.

7.4 Gestão de Incidentes

A gestão de incidentes de segurança da informação tem como objetivo assegurar que todos os eventos que possam comprometer a confidencialidade, integridade, disponibilidade ou legalidade das informações da Ótima sejam devidamente identificados, registrados, analisados, tratados e monitorados, promovendo a melhoria contínua dos controles de segurança.

O processo de tratamento de incidentes deve seguir as seguintes etapas:

- ✓ **Detecção e notificação:** todo colaborador, parceiro ou prestador de serviço deve reportar imediatamente qualquer suspeita ou ocorrência de incidente ao canal oficial da Segurança da Informação (si@otima.digital) ou ao seu gestor imediato.
- ✓ **Registro:** os incidentes reportados devem ser registrados em sistema ou documento formal, contendo data, horário, descrição do evento, responsável pelo reporte e ativos envolvidos.
- ✓ **Classificação e priorização:** os incidentes serão classificados de acordo com sua gravidade, impacto ao negócio, alcance e urgência de resposta, permitindo definir a ordem de tratamento.
- ✓ **Resposta e contenção:** medidas devem ser aplicadas para mitigar impactos imediatos, restaurar serviços afetados e impedir a propagação do incidente.
- ✓ **Investigação e análise de causa:** a área de Gestão de Segurança da Informação conduzirá investigação técnica, buscando identificar causas raiz e eventuais falhas em processos, controles ou comportamentos.
- ✓ **Preservação de evidências:** sempre que aplicável deverão ser preservadas evidências digitais que permitam investigação técnica, análise forense ou atendimento às exigências legais.
- ✓ **Recuperação:** após a contenção do incidente deverão ser executadas ações para restabelecimento seguro dos serviços.
- ✓ **Lições aprendidas e correções:** após o tratamento, será realizada reunião de análise pós-incidente, com registro de lições aprendidas e definição de planos de ação corretivos e preventivos.
- ✓ **Comunicação:** incidentes relevantes devem ser comunicados à alta direção, ao Comitê Gestor de Segurança da Informação (CGSI) e, quando aplicável, a órgãos reguladores, clientes ou parceiros, conforme exigências legais e contratuais.

Esse processo garante que incidentes sejam tratados de forma estruturada, documentada e transparente, fortalecendo a resiliência organizacional e a confiança das partes interessadas.

7.5 Objetivos de Segurança da Informação

A Ótima estabelece objetivos mensuráveis de segurança da informação, alinhados à Política de Segurança da Informação, aos resultados da gestão de riscos e aos objetivos estratégicos

do negócio, revisados anualmente pelo Comitê Gestor de Segurança da Informação (CGSI). Exemplos de objetivos:

- ✓ Garantir que 100% dos colaboradores realizem treinamentos anuais de segurança da informação
- ✓ Manter o tempo médio de resposta a incidentes críticos inferior a 4 horas
- ✓ Garantir que 100% dos ativos críticos estejam cobertos por backup validado
- ✓ Reduzir em 20% os riscos classificados como altos em cada ciclo anual de avaliação

Os indicadores são monitorados periodicamente e reportados à alta direção e o acompanhamento dos objetivos é de responsabilidade do Comitê Gestor de Segurança da Informação (CGSI), com apoio das áreas envolvidas.

7.6 Declaração de Aplicabilidade (SoA)

A Ótima mantém uma Declaração de Aplicabilidade (Statement of Applicability – SoA), que contém a relação dos controles de segurança da informação baseados no Anexo A da ISO/IEC 27001:2022, indicando:

- ✓ Controles aplicáveis e não aplicáveis
- ✓ Justificativa para inclusão ou exclusão
- ✓ Estado de implementação
- ✓ Referência aos controles internos existentes

A SoA é revisada sempre que houver mudanças significativas no ambiente de risco ou no SGSI. A Declaração de Aplicabilidade é baseada nos resultados do processo de avaliação e tratamento de riscos de segurança da informação.

7.7 Monitoramento e Medição

A Ótima estabelece os indicadores a seguir, para monitorar a eficácia do SGSI, incluindo, mas não se limitando a:

- ✓ Número de incidentes de Segurança da Informação registrados por período;
- ✓ Tempo médio de resposta e de resolução de incidentes de segurança;
- ✓ Percentual de conformidade com as políticas, normas e procedimentos internos;
- ✓ Percentual de ativos críticos protegidos e atualizados conforme as políticas corporativas;
- ✓ Percentual de vulnerabilidades tratadas dentro do prazo (SLA) definido pela organização;
- ✓ Disponibilidade dos sistemas e serviços considerados críticos para o negócio;
- ✓ Percentual de revisões periódicas de acessos realizadas dentro do prazo estabelecido;
- ✓ Percentual de colaboradores que concluíram os treinamentos obrigatórios de Segurança da Informação, Privacidade e Proteção de Dados;
- ✓ Percentual de êxito nos testes de restauração de backups;
- ✓ Quantidade de não conformidades identificadas em auditorias internas e externas e respectiva taxa de tratamento;
- ✓ Percentual de ações corretivas implementadas dentro do prazo estabelecido;
- ✓ Evolução do nível de risco residual dos ativos críticos monitorados pelo SGSI.

Estes indicadores são monitorados e analisados na gestão do SGSI e utilizados para melhoria contínua. A responsabilidade pela revisão dos indicadores é da Diretoria de Segurança da Informação.

7.8 Análise Crítica pela Direção

A alta direção realiza, no mínimo anualmente, a análise crítica do SGSI para garantir sua adequação, suficiência e eficácia. A análise considera:

- ✓ Resultados de auditorias internas
- ✓ Status de ações corretivas
- ✓ Mudanças no contexto interno e externo
- ✓ Desempenho dos indicadores de segurança
- ✓ Situação dos riscos

As decisões e ações resultantes são documentadas.

7.9 Não Conformidades e Ações Corretivas

A Ótima estabelece processo para tratamento de não conformidades relacionadas ao SGSI. Quando uma não conformidade ocorre:

- ✓ Ela é registrada e analisada
- ✓ A causa raiz é identificada
- ✓ Ações corretivas são definidas e implementadas
- ✓ A eficácia das ações é avaliada

Os registros são mantidos para fins de auditoria e melhoria contínua. A gestão das não conformidades é de responsabilidade da Diretoria de Segurança da Informação, com apoio das áreas envolvidas na causa identificada. As não conformidades são priorizadas conforme seu nível de impacto e risco, devendo ser tratadas dentro de prazos definidos pela Diretoria de Segurança da Informação, conforme sua criticidade.

7.10 Controle de Documentos

Todos os documentos do SGSI são controlados para garantir:

- ✓ Identificação e versionamento
- ✓ Aprovação antes da publicação
- ✓ Revisão periódica
- ✓ Disponibilidade das versões atualizadas
- ✓ Proteção contra uso indevido

Documentos obsoletos são devidamente identificados e arquivados conforme política de retenção.

8. Gestão dos processos em tecnologia da informação

A Diretoria de Segurança da Informação da Ótima é responsável por estabelecer e apoiar a implementação de processos, políticas e procedimentos da organização para a gestão da segurança da informação e os controles necessários manter a integridade, disponibilidade, confidencialidade e autenticidade das informações contidas no ambiente corporativo, com o objetivo de aumentar eficácia e reduzir eventos que possam causar impactos ou incidentes de segurança da informação.

8.1 Possui como diretrizes básicas

- ✓ Gestão dos acessos: toda credencial de acesso é um perfil pertencente a um grupo de privilégios e restrições, cada colaborador possui uma credencial/login, que deve ser identificável, auditável e único.
- ✓ O processo de contratação e desligamento dos colaboradores deve ser seguido, conforme estabelecido em procedimento interno iniciado junto ao departamento de recursos humanos, tal qual transferências, afastamentos entre outras ações envolvendo a movimentação dos colaboradores.
- ✓ Garantir que os ativos (dados e informações) sejam utilizados apenas para as finalidades aprovadas pela organização, com monitoração, rastreabilidade e auditoria, com o preceito de atribuir o menor privilégio, acesso somente ao que é necessário para a realização das atividades dos colaboradores, parceiros e partes interessadas.
- ✓ Gestão, detecção e tratamento de vulnerabilidades.
- ✓ Desenvolvimento Seguro (Secure SDLC), todos os sistemas, aplicações, APIs e integrações desenvolvidos ou mantidos pela Ótima deverão seguir práticas de desenvolvimento seguro durante todo o ciclo de vida do software, incluindo análise de requisitos de segurança, revisão de código quando aplicável, testes de segurança, homologação e validação antes da disponibilização em produção.
- ✓ Os ambientes de Desenvolvimento, Homologação, Testes e Produção deverão permanecer segregados, possuindo controles de acesso independentes, bases de dados distintas sempre que possível e procedimentos específicos para movimentação de versões entre ambientes.
- ✓ Registro e monitoramento de eventos (Logs), todos os sistemas, aplicações, servidores, dispositivos de rede e demais ativos críticos deverão manter registros de eventos relevantes para fins de auditoria, investigação de incidentes, rastreabilidade e atendimento às exigências legais e regulatórias, observadas as políticas de retenção de registros da organização.
- ✓ As chaves criptográficas utilizadas para proteção das informações deverão possuir controle de geração, armazenamento, distribuição, utilização, rotação, revogação e descarte, conforme requisitos técnicos e níveis de criticidade definidos pela organização.
- ✓ Pentest nos sistemas web anualmente e scans de vulnerabilidade trimestrais ou conforme grandes alterações no ambiente.
- ✓ Prevenção a ameaças e ataques cibernéticos, bem como plano de resposta a incidentes de segurança da informação.
- ✓ Plano de resposta a violação de dados.
- ✓ Melhoria contínua dos processos e recursos necessários à política de segurança da informação.
- ✓ Política de senha deve ser mantida, senha deve possuir mínimo de 12 caracteres, complexidade e sempre que tecnicamente possível, os acessos administrativos, privilegiados, remotos e aos sistemas que tratem informações classificadas como

Confidenciais ou Restritas deverão utilizar autenticação multifator como mecanismo adicional de proteção.

- ✓ Revisões de acesso devem ocorrer sazonalmente, conforme as práticas internas de perfil de acessos.
- ✓ Uso de antivírus: todas as estações de trabalho, dispositivos móveis e servidores devem ter a solução corporativa do antivírus instalado. A atualização do antivírus deve ser automatizada, conforme as rotinas estabelecidas e possível no fornecedor do aplicativo. Os usuários não possuem permissão para desabilitar o programa antivírus instalado nas estações de trabalho e dispositivos móveis.
- ✓ Uso do correio eletrônico (e-mail) corporativo: o correio eletrônico fornecido pela Ótima é um instrumento de comunicação interna e externa para a realização do negócio da empresa. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da empresa, não podem ser contrárias à legislação vigente e nem aos princípios éticos da Ótima, conforme explicitado em nosso código de conduta e ética. Nossos domínios são hospedados na Microsoft, que dispõe de um robusto sistema de proteção cibernética e compliance corporativo.
- ✓ Novos sistemas, apps e equipamentos: O setor de ti/infra é responsável pela aplicação da política da Ótima em relação à definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos apps ou de novos equipamentos dentro da corporação será validada e homologada pela área de ti/infra. Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.
- ✓ Internet: O acesso à internet é autorizado aos usuários conforme seu perfil; são acessos aos conteúdos que necessitarem para o desenvolvimento de suas atividades na empresa. Demais conteúdos são bloqueados por padrão. Há uma política específica para esse controle onde um proxy baseado em Zero Trust efetua este controle. Os colaboradores são cientes deste monitoramento.
- ✓ Sistemas de telecomunicações: O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da Ótima, assim como o uso de eventuais ramais virtuais instalados nos computadores de responsabilidade do setor de suporte. Todas as ligações são gravadas. A área de qualidade efetua auditorias constantes com feedback às gerências da Ótima.
- ✓ Programas e apps: a Ótima respeita os direitos autorais dos programas que utiliza, reconhece que deve pagar o justo valor por eles. É terminantemente proibido o uso de programas ilegais (sem licenciamento) na corporação.
- ✓ Backup: todos os dados da Ótima e sob sua responsabilidade são protegidos através de rotinas sistemáticas de backup com criptografia em trânsito e em repouso. Há cópias de segurança dos sistemas e servidores da rede executados diariamente e possuem política específica para esse fim.
- ✓ Retenção de dados: a Ótima não efetua retenção de dados pessoais, sensíveis ou de qualquer outra natureza, exceto para cumprir a legislação vigente no país, atender normas de órgãos reguladores ou simplesmente para atender exigências contratuais.
- ✓ O ciclo de vida da informação inicia nos primeiros contatos com os clientes e se encerra conforme disposto neste parágrafo, não havendo obrigações legais a Ótima,

contratuais ou para atender órgãos reguladores, os dados serão higienizados assim que esses 3 pilares tiverem seus ciclos encerrados.

- ✓ O descarte seguro de dados ocorre no encerramento do ciclo de vida da informação, no meio digital se dá por exclusão total dos dados ou por criptografia anonimizando esses dados, tornando irrecuperáveis e não identificáveis, caso sua exclusão seja impossibilitada. No meio físico, ocorre por trituração e ou envio a empresa certificada para estas ações.
- ✓ Segurança e integridade dos bancos de dados: o gerenciamento do(s) banco(s) de dados é responsabilidade do setor de Dados, que visa protegê-los usando as tecnologias digitais disponíveis, mantendo-os íntegros e disponíveis ao negócio com as devidas configurações necessárias ao seu funcionamento seguro.
- ✓ Propriedade intelectual: são de propriedade da Ótima todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a empresa conforme aceite do código de conduta e ética.
- ✓ Política de dispositivos móveis e estações de trabalho: tais equipamentos devem permanecer o maior tempo possível disponível aos colaboradores para que estes possam exercer suas funções em sua plenitude. Os equipamentos devem conter antivírus e somente os apps homologados pela empresa. Em nosso código de ética são descritos os compromissos e responsabilidades dos colaboradores no tocante a todos os ativos da empresa. Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade da Ótima ou particular, com prévia aprovação da gerência de ti, como: notebooks, smartphones e pen drives. Todos deverão estar de acordo com nossa política de acessos.
- ✓ Utilização da rede: o acesso à rede interna da empresa é controlado; estações ou dispositivos não autorizados não conseguirão fazer uso dos recursos de ti da empresa. Para visitantes, temos uma rede completamente apartada, com internet disponível e monitorada. O acesso à rede interna por dispositivos que não pertencem à Ótima passa por aprovação da gerência de ti e homologação pela equipe de suporte; dispositivos sem antivírus não terão permissão para trafegar na rede interna. Todas as ações são monitoradas na rede. A rede de computadores da empresa é totalmente segmentada, não há exceções.
- ✓ Dispositivos de armazenamento externo: o uso de pendrives ou quaisquer dispositivos de armazenamento externo, enclosure, smartphones somente serão permitidos em caso de autorização da Diretoria de Segurança da Informação com solicitação formal da gerência do colaborador solicitante. Mesmo assim, sua utilização, estará sujeita à aprovação e higienização das nossas ferramentas de segurança, antivírus, anti-malware e proteção contra ransomware.
- ✓ Auditorias: A Ótima estabelece um programa formal de auditorias internas do SGSI, realizado no mínimo anualmente, com base em critérios definidos, escopo, frequência e métodos. As auditorias avaliam a conformidade com a ISO 27001, políticas internas e requisitos legais, devendo, sempre que possível, ser conduzidas por profissionais independentes das atividades auditadas, garantindo imparcialidade e objetividade no processo. Os resultados são documentados e reportados à alta direção e ao CGSI.

- ✓ A empresa, possui código de ética e conduta, bem como manual do colaborador informado e distribuído no onboard, processo este que visa conscientizar novos colaboradores quanto a missão da Ótima, seus valores e sua visão bem como estabelecer direitos e deveres de cada colaborador dentro da corporação.
- ✓ Todos os colaboradores e visitantes devem usar crachá de identificação nas dependências da Empresa.
- ✓ Os escritórios possuem CFTV, vigilância, alarme de incêndio portaria para controle de entrada e identificação e são climatizados.
- ✓ Os Datacenter da Ótima possuem nível T3 de certificação em segurança.

8.2 Continuidade dos Negócios

A Ótima mantém um Programa de Continuidade de Negócios destinado a assegurar a continuidade dos processos críticos, minimizar os impactos decorrentes de interrupções operacionais e restabelecer os serviços essenciais em níveis compatíveis com os requisitos do negócio, de seus clientes e das demais partes interessadas.

O Plano de Continuidade dos negócios (PCN) estabelece as diretrizes para resposta a eventos que possam comprometer as operações da organização, incluindo, mas não se limitando a desastres naturais, falhas de infraestrutura, indisponibilidade de serviços, incidentes cibernéticos, falhas de comunicação, interrupções de energia, indisponibilidade de fornecedores críticos, erro humano ou quaisquer outras situações capazes de afetar a continuidade dos serviços.

Como complemento ao PCN, a Ótima mantém Plano de Recuperação de Desastres (PRD), contendo os procedimentos técnicos necessários para recuperação da infraestrutura tecnológica, dos sistemas corporativos, das bases de dados, das comunicações e dos demais ativos essenciais ao restabelecimento das operações.

A infraestrutura tecnológica da Ótima foi projetada considerando princípios de alta disponibilidade, resiliência e redundância. O ambiente operacional é composto por dois Datacenters com certificação Tier III, localizados em regiões distintas, sendo um ambiente principal na SBA Edge, em São Paulo/SP, e um ambiente de contingência em Bauru/SP. Ambos possuem infraestrutura redundante, conectividade de dados e voz por meio de múltiplos links de alta capacidade, utilização de protocolos de redundância de roteamento e demais mecanismos destinados a reduzir pontos únicos de falha e aumentar a disponibilidade dos serviços.

Os processos de backup, replicação de dados, monitoramento da infraestrutura, gerenciamento de incidentes, gestão de mudanças, gestão de riscos e recuperação de ambientes integram a estratégia de continuidade da organização, proporcionando maior capacidade de resposta diante de eventos adversos.

Os Planos de Continuidade de Negócios (PCN) e de Recuperação de Desastres (PRD) são periodicamente testados, revisados e atualizados com o objetivo de validar sua eficácia, assegurar a capacidade de recuperação dos serviços críticos e identificar oportunidades de melhoria.

Os testes poderão contemplar cenários de indisponibilidade de infraestrutura, falhas de sistemas, perda de conectividade, comprometimento de ativos tecnológicos, incidentes de segurança da informação, perda de dados, indisponibilidade de fornecedores críticos e demais situações relevantes para o ambiente operacional da organização.

Os resultados dos testes, evidências obtidas, lições aprendidas, desvios identificados e planos de ação decorrentes são formalmente registrados e utilizados para o aprimoramento contínuo dos processos de continuidade, recuperação de desastres e do Sistema de Gestão de Segurança da Informação (SGSI).

A periodicidade dos testes e revisões será definida pela Diretoria de Segurança da Informação em conjunto com o Comitê Gestor de Segurança da Informação (CGSI), considerando a criticidade dos serviços, alterações significativas na infraestrutura, resultados da gestão de riscos, incidentes ocorridos, requisitos legais, regulatórios, contratuais e necessidades do negócio.
A estratégia de Continuidade de Negócios é continuamente revisada como parte do processo de melhoria contínua do SGSI, assegurando que os controles implementados permaneçam eficazes, proporcionais aos riscos identificados e alinhados aos objetivos estratégicos da organização.

9. Papéis e Responsabilidades

A governança da Segurança da Informação na Ótima é estruturada por meio da definição clara de papéis, responsabilidades e autoridades, assegurando que o Sistema de Gestão de Segurança da Informação (SGSI) seja implementado, mantido e continuamente aprimorado.

9.1 Alta Direção

Compete à Alta Direção:

- ✓ Demonstrar liderança e comprometimento com o Sistema de Gestão de Segurança da Informação (SGSI);
- ✓ Aprovar esta Política de Segurança da Informação e os demais normativos relacionados;
- ✓ Assegurar os recursos humanos, financeiros e tecnológicos necessários para a implementação, manutenção e melhoria contínua do SGSI;
- ✓ Promover a cultura de Segurança da Informação em toda a organização;
- ✓ Acompanhar o desempenho do SGSI por meio de indicadores, auditorias, análises críticas e gestão de riscos;
- ✓ Garantir que os objetivos de Segurança da Informação estejam alinhados ao planejamento estratégico da organização.

9.2 Diretoria de Segurança da Informação

Compete à Diretoria de Segurança da Informação:

- ✓ Estabelecer, implementar, manter e aprimorar continuamente o Sistema de Gestão de Segurança da Informação;
- ✓ Elaborar, revisar e manter atualizadas as políticas, normas, procedimentos e demais documentos relacionados à Segurança da Informação;
- ✓ Coordenar os processos de gestão de riscos, gestão de vulnerabilidades, resposta a incidentes e conformidade;
- ✓ Monitorar os indicadores de desempenho do SGSI;
- ✓ Apoiar as áreas da organização na implementação dos controles de segurança;
- ✓ Coordenar auditorias internas e apoiar auditorias externas relacionadas ao SGSI;
- ✓ Reportar periodicamente à Alta Direção e ao Comitê Gestor de Segurança da Informação (CGSI) a situação da segurança da informação na organização.

9.3 Comitê Gestor de Segurança da Informação (CGSI)

Compete ao Comitê Gestor de Segurança da Informação:

- ✓ Apoiar a Alta Direção na definição das estratégias de Segurança da Informação;
- ✓ Aprovar políticas, diretrizes e prioridades relacionadas ao SGSI;
- ✓ Acompanhar os indicadores estratégicos de Segurança da Informação;
- ✓ Supervisionar a gestão de riscos corporativos relacionados à Segurança da Informação;

- ✓ Deliberar sobre incidentes relevantes, riscos críticos e exceções às políticas corporativas;
- ✓ Avaliar oportunidades de melhoria e apoiar a evolução contínua do SGSI.

9.4 Gestores das Áreas

Compete aos gestores:

- ✓ Garantir que os colaboradores sob sua responsabilidade cumpram esta Política e os demais normativos internos;
- ✓ Definir e aprovar os perfis de acesso necessários às atividades de suas equipes, observando os princípios do menor privilégio e da necessidade de conhecimento (Need to Know);
- ✓ Classificar as informações produzidas ou tratadas por sua área;
- ✓ Apoiar a identificação, avaliação e tratamento dos riscos relacionados aos processos sob sua responsabilidade;
- ✓ Comunicar à Diretoria de Segurança da Informação qualquer situação que possa representar risco relevante à organização.

9.5 Diretoria de Tecnologia da Informação

Compete à Diretoria de Tecnologia da Informação:

- ✓ Implementar e manter os controles técnicos definidos pelo SGSI;
- ✓ Administrar a infraestrutura tecnológica de forma segura e em conformidade com as políticas corporativas;
- ✓ Garantir a disponibilidade, integridade e segurança dos serviços de tecnologia;
- ✓ Apoiar a implementação das medidas de proteção, monitoramento, backup, recuperação de desastres, gestão de vulnerabilidades e demais controles técnicos necessários à proteção dos ativos da organização.

9.6 Recursos Humanos

Compete à área de Recursos Humanos:

- ✓ Apoiar os processos de admissão, movimentação e desligamento de colaboradores, assegurando que os procedimentos relacionados aos acessos e às responsabilidades de Segurança da Informação sejam cumpridos;
- ✓ Apoiar os programas de conscientização, treinamentos e campanhas relacionados à Segurança da Informação, Privacidade e Proteção de Dados;
- ✓ Manter registros das ações de treinamento e conscientização realizadas.

9.7 Colaboradores, Terceiros e Prestadores de Serviços

Todos os colaboradores, terceiros, fornecedores e prestadores de serviços que atuem em nome da Ótima devem cumprir integralmente esta Política de Segurança da Informação e os demais normativos internos aplicáveis, observando as responsabilidades descritas no Item 5 desta Política.

9.8 Proprietários dos Ativos de Informação

Esse conceito é muito valorizado pela ISO 27001.

Exemplo:

Todo ativo de informação deverá possuir um responsável formal, encarregado de:

- ✓ classificar a informação;
- ✓ aprovar acessos;
- ✓ revisar permissões;
- ✓ definir retenção;

- ✓ validar descarte;
- ✓ apoiar a gestão dos riscos associados.

10. Dados pessoais e LGPD

A Ótima reconhece a privacidade e a proteção dos dados pessoais como direitos fundamentais e mantém um Programa de Governança em Privacidade integrado ao Sistema de Gestão de Segurança da Informação (SGSI), observando os requisitos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), demais legislações aplicáveis e boas práticas internacionais.

O tratamento de dados pessoais realizado pela organização observa os princípios estabelecidos pela LGPD, incluindo:

- ✓ Finalidade;
- ✓ Adequação;
- ✓ Necessidade;
- ✓ Livre acesso;
- ✓ Qualidade dos dados;
- ✓ Transparência;
- ✓ Segurança;
- ✓ Prevenção;
- ✓ Não discriminação;
- ✓ Responsabilização e prestação de contas.

A Ótima adota medidas técnicas e administrativas apropriadas para proteger os dados pessoais contra acessos não autorizados, perda, destruição, alteração, divulgação ou qualquer forma de tratamento inadequado ou ilícito, considerando os riscos inerentes às operações realizadas.

Sempre que possível, novos processos, produtos, serviços, aplicações e projetos deverão incorporar os conceitos de **Privacy by Design** e **Privacy by Default**, assegurando que a privacidade e a proteção dos dados pessoais sejam consideradas desde sua concepção e mantidas durante todo o ciclo de vida da informação.

O tratamento de dados pessoais observará exclusivamente as finalidades legítimas relacionadas às atividades da organização, respeitando os princípios da minimização dos dados, da necessidade e da limitação da retenção, mantendo apenas as informações estritamente necessárias para o cumprimento de obrigações legais, regulatórias, contratuais ou para a execução dos serviços prestados.

A Ótima mantém controles destinados à gestão dos direitos dos titulares de dados pessoais, ao atendimento de incidentes envolvendo dados pessoais, ao gerenciamento de riscos relacionados à privacidade, à avaliação de impactos quando aplicável e ao monitoramento contínuo da conformidade com a legislação vigente.

Todos os colaboradores, terceiros e prestadores de serviços que realizem tratamento de dados pessoais em nome da Ótima deverão observar as diretrizes desta Política, da Política de Privacidade, dos contratos firmados e dos demais normativos internos relacionados à proteção de dados pessoais.

Os dados pessoais armazenados pela organização são classificados, protegidos e monitorados conforme seu nível de criticidade, podendo ser utilizados mecanismos de criptografia, controle de acesso, autenticação multifator, registro de eventos, monitoramento contínuo e demais controles técnicos e administrativos compatíveis com os riscos identificados.

O descarte dos dados pessoais ocorrerá ao término de seu ciclo de vida, observando os prazos legais, regulatórios e contratuais aplicáveis, mediante utilização de métodos seguros que impeçam sua recuperação ou identificação indevida.

11. Sanções

O cumprimento desta Política de Segurança da Informação é obrigatório para todos os colaboradores, administradores, estagiários, aprendizes, terceiros, fornecedores, parceiros e prestadores de serviços que tenham acesso aos ativos físicos, digitais ou às informações sob responsabilidade da Ótima.

Qualquer suspeita de violação desta Política, das normas internas de Segurança da Informação, da legislação aplicável ou de requisitos contratuais deverá ser comunicada imediatamente à Diretoria de Segurança da Informação por meio dos canais corporativos oficiais estabelecidos pela organização, para que sejam adotadas as medidas de contenção, investigação e tratamento cabíveis.

Toda ocorrência será analisada conforme sua natureza, criticidade, impacto ao negócio, requisitos legais e evidências disponíveis, assegurando tratamento imparcial, confidencial e proporcional à gravidade dos fatos.

O descumprimento desta Política poderá caracterizar infração disciplinar e resultar na aplicação das medidas administrativas previstas nas normas internas da Ótima, sem prejuízo das responsabilidades civis, administrativas e criminais cabíveis, incluindo, quando aplicável:

- ✓ Orientação formal;
- ✓ Advertência verbal ou escrita;
- ✓ Suspensão disciplinar;
- ✓ Restrição ou revogação de acessos aos ativos e sistemas corporativos;
- ✓ Rescisão do vínculo contratual ou empregatício;
- ✓ Comunicação às autoridades competentes, quando exigido por lei;
- ✓ Adoção das medidas judiciais cabíveis para reparação de eventuais danos causados à organização ou a terceiros.

Constituem exemplos de condutas passíveis de apuração disciplinar, sem prejuízo de outras previstas na legislação ou nos normativos internos:

- ✓ Compartilhar credenciais de acesso, senhas, certificados digitais, tokens ou outros mecanismos de autenticação;
- ✓ Acessar informações, sistemas ou recursos tecnológicos sem autorização ou além dos privilégios concedidos;
- ✓ Divulgar, copiar, remover, alterar ou utilizar informações corporativas, de clientes, parceiros ou terceiros sem autorização;
- ✓ Descumprir as diretrizes de classificação da informação, confidencialidade ou proteção de dados pessoais;
- ✓ Instalar, utilizar ou distribuir softwares, equipamentos ou serviços não autorizados pela organização;
- ✓ Introduzir, deliberadamente ou por negligência, códigos maliciosos, programas não homologados ou quaisquer recursos que possam comprometer a segurança do ambiente corporativo;
- ✓ Burlar ou tentar contornar controles de segurança implementados pela organização;
- ✓ Descumprir as diretrizes relacionadas ao uso dos ativos corporativos, dos recursos tecnológicos e dos dispositivos disponibilizados pela empresa;
- ✓ Deixar de comunicar incidentes de Segurança da Informação ou situações que possam representar risco relevante para a organização;
- ✓ Violar esta Política, o Código de Ética e Conduta, a Política de Privacidade, os contratos de confidencialidade ou quaisquer outros normativos internos relacionados à Segurança da Informação.

A aplicação das medidas disciplinares observará os princípios da razoabilidade, proporcionalidade, ampla análise dos fatos e conformidade com a legislação vigente,

considerando a gravidade da ocorrência, os riscos envolvidos, os impactos causados, a existência de reincidência e demais circunstâncias relevantes.
A Ótima reafirma seu compromisso com a proteção das informações, com a ética, com a conformidade legal e com a melhoria contínua de seu Sistema de Gestão de Segurança da Informação (SGSI), esperando de todos os seus colaboradores, parceiros e terceiros postura compatível com os valores e princípios estabelecidos nesta Política.

12. Disposições gerais
As dúvidas decorrentes de fatos não descritos nesta política deverão ser encaminhadas à governança para avaliação e decisão. Esta política entra em vigor a partir da data de sua publicação e pode ser alterada a qualquer tempo, por decisão da diretoria ou pela sua atualização em si, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento. Esta política e o sistema de gestão de segurança da informação são revisados no mínimo anualmente.
Exceções às diretrizes estabelecidas nesta Política somente poderão ser concedidas mediante aprovação formal da Diretoria de Segurança da Informação, após análise dos riscos envolvidos.

13. Privacidade de dados
Na Ótima, privacidade e segurança são prioridades, temos o compromisso com a transparência no tratamento de dados pessoais dos nossos usuários / clientes / funcionários / parceiros. Este compromisso está implícito em nossa política de privacidade de dados disponível em nosso site. Nossa política de privacidade se aplica a pessoas ligadas ou não a empresa, é também nosso compromisso com a sociedade.
A presente Política de Segurança da Informação complementa a Política de Privacidade da Ótima. Enquanto este documento estabelece as diretrizes para proteção das informações e do Sistema de Gestão de Segurança da Informação (SGSI), a Política de Privacidade disciplina especificamente o tratamento dos dados pessoais, os direitos dos titulares e as práticas de privacidade adotadas pela organização.
https://Ótima.digital/politica/politica-de-privacidade-de-dados/

14. Termos e Definições
Ameaça: Todo e qualquer evento que possa explorar uma vulnerabilidade, quer ela seja conhecida ou não.
Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade.
Ativo: Qualquer coisa que tenha ou possa gerar valor para a Ótima e deve ser adequadamente protegido.
Autenticidade: Garantia de que a informação é genuína e sua origem pode ser validada.
CGSI: Comitê Gestor de Segurança da Informação.
Colaborador: Empregado, estagiário, menor aprendiz ou qualquer outro indivíduo que venha a ter relacionamento profissional, direta ou indiretamente, com a Ótima.
Confidencialidade: Garantia de que o grau em que o acesso à informação é restrito a um grupo definido e autorizado a ter este acesso.
Dados Pessoais: Informação relacionada a pessoa natural identificada ou identificável.
Disponibilidade: é o grau em que a informação está disponível para o usuário e para o sistema de informação em operação, quando a organização precisa dela.
Gestão de Riscos: Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.
GSI: Departamento de Gestão de Segurança da Informação.

Integridade: Garantia de que a informação está atualizada sem erros.
ISO: Organização Internacional de Normalização e **IEC:** Comissão Eletrotécnica Internacional.
LGPD: Lei 13.709 de 14 de agosto de 2018, Lei geral de proteção de dados pessoais. Dispõe sobre o tratamento de dados pessoais.
Malware: Software malicioso projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa.
MFA: Significa Autenticação Multifator (Multi-Factor Authentication) — e é um dos controles de segurança mais recomendados, pois para provar sua identidade ele exige dois ou mais fatores de autenticação.
Privacy by Design – abordagem segundo a qual requisitos de privacidade e proteção de dados pessoais são considerados desde a concepção de processos, sistemas, produtos e serviços.
Privacy by Default – princípio segundo o qual sistemas e processos devem operar, por padrão, com o maior nível de proteção de dados pessoais possível, limitando o tratamento ao estritamente necessário.
Risco: Probabilidade de uma ameaça explorar uma vulnerabilidade.
SGSI: Sistema de gestão de segurança da informação.
SI: Segurança da Informação.
TI: Tecnologia da Informação.
Titular de Dados – pessoa natural a quem se referem os dados pessoais objeto de tratamento, conforme definido na LGPD.
Tratamento de Dados Pessoais – toda operação realizada com dados pessoais, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, armazenamento, eliminação ou qualquer outra forma prevista na LGPD.
Vulnerabilidade: Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

15. Histórico de atualizações

Elaboração revisão	Data	Versão	Escopo	Observação	Aprovação	Data publicação
F. Ferreira	05/02/2014	1	Edição	Revisão completa	Diretoria	23/02/2014
F. Ferreira	20/11/2015	2	Rev.	Sem alterações	Diretoria	26/11/2015
F. Ferreira	15/09/2017	3	Rev.	Atualização itens 12 e 13	Diretoria	18/09/2017
F. Ferreira	30/05/2018	4	Rev.	Atualização itens 12 e 13	Diretoria	10/06/2018
F. Ferreira	18/02/2019	5	Rev.	Atualização item 13	Diretoria	23/02/2019
F. Ferreira	13/04/2020	6	Rev.	Atualização itens 10 e 12	Diretoria	18/04/2020
F. Ferreira / Luiz Neto	10/07/2021	7	Rev.	Revisão completa	Diretoria	18/07/2021
F. Ferreira / Luiz Neto	15/08/2021	8	Rev.	Atualização item 12	Diretoria	19/08/2021
F. Ferreira / Luiz Neto	05/10/2022	9	Rev.	Revisão completa	Diretoria	12/10/2022
F. Ferreira / Luiz neto	04/02/2023	10	Rev.	Revisão completa	Diretoria	20/02/2023
F. Ferreira / Luiz neto	23/01/2024	11	Rev.	Atualização item 10	Diretoria	23/01/2024
F. Ferreira / L. Marcelino	15/07/2024	12	Rev.	Ajuste Item 8	Diretoria	18/07/2024

F. Ferreira / L. Marcelino	31/07/2025	13	Rev.	Revisão Completa	Diretoria	05/08/2025
F. Ferreira / L. Marcelino	16/09/2025	14	Rev.	Revisão	Diretoria	17/09/2025
F. Ferreira / L. Marcelino	03/05/2026	15	Rev.	Revisão	Diretoria	03/05/2026
F. Ferreira / L. Marcelino	05/07/2026	16	Rev.	Revisão Completa	Diretoria	05/07/2026