
 <b>ostec</b> Segurança digital de resultados	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>			
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	1 de 12

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**  
**(PSI)**


<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

 <b>ostec</b> <small>Segurança digital de resultados</small>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>			
	<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>
PL-GR-001	00	20/09/2024	Aprovado	2 de 12

## SUMÁRIO

1	OBJETIVO.....	3
2	ABRANGÊNCIA .....	4
3	DEFINIÇÕES .....	4
4	RESPONSABILIDADES.....	6
5	DIRETRIZES.....	7
5.1	Ações de segurança da informação e privacidade.....	9
6	POLÍTICAS, PROCEDIMENTOS E REGISTROS.....	9
7	DISTRIBUIÇÃO E IMPLEMENTAÇÃO .....	11
8	VEDAÇÕES .....	11
9	DISPOSIÇÕES FINAIS.....	12
10	NATUREZA DAS ALTERAÇÕES.....	12

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público


 <b>ostec</b> <small>Segurança digital de resultados</small>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>			
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	3 de 12

## 1 OBJETIVO

A Política de Segurança da Informação (PSI) tem como objetivo estabelecer diretrizes e princípios que garantam a confidencialidade, integridade, disponibilidade e privacidade das informações tratadas pelo **Grupo OSTEC**. A PSI é fundamentada nas melhores práticas internacionais, especialmente nas normas da família ISO 27000, como a ISO/IEC 27001, que fornece os requisitos para um sistema de gestão da segurança da informação (**SGSI**), e a ISO/IEC 27701, que expande o escopo para a proteção de dados pessoais (**SGPI**), alinhando-se com legislações como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR). São objetivos da **Política de Segurança da Informação**:

- a) estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;
- b) estabelecer orientações gerais de segurança da informação e privacidade, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confidencialidade, privacidade e autenticidade das informações;
- c) estabelecer competências e responsabilidades quanto à segurança da informação e privacidade;
- d) nortear a elaboração das políticas ou normas necessárias à efetiva implementação da segurança da informação e privacidade;
- e) promover o alinhamento das ações de segurança da informação e privacidade com as estratégias de planejamento organizacional do **Grupo OSTEC**.

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

 <b>ostec</b> <small>Segurança digital de resultados</small>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>			
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	4 de 12


## 2 ABRANGÊNCIA

O **Grupo OSTE**C reafirma seu compromisso com a segurança da informação e privacidade, implementando e monitorando rigorosamente seus controles para assegurar a confidencialidade, integridade, disponibilidade e privacidade de todos os ativos de informação. Nossa atuação é pautada pelo cumprimento das legislações vigentes, regulamentações aplicáveis e requisitos contratuais estabelecidos com clientes, colaboradores e demais partes interessadas. Estamos continuamente empenhados em aprimorar nossos produtos, processos e serviços, buscando sempre a excelência e a melhoria contínua em todas as nossas operações, sendo assim:

- a) fica instituída a Política de Segurança da Informação do Grupo OSTEC, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação e privacidade;
- b) esta Política de Segurança da Informação (PSI) aplica-se a todas as empresas do **Grupo OSTE**C e deve ser observada por todos os usuários de informação, sejam colaboradores, prestadores de serviços ou terceiros autorizados;
- c) todos os tipos de informações tratadas pelo **Grupo OSTE**C, incluindo dados pessoais de clientes, colaboradores, parceiros, fornecedores, e quaisquer outros dados confidenciais, proprietários ou sensíveis;
- d) todos os sistemas de informação, dispositivos, redes, servidores, aplicativos, bancos de dados, e quaisquer outros recursos tecnológicos utilizados no tratamento de informações;
- e) todos os processos e procedimentos relacionados à gestão da segurança da informação e à proteção de dados pessoais, incluindo o desenvolvimento, operação, manutenção, e descarte de ativos de informação;
- f) todos os colaboradores, incluindo funcionários, estagiários, temporários, contratados, e terceiros que desempenham funções nas dependências do **Grupo OSTE**C, ou em nome da empresa, independentemente de sua localização geográfica;
- g) todas as instalações físicas do **Grupo OSTE**C, incluindo escritórios, centros de dados, e quaisquer outros locais onde os ativos de informação sejam armazenados, processados ou transmitidos;
- h) todos os fornecedores de serviços terceirizados e parceiros comerciais que tenham acesso a informações e sistemas do **Grupo OSTE**C, ou que forneçam serviços críticos para as operações da empresa.

## 3 DEFINIÇÕES


<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

 <b>ostec</b> <small>Segurança digital de resultados</small>		<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>		
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	5 de 12

Para o entendimento claro e consistente desta Política de Segurança da Informação, são adotadas as seguintes definições:

- a) **Ativo de informação:** qualquer dado, sistema, software, hardware, documento ou recurso físico que tenha valor para a organização e necessite de proteção adequada.
- b) **Controle de acesso:** medidas para garantir que o acesso a ativos seja autorizado e restrito com base nos requisitos de negócios e segurança;
- c) **Autenticação:** processo de fornecer garantia de que uma característica alegada de uma entidade, como a identidade de um usuário ou dispositivo, é correta. A autenticação é fundamental para garantir que apenas indivíduos ou sistemas autorizados possam acessar determinados recursos ou informações;
- d) **Confidencialidade:** propriedade de que a informação não seja disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados;
- e) **Integridade:** propriedade de precisão e completude das informações;
- f) **Disponibilidade:** propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;
- g) **Privacidade:** controle sobre a coleta, armazenamento, uso e compartilhamento de dados pessoais, em conformidade com as legislações aplicáveis;
- h) **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- i) **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- j) **Titular do dado:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- k) **Parte interessada:** pessoa ou organização que pode afetar, ser afetada por, ou perceber-se afetada por uma decisão ou atividade. **Ex:** clientes, colaboradores, fornecedores, acionistas, órgãos reguladores, e parceiros de negócios.
- l) **Violação de privacidade:** situação em que dados pessoais são processados de forma inadequada, resultando em violação de um ou mais requisitos de proteção à privacidade, comprometendo a confidencialidade, integridade ou disponibilidade desses dados.
- m) **Sistema de gestão de segurança da informação (SGSI):** consiste em políticas, procedimentos, diretrizes, e recursos e atividades associados, geridos coletivamente por uma organização com o objetivo de proteger seus ativos de informação.

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

 <b>ostec</b> <small>Segurança digital de resultados</small>		<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>		
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	6 de 12

n) **Sistema de gestão de privacidade da informação (SGPI):** conjunto de políticas, processos e controles implementados para gerenciar e proteger dados pessoais, assegurando que a organização esteja em conformidade com as legislações de privacidade e garantindo que os direitos dos titulares dos dados sejam respeitados em todas as operações da organização.

#### 4 RESPONSABILIDADES

A estrutura de Gestão de Segurança da Informação e Privacidade é composta por:

a) **Alta direção:** responsável por assegurar o cumprimento da Política de Segurança da Informação (PSI) em todo o **Grupo OSTEC** e por fornecer os recursos necessários para sua implementação eficaz. A Alta Direção também é responsável por demonstrar comprometimento com a segurança da informação e promover uma cultura de segurança dentro da organização;


b) **Comitê do sistema de gestão de privacidade da informação (SGPI):** responsável pela governança da PSI e pela realização de revisões anuais, ou sempre que houver mudanças significativas, para garantir a conformidade com requisitos legais e regulamentares. O Comitê deve garantir que as revisões da política sejam realizadas adequadamente e que todas as políticas permaneçam consistentes e alinhadas com os objetivos estratégicos e operacionais do **Grupo OSTEC**;

c) **Gestores:** devem garantir que todos os membros de suas equipes compreendam e sigam a PSI, promovendo uma cultura de conformidade e segurança da informação e privacidade. São responsáveis por comunicar mudanças relevantes na política e assegurar que todos os colaboradores sob sua supervisão recebam o treinamento adequado sobre segurança da informação e privacidade;

d) **Encarregado pelo tratamento de dados pessoais (DPO):** responsável por monitorar a conformidade com a legislação de proteção de dados pessoais e com a PSI. Atua como ponto de contato entre o **Grupo OSTEC** e as autoridades de proteção de dados, e é responsável por gerenciar solicitações de titulares de dados e coordenar respostas a incidentes de segurança envolvendo dados pessoais;

e) **Gestor de segurança da informação:** responsável por desenvolver, implementar e manter a PSI, assim como garantir que todas as medidas de segurança sejam adequadamente aplicadas e que os incidentes de segurança sejam respondidos de maneira eficaz. O gestor também coordena as atividades relacionadas à segurança da informação e privacidade, conduz avaliações de risco e garante que todas as práticas de segurança estejam alinhadas com as políticas organizacionais;

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

 <b>ostec</b> <small>Segurança digital de resultados</small>		<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>		
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	7 de 12

f) **Gerente de infraestrutura:** responsável por coordenar as atividades operacionais associadas à segurança da informação, incluindo a implementação de medidas de proteção e a resposta a incidentes. É encarregado de receber e avaliar relatos de suspeitas ou confirmações de falhas, ameaças, eventos ou incidentes de segurança da informação, tomando as ações necessárias para mitigar riscos;

g) **Equipe de infraestrutura:** responsável pela implementação de medidas técnicas e administrativas para proteger os ativos de informação, garantindo a segurança, disponibilidade, integridade, confidencialidade e privacidade dos dados. A equipe deve executar atividades de manutenção e monitoramento dos sistemas, bem como colaborar na resposta a incidentes de segurança e privacidade;

h) **Todos os usuários:** todos os indivíduos ou organizações que tenham acesso aos sistemas e informações do **Grupo OSTECS** são responsáveis por cumprir esta Política de Segurança da Informação, bem como as diretrizes, medidas e procedimentos associados. Devem agir de forma a proteger a confidencialidade, integridade e disponibilidade e privacidade das informações, reportando imediatamente quaisquer incidentes ou suspeitas de violação de segurança.

## 5 DIRETRIZES

As ações de segurança da informação e privacidade do **Grupo OSTECS** e suas empresas são guiadas pelos princípios que regem a boa governança corporativa e a responsabilidade empresarial, incluindo os seguintes princípios:

a) **Confidencialidade, integridade, disponibilidade e privacidade das informações:**

i. **Confidencialidade:** Proteger as informações contra acessos não autorizados, mantendo sua privacidade;


ii. **Integridade:** Assegurar que as informações sejam precisas e confiáveis, protegendo-as contra modificações não autorizadas;

iii. **Disponibilidade:** Garantir que as informações estejam sempre acessíveis a quem necessita, assegurando continuidade operacional;

iv. **Privacidade:** Respeitar e proteger os dados pessoais conforme a legislação aplicável.

b) **Continuidade dos processos e serviços essenciais:** assegurar que os processos e serviços críticos para o funcionamento das empresas do **Grupo OSTECS** e o atendimento aos clientes sejam mantidos de acordo com o SLA estabelecido, mesmo diante de incidentes de segurança e privacidade;

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

 Segurança digital de resultados	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>			
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	8 de 12

c) **Economicidade da proteção dos ativos de informação:** proteger os ativos de informação de maneira eficaz e eficiente, otimizando recursos e garantindo o melhor retorno sobre os investimentos em segurança e privacidade. Investimentos em segurança da informação e privacidade devem ser proporcionais aos riscos e ao valor dos ativos de informação envolvidos, considerando as ameaças identificadas e a criticidade das operações;

d) **Respeito ao acesso à informação, proteção de dados pessoais e privacidade:** assegurar que o acesso à informação seja equilibrado com a necessidade de proteger dados pessoais e respeitar a privacidade dos indivíduos, em conformidade com a legislação aplicável. O acesso a recursos de tecnologia da informação deve ser baseado no princípio do menor privilégio, garantindo que colaboradores e terceiros tenham apenas as permissões necessárias para desempenhar suas funções, conforme aprovado pela administração;

e) **Responsabilidade do usuário:** todos os usuários de informação são responsáveis por suas ações, especialmente aquelas que possam comprometer a segurança e privacidade dos ativos de informação, assim como:

i. todos os contratos de prestação de serviços celebrados pelas empresas do **Grupo OSTE**C devem incluir uma cláusula específica que determine a obrigatoriedade de conformidade com esta Política de Segurança da Informação, bem como com quaisquer outras políticas ou normas correlatas;

ii. o acesso aos recursos de tecnologia da informação do **Grupo OSTE**C está condicionado à assinatura de um Termo de Responsabilidade ou Confidencialidade, preferencialmente de forma eletrônica, no qual o usuário declara estar ciente dos termos desta Política, das responsabilidades e compromissos decorrentes do uso desses recursos, bem como das penalidades aplicáveis em caso de descumprimento das normas de segurança da informação e privacidade estabelecidas pelo grupo.


f) **Alinhamento estratégico:** alinhar a Política de Segurança da Informação com o planejamento estratégico do **Grupo OSTE**C e suas empresas, garantindo coerência com os objetivos de negócio e outras normas internas de segurança da informação e privacidade;

g) **Conformidade com legislação e regulamentos:** assegurar que todas as normas e ações de segurança da informação e privacidade estejam em conformidade com as leis e regulamentos aplicáveis, incluindo, mas não se limitando à Lei Geral de Proteção de Dados (LGPD) e outras normas relevantes;

h) **Educação e comunicação:** fomentar uma cultura de segurança da informação e privacidade por meio de programas contínuos de educação e comunicação, garantindo que todos os colaboradores e parceiros estejam cientes de suas responsabilidades e das melhores práticas de segurança e privacidade;

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público



	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>			
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	9 de 12

i) **Melhoria contínua:** Promover a melhoria contínua das práticas de segurança da informação e privacidade, adaptando-se às novas ameaças e tendências tecnológicas;

j) **Colaboração e cooperação:** Promover a colaboração interna e externa, com colaboradores, parceiros, fornecedores e clientes, para fortalecer as práticas de segurança da informação e privacidade e compartilhar conhecimentos e experiências.

As diretrizes, supracitadas, formam os pilares da gestão de segurança da informação e privacidade no **Grupo OSTECS**, orientando a elaboração de políticas e normas complementares, com foco na melhoria contínua e adaptação a novas ameaças e requisitos legais.

As políticas, normas, procedimentos, manuais e metodologias de segurança da informação e privacidade do **Grupo OSTECS** devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação e privacidade.

### 5.1 Ações de segurança da informação e privacidade

As ações de segurança da informação e privacidade devem considerar, mas não limitar-se, aos itens relacionados abaixo:


- a) considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do **Grupo OSTECS**;
- b) ser tratadas de forma integrada, respeitando as especificidades e a autonomia das empresas do **Grupo OSTECS**;
- c) ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;
- d) visar à prevenção da ocorrência de incidentes.

A Política de Segurança da Informação e suas atualizações, bem como as políticas específicas de segurança e privacidade do **Grupo OSTECS** devem ser amplamente divulgadas a todos os Usuários de Informação com o objetivo de promover sua observância, conscientização e a formação de uma cultura sólida de segurança da informação e privacidade.

## 6 POLÍTICAS, PROCEDIMENTOS E REGISTROS

A Política de Segurança da Informação, juntamente com os demais normativos derivados desta política, faz parte do arcabouço normativo da Gestão de Segurança da Informação e Privacidade do **Grupo OSTECS**.

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

 <small>Segurança digital de resultados</small>	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>			
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	10 de 12


A Gestão da Segurança da Informação e Privacidade é composta, no mínimo, pelos seguintes processos:

- a) **Tratamento da informação:** processos relacionados à classificação, armazenamento, transmissão, e descarte seguro de informações sensíveis e confidenciais;
- b) **Segurança física e do ambiente:** medidas para proteger instalações físicas e o ambiente de TI contra acessos não autorizados, danos ou interferências;
- c) **Gestão de incidentes em segurança da informação e privacidade:** processos para detectar, responder e recuperar-se de incidentes de segurança e privacidade que possam comprometer a confidencialidade, integridade, disponibilidade ou privacidade das informações;
- d) **Gestão de ativos:** inventário e controle de ativos de informação, assegurando sua proteção adequada ao longo de seu ciclo de vida;
- e) **Gestão do uso dos recursos operacionais e de comunicações:** normas para o uso seguro e adequado de recursos como e-mail, acesso à internet, mídias sociais e serviços de computação em nuvem;
- f) **Controles de acesso:** implementação de mecanismos de controle para garantir que apenas indivíduos autorizados tenham acesso a recursos e informações específicos;
- g) **Gestão de riscos:** identificação, avaliação e tratamento de riscos associados à segurança da informação e privacidade;
- h) **Gestão de continuidade:** planejamento e implementação de medidas para assegurar a continuidade dos processos críticos de negócio em caso de incidentes de segurança ou interrupções;
- i) **Auditoria e conformidade:** processos para avaliar a conformidade com a política de segurança da informação, normas internas, e regulamentações externas, incluindo auditorias regulares;

O Comitê do sistema de gestão Segurança da Informação e Privacidade poderá definir outros processos de Gestão de Segurança da Informação e Privacidade, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação e privacidade.

Para cada um dos processos que constituem a Gestão de Segurança da Informação e Privacidade, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>			
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	11 de 12

Esses processos formam a base da Gestão da Segurança da Informação e Privacidade no **Grupo OSTEC**. As políticas, normas, procedimentos, orientações e manuais que regem esses processos são estabelecidos através das seções subsequentes.

## 7 DISTRIBUIÇÃO E IMPLEMENTAÇÃO

A Política de Segurança da Informação (PSI) terá plena divulgação para os membros das empresas que compoem o **Grupo OSTEC**, tal como disposto:


- a) a Política de Segurança da Informação (PSI) deve ser disponibilizada a todos os colaboradores das empresas que compõem o **Grupo OSTEC**, através dos canais de comunicação internos.
- b) sempre que uma nova versão ou uma revisão significativa for realizada, um aviso global será enviado a todos os colaboradores para notificá-los sobre as mudanças.
- c) o documento estará acessível por meio de um link na intranet do **Grupo OSTEC**.

## 8 VEDAÇÕES

São vedadas as seguintes ações em relação à segurança da informação e privacidade no âmbito do **Grupo OSTEC**:

- a) o uso de informações e recursos de tecnologia da informação do **Grupo OSTEC** para fins não autorizados ou alheios às atividades profissionais, incluindo, mas não se limitando a, uso pessoal, atividades ilícitas, ou qualquer uso que possa comprometer a segurança, privacidade e a integridade dos sistemas e dados;
- b) a instalação de software, aplicativos ou qualquer outro tipo de programa nos dispositivos e sistemas do **Grupo OSTEC** sem a prévia autorização da equipe responsável pela segurança da informação e privacidade;
- c) a divulgação de informações confidenciais ou sensíveis, incluindo dados pessoais de clientes, colaboradores ou parceiros, sem a devida autorização e fora dos procedimentos estabelecidos pela política de segurança da informação;
- d) o compartilhamento de credenciais de acesso, como senhas e tokens, com qualquer pessoa, interna ou externamente ao **Grupo OSTEC**, exceto quando especificamente autorizado e documentado pelas políticas internas;
- e) a manipulação, alteração ou exclusão de registros de dados e informações sem autorização expressa, fora dos procedimentos de controle e auditoria estabelecidos.

<b>Elaborador por</b>	<b>Aprovado por</b>	<b>Nível de Confidencialidade</b>
Daniel Cadorin	Comitê do SGPI	Público

 <b>ostec</b> <small>Segurança digital de resultados</small>		<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - EXTERNO</b>		
<b>Código</b>	<b>Revisão</b>	<b>Data de criação</b>	<b>Status</b>	<b>Pág.</b>
PL-GR-001	00	20/09/2024	Aprovado	12 de 12

## 9 DISPOSIÇÕES FINAIS

São disposições finais associadas a Política de segurança da informação do **Grupo OSTEC**:

- a) as empresas do Grupo OSTEC devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e privacidade;
- b) a conscientização, capacitação e sensibilização em segurança da informação e privacidade devem ser adequadas aos papéis e responsabilidades dos colaboradores;
- c) as denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação ou Encarregado de Proteção de Dados e devem ser feitas através dos seguintes canais: E-mail: [dpo@grupoostec.com](mailto:dpo@grupoostec.com)
- d) esta Política de Segurança da Informação deverá ser revisada periodicamente, com frequência mínima anual, ou sempre que houver mudanças significativas nos requisitos legais, regulamentares ou nos processos internos do **Grupo OSTEC**;
- e) o cumprimento desta Política, bem como das demais políticas que a complementam, deve ser avaliado periodicamente, com revisões no mínimo anuais, pelo **Grupo OSTEC** por meio de verificações de conformidade;
- f) a não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa;
- g) os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidos ao Comitê do sistema de gestão de Segurança da Informação e Privacidade.

## 10 NATUREZA DAS ALTERAÇÕES

Tabela – Histórico de revisões

Data	Revisão	Descrição	Alterado por	Aprovado por
23/09/2024	00	Elaboração inicial do documento	Daniel Cadorin	Comitê do SGPI

Elaborador por	Aprovado por	Nível de Confidencialidade
Daniel Cadorin	Comitê do SGPI	Público