PIRELLI - Inovação para Performance e Sustentabilidade

PDTI
Plano Diretor de Tecnologia da Informação
Período 2025/2026

Julho / 2024

Sumário

1 - Introdução

Este documento tem como objetivo apresentar um Plano Diretor de Tecnologia da Informação para a Pirelli para o período de 2025/2026.

O Plano Diretor de Tecnologia da Informação (PDTI) é um instrumento essencial para a gestão dos recursos e processos de TI em uma organização. Orienta a formulação de estratégias de TI de maneira assertiva, contribuindo para o sucesso do Negócio. Detalha os processos de TI utilizados pela organização para gerenciar suas operações. Ele serve como um guia para tomada de decisões relacionadas aos processos integrados e permite priorizar e implementar tarefas de acordo com as estratégias previamente formuladas. Ajuda a controlar decisões e facilita a gestão dos recursos da Tecnologia da Informação (TI), além de prover o alinhamento da Estratégia com a área de TI da instituição.

Assim, este documento contém um diagnóstico da área de TI, os macroprocessos que precisam ser trabalhados no referido biênio, as necessidades de aquisições, bem como um cronograma e os custos de tudo que precisa ser implantado.

2 – Referencial Estratégico

2.1. Nome da Empresa

Pirelli Pneus

2.2. Ramo de Atividade

Fábrica de Artefatos de Borracha; Fabricação de outras Peças e Acessórios para Veículos Automotores; Quanto à situação atual, a Pirelli reportou resultados acima das metas para o ano de 2023, com receitas de 6,65 bilhões de euros, um EBIT ajustado de 1 bilhão de euros e um lucro líquido de 495,9 milhões de euros. A empresa também confirmou sua liderança em índices-chave de sustentabilidade e alcançou metas de descarbonização dois anos antes do previsto.

2.3. Missão

Garantir a máxima Qualidade dos Produtos, a Excelência dos Sistemas e Processos de Produção.

2.4. Visão

Ser reconhecida por colaboradores, parceiros e clientes como a maior revenda Pirelli de sua área de atuação, por meio da excelência e respeito nas relações comerciais, interpessoais e ambientais.

2.5. Valores

Lealdade e Seriedade; Transparência; Crescimento Sustentável; Foco no Cliente; Responsabilidade e Busca de Resultados; Excelência Profissional; Inovação; Qualidade e Desempenho; Integração; Velocidade.

2.6. Alinhamento da TI ao Planejamento Estratégico

Para alinhar a área de TI ao planejamento estratégico da empresa, pretende-se atualizar o parque computacional, melhorar a gestão e implantar a chamada governança de TI. A área de TI também visa primar pela ética profissional, sustentabilidade, qualidade e excelência dos produtos e serviços oferecidos aos clientes, aumentar e melhorar o conhecimento, atualizar o ambiente WEB, minimizar custos e auferir lucros, se possível.

3 – Diagnóstico

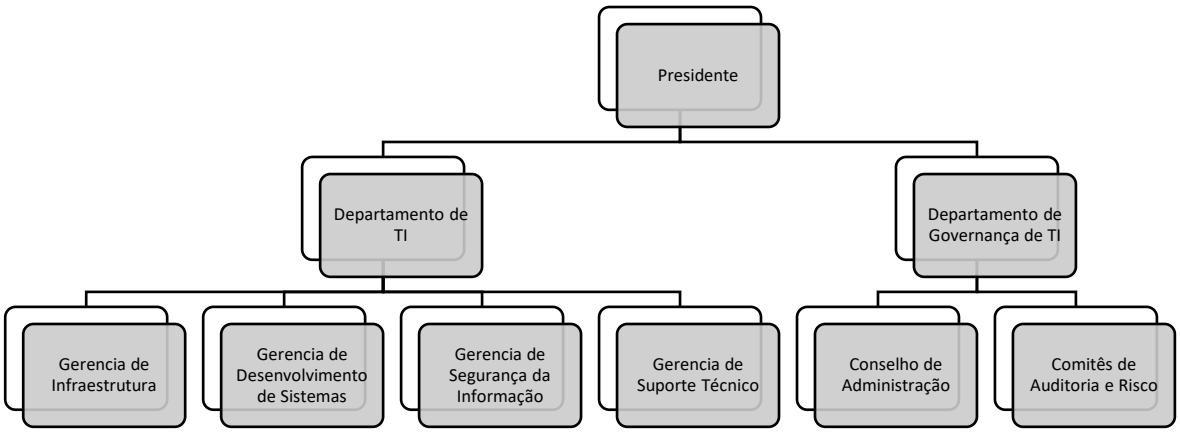
3.1. Análise SWOT da TI

A análise SWOT é uma ferramenta de planejamento estratégico que ajuda a identificar as Forças, Fraquezas, Oportunidades e Ameaças de uma organização ou projeto. Originada na década de 1960, ela permite uma avaliação abrangente do cenário interno e externo, facilitando a tomada de decisões e o alinhamento estratégico.

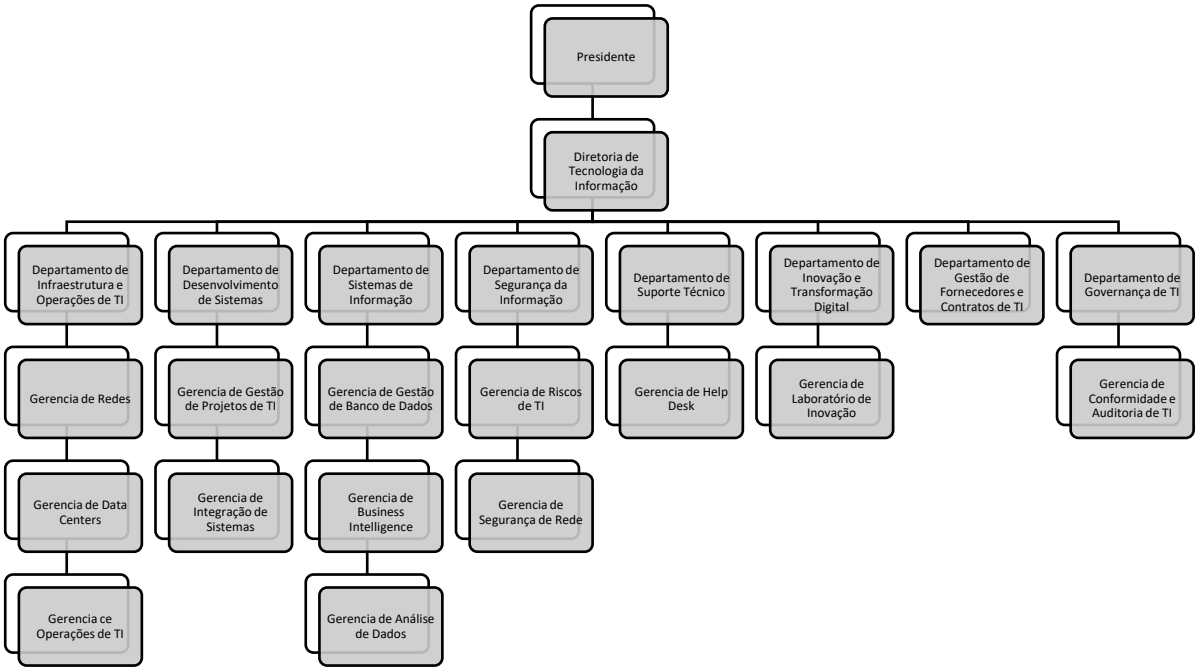
Forças	Fraquezas
• Comprometimento da administração superior com a área de TI. • Práticas eficientes de desenvolvimento de sistemas e portais web.	• Falta de capacitação contínua da equipe de TI. • Comunicação interna ineficaz. • Estrutura organizacional da área de TI inadequada. • Atendimento ao usuário deficiente. • Sistemas de Informação desatualizados. • Necessidade de implementação da governança de TI. • Inexistência de ações de sustentabilidade • Necessidade de melhorar a qualidade nos processos de desenvolvimento de software; • Baixa utilização da intranet; Inexistência de ações de sustentabilidade e de ética; • Inexistência de uma Política de Segurança da Informação; • Necessidade de melhorar processos de gestão do conhecimento;
Oportunidades	**Ameaças**
• Utilização de tecnologias livres e/ou gratuitas. • Tendências e inovações em TIC que a serem adotadas. • Possibilidade de padronização e integração das soluções de TIC.	• Resistência da organização às mudanças tecnológicas. • Rotatividade da equipe técnica. • A rápida evolução tecnológica e à concorrência no setor. • Ataques cibernéticos; • Mudanças na legislação;

3.2. Estrutura Organizacional Atual

A Pirelli precisa atualizar sua estrutura organizacional na área de TI para enfrentar desafios futuros, como a necessidade de maior agilidade em um mercado automotivo em rápida transformação, especialmente com o aumento dos veículos elétricos e a demanda por pneus especializados. Além disso, a digitalização contínua e a inovação em processos podem exigir uma estrutura mais flexível e adaptável para manter a competitividade e a eficiência operacional. Mudanças estruturais podem ser necessárias para melhor capitalizar as homologações e acelerar a inovação de produtos e processos, conforme destacado no plano industrial da empresa.



3.2. Estrutura Organizacional Proposta



4 – Planejamento dos Macroprocessos Estratégicos para a Área de Tecnologia

4.1 Governança de TI

A Governança de TI é uma quebra da Governança Corporativa e abrange um conjunto de normas, práticas, ações, competências e responsabilidades necessárias para alinhar os recursos de TI à estratégia organizacional. Ou seja, a Governança de TI é um conjunto de estratégias relacionadas às políticas de governança corporativa (baseando-se na missão, visão e valores da organização), mas com ênfase nos processos de gestão dos recursos tecnológicos, responsável por alinhar as políticas e estratégias da área de TI com as necessidades das demais áreas.

4.1.1 Princípios de TI

Princípios e diretrizes são considerados regras gerais que norteiam os conceitos de uma matéria, orientando a tomada de decisão. Constituem proposições estruturantes para determinado fim, ou seja, são alicerces de um assunto. A ISO/IEC 38500 fornece seis princípios básicos de governança de TI em suas normas: responsabilidade, estratégia, aquisições, desempenho, conformidade e comportamento humano. Elas estão registradas no site da ABNT, a Associação Brasileira de Normas Técnicas:

Princípio	Detalhamento	Origem
Responsabilidade	Envolver-se ativamente na sustentabilidade ambiental e social, assegurando práticas empresariais responsáveis e sustentáveis.	Relatório de Sustentabilidade da Pirelli
Estratégia	Integrar a sustentabilidade nas estratégias de negócios, promovendo inovação e melhorando continuamente os processos e produtos.	Estratégia Corporativa da Pirelli
Aquisições	Garantir que os fornecedores cumpram padrões éticos, ambientais e sociais, alinhando-se aos valores da Pirelli.	Código de Conduta de Fornecedores da Pirelli
Desempenho	Monitorar e melhorar continuamente o desempenho ambiental, social e de governança, estabelecendo metas e indicadores claros.	Relatório Anual de Desempenho da Pirelli
Conformidade	Assegurar que todas as operações da empresa estejam em conformidade com as leis, regulamentos e normas internacionais aplicáveis.	Programa de Conformidade da Pirelli
Comportamento Humano	Promover um ambiente de trabalho inclusivo e diverso, assegurando o respeito aos direitos humanos e combatendo qualquer forma de discriminação ou assédio.	Política de Diversidade e Inclusão da Pirelli

4.1.2 Iniciativas Estratégicas

Visando alinhar a área de TI ao planejamento estratégico da empresa, estão sendo propostas as seguintes Iniciativas Estratégicas:

Objetivo Estratégico	Iniciativas Estratégicas
OE01 – Reestruturar a área de TI	IE01- Atualizar o Parque Computacional.
	IE02- Evoluir estrutura de dados e de comunicação para a área de TI.
	IE03- Ampliar o desenvolvimento e manutenção de sistemas informatizados.
	IE04- Avaliar tecnologias e métodos a serem requeridos para a modernização da internet e intranet.
OE02 – Melhorar a gestão e implantar a governança de TI.	IE05- Implantar Governança de TI.
	IE06- Evoluir sistema de gestão de projetos da TI da Alfa Segurança.
	IE07- Implantar política de gestão de RH.
OE03 – Primar pela ética profissional, sustentabilidade, qualidade e excelência dos produtos e serviços oferecidos aos clientes.	IE09- Criar Comissão de Ética
	IE10- Criar Código de Ética.
	IE11- Implantar ações de sustentabilidade.
	IE12- Implantar programa de melhoria de processos de desenvolvimento de software da Alfa Segurança.
OE04 – Aumentar e melhorar o conhecimento.	IE13- Realizar diagnóstico para melhorar o conhecimento na TI.
	IE14- Melhorar processos e implantar novas tecnologias/práticas de gestão do conhecimento.
	IE15- Implementar plano de capacitação de TI.
OE05 – Auferir lucros por intermédio da área de TI.	IE16- Criar Plano de Negócios para desenvolver novo produto ou serviço.
OE06 – Melhorar a Segurança da Informação	IE17- Criar política de segurança da informação para a área de TI.

4.1.3 Plano de Ações – Biênio 2025/2026

OE	IE	Ações / Projetos	Início	Término
1	1	Levantamento do hardware e software existente.	Jan 25	Dez 26
1	1	Decisão sobre quantidades e o que Atualizar.	Jan 25	Dez 26
1	1	Contratações.	Jan 25	Dez 26
1	2	Criar projeto para evoluir estrutura de dados e de comunicação para a área de TI.	Jan 25	Dez 26
1	2	Contratar empresa especializada para realizar o projeto.	Fev 25	Mar 26
1	2	Implementar o novo projeto de estrutura de dados e comunicação.	Abr 25	Jun 26
2	1	Implantar Governança de TI.	Jan 25	Dez 26
2	1	Contratar consultor especializado em Governança de TI.	Fev 25	Mar 26
2	1	Elaboração e aprovação da Política de Governança de TI.	Abr 25	Jun 26
2	1	Implementação da Política de Governança de TI.	Jul 25	Set 26
2	2	Evoluir sistema de gestão de projetos da TI da Segurança.	Jan 25	Dez 26
2	2	Contratar empresa especializada para realizar a evolução do sistema.	Fev 25	Mar 26
2	2	Implementar a nova versão do sistema de gestão de projetos.	Abr 25	Jun 26
2	3	Implantar política de gestão de RH.	Jan 25	Dez 26
2	3	Elaboração e aprovação da Política de Gestão de RH.	Fev 25	Mar 26
2	3	Implementação da Política de Gestão de RH.	Abr 25	Jun 26
2	4	Criar Comissão de Ética.	Jan 25	Dez 26
3	1	Divulgar o Código de Ética para os profissionais da área de TI.	Abr 25	Jun 26
3	2	Implantar ações de sustentabilidade.	Jan 25	Dez 26
3	2	Realizar diagnóstico das ações de sustentabilidade em andamento.	Fev 25	Mar 26

4.2. Gestão da Segurança da Informação

A Gestão da Segurança da Informação é fundamental para proteger os ativos digitais de uma organização. Ela envolve a implementação de práticas, políticas e procedimentos que visam garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas.

4.2.1 Política de Segurança da Informação

A Política de Segurança da Informação da Pirelli encontra-se no anexo II do presente documento.

4.3. Gestão do Conhecimento

4.3.1 Diagnóstico de Gestão do Conhecimento na TI

Para realização do diagnóstico sobre a Gestão do Conhecimento foi utilizado o Método Maturidade em Gestão do Conhecimento constante de (BATISTA, 2012), onde foi verificada a pontuação constante das tabelas abaixo (itens de 1 a 42), atribuindo uma nota, conforme critérios abaixo:

Para os itens de 1 a 36 utilizar os valores de 1 a 5 da tabela abaixo:

Situação Atual	Escala de Pontuação
As ações descritas são muito bem realizadas	5
As ações descritas são bem realizadas	4
As ações descritas são realizadas de forma adequada	3
As ações descritas são mal realizadas	2
As ações descritas são muito mal realizadas ou ainda não são realizadas	1

Para os itens de 37 a 42 utilizar os valores de 1 a 5 da tabela abaixo:

Situação Atual	Escala de Pontuação
Houve melhoria em todos os indicadores utilizados	5
Houve melhoria em quase todos os indicadores utilizados	4
Houve melhoria nos resultados da maioria dos indicadores utilizados	3
Houve melhoria nos resultados de alguns indicadores utilizados	2
A organização não melhorou ou ainda não é possível comprovar melhorias por ausência de indicadores	1

CRITÉRIO 1.0: LIDERANÇA EM GESTÃO DO CONHECIMENTO		PONTUAÇÃO
1	A organização compartilha o Conhecimento, a Visão e a Estratégia de GC fortemente alinhados com a visão, missão e objetivos estratégicos da organização.	4
2	Arranjos organizacionais foram implantados para formalizar as iniciativas de GC (exemplos: Uma unidade central de coordenação da gestão da informação/conhecimento; Gestor Chefe de Gestão da Informação/Conhecimento; Equipes de Melhoria da Qualidade; Comunidades de Prática; e Redes de Conhecimento).	4
3	Recursos financeiros são alocados nas iniciativas de GC.	3
4	A organização tem uma política de proteção da informação e do conhecimento (exemplos: proteção da propriedade intelectual, segurança da informação e do conhecimento e política de acesso, integridade, autenticidade e sigilo das informações).	3
5	A alta administração e as chefias intermediárias servem de modelo ao colocar em prática os valores de compartilhamento do conhecimento e de trabalho colaborativo. Eles passam mais tempo disseminando informação para suas equipes e facilitando o fluxo horizontal de informação entre suas equipes e equipes de outros departamentos/divisões/unidades.	3
6	A alta administração e as chefias intermediárias promovem reconhecem e recompensam a melhoria do desempenho, o aprendizado individual e organizacional, o compartilhamento de conhecimento e a criação do conhecimento e inovação.	4
SUBTOTAL CRITÉRIO 1.0: LIDERANÇA EM GESTÃO DO CONHECIMENTO ORGANIZACIONAL - CGO		21

CRITÉRIO 2.0: PROCESSO		PONTUAÇÃO
7	A organização define suas competências essenciais (capacidades importantes do ponto de vista estratégico que concede à organização vantagem comparativa) e as alinha à sua missão e aos objetivos da organização.	3
8	A organização modela seus sistemas de trabalho e processos de apoio e finalísticos chave para agregar (“ao invés de criar”) valor ao cliente e alcançar alto desempenho institucional.	4
9	Na modelagem de processos são contemplados os seguintes fatores: novas tecnologias, compartilhamento de conhecimento na organização, flexibilidade, eficiência, eficácia e efetividade para o cliente.	4
10	A organização tem um sistema organizado para gerenciar situações de crise ou eventos imprevistos que assegura a continuidade das operações, prevenção e recuperação.	4

11	A organização implementa e gerencia os processos de apoio e finalísticos chave para assegurar o atendimento dos requisitos do cliente e a manutenção dos resultados da organização.	3
12	A organização avalia e melhora continuamente seus processos de apoio e finalísticos para alcançar um melhor desempenho, reduzir a variação, melhorar produtos e serviços públicos, e para manter-se atualizada com as práticas de excelência em gestão.	4
SUBTOTAL CRITÉRIO 2.0: PROCESSO		22

CRITÉRIO 3.0: PESSOAS		**PONTUAÇÃO**
13	Os programas de educação e capacitação, assim como os de desenvolvimento de carreiras ampliam o conhecimento, as habilidades e as capacidades do servidor público, servem de apoio para o alcance dos objetivos da organização e contribuem para o alto desempenho institucional.	4
14	A organização dissemina de maneira sistemática informações sobre os benefícios, a política, a estratégia, o modelo, o plano e as ferramentas de GC para novos funcionários/servidores da organização.	4
15	A organização tem processos formais de "*mentoring*", "*coaching*" e tutoria.	3
16	A organização conta com banco de competências dos seus servidores públicos.	3
17	A colaboração e o compartilhamento do conhecimento são ativamente reconhecidos e recompensados/corrigidos.	3
18	A organização do trabalho contempla a formação de pequenas equipes/grupos (exemplos: grupos de trabalho, comissões, círculos de qualidade, equipes de melhoria de processos de trabalho, equipes interfuncionais, equipes interdepartamentais, comunidades de prática) e a estrutura por processos para enfrentar as preocupações e os problemas no local de trabalho.	3
SUBTOTAL CRITÉRIO 3.0: PESSOAS		20

CRITÉRIO 4.0: TECNOLOGIA		**PONTUAÇÃO**
19	A alta administração implantou uma infraestrutura de tecnologia da informação – TI (exemplos: Internet, Intranet e sítio na Rede Mundial de Computadores (web) e dotou a organização com a estrutura necessária para facilitar a efetiva GC).	3
20	A infraestrutura de TI está alinhada com a estratégia de GC da organização.	3
21	Todas as pessoas da organização têm acesso a computador.	3
22	Todas as pessoas têm acesso à Internet/intranet e a um endereço de e-mail.	3
23	As informações disponíveis no sítio da web/intranet são atualizadas regularmente.	3

24	A Intranet (ou uma rede similar) é usada como a principal fonte de comunicação em toda a organização como apoio à transferência de conhecimento e ao compartilhamento de informação.	3
SUBTOTAL CRITÉRIO 4.0: TECNOLOGIA		18

CRITÉRIO 5.0: PROCESSOS DE CONHECIMENTO		**PONTUAÇÃO**
25	A organização tem processos sistemáticos de identificação, criação, armazenamento, compartilhamento e utilização do conhecimento.	4
26	A organização conta com um mapa de conhecimento e distribui os ativos ou recursos de conhecimento por toda a organização.	4
27	O conhecimento adquirido após a execução de tarefas e a conclusão de projetos é registrado e compartilhado.	2
28	O conhecimento essencial de servidores públicos que estão saindo da organização é retido.	3
29	A organização compartilha as melhores práticas e lições aprendidas por toda a organização para que não haja um constante “reinventar da roda” e retrabalho.	3
30	As atividades de “benchmarking” são realizadas dentro e fora da organização, os resultados são usados para melhorar o desempenho organizacional e criar conhecimento.	4
SUBTOTAL CRITÉRIO 5.0: PROCESSOS DE CONHECIMENTO		20

CRITÉRIO 6.0: APRENDIZAGEM E INOVAÇÃO		**PONTUAÇÃO**
31	A organização articula e reforça continuamente como valores a aprendizagem e a inovação.	4
32	A organização considera a atitude de assumir riscos ou o fato de cometer erros como oportunidades de aprendizagem desde que isso não ocorra repetidamente.	4
33	Equipes interfuncionais são formadas para resolver problemas ou lidar com situações preocupantes que ocorrem em diferentes unidades gerenciais da organização.	3
34	As pessoas sentem que recebem autonomia dos seus superiores hierárquicos e que suas ideias e contribuições são geralmente valorizadas pela organização.	3
35	As chefias intermediárias estão dispostas a usar novas ferramentas e métodos.	4
36	As pessoas são incentivadas a trabalhar junto com outros e a compartilhar informação.	4
SUBTOTAL CRITÉRIO 6.0: APRENDIZAGEM E INOVAÇÃO		22

CRITÉRIO 7.0: RESULTADOS DA GESTÃO DO CONHECIMENTO		PONTUAÇÃO
37	A organização tem um histórico de sucesso na implementação da GC e de outras iniciativas de mudança que pode ser comprovado com resultados de indicadores de desempenho.	3
38	São utilizados indicadores para avaliar o impacto das contribuições e das iniciativas de GC nos resultados da organização.	3
39	A organização melhorou – graças às contribuições e às iniciativas da GC – os resultados relativos aos indicadores de qualidade dos produtos e serviços.	3
40	A organização melhorou – graças às contribuições e às iniciativas de GC – os resultados relativos aos indicadores de eficiência.	3
41	A organização melhorou – graças às contribuições e às iniciativas de GC – os resultados relativos aos indicadores de efetividade social.	3
42	A organização melhorou – graças às contribuições e às iniciativas de GC – a capacidade de realização dos seus objetivos estratégicos: linhas de negócio e de gestão.	3
SUBTOTAL CRITÉRIO 7.0: RESULTADOS DA GESTÃO DO CONHECIMENTO RESULTADOS DA GESTÃO DO CONHECIMENTO		18

Fonte: Adaptado da publicação da Asian Productivity Organizational (APO) – KM Facilitator's Guide.

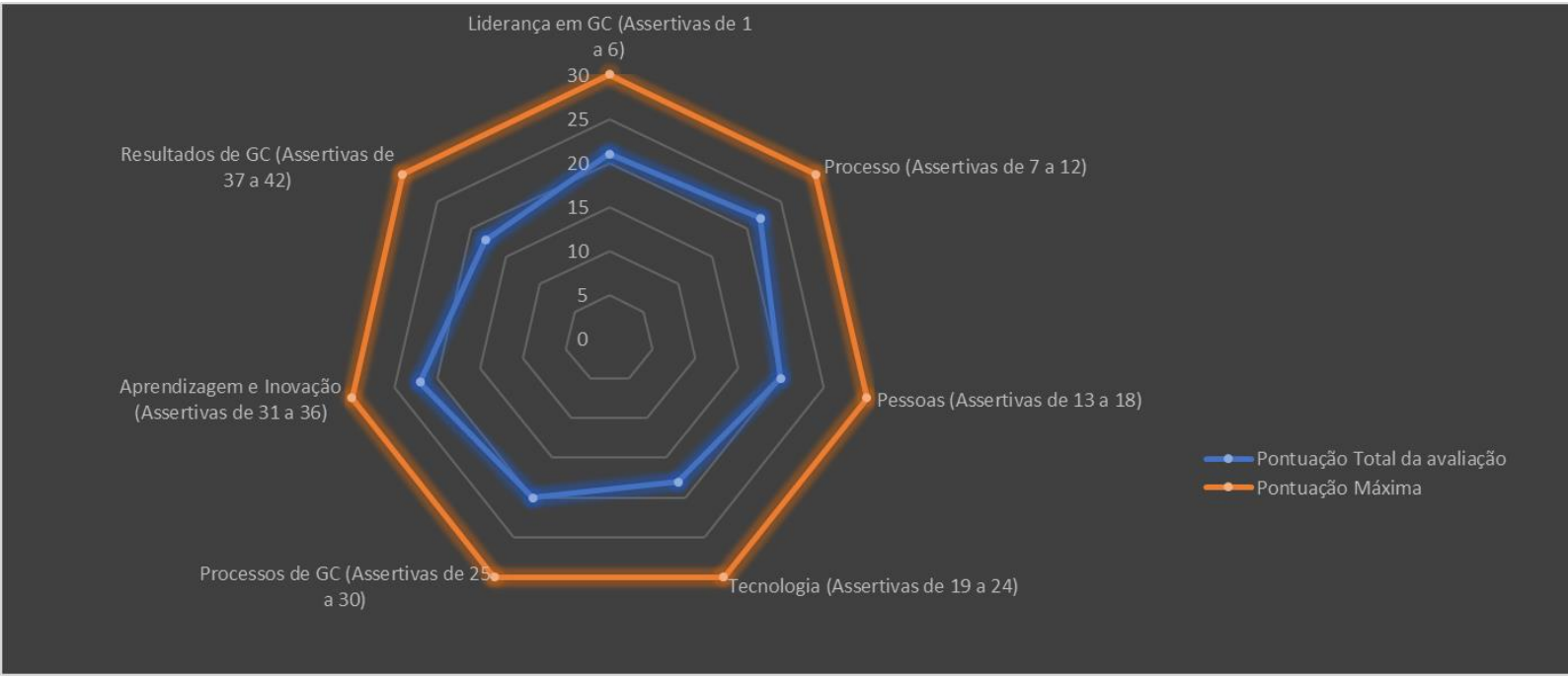
Tabela Resumo da Pontuação e Gráfico

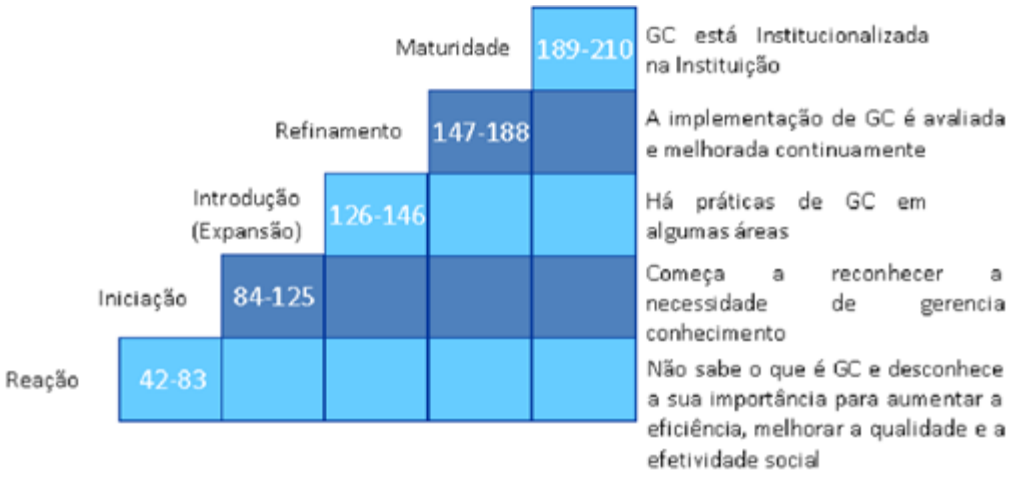
Critério	Pontuação por Critério Pontuação Total da avaliação (1)		Pontuação Máxima (2)
1.0	Liderança em GC (Assertivas de 1 a 6)	21	30
2.0	Processo (Assertivas de 7 a 12)	22	30
3.0	Pessoas (Assertivas de 13 a 18)	20	30
4.0	Tecnologia (Assertivas de 19 a 24)	18	30
5.0	Processos de GC (Assertivas de 25 a 30)	20	30
6.0	Aprendizagem e Inovação (Assertivas de 31 a 36)	22	30
7.0	Resultados de GC (Assertivas de 37 a 42)	18	30
	TOTAL	141	210

Fonte: KM Facilitator's Guide da APO

Legenda:

Na Coluna (1), escreva o subtotal da pontuação por critério. Ao final, some as pontuações individuais dos critérios e escreve o valor no TOTAL.





Com base na pontuação total obtida nos critérios e conforme ilustrado na figura acima, o Método Maturidade em Gestão do Conhecimento constante de (BATISTA, 2012) ratificou a média. Pontuação – patamar “Introdução (Expansão)”.
Desta forma, 141 pontos totais de 210 pts. representam 67.14% do que se poderia atingir.

4.3.2 Proposta de Processos e Tecnologias de Gestão do Conhecimento para TI

Com base no diagnostico acima estão sendo propostos os seguintes processos e práticas para a área de TI da Pirelli.

OBTER/CRIAR	PROTEGER
Pesquisa e Desenvolvimento	Criptografia
Benchmarking	Certificação Digital

4.3.3 Mapeamento de competências para a área de TI

Matriz de competências/Funções													
Grau de Conhecimento: N - Não necessário B - Básico (tem noção, superficial) D - Domina (suficiente, usa no dia-dia) E - Especialista (larga experiência)	**FUNÇÕES / PERFIS**												
COMPETÊNCIAS (MÓDULOS DE FORMAÇÃO)	Chefe da Pirelli	Diretor de TI	Diretor de Tecnologia	Gerente de Desenvolvimento	Desenvolvedor	Gerente de Infraestrutura	Administrador de Redes	Administrador de Sistemas	Gerente de Segurança da Informação	Analista de Segurança de Informação	Gerente de Suporte Técnico	Técnico de Suporte	
Gestão de TI													
Gerenciamento de Projetos	E	E	B	N	N	E	N	N	B	B	N	N	
PMBoK	E	E	B	N	N	E	N	N	B	B	N	N	
Scrum	E	E	B	N	N	E	N	N	B	B	N	N	
Kanban	E	E	B	N	N	E	N	N	B	B	N	N	
Governança de TI	E	E	B	N	N	E	N	N	B	B	N	N	
COBIT	E	E	B	N	N	E	N	N	B	B	N	N	
ITIL	E	E	B	N	N	E	N	N	B	B	N	N	
Liderança	E	E	B	N	N	E	N	N	B	B	N	N	
Desenvolvimento													
Linguagens de Programação	N	D	E	E	E	D	B	B	D	E	N	B	
Java	N	D	E	E	E	D	B	B	D	E	N	B	
Python	N	D	E	E	E	D	B	B	D	E	N	B	
C++	N	D	E	E	E	D	B	B	D	E	N	B	
C#	N	D	E	E	E	D	B	B	D	E	N	B	
JavaScript	N	D	E	E	E	D	B	B	D	E	N	B	
R	N	D	E	E	E	D	B	B	D	E	N	B	
Cobol	N	D	E	E	E	D	B	B	D	E	N	B	

Desenvolvimento Web	N	D	E	E	E	D	B	B	D	E	N	B	
HTML	N	D	E	E	E	D	B	B	D	E	N	B	
CSS	N	D	E	E	E	D	B	B	D	E	N	B	
Frameworks	N	D	E	E	E	D	B	B	D	E	N	B	
React	N	D	E	E	E	D	B	B	D	E	N	B	
Angular	N	D	E	E	E	D	B	B	D	E	N	B	
Banco de Dados	N	D	E	E	E	D	B	B	D	E	N	B	
DevOps	N	D	E	E	E	D	B	B	D	E	N	B	
Jenkins	N	D	E	E	E	D	B	B	D	E	N	B	
Docker	N	D	E	E	E	D	B	B	D	E	N	B	
Segurança da Informação													
Redes de Computadores	N	E	B	D	N	B	E	D	E	D	B	D	
IPv4	N	E	B	D	N	E	E	D	E	D	B	B	
IPv6	N	E	B	D	N	E	E	D	E	D	B	B	
Sistemas Operacionais	N	E	B	D	N	E	E	D	E	D	B	D	
Windows	N	E	B	D	N	D	E	D	E	D	B	B	
Linux	N	E	B	D	E	D	E	D	E	D	B	B	
Defesa Cibernética	N	E	B	D	N	B	E	D	E	D	B	B	
Auditoria de Sistemas	N	E	B	D	N	B	E	D	E	D	B	B	
Investigação Forense	N	E	B	D	N	B	E	D	E	D	B	B	
Teste de Invasão	N	E	B	D	N	B	E	D	E	D	B	B	
Técnicas													
Análise de Dados	B	D	E	B	B	E	E	D	E	E	D	D	
BI	B	D	E	B	B	E	E	D	E	E	D	D	
Infraestrutura de TI	B	D	E	B	E	E	E	D	E	E	D	D	
Servidores	B	D	E	B	D	E	E	D	E	E	D	D	
Armazenamento	B	D	E	B	B	E	E	D	E	E	D	D	
Computação em nuvem	B	D	E	B	D	E	E	D	E	E	D	D	
Suporte													
Técnico	N	B	D	N	D	D	D	D	B	B	E	D	
Hardware	N	B	D	N	D	D	E	D	B	B	E	D	
Software	N	B	D	N	D	D	E	D	B	B	E	D	
Atendimento ao usuário	N	B	D	N	D	N	N	N	B	B	E	D	
Manutenção de Computadores	N	B	D	N	D	N	N	N	B	B	E	D	
Instalação e Configuração	N	B	D	N	D	B	N	N	B	B	E	D	
Ferramentas de TI	N	B	D	N	D	B	N	N	B	B	E	D	
Comunicação	N	B	D	N	D	N	N	N	B	B	E	D	

4.4. Ética Profissional e Desenvolvimento Sustentável

4.4.1 Ética Profissional:

a) Código de Ética

O Código de Ética da Pirelli encontra-se no anexo III do presente documento

4.4.2 Desenvolvimento Sustentável

a) Educação Ambiental

Proposta de desenvolvimento sustentável para a Pirelli para os próximos dois anos:

Título: “Pirelli Verde 2026: Educação e Ação para um Futuro Sustentável”

Visão Geral: A Pirelli Verde 2026 é uma iniciativa abrangente que visa integrar a educação ambiental e a responsabilidade socioambiental no núcleo dos negócios da Pirelli. O programa se concentrará em dois pilares principais: Educação para Sustentabilidade e Inovação Responsável.

1. Educação para Sustentabilidade:

Programa de Conscientização Ambiental: Desenvolver e implementar um programa de treinamento para todos os funcionários, focando na importância da sustentabilidade ambiental e nas práticas que podem ser adotadas no local de trabalho e em casa.
Parcerias Educacionais: Colaborar com instituições de ensino para criar programas de estudo e workshops que promovam a conscientização ambiental entre os jovens.
Campanhas de Comunicação: Utilizar todos os canais de comunicação da empresa para disseminar informações sobre práticas sustentáveis e o impacto ambiental das atividades humanas.

2. Inovação Responsável:
Desenvolvimento de Produtos Sustentáveis: Continuar a pesquisa e desenvolvimento de materiais mais sustentáveis e processos de produção que minimizem o impacto ambiental.
Redução de Resíduos e Reciclagem: Estabelecer metas para reduzir resíduos em todas as operações e aumentar a taxa de reciclagem de materiais.

Energia Renovável e Eficiência: Expandir o uso de energias renováveis nas operações da Pirelli e melhorar a eficiência energética em todas as instalações.

b) Responsabilidade Socioambiental

Metas de Responsabilidade Socioambiental para 2026:

Educação: Alcançar 100% de participação dos funcionários nos programas de treinamento de sustentabilidade.

Produtos Sustentáveis: Aumentar a receita de produtos Green Performance para 60% do total de receitas da Pirelli.

Emissões de CO2: Reduzir as emissões de CO2 em 20% em relação aos níveis de 2021.

Consumo de Água: Diminuir o consumo de água em 30% em comparação com 2021.

Energia Renovável: Garantir que 50% da energia utilizada seja proveniente de fontes renováveis.

Implementação:

Comitê de Sustentabilidade: Formar um comitê dedicado para supervisionar a implementação da Pirelli Verde 2026, composto por membros de diferentes departamentos e níveis hierárquicos.

Relatórios e Avaliação: Publicar relatórios anuais sobre o progresso das iniciativas de sustentabilidade e realizar avaliações periódicas para garantir que as metas estejam sendo alcançadas.

4.5. Gestão da Qualidade

4.5.1 Melhoria da Qualidade (CMMI 1.3)

A Pirelli, reconhecida globalmente pela qualidade de seus produtos, está em constante busca pela excelência em seus processos, especialmente no que tange ao desenvolvimento de software. Nesse contexto, o Modelo de Maturidade de Capacidade Integrado (CMMI) surge como um framework essencial para aprimorar a qualidade e eficiência do processo de desenvolvimento.

Atualmente, a Pirelli encontra-se no Nível 2 - Gerenciado do CMMI, o que significa que já possui processos estabelecidos que são planejados e executados de acordo com a política, os procedimentos, as ferramentas e os recursos da empresa. No entanto, para alcançar o Nível 3 - Definido, onde os processos são bem caracterizados e entendidos, e são descritos em padrões, procedimentos, ferramentas e métodos, a empresa precisa implementar dois processos chave que ainda não foram adotados pela área de TI.
Os processos do Nível 2 que necessitam de implementação são:

- Gerenciamento de Acordos de Fornecedores (SAM): Este processo é vital para estabelecer acordos de gestão com fornecedores que se alinham com as necessidades do projeto e da organização. A implementação eficaz do SAM garantirá que os fornecedores e a Pirelli estejam em sintonia, resultando em entregas de software mais confiáveis e de alta qualidade.
- Planejamento de Trabalho (WP): O Planejamento de Trabalho envolve a criação de planos que definem as atividades necessárias para atingir os objetivos do projeto. Com um planejamento robusto, a Pirelli poderá antecipar riscos, gerenciar recursos de forma mais eficiente e garantir que as metas do projeto sejam atingidas dentro do prazo e do orçamento.

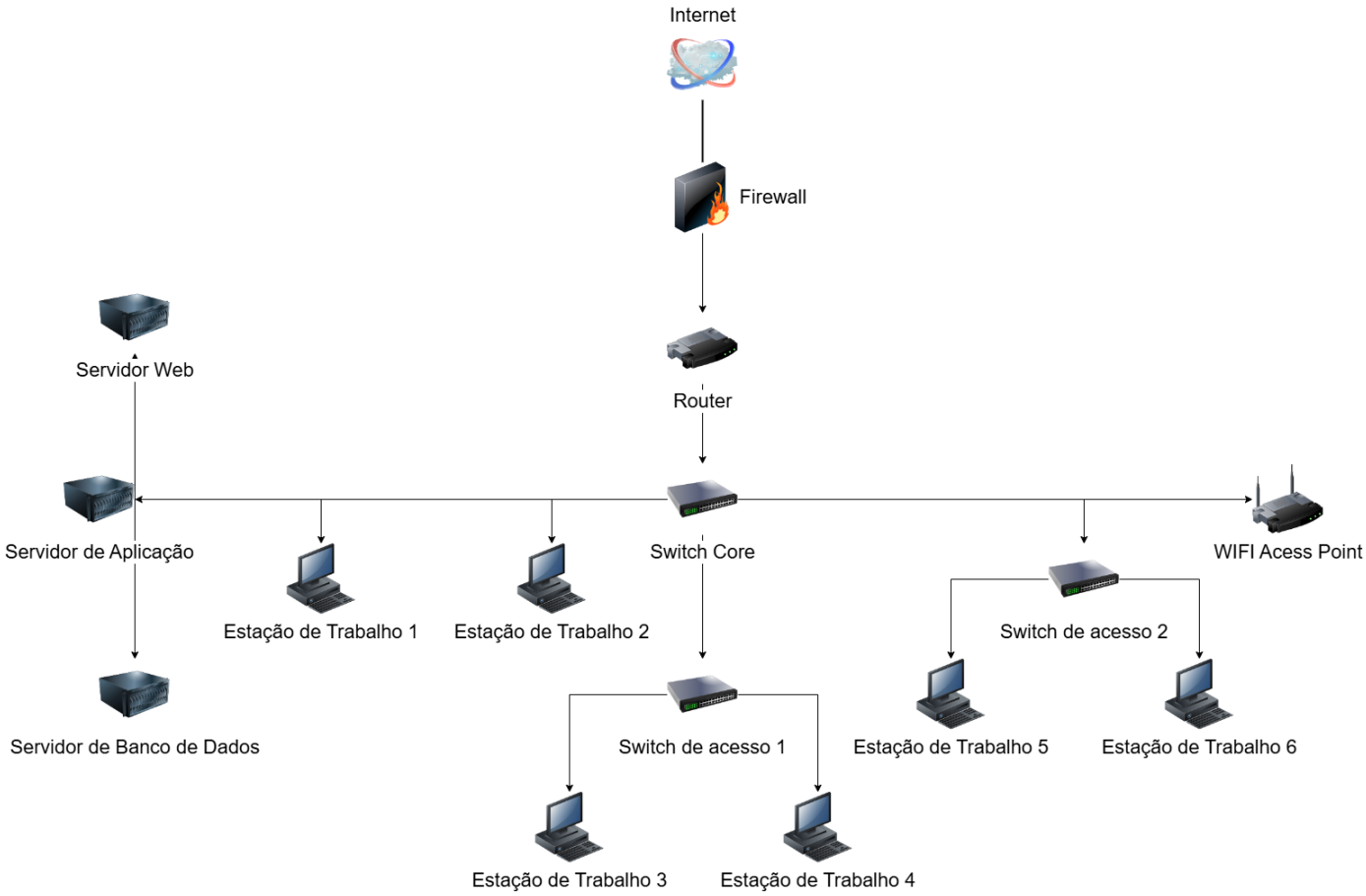
4.6. Empreendedorismo

Plano de Negócio para a área de TI (anexo).

O Plano de Negócio encontra-se no anexo III do presente documento.

5 – Arquitetura e Infraestrutura de TI

5.1 Atual



Descritivo Resumido da Estrutura

- Internet: Ponto de entrada e saída para a conexão externa.
- Firewall: Protege a rede interna contra ameaças externas.
- Router Principal: Roteador que gerencia o tráfego de dados na rede.
- Switch Core: Switch central que conecta todos os dispositivos principais e outros switches da rede.
- Servidores: Hospedam serviços e aplicações essenciais para a empresa.
- Estações de Trabalho: Computadores utilizados pelos funcionários para realizar suas atividades.
- Switches de Acesso: Switches que distribuem a conexão de rede para as estações de trabalho em diferentes áreas da empresa.

- Wi-Fi AP: Ponto de acesso que fornece conectividade sem fio aos dispositivos móveis e laptops.

Problemas Identificados e Necessidade de Atualização

1. **Capacidade do Firewall:**

Problema: O firewall atual não suporta o aumento de tráfego e as novas ameaças cibernéticas.

Atualização Necessária: Investir em um firewall com maior capacidade de processamento e funcionalidades de segurança avançadas.

2. **Router Principal:**

Problema: O router principal tornar-se um ponto de falha único, comprometendo toda a rede em caso de problemas.

Atualização Necessária: Implementar redundância com um segundo router para failover automático.

3. **Switch Core:**

Problema: Dependência de um único switch core pode causar gargalos e pontos de falha.

Atualização Necessária: Adicionar um switch core redundante para melhorar a resiliência da rede.

4. **Servidores**:

Problema: Servidores estar desatualizados ou com baixa capacidade de armazenamento e processamento.

Atualização Necessária: Realizar upgrade dos servidores ou migrar para soluções em nuvem.

5. **Switches de Acesso:**

Problema: Switches de acesso estar sobrecarregados ou desatualizados.

Atualização Necessária: Substituir switches antigos por modelos mais novos e com maior capacidade de portas.

6. **Wi-Fi AP:**

Problema: Cobertura Wi-Fi é insuficiente, causando problemas de conectividade para dispositivos móveis.

Atualização Necessária: Instalar pontos de acesso adicionais para garantir cobertura adequada em todas as áreas da empresa.

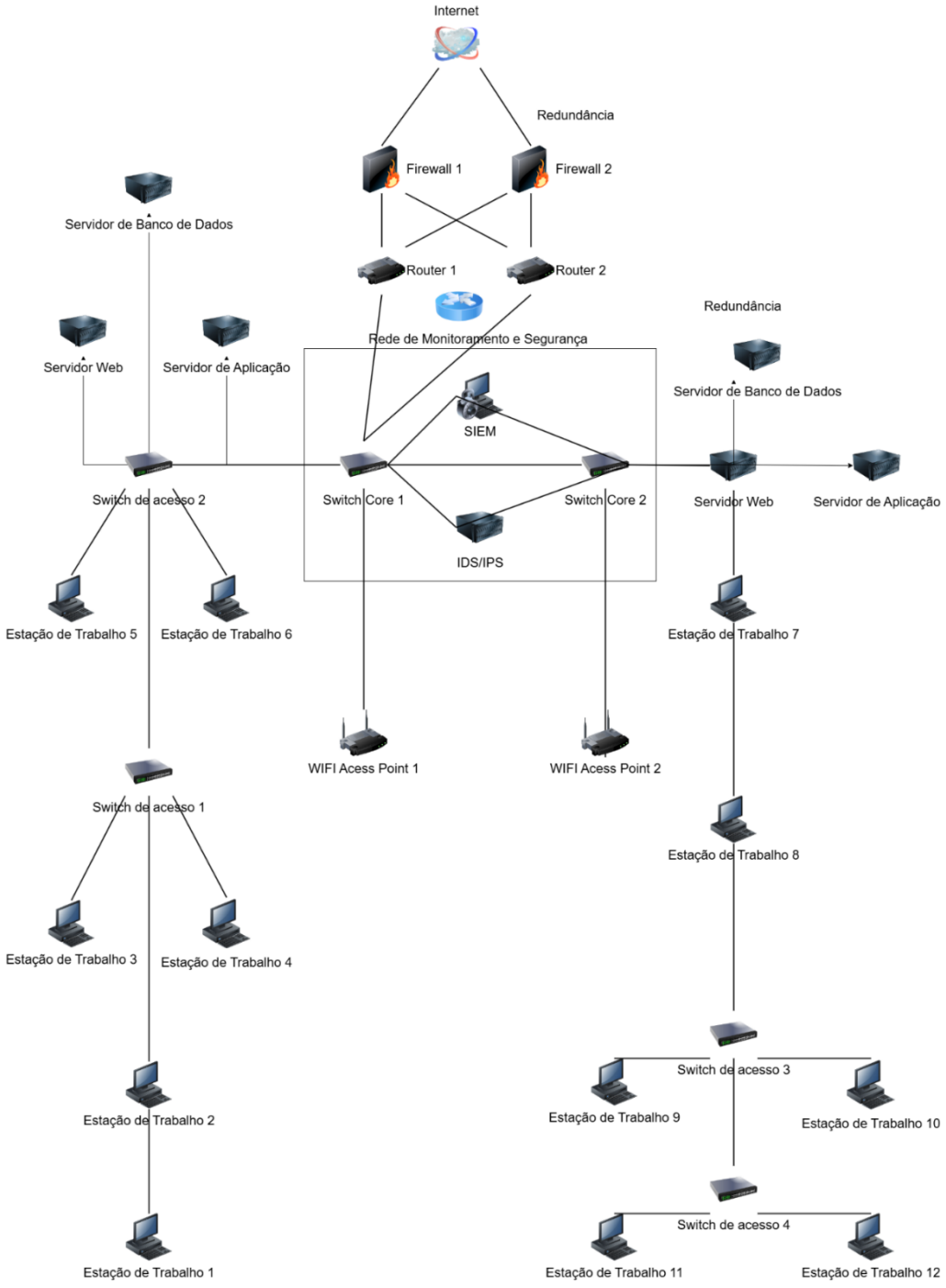
7. **Segurança e Monitoramento:**

Problema: Falta de monitoramento contínuo e proteção contra ameaças internas.

Atualização Necessária: Implementar soluções de monitoramento de rede e segurança interna, como IDS/IPS e sistemas de gerenciamento de eventos de segurança (SIEM).

5.2 Proposta

Os problemas resolvidos e as necessidades atualizadas e implantadas na topologia.



Descritivo das Atualizações Implementadas

4 **Firewall**:
- **Atualização**: Adição de um firewall redundante (1, 2) para aumentar a segurança e a capacidade de processamento.

5 **Router**:
- **Atualização**: Implementação de um router redundante (1, 2) para garantir continuidade em caso de falha do router principal.

6 **Switch Core**:
- **Atualização**: Adição de um switch core redundante (1, 2) para evitar gargalos e pontos únicos de falha.

7 **Servidores**:
- **Atualização**: Atualização dos servidores principais (1) e adição de servidores redundantes (2) para maior capacidade e segurança.

8 **Switches de Acesso**:
- **Atualização**: Substituição dos switches de acesso antigos por novos switches atualizados (1, 2, 3, 4) com maior capacidade de portas.

9 **Wi-Fi AP**:
- **Atualização**: Instalação de pontos de acesso adicionais e atualizados (1, 2) para melhorar a cobertura Wi-Fi.

10 **Segurança e Monitoramento**:
- **Atualização**: Implementação de sistemas IDS/IPS (AA) e SIEM (BB) para monitoramento contínuo e proteção contra ameaças internas e externas.

Compra de atualização de implementação

Hardware	Quantidade
Firewall redundante	**1**
Router redundante	**1**
Switch core redundante	**1**
Servidor Web	**1**
Servidor de Aplicação	**1**
Servidor de Banco de Dados	**1**
Novos switches de acesso	**2**
Pontos de acesso Wi-Fi adicionais e atualizados	**1**
Sistemas IDS/IPS	**1**
Sistema SIEM	**1**
Total	**14**

6 – Custos

Hardware

Item	Quantidade	Preço Unitário	Preço Total
Servidor de Banco de Dados (PowerEdge, DELL, 2x Intel Xeon, 256GB RAM, 4TB SSD, RAID 10)	2	R$ 8.142,00	R$ 16.284,00
Servidor de Aplicação (PowerEdge, DELL, 2x Intel Xeon, 128GB RAM, 2TB SSD)	2	R$ 7.037,00	R$ 14.074,00
Servidor de WEB (ProLiant, HP, 2x Intel Xeon, 64GB RAM, 1TB SSD)	2	R$ 8.229,49	R$ 16.458,98
Estação de Trabalho (OptiPlex, DELL, Intel Core i7, 16GB RAM, 512GB SSD)	12	R$ 6.200,00	R$ 74.400,00
Firewall (ASA, Cisco, 10 Gbps throughput, 1,000,000 connections/sec)	2	R$ 50.000,00	R$ 100.000,00
Roteador (ISR, Cisco, 20 Gbps throughput, 4 WAN ports)	2	R$ 50.000,00	R$ 100.000,00
Switch Core (Catalyst, Cisco, 48 ports, 10 Gbps, Layer 3)	2	R$ 65.000,00	R$ 130.000,00
Switch (Aruba, HP, 24 ports, 1 Gbps, PoE+)	4	R$ 16.000,00	R$ 64.000,00
Wi-Fi AP (UniFi, Ubiquiti, 802.11ac, 4x4 MU-MIMO, 1.7 Gbps)	2	R$ 2.200,00	R$ 4.400,00
IDS/IPS (Palo Alto, 5 Gbps throughput, 100,000 connections/sec)	1	R$ 80.000,00	R$ 80.000,00
SIEM (Splunk, marca, etc)	1	R$ 50.000,00	R$ 50.000,00
Total	32		R$ 649.616,98

Software

Item	Quantidade	Preço Unitário	Preço Total
Sistema Operacional dos Servidores	6	R$ 15.000,00	R$ 60.000,00
VPN	12	R$ 240 por mês	R$ 34.560,00 por ano
Antivírus Avast	12	R$ 300 por ano	R$ 3.600 por ano
Licença Operacional do Windows (Estação de trabalho)	12	R$ 1.000	R$ 12.000,00
Provedor de Internet	2	R$ 2.500,00	R$ 5.000,00
Licença IDS/IPS	1	R$ 15.000,00	R$ 15.000,00
Licença SIEM	1	R$ 25.000,00	R$ 25.000,00
Total	56		R$ 155.160,00

Serviços

Item	Quantidade	Preço Unitário	Preço Total
Instalação de Firewalls	2	R$ 5.000,00	R$ 10.000,00
Configurações de Routers	2	R$ 4.000,00	R$ 8.000,00
Configurações de Switches Core	2	R$ 6.000,00	R$ 12.000,00
Configurações de Switches	4	R$ 3.000,00	R$ 12.000,00
Instalação de Servidores	4	R$ 7.500,00	R$ 30.000,00
Configuração de Wi-Fi AP	2	R$ 2.500,00	R$ 5.000,00
Configuração de IDS/IPS	1	R$ 10.000,00	R$ 10.000,00
Configuração de SIEM	1	R$ 12.500,00	R$ 12.500,00
Manutenção e Suporte Anual	2 anos	R$ 75.000,00	R$ 150.000,00
Treinamento constante da matriz de competências	37	R$ 2.000,00	R$ 74.000,00
Total			R$ 323.500,00

TOTAL GERAL.....R$ 1.128.276,98

7 – Conclusão

O Plano Diretor de Tecnologia da Informação (PDTI) elaborado para a Pirelli para o biênio 2025/2026 atinge com sucesso os objetivos estabelecidos na introdução deste documento. Desde o diagnóstico detalhado da área de TI até a definição dos macroprocessos a serem trabalhados, cada item apresentado reforça a capacidade da organização de gerenciar suas operações de TI de maneira eficiente e alinhada às suas estratégias empresariais.

Os processos descritos ao longo do PDTI orientam de forma assertiva a formulação e implementação das estratégias de TI, garantindo que todas as ações estejam alinhadas com os objetivos de negócio da Pirelli. Através da priorização das tarefas e da tomada de decisões informadas, o PDTI serve como um guia robusto para a gestão dos recursos e processos de TI.

Além disso, o detalhamento das necessidades de aquisições, juntamente com um cronograma e a estimativa de custos, proporciona uma visão clara e estruturada de todo o planejamento necessário para o período. Esse nível de detalhamento assegura que cada etapa do processo seja executada de forma organizada e dentro do prazo estabelecido.

Em suma, este documento não só atende aos objetivos iniciais de oferecer um plano estratégico e de planejamento para a área de TI, mas também facilita a gestão de recursos, a implementação de novas tecnologias e o alinhamento estratégico entre TI e os objetivos institucionais. Dessa forma, o PDTI da Pirelli para 2025/2026 se configura como um instrumento essencial para o sucesso contínuo e o crescimento sustentável da organização.

8 – Glossário ou Lista de Abreviaturas e Siglas

Abreviaturas / Siglas	Significados / Descrição
PDTI	Plano Diretor de Tecnologia da Informação
TI	Tecnologia da Informação
DITEC	Diretoria de Tecnologia e Infraestrutura
EBIT	Earnings Before Interest and Taxes ("Lucros Antes de Juros e Impostos")
SWOT	Forças (Strengths), Fraquezas (Weaknesses), Oportunidades (Opportunities) e Ameaças (Threats)
TIC	Tecnologia da informação e Comunicação
OE	Objetivo Estratégico
IE	Iniciativas Estratégicas
GC	Gestão do Conhecimento
CGO	Chief Governance Officer ou diretor(a) de governança corporativa
APO	Asian Productivity Organization (É uma organização intergovernamental)
ONG's	Organização não governamental
CMMI	Capability Maturity Model Integration (Modelo de Capacidade e Maturidade Integrado)
SAM	Gerenciamento de Acordos de Fornecedores
WP	Planejamento de Trabalho
AP	Acess Point (Ponto de acesso)
SIEM	Security Information and Event Management – ou Gerenciamento e Correlação de Eventos de Segurança
IDS/IPS	Os Sistemas de Detecção de Intrusão (IDS) analisam o tráfego de rede para detectar assinaturas de ataques cibernéticos conhecidos. Os Sistemas de Prevenção de Intrusão (IPS)

9 – Referências

ARAÚJO FILHO, J. C. de F.; CASTRO, A. A. Manual de informática jurídica e direito da informática. São Paulo: Companhia Forense, 2005. ROVER, A. J. Direito e informática. São Paulo: Manoele, 2004.

BATISTA, Fabio Ferreira. Modelo de gestão do conhecimento para a administração pública brasileira: como implementar a gestão do conhecimento para produzir resultados em benefício do cidadão – Brasília: Ipea, 2012.

COIMBRA, José de Ávila Aguiar. Fronteiras da ética. 1ª edição. São Paulo: Editora Senac, 2002.

CHIAVENATO, Idalberto. Empreendedorismo: dando asas ao espírito empreendedor. 2. ed. São Paulo Saraiva 2008. 281 p. ISBN 9788502064232 Classificação: 65.016 C532e 2. ed. rev. e ampl. Ac.2096

DORNELAS, José Carlos Assis. Empreendedorismo corporativo: como ser empreendedor, inovar e se diferenciar na sua empresa. Rio de Janeiro Campus 2003. 183 p. ISBN8535212620 Classificação: 65.016 D713e Ac.1222

DORNELAS, José Carlos Assis. Empreendedorismo: transformando ideias em negócios. 2ed. Rio de Janeiro: Campus, 2003. Classificação: 65.016 D713e Ac.1220

DEITEL, H. M.; DEITEL, P. J. Internet e world wide web: como programar. São Paulo: Bookman, 2003.

SANTANA FILHO, O. V. Introdução à internet. São Paulo: Editora Senac, 2002

FERNANDES e ABREU. Implantando a Governança de TI. 2a ed. – Rio de Janeiro. Brasport, 2008,

GITMAN, Laurence J. Princípios de administração financeira. 10 ed. São Paulo: Pearson Addison Wesley, 2004

GUEVARA, Arnoldo José de Hoyos; ROSINI, Alessandro Marco; SILVA, José Utemar da; RODRIGUES, Mônica Cairrão. Consciência e desenvolvimento sustentável nas organizações: reflexões sobre um dos maiores desafios da nossa época. Rio de Janeiro: Elsevie r, 2009. 228 p. ISBN 9788535232813 Classificação: 502.131.1 C755
Ac.4188

LASZLO, Chris. Valor sustentável: como as empresas mais expressivas do mundo estão obtendo bons resultados pelo empenho em iniciativas de cunho social. Rio de Janeiro: Qualitymark, 2008. 209 p. ISBN 9788573038231
Classificação: 658:502.131.1 L337v = 690 Ac.4149

LOPES DE SÁ, Antônio. Ética profissional. 6ª edição. São Paulo: Editora Atlas, 2004.

MUÑOZ-SECA, Beatriz. Transformando conhecimento em resultados: a gestão do conhecimento como diferencial na busca de mais produtividade e competitividade. São Paulo: Clio, 2004.

KELDMAN, Kim. Gerência de projetos: fundamentos. São Paulo: Campus, 2005.

PASSOS, Elizete. Ética nas organizações. 1ª edição. São Paulo: Editora Atlas, 2004.

PHILIPPI JR., Arlindo; ROMÉRO, Marcelo de Andrade; BRUNA, Gilda Collet. Curso de gestão ambiental. Barueri: Manole, 2004. 1045 p. (Coleção ambiental) ISBN 8520420559 Classificação: 504.06 C977 Ac.4186

TEIXEIRA FILHO, Jayme. Gerenciando Conhecimento. Rio de Janeiro. Ed. SENAC, 2002.

WEILL, Peter e ROSS, Jeanne W. Governança de TI - Tecnologia da Informação. São Paulo. M.Books, 2005.
VARGAS, Ricardo Viana. Manual prático do plano de projeto. São Paulo: Brasport, 2005.
VIEIRA, E. Os bastidores da internet no Brasil. São Paulo: Manole, 2003.
Certificado Digital. Serasa, São Paulo-SP. Disponível em: www.Serasacertificadodigital.com.br. Acesso em: 01 mai. 2024.
Treinamento em PHP. Caelum, Venâncio 2000, Brasília-DF. Disponível em: www.Caelum.com.br. Acesso em: 01 mai. 2024.
Treinamento em JAVA. Caelum, Venâncio 2000, Brasília-DF. Disponível em: www.Caelum.com.br. Acesso em: 01 mai. 2024.
Nobreak APC Back-UPS. DELL, Eldorado do Sul-RS. Disponível em: www.DELL.com.br. Acesso em: 01 mai. 2024.
Notebook Dell Inspiron 14 séries 5000. DELL, Eldorado do Sul-RS. Disponível em: www.DELL.com.br. Acesso em: 01 mai. 2024.
Servidor Dell Power Edge. DELL, Eldorado do Sul-RS. Disponível em: www.DELL.com.br. Acesso em: 01 mai. 2024.
Switch Dell Ethernet Gigabit avançado. DELL, Eldorado do Sul-RS. Disponível em:www.DELL.com.br. Acesso em: 01 mai. 2024.
HP Windows server 2012 R2 Standart Português 74891-201. Processtec, Pina, Recife-PE. Disponível em: www.Processetec.com.br. Acesso em: 01 mai. 2024.
Workstation Dell precision T1700. DELL, Eldorado do Sul-RS. Disponível em: www.DELL.com.br. Acesso em: 01 mai. 2024.
3cx phone system 512 sc. 3CX, Eldorado do Sul-RS. Disponível em: www.DELL.com.br. Acesso em: 01 mai. 2024.
Terra. Disponível em: http://economia.terra.com.br/seguranca-privada-e-mercado-arriscado.parapmes,a58877561f66b310VgnCLD200000bbcceb0aRCRD.html. Acesso em: 16 mai. 2024.
ISO, Londres. Disponível em: www.iso.org/iso/home/about.htm. Acesso em: 16 mai. 2024.
CMMI, Disponível em: http://cmmiinstitute.com/#home. Acesso em: 16 mai. 2024.
SBGC, São Paulo-SP. Disponível em: www.sbgc.org.br/sbgc/. Acesso em: 16 mai. 2024.

10 – Assinaturas

10.1 Responsáveis

Responsáveis	Assinaturas
Marcus Vinícius	
Luiz Felipe	
Luiz Otávio	
Diego Queiroz	

10.2 Diretor de TI

Diretor de TI	
Gerson Gimenes	

ANEXOS

Anexo I - PLANO DE NEGÓCIOS DA TI

Plano de Negócios

1. Institucional

1.1. Porto Seguro

1.2. A Porto Seguro, fundada em 1945, é hoje um dos maiores grupos seguradores do Brasil, com mais de 35 milhões de clientes e atuação em diversos segmentos, como:

- **Seguros:** Auto, residência, saúde, vida, empresarial, viagem, dentre outros.
- **Serviços financeiros:** Cartão Porto Seguro, investimentos, previdência privada.
- **Soluções automotivas:** Consórcio Porto Seguro, Leão Veículos.

2. Produto/serviço

O Seguro Autorelli para Frota da Porto Seguro em parceria com a Pirelli oferece proteção completa juntamente com a tecnologia dos pneus da Pirelli que por meio do aplicativo, mostrará borracharias credenciadas próximas ou até mesmo agendar no local da empresa que forneceu o pedido para que seja feita a troca, notificará a hora de troca ou substituição dos pneus para os veículos da sua empresa, minimizando os impactos financeiros de imprevistos e garantindo a tranquilidade necessária para o seu negócio funcionar sem preocupações.

Características principais:

- **Coberturas personalizáveis:** Escolha as coberturas que melhor atendem às suas necessidades, incluindo:
  - Colisão
  - Roubo e Furto
  - Danos a Terceiros
  - Acidentes Pessoais de Passageiros
  - Fiança para Liberação de Veículo
  - Assistência 24 Horas
  - Carro Reserva
  - Extensão de Cobertura para Vidros
  - Danos Morais e Estéticos
  - Equipamentos

- Reposição de 0km
- Troca de pneus desgastados ou furados

- **Flexibilidade para frotas de todos os portes:** A Porto Seguro oferece soluções personalizadas para frotas de todos os portes, desde pequenas empresas com poucos veículos até grandes corporações com centenas ou milhares de unidades.
- **Descontos para frotas:** Quanto maior a frota, maior o desconto que você pode obter no Seguro Auto para Frota da Porto Seguro.
- **Prevenção de riscos:** A Porto Seguro oferece diversos serviços de prevenção de riscos, como treinamentos para motoristas e campanhas de conscientização, com o objetivo de reduzir o número de sinistros e garantir a segurança dos condutores.
- **Atendimento personalizado:** A Porto Seguro conta com uma equipe de profissionais qualificados e experientes para oferecer um atendimento personalizado e de alta qualidade aos seus clientes.
- **Tecnologia inovadora:** A Porto Seguro oferece diversos serviços inovadores para facilitar a gestão do seu seguro, como portais online para gestão de apólices e acompanhamento de sinistros, aplicativos mobile e serviços de telemática.

3. Mercado e Consumidores

3.1. Consumidores Potenciais (Clientes)

Quem são:

- **Empresas:**
  - Pequenas, médias e grandes empresas que possuem frotas de veículos, como:
    - Empresas de táxi e transporte urbano;
    - Empresas de logística e entrega;
    - Empresas de aluguel de carros;
    - Concessionárias e lojas de veículos;
    - Frotas de serviços públicos (prefeituras, governos estaduais, etc.);
    - Empresas de outros segmentos que possuem frotas de veículos para seus colaboradores ou operações.

- **Profissionais autônomos:**
    - Taxistas;
    - Motoristas de aplicativo;
    - Vendedores;
    - Representantes comerciais;
    - Outros profissionais que utilizam veículos em seu trabalho.

Localização:

- **Presença nacional:** A Porto Seguro oferece o Seguro Auto Frota em todo o Brasil, com atendimento em todas as regiões do país.
- **Concentração nas regiões Sul e Sudeste:** De acordo com dados da própria Porto Seguro, as regiões Sul e Sudeste concentram a maior parte dos clientes do Seguro Auto Frota.

Faixa etária:

- **Faixa etária ampla:** A Porto Seguro não divulga informações específicas sobre a faixa etária dos clientes do Seguro Auto Frota. No entanto, considerando o perfil dos tomadores de seguro (empresas e profissionais autônomos), é possível inferir que a faixa etária dos tomadores provavelmente se concentra entre 25 e 65 anos.

Sexo:

- **Prevalência do sexo masculino:** É provável que haja uma prevalência do sexo masculino entre os tomadores do Seguro Auto Frota, considerando que as atividades de direção profissional, em geral, são predominantemente exercidas por homens No entanto, a Porto Seguro não divulga dados específicos sobre a proporção de homens e mulheres entre seus clientes.

Outros dados importantes:

- **Porte da frota:** A Porto Seguro oferece o Seguro Auto Frota para frotas de diversos portes, desde pequenas frotas com poucos veículos até grandes frotas com centenas ou milhares de veículos.
- **Tipos de veículos:** O Seguro Auto Frota cobre diversos tipos de veículos, como carros, motos, caminhões, ônibus, vans e outros.

- **Histórico de sinistros:** O histórico de sinistros da frota é um dos principais fatores considerados na hora da cotação do Seguro Auto Frota. Frotas com histórico de sinistros frequentes podem ter um custo de seguro mais elevado.
- **Coberturas:** A Porto Seguro oferece diversas coberturas para o Seguro Auto Frota, como:
    - Danos a terceiros;
    - Danos próprios;
    - Roubo e furto;
    - Incêndio e explosão;
    - Acidentes pessoais do motorista e passageiros;
    - Assistência 24 horas
- **Vantagens:** O Seguro Auto Frota da Porto Seguro oferece diversas vantagens, como:
    - Descontos para frotas com bom histórico de sinistros;
    - Condições especiais de pagamento;
    - Assistência 24 horas completa;
    - Rede credenciada de oficinas e serviços;
    - Atendimento personalizado.

3.2. Tamanho do Mercado e Proposta de Valor

Tamanho do Mercado:

- **Grande e em crescimento:** O mercado de seguro auto para frotas no Brasil é considerado grande e em constante crescimento. Em 2023, o mercado movimentou R$ 233,9 bilhões em prêmios, com um crescimento de 12,38% em relação ao ano anterior.
- **Baixa penetração:** Apesar do tamanho do mercado, a penetração do seguro auto para frotas no Brasil ainda é considerada baixa, com apenas 30% da frota segurada.

Isso significa que existe um grande potencial de crescimento para o mercado nos próximos anos.

- **Fatores de crescimento:** O crescimento do mercado de seguro auto para frotas é impulsionado por diversos fatores, como:
    - Aumento da frota de veículos no Brasil;
    - Aumento da consciência sobre a importância do seguro auto;
    - Crescimento do e-commerce e da logística;
    - Aumento da regulamentação do setor de transporte.

Tendências do Mercado:

- **Digitalização:** A digitalização é uma das principais tendências do mercado de seguro auto para frotas. As seguradoras estão investindo em plataformas digitais para oferecer aos clientes uma experiência mais rápida, fácil e conveniente.
- **Telemática:** A telemática, que utiliza dispositivos para coletar dados sobre o comportamento dos motoristas, é outra tendência importante do mercado. As seguradoras estão usando esses dados para oferecer preços mais personalizados e seguros mais eficientes.
- **Segurança:** A segurança é uma das principais preocupações das empresas que possuem frotas de veículos. As seguradoras estão oferecendo soluções inovadoras para ajudar as empresas a reduzir o risco de acidentes e sinistros.
- **Sustentabilidade:** A sustentabilidade também é uma questão cada vez mais importante para as empresas. As seguradoras estão oferecendo descontos e benefícios para empresas que adotam práticas sustentáveis.

Proposta de Valor da Porto Seguro:

- **A Porto Seguro é a líder do mercado de seguro auto para frotas no Brasil, com uma participação de mercado de aproximadamente 20%.**
- **A empresa oferece uma ampla gama de produtos e serviços para atender às necessidades de empresas de todos os portes.**
- **A Porto Seguro possui uma rede credenciada de oficinas e serviços em todo o Brasil.**

- **A empresa oferece um atendimento personalizado e de alta qualidade.**
- **A Porto Seguro está comprometida com a inovação e oferece soluções inovadoras para seus clientes.**
- **A empresa é reconhecida por sua solidez financeira e pela qualidade de seus serviços.**

Alguns dos diferenciais da Porto Seguro no mercado de seguro auto para frotas incluem:

- **Programa Porto Seguro Frota Responsável:** Um programa que oferece descontos para empresas que adotam boas práticas de segurança no trânsito.
- **Porto Seguro Telemática:** Uma solução que utiliza telemática para oferecer preços mais personalizados e seguros mais eficientes.
- **Porto Seguro Digital:** Uma plataforma digital que oferece aos clientes uma experiência mais rápida, fácil e conveniente.
- **Porto Seguro Conecta:** Um aplicativo que permite aos motoristas acompanhar o status do seu seguro, solicitar assistência e realizar outros serviços.

4. Concorrência

4.1. Empresas e produtos concorrentes

- **Bradesco Auto:**
  - Oferece o programa "Bradesco Pneus", que garante a troca de pneus em caso de desgaste prematuro.
  - O programa também oferece descontos em serviços de manutenção e revisão.
  - O Bradesco Auto possui um aplicativo que permite aos clientes acompanhar o status do seu seguro, solicitar assistência e realizar outros serviços.
- **Itaú Seguros Auto:**
  - Oferece o programa "Itaú Pneus", que oferece descontos em pneus e serviços de montagem.
  - O programa também oferece a opção de pagamento parcelado sem juros.
  - O Itaú Seguros Auto possui um aplicativo que permite aos clientes consultar coberturas, solicitar sinistros e realizar outros serviços.
- **Mapfre Seguros:**

  - Oferece o programa "Mapfre Pneus", que garante a troca de pneus em caso de avaria ou desgaste prematuro.
  - O programa também oferece descontos em serviços de borracharias credenciadas.
  - A Mapfre Seguros possui um aplicativo que permite aos clientes acionar assistência 24 horas, consultar sinistros e realizar outros serviços.
- **Tokio Marine Seguros:**
  - Oferece o programa "Tokio Pneus", que oferece descontos em pneus e serviços de montagem.
  - O programa também oferece a opção de pagamento parcelado sem juros.
  - A Tokio Marine Seguros possui um aplicativo que permite aos clientes consultar apólices, solicitar assistência e realizar outros serviços.
- **Allianz Seguros:**
  - Oferece o programa "Allianz Pneus", que garante a troca de pneus em caso de avaria ou desgaste prematuro.
  - O programa também oferece descontos em serviços de borracharias credenciadas.
  - A Allianz Seguros possui um aplicativo que permite aos clientes acionar assistência 24 horas, consultar sinistros e realizar outros serviços.

Produtos:

- **Programa Pneu Seguro da Michelin:**
  - Oferece a troca gratuita de pneus em caso de avaria ou desgaste prematuro.
  - O programa também oferece descontos em serviços de montagem e balanceamento.
  - O programa Pneu Seguro da Michelin não está vinculado a nenhuma companhia de seguro específica, podendo ser adquirido por qualquer cliente.
- **Programa Goodyear Super Pneu:**
  - Oferece a troca gratuita de pneus em caso de avaria ou desgaste prematuro.
  - O programa também oferece descontos em serviços de montagem e alinhamento.
  - O programa Goodyear Super Pneu não está vinculado a nenhuma companhia de seguro específica, podendo ser adquirido por qualquer cliente.

5. Plano de Marketing e Vendas

1.1. Definição do Público-Alvo:

- Empresas de todos os portes que possuem frotas de veículos (táxis, transporte urbano, logística, entrega, aluguel de carros, etc.);
- Profissionais autônomos que utilizam veículos em seu trabalho (taxistas, motoristas de aplicativo, vendedores, etc.).

1.2. Canais de Comunicação:

- **Marketing Digital:**
  - Criação de um website específico para o Seguro Auto Frota com troca de pneus Pirelli e notificação por app;
  - Campanhas de marketing de conteúdo em blogs e redes sociais;
  - Anúncios online direcionados para o público-alvo;
  - E-mail marketing para clientes potenciais e existentes.
- **Marketing Tradicional:**
  - Publicidade em revistas e jornais especializados;
  - Participação em feiras e eventos do setor;
  - Telemarketing para empresas e profissionais autônomos.
- **Vendas:**
  - Força de vendas direta composta por corretores de seguros;
  - Vendas online através do website e de outros canais digitais;
  - Parcerias com empresas de leasing e outras empresas que atendem ao público-alvo.

1.3. Promoções e Descontos:

- Oferecer descontos para empresas que aderirem ao programa de troca de pneus Pirelli;
- Oferecer descontos para empresas que contratarem o seguro online;
- Criar pacotes promocionais que incluam o seguro, a troca de pneus e outros serviços.

1.4. Fidelização de Clientes:

- Oferecer um programa de fidelidade que recompense os clientes por sua lealdade;
- Oferecer serviços diferenciados para clientes fiéis, como atendimento prioritário e descontos exclusivos;
- Realizar pesquisas de satisfação para identificar oportunidades de melhoria.

2. Planos de Propaganda e Promoção:

2.1. Campanha de Lançamento:

- Criar uma campanha de lançamento que comunique os benefícios do Seguro Auto Frota com troca de pneus Pirelli e notificação por app;
- A campanha deve ser veiculada em diversos canais de comunicação, como marketing digital, marketing tradicional e relações públicas.
- O objetivo da campanha é gerar awareness e interesse pelo produto, além de captar leads qualificados.

2.2. Campanhas de Marketing Contínuo:

- Criar campanhas de marketing contínuo para promover o Seguro Auto Frota e seus diferenciais;
- As campanhas devem ser direcionadas para o público-alvo e utilizar diversos formatos, como vídeos, banners e anúncios em redes sociais.
- O objetivo das campanhas é manter o produto na mente dos consumidores e gerar conversões.

2.3. Relações Públicas:

- Criar um programa de relações públicas para divulgar o Seguro Auto Frota para a imprensa e influenciadores;
- O programa deve incluir a participação em eventos do setor, a realização de press releases e a criação de conteúdo para mídias sociais.
- O objetivo do programa de relações públicas é gerar credibilidade para o produto e alcançar um público mais amplo.

3. Atendimento ao Cliente:

3.1. Canais de Atendimento:

- A Porto Seguro oferecerá um atendimento ao cliente completo e multicanal, através dos seguintes canais:
    - Telefone;
    - Chat online;
    - E-mail;
    - Aplicativo mobile;
    - Presencialmente nas agências da Porto Seguro.
- A empresa também oferecerá um serviço de autoatendimento através do seu website e aplicativo mobile.

3.2. Qualidade do Atendimento:

- A Porto Seguro investirá na qualidade do seu atendimento ao cliente, através da:
    - Contratação e treinamento de profissionais qualificados;
    - Implementação de processos eficientes;
    - Utilização de tecnologia para otimizar o atendimento.
- A empresa também medirá a satisfação dos clientes através de pesquisas de opinião e outros indicadores.

4. Pesquisa de Mercado:

4.1. Necessidade da Pesquisa:

- A realização de uma pesquisa de mercado é **recomendada** para o lançamento do Seguro Auto Frota com troca de pneus Pirelli e notificação por app.
- A pesquisa ajudará a empresa a:
    - Identificar as necessidades e expectativas do público-alvo;
    - Avaliar o potencial do mercado;
    - Definir o posicionamento do produto;

- Desenvolver estratégias de marketing e vendas mais eficazes.

6. Operações /Etapas

1. Encontre o Seguro Ideal:

- Pesquise e compare planos online com ferramentas fáceis de usar.
- Converse com especialistas para tirar dúvidas e receber ajuda personalizada.
- Receba uma proposta detalhada e transparente por e-mail ou app.

2. Contrate de Forma Segura:

- Assine o contrato digitalmente com total segurança.
- Receba a apólice digital imediatamente no seu e-mail e app.

3. Ative seus Benefícios:

- Ative a troca de pneus Pirelli com agendamento online simples.
- Baixe o app para acompanhar o seguro, solicitar assistência e muito mais.

4. Tenha Suporte Completo:

- Conte com uma equipe de especialistas para te auxiliar em tudo.
- Tire dúvidas, acione assistência e acompanhe tudo pelo app.

5. Pague com Praticidade:

- Escolha a forma de pagamento que mais combina com você.
- Acesse o app ou portal do cliente para pagar suas contas.

6. Renove sem Surpresas:

- Receba avisos de renovação com antecedência.
- Renove online ou com a ajuda de um especialista.

7. Mantenha-se Seguro:

- Dirija com segurança e previna acidentes.
- Conte com a Porto Seguro em caso de imprevistos.

7. Planos e Projeções Financeiras

1. Receita:

- **Prêmios de seguro:** A principal fonte de receita do Seguro Auto Frota será proveniente dos prêmios pagos pelos clientes. O valor do prêmio será calculado com base em diversos fatores, como o perfil do cliente, o tipo de veículo e o histórico de sinistros.
- **Venda de pneus:** A Porto Seguro também poderá gerar receita com a venda de pneus Pirelli para os clientes do Seguro Auto Frota. A empresa poderá oferecer descontos especiais para os clientes do seguro.
- **Taxas de serviço:** A Porto Seguro poderá cobrar taxas de serviço para alguns serviços, como a troca de pneus e a emissão de apólices.

2. Custos:

- **Sinistros:** O principal custo do Seguro Auto Frota será com o pagamento de sinistros. A Porto Seguro precisará reservar uma quantia significativa de recursos para pagar os sinistros dos seus clientes.
- **Aquisição de pneus:** A Porto Seguro precisará comprar pneus Pirelli para oferecer aos seus clientes do Seguro Auto Frota. O custo dos pneus poderá variar de acordo com o modelo e a marca.
- **Marketing e vendas:** A Porto Seguro precisará investir em marketing e vendas para promover o Seguro Auto Frota e captar novos clientes. Os custos com marketing e vendas podem incluir publicidade, comissões de corretores e salários de vendedores.
- **Administração:** A Porto Seguro precisará arcar com custos administrativos para gerenciar o Seguro Auto Frota. Esses custos podem incluir salários de funcionários, aluguel de escritórios e despesas com tecnologia.

3. Retorno sobre o Investimento (ROI):

- O tempo necessário para o retorno do investimento (ROI) no Seguro Auto Frota dependerá de diversos fatores, como o volume de vendas, a sinistralidade e a taxa de desconto.

- É importante realizar um estudo de viabilidade financeira para estimar o ROI do projeto. O estudo de viabilidade deve considerar todos os custos e receitas previstos.
- A Porto Seguro possui uma equipe de especialistas em análise financeira que poderá auxiliar na elaboração do estudo de viabilidade.

8. Análise de Risco

Objetivo: Identificar e avaliar os principais riscos que podem afetar o desenvolvimento e a implementação do Seguro Auto Frota da Porto Seguro com troca de pneus Pirelli e notificação por app, e definir medidas de contingência para mitigá-los.

Metodologia:

1. **Identificação de Riscos:** Brainstorming e análise de especialistas.
2. **Avaliação de Riscos:** Probabilidade e impacto de cada risco.
3. **Definição de Contingências:** Medidas para mitigar cada risco.

RISCO	PROBABILIDADE	IMPACTO	CONTINGÊNCIA
Baixa aceitação do produto pelos clientes	3	2	Campanhas de marketing direcionadas, programa de fidelidade, pesquisas de satisfação.
Aumento da sinistralidade	2	1	Seleção rigorosa de clientes, programas de prevenção de acidentes, monitoramento constante da sinistralidade.
Falhas no aplicativo	2	2	Testes rigorosos do aplicativo, equipe de suporte técnico dedicada, atualizações frequentes do aplicativo.
Dificuldades na logística de troca de pneus	3	2	Parcerias com empresas de borracharias credenciadas, sistema de agendamento online eficiente,

			monitoramento da qualidade do serviço.
Aumento da concorrência	1	2	Diferenciação do produto com base em benefícios exclusivos, foco em nichos de mercado, investimento em inovação.
Falhas na integração com sistemas de terceiros	3	2	Testes rigorosos da integração, equipe de suporte técnico dedicada, planos de contingência para falhas na integração.
Mudanças na legislação	3	1	Monitoramento constante das mudanças na legislação, equipe jurídica especializada, adaptações rápidas do produto à nova legislação.
Falhas na segurança da informação	3	1	Implementação de medidas robustas de segurança da informação, treinamento de funcionários em segurança da informação, testes de segurança regulares.

Legenda:

	NÍVEL DE RISCO
PROBABILIDADE	(1 Alta, 2 Média e 3 Baixa)
IMPACTO	(1 Alto, 2 Médio e 3 Baixo)

9. Tecnologias

1. Tecnologias para o Produto:

- **Sistema de gestão de apólices:** Para gerenciar as informações dos clientes, apólices, sinistros e pagamentos.
- **Sistema de precificação:** Para calcular o valor do prêmio do seguro com base no perfil do cliente, tipo de veículo e histórico de sinistros.
- **Plataforma de agendamento online:** Para que os clientes possam agendar a troca de pneus Pirelli.
- **Aplicativo mobile:** Para que os clientes possam acompanhar o seguro, solicitar assistência e realizar outros serviços.
- **Dispositivos telemáticos:** Para coletar dados sobre o comportamento dos motoristas e oferecer serviços personalizados.

2. Tecnologias para Infraestrutura:

- **Servidores:** Para armazenar dados e executar aplicativos.
- **Rede de comunicação:** Para conectar os diferentes sistemas e dispositivos.
- **Segurança da informação:** Para proteger os dados dos clientes e da empresa.

3. Obtenção das Tecnologias:

- **Desenvolvimento interno:** A Porto Seguro pode desenvolver algumas das tecnologias internamente, com sua própria equipe de desenvolvedores.
- **Aquisição de software:** A empresa pode adquirir softwares prontos de fornecedores terceirizados.
- **Parcerias:** A Porto Seguro pode firmar parcerias com outras empresas para desenvolver ou utilizar tecnologias conjuntas.

10. Assinaturas

Responsáveis	Assinaturas
Marcus Vinícius	
Luiz Felipe	
Luiz Otávio	
Diego Queiroz	
Diretor de TI	
Gerson Gimenes	

Anexo II - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

1. Sobre a Política de Segurança da Informação (PSI)

A Política de Segurança da Informação (PSI) é um documento formal que define as regras, diretrizes e procedimentos a serem seguidos por uma organização para proteger seus ativos de informação, incluindo dados, sistemas e infraestrutura. Ela estabelece responsabilidades, boas práticas e medidas de segurança para garantir a confidencialidade, integridade e disponibilidade das informações, minimizando riscos de ameaças e incidentes. A PSI é fundamental para a segurança cibernética e proteção de dados em empresas e instituições.

2. Conceitos e Definições

Ativo: todo e qualquer bem do patrimônio da organização, incluindo informações, sistemas, equipamentos, infraestrutura, pessoas e imagem.

Ativo Crítico e Sensível: ativo que, caso seja comprometido, pode causar danos significativos à organização, como perda financeira, interrupção de serviços, danos à reputação ou comprometimento da segurança de outros ativos.

Cavalo de Troia (Trojan horse): tipo de malware que se disfarça como um programa legítimo para enganar o usuário e obter acesso ao sistema, permitindo a instalação de outros programas maliciosos ou o roubo de informações.

Código Executável: conjunto de instruções em linguagem de máquina que podem ser executadas por um computador para realizar uma tarefa específica.

Código Malicioso (Malware): software projetado para causar danos a um sistema, roubar informações ou realizar outras atividades maliciosas. Exemplos incluem vírus, worms, trojans, ransomware e spyware.

Colaborador Interno: funcionário, estagiário, terceirizado ou qualquer pessoa que tenha um vínculo formal com a organização e acesso aos seus ativos de informação.

Colaborador Externo: pessoa ou entidade que não possui um vínculo formal com a organização, mas que pode ter acesso aos seus ativos de informação, como fornecedores, clientes, parceiros e visitantes.

Confidencialidade: princípio da segurança da informação que garante que apenas pessoas autorizadas tenham acesso às informações sensíveis, protegendo-as de acessos não autorizados e divulgação indevida.

Comunicadores Instantâneos: aplicativos ou softwares que permitem a troca de mensagens de texto, áudio, vídeo e arquivos em tempo real pela internet.

Custodiante: pessoa ou área responsável por armazenar, gerenciar e proteger os ativos de informação de acordo com as políticas e procedimentos da organização.

Cyberbullying: prática de usar tecnologias digitais para intimidar, humilhar, assediar ou difamar uma pessoa, causando danos psicológicos e emocionais.

Dados Pessoais: qualquer informação relacionada a uma pessoa natural identificada ou identificável, como nome, RG, CPF, endereço, telefone, e-mail, dados de localização, etc.

Dados Pessoais Sensíveis: categoria especial de dados pessoais que exigem maior proteção, como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos.

Disponibilidade: princípio da segurança da informação que garante que as informações e os recursos estejam acessíveis e utilizáveis pelas pessoas autorizadas quando necessário.

Informação: conjunto de dados organizados e processados que possuem significado e valor para uma pessoa ou organização.

Informação Sensível: informação que, se divulgada ou acessada sem autorização, pode causar prejuízo à organização ou aos indivíduos a quem se refere.

Integridade: princípio da segurança da informação que garante que as informações não sejam alteradas ou destruídas sem autorização, mantendo sua exatidão, consistência e confiabilidade.

Parceiros: pessoas ou organizações externas que possuem um relacionamento comercial ou de colaboração com a organização e que podem ter acesso aos seus ativos de informação.

Peer to Peer (P2P): modelo de rede de computadores em que todos os dispositivos conectados têm funções e responsabilidades iguais, compartilhando recursos e informações diretamente entre si, sem a necessidade de um servidor central.

Segurança da Informação: conjunto de práticas, políticas, procedimentos e tecnologias que visam proteger as informações de acessos não autorizados, uso indevido, divulgação, modificação, destruição ou perda.

Spam: envio em massa de mensagens eletrônicas não solicitadas, geralmente com fins comerciais ou maliciosos.

Usuário: pessoa que utiliza um sistema, serviço ou recurso de tecnologia da informação.

Vírus: tipo de malware que se propaga infectando outros arquivos ou programas, podendo causar danos ao sistema, roubar informações ou realizar outras atividades maliciosas.

Worm: tipo de malware que se auto replica e se espalha pela rede, consumindo recursos do sistema e podendo causar interrupções nos serviços.

3. *Objetivos da Política de Segurança da Informação*

- **Estabelecer diretrizes** claras e abrangentes para a proteção dos ativos de informação da organização, definindo responsabilidades, procedimentos e controles de segurança.
- **Nortear** as ações e decisões relacionadas à segurança da informação, fornecendo um framework para a implementação de medidas de proteção e resposta a incidentes.
- **Prevenir** a ocorrência de incidentes de segurança, como ataques cibernéticos, vazamento de dados, perda de informações e interrupção de serviços, através da identificação e mitigação de riscos.
- **Garantir a normalidade e a continuidade** das operações da organização, mesmo em caso de incidentes de segurança, através da implementação de planos de contingência e recuperação de desastres.
- **Atender aos requisitos legais, regulamentares e contratuais** aplicáveis à proteção de dados e informações, garantindo a conformidade com as leis e normas vigentes.
- **Minimizar os riscos** de danos, perdas financeiras, perda de participação no mercado, perda de confiança de clientes e parceiros, ou qualquer outro impacto negativo nas atividades da organização, decorrentes de incidentes de segurança.
- **Assegurar o treinamento contínuo** dos colaboradores em relação à segurança da informação, conscientizando-os sobre a importância de proteger os ativos de informação e capacitando-os a identificar e responder a ameaças.
- **Garantir que todas as responsabilidades** relacionadas à segurança da informação sejam claramente definidas e atribuídas aos colaboradores, estabelecendo uma estrutura de governança para a gestão da segurança da informação.

4. *Aplicação da Política de Segurança da Informação*

A Política de Segurança da Informação (PSI) é um documento de aplicação abrangente, que se estende a todos os níveis e áreas da organização. Ela deve ser observada por:

- **Todos os funcionários:** independentemente do cargo ou função, todos os colaboradores internos da organização são responsáveis por seguir as diretrizes da PSI em suas atividades diárias.
- **Prestadores de serviços:** empresas e profissionais terceirizados que atuam em nome da organização também devem seguir a PSI, garantindo a proteção das informações e dos recursos tecnológicos aos quais têm acesso.

- **Estagiários:** mesmo com vínculo temporário, os estagiários devem ser conscientizados sobre a importância da segurança da informação e seguir as normas estabelecidas na PSI.
- **Afins:** a PSI também se aplica a qualquer pessoa que tenha acesso aos ativos de informação da organização, como consultores, parceiros de negócios e visitantes.

A aplicação da PSI visa garantir a proteção das informações e o uso adequado dos recursos tecnológicos em toda a rede da organização. Para isso, é fundamental que todos os usuários:

- **Mantenham-se atualizados:** a PSI deve ser um documento vivo, sujeito a revisões e atualizações periódicas. É responsabilidade de cada usuário manter-se informado sobre as normas e diretrizes da PSI, buscando orientação da Gerência de Tecnologia da Informação (GTI) sempre que necessário.
- **Busquem orientação:** em caso de dúvidas sobre a aquisição, uso, armazenamento ou descarte de informações, os usuários devem procurar a GTI para obter orientação e esclarecimentos.

5. *Princípios da Política de Segurança da Informação*

Uso Responsável dos Recursos Tecnológicos:

- **Finalidade Profissional:** Os equipamentos de informática, comunicação, sistemas e informações devem ser utilizados prioritariamente para a realização de atividades profissionais, com foco no cumprimento dos objetivos da organização.
- **Senso de Responsabilidade:** Os usuários devem agir com responsabilidade e ética no uso dos recursos tecnológicos, evitando práticas que possam comprometer a segurança da informação ou causar danos à organização.
- **Preceitos Éticos:** O uso dos recursos tecnológicos deve estar em conformidade com os princípios éticos da sociedade, respeitando a privacidade, a propriedade intelectual e os direitos individuais.
- **Legalidade:** Todas as atividades realizadas com os recursos tecnológicos devem estar em conformidade com as leis e regulamentos aplicáveis, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Finalidade Educacional:** No caso de alunos, o uso dos recursos tecnológicos deve estar voltado para estudos, atividades educacionais e pesquisas acadêmicas, contribuindo para o desenvolvimento do conhecimento.

Respeito à Privacidade e Proteção de Dados Pessoais:

- **Privacidade dos Usuários:** A PSI garante o respeito à privacidade dos usuários, protegendo seus dados pessoais de acessos não autorizados, uso indevido ou divulgação.
- **Ética:** A coleta, armazenamento, tratamento e compartilhamento de dados pessoais devem ser realizados de forma ética e transparente, informando os usuários sobre a finalidade do uso de seus dados e seus direitos.
- **Conformidade com a LGPD:** A PSI deve estar em conformidade com a Lei Geral de Proteção de Dados Pessoais, garantindo o cumprimento dos direitos dos titulares de dados, como o acesso, a correção, a portabilidade e a exclusão de seus dados.

6. *Requisitos da Política de Segurança da Informação*

A comunicação efetiva da Política de Segurança da Informação (PSI) é fundamental para garantir sua aplicação e promover uma cultura de segurança na empresa. Para isso, a PSI deve ser comunicada a todos os envolvidos, incluindo:

- **Funcionários:** Todos os colaboradores, independentemente do cargo ou função, devem ter conhecimento da PSI e de suas responsabilidades na proteção dos ativos de informação da empresa.

- **Prestadores de serviços:** Empresas e profissionais terceirizados que atuam em nome da empresa também devem receber a PSI e ser conscientizados sobre a importância de seguir suas diretrizes.
- **Estagiários:** Mesmo com vínculo temporário, os estagiários devem ser informados sobre a PSI e suas implicações para o uso dos recursos tecnológicos da empresa.
- **Afins:** A PSI deve ser comunicada a qualquer pessoa que tenha acesso aos ativos de informação da empresa, como consultores, parceiros de negócios e visitantes.

A comunicação da PSI pode ser realizada por diversos meios, como:

- **Treinamentos:** Realizar treinamentos presenciais ou online para apresentar a PSI e suas diretrizes, esclarecendo dúvidas e promovendo a conscientização sobre a importância da segurança da informação.
- **Intranet:** Disponibilizar a PSI na intranet da empresa, facilitando o acesso e a consulta por todos os colaboradores.
- **E-mail:** Enviar a PSI por e-mail para todos os funcionários, prestadores de serviços e estagiários, solicitando a leitura e o aceite das normas estabelecidas.
- **Reuniões:** Apresentar a PSI em reuniões de equipe, reforçando a importância da segurança da informação e incentivando a participação de todos na proteção dos ativos da empresa.
- **Cartazes e materiais informativos:** Divulgar cartazes e materiais informativos sobre a PSI em locais estratégicos da empresa, como murais, elevadores e áreas de convivência.

7. *Monitoramento e Auditoria*

Para garantir o cumprimento das regras estabelecidas nesta Política de Segurança da Informação (PSI), bem como para fins de segurança e prevenção à fraude, a Pirelli reserva-se o direito de:

- **Monitorar o uso dos recursos tecnológicos:** A empresa poderá monitorar o uso de computadores, dispositivos móveis, redes, sistemas e aplicativos, incluindo o acesso à internet, e-mails, mensagens instantâneas e outras formas de comunicação eletrônica.
- **Auditar registros e logs:** A empresa poderá realizar auditorias periódicas nos registros e logs de atividades dos sistemas e aplicativos, a fim de verificar o cumprimento da PSI, identificar possíveis vulnerabilidades e detectar atividades suspeitas.
- **Investigar incidentes de segurança:** Em caso de suspeita de violação da PSI ou de incidentes de segurança, a empresa poderá realizar investigações internas, utilizando ferramentas e técnicas forenses para coletar evidências e identificar os responsáveis.
- **Aplicar medidas disciplinares:** Em caso de violação comprovada da PSI, a empresa poderá aplicar medidas disciplinares aos responsáveis, de acordo com as normas internas e a legislação trabalhista.

8. *Responsabilidades Específicas*

8.1. *Dos Usuários em geral*

Funcionários, prestadores de serviços, estagiários e demais colaboradores da Pirelli, em qualquer nível hierárquico e dentro de sua esfera de competência, são responsáveis por:

- **Cumprir e zelar pela aplicação efetiva** das normas e princípios da segurança da informação, contribuindo para a proteção dos ativos da empresa.
- **Respeitar os critérios legais e éticos** que envolvem a instituição, agindo com responsabilidade e integridade no uso dos recursos tecnológicos.
- **Assumir a responsabilidade por danos ou prejuízos** causados à empresa ou a terceiros, decorrentes do descumprimento das diretrizes e normas estabelecidas nesta Política de Segurança da Informação.

Cabe a todos os usuários as seguintes práticas:

- **Cumprir fielmente as políticas, normas e procedimentos de Segurança da Informação:** Seguir as regras estabelecidas nesta PSI e em outros documentos relacionados à segurança da informação, buscando sempre agir de forma preventiva e proativa na proteção dos ativos da empresa.
- **Buscar orientação do superior hierárquico ou da área de Tecnologia da Informação (TI):** Em caso de dúvidas sobre a aplicação da PSI ou sobre qualquer questão relacionada à segurança da informação, os usuários devem buscar orientação junto ao seu superior hierárquico ou à equipe de TI da empresa.

8.2. Política de Senhas

Responsabilidade Individual e Intransferível:

Os colaboradores, terceiros e usuários externos assumem total responsabilidade pelo uso adequado das credenciais (usuário e senha) fornecidas para acesso à rede, aplicações internas, externas (Cloud/SaaS), aplicativos móveis, internet e sistemas da empresa. Essa responsabilidade é individual e intransferível, ou seja, cada usuário é responsável por suas próprias credenciais e não deve compartilhá-las com terceiros.

Boas Práticas de Segurança:

Para garantir a segurança das informações e dos sistemas da empresa, os usuários devem seguir as seguintes boas práticas de segurança em relação às suas senhas:

- **Criação de senhas fortes:** Utilizar senhas complexas, com pelo menos 8 caracteres, incluindo letras maiúsculas e minúsculas, números e símbolos. Evitar o uso de informações pessoais, sequências numéricas ou palavras comuns.
- **Não reutilizar senhas:** Utilizar senhas diferentes para cada sistema ou aplicação, evitando a reutilização de senhas antigas.
- **Troca periódica de senhas:** Alterar as senhas periodicamente, de acordo com a política de segurança da empresa.
- **Confidencialidade das senhas:** Não compartilhar senhas com terceiros, nem anotá-las em locais de fácil acesso.
- **Atenção a phishing e golpes:** Estar atento a e-mails e mensagens suspeitas que solicitem informações de login ou senhas.

Consequências do uso inadequado:

O uso inadequado das senhas, como o compartilhamento com terceiros ou a utilização de senhas fracas, pode comprometer a segurança das informações da empresa e resultar em graves consequências, como:

- **Acesso não autorizado a dados confidenciais:** Pessoas não autorizadas podem ter acesso a informações sensíveis da empresa, como dados financeiros, informações de clientes e segredos comerciais.
- **Vazamento de dados:** Informações confidenciais podem ser divulgadas indevidamente, causando danos à reputação da empresa e prejuízos financeiros.
- **Infecção por malware:** Computadores e dispositivos podem ser infectados por vírus, worms e outros tipos de malware, comprometendo o funcionamento dos sistemas e a segurança das informações.
- **Ataques de ransomware:** Hackers podem sequestrar dados da empresa e exigir pagamento de resgate para liberá-los.
- **Medidas disciplinares:** O uso inadequado das senhas pode resultar em medidas disciplinares para o usuário, de acordo com as normas internas da empresa e a legislação trabalhista.

8.3 Redes sem fio

Disponibilização e Regras:

A Pirelli disponibiliza rede sem fio (wireless) para uso de dispositivos móveis em suas dependências. O acesso a essa rede está sujeito a regras específicas, monitoramento e configurações definidas pela empresa. Essas medidas visam garantir a privacidade dos usuários, a segurança das informações e o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD).

Responsabilidade do Usuário:

É de inteira responsabilidade do proprietário do equipamento ou dispositivo:

- **Guarda do equipamento:** O usuário é responsável por manter seu dispositivo seguro, evitando perdas, furtos ou acessos não autorizados.
- **Conteúdo instalado:** O usuário é responsável por todo o conteúdo armazenado em seu dispositivo, incluindo softwares, músicas, fotos e outros arquivos. A empresa não se responsabiliza por danos ou perdas de dados decorrentes de softwares maliciosos, vírus ou outros problemas de segurança.
- **Uso da rede sem fio:** O usuário deve utilizar a rede sem fio de forma responsável, respeitando as regras de uso estabelecidas pela empresa e evitando atividades que possam comprometer a segurança da rede ou de outros usuários.

Recomendações de Segurança:

Para garantir a segurança de seus dispositivos e informações ao utilizar a rede sem fio da empresa, os usuários devem seguir as seguintes recomendações:

- **Manter o dispositivo atualizado:** Instalar as atualizações de segurança do sistema operacional e dos aplicativos, a fim de corrigir vulnerabilidades e proteger o dispositivo contra ameaças.
- **Utilizar softwares de segurança:** Instalar e manter atualizado um software antivírus e antispyware para proteger o dispositivo contra malware.
- **Utilizar senhas fortes:** Proteger o acesso ao dispositivo e à rede sem fio com senhas fortes e complexas, que não sejam facilmente descobertas por terceiros.
- **Evitar o acesso a sites suspeitos:** Não acessar sites desconhecidos ou suspeitos, que possam conter malware ou representar riscos à segurança do dispositivo.
- **Utilizar conexões seguras:** Ao acessar sites que exigem informações pessoais ou financeiras, verificar se a conexão é segura (https://) e se o certificado de segurança do site é válido.
- **Desconectar da rede sem fio quando não estiver em uso:** Ao finalizar o uso da rede sem fio, desconectar o dispositivo para evitar o acesso não autorizado.

8.4 Segmentação de ambiente, Publicações internas e externas

Validação e Aprovação:

Toda aplicação publicada a partir do Datacenter da Pirelli deverá passar por um rigoroso processo de validação e aprovação, envolvendo as seguintes áreas:

- **Segurança da Informação:** Responsável por avaliar os riscos de segurança da aplicação, verificar a implementação de controles de segurança adequados e garantir a proteção dos dados e informações da empresa.
- **Segurança Operacional:** Responsável por avaliar a estabilidade, disponibilidade e performance da aplicação, garantindo que ela opere de forma eficiente e segura.
- **Arquitetura e Ambiente:** Responsável por avaliar a arquitetura da aplicação e sua integração com o ambiente de TI da empresa, garantindo a compatibilidade e o bom funcionamento.
- **Coordenação de Middleware:** Responsável por aprovar a publicação da aplicação no ambiente de produção, após a validação pelas áreas de segurança da informação, segurança operacional e arquitetura.

Segmentação de Ambientes:

A Pirelli adota uma política de segmentação de ambientes para garantir a segurança e a estabilidade das aplicações. Os ambientes são divididos em:

- **Desenvolvimento:** Ambiente utilizado para a criação e desenvolvimento de novas aplicações, onde os testes iniciais são realizados.
- **Homologação:** Ambiente utilizado para testar a aplicação em um ambiente similar ao de produção, a fim de identificar e corrigir possíveis erros e falhas.
- **Produção:** Ambiente onde a aplicação é disponibilizada para os usuários finais, após passar por todas as etapas de validação e aprovação.

Publicações Internas e Externas:

As aplicações podem ser classificadas como internas ou externas, de acordo com o público-alvo:

- **Internas:** Aplicações destinadas ao uso exclusivo dos colaboradores da Pirelli, acessíveis apenas a partir da rede interna da empresa ou através de VPN.
- **Externas:** Aplicações destinadas ao público externo, como clientes, parceiros ou fornecedores, acessíveis a partir da internet.

8.5 Dos Gestores/Gerentes

Cabe a todo gestor de área:

- **Garantir a implementação de mecanismos para descarte seguro de informações:** Estabelecer e supervisionar processos que garantam o descarte seguro de informações confidenciais, tanto em formato físico quanto digital, de acordo com as políticas da empresa e a legislação vigente.
- **Manter postura exemplar em relação à Segurança da Informação:** Agir como modelo de conduta para os colaboradores sob sua gestão, demonstrando comprometimento com as práticas de segurança da informação e incentivando o cumprimento das normas e procedimentos.
- **Cumprir a política, normas e procedimentos de Segurança da Informação:** Seguir rigorosamente as diretrizes estabelecidas nesta PSI e em outros documentos relacionados à segurança da informação, garantindo a proteção dos ativos da empresa.
- **Garantir acesso e conhecimento da política:** Assegurar que todos os colaboradores sob sua gestão tenham acesso à PSI, às normas e aos procedimentos de segurança da informação, promovendo treinamentos e atividades de conscientização para garantir o entendimento e a aplicação das regras.

Além dessas responsabilidades, os gestores também devem:

- **Identificar e reportar incidentes de segurança:** Estar atentos a possíveis incidentes de segurança e reportá-los imediatamente à área de TI ou ao responsável pela segurança da informação na empresa.
- **Colaborar com as auditorias e investigações:** Prestar apoio e colaborar com as auditorias e investigações internas relacionadas à segurança da informação, fornecendo informações e documentos quando solicitados.
- **Revisar e atualizar os procedimentos da área:** Revisar periodicamente os procedimentos de segurança da informação da área sob sua gestão, atualizando-os sempre que necessário para garantir a adequação às novas tecnologias e ameaças.

8.6 Dos Proprietários de Ativos de Informação

O proprietário da informação, que pode ser um gerente, coordenador ou líder de equipe de uma determinada área ou projeto, é o principal responsável pela gestão e proteção das informações sob sua responsabilidade. Suas atribuições incluem:

Manutenção, Revisão e Cancelamento de Autorizações:

- **Manutenção:** Garantir que as informações sob sua responsabilidade estejam sempre atualizadas, precisas e completas.
- **Revisão:** Revisar periodicamente as autorizações de acesso concedidas, verificando se ainda são necessárias e se estão de acordo com as políticas da empresa.
- **Cancelamento:** Revogar as autorizações de acesso quando não forem mais necessárias ou quando houver indícios de uso indevido das informações.

Responsabilidades Específicas:

Cabe ao proprietário da informação:

- **Elaborar matriz de autorizações de acesso:** Criar e manter uma matriz que relacione os cargos e funções da empresa às autorizações de acesso concedidas para cada informação ou conjunto de informações sob sua responsabilidade. Essa matriz deve ser clara e objetiva, facilitando a gestão e o controle dos acessos.
- **Manter registro e controle de autorizações:** Registrar e controlar todas as autorizações de acesso concedidas, incluindo a data de concessão, o usuário autorizado e o tipo de acesso permitido. Esse registro deve ser atualizado sempre que houver alterações nas autorizações.
- **Suspensão ou alteração de autorizações:** Tomar as medidas necessárias para suspender ou alterar as autorizações de acesso quando necessário, seja por mudança de função do usuário, término do vínculo com a empresa ou suspeita de uso indevido das informaçõe

8.7 Descarte seguro para ativos de informação

Verificação Prévia:

Antes de entregar qualquer ativo de informação da Pirelli para leilão, remanejamento ou reutilização, é obrigatória a realização de uma verificação completa para garantir a segurança dos dados e informações armazenados. Essa verificação deve assegurar que:

- **Dados pessoais:** Todos os dados pessoais, incluindo informações de clientes, funcionários e fornecedores, sejam completamente removidos ou anonimizados, de acordo com a Lei Geral de Proteção de Dados (LGPD).
- **Informações sigilosas:** Informações confidenciais da empresa, como segredos comerciais, estratégias de negócios e dados financeiros, sejam completamente removidas ou protegidas por criptografia forte.
- **Softwares:** Softwares licenciados e informações de propriedade intelectual da empresa sejam removidos ou desativados, de acordo com os termos de licença e as políticas da empresa.

Sanitização de Dados:

A remoção de dados e informações dos ativos de informação deve ser realizada por meio de técnicas e softwares de sanitização que garantam a irrecuperabilidade dos dados originais. A simples formatação do dispositivo não é suficiente, pois os dados podem ser recuperados por meio de ferramentas especializadas.

Métodos de Sanitização:

Existem diversos métodos de sanitização de dados, como:

- **Sobrescrita de dados:** Substituição dos dados originais por dados aleatórios, várias vezes, para garantir que as informações originais sejam irrecuperáveis.
- **Desmagnetização:** Aplicação de um forte campo magnético para apagar os dados armazenados em discos rígidos e fitas magnéticas.
- **Destruição física:** Destruição completa do dispositivo de armazenamento, como a trituração de discos rígidos e a incineração de fitas magnéticas.

Responsabilidade:

A responsabilidade pelo descarte seguro dos ativos de informação é do proprietário do ativo ou do gestor da área responsável. É fundamental garantir que o processo de sanitização seja realizado de forma correta e completa, evitando o vazamento de informações confidenciais e o descumprimento da LGPD.

8.8 Da Gerência de Tecnologia da Informação

A Gerência de Tecnologia da Informação (GTI) é a área responsável por gerenciar o uso das tecnologias na Pirelli, garantindo o bom andamento dos negócios e a segurança das informações. Para isso, a GTI conta com uma equipe de Segurança da Informação dedicada ao planejamento e execução de ações preventivas e ao tratamento de incidentes.

Responsabilidades da GTI:

Cabe à GTI:

- **Atualizar e publicar a PSI e as Normas de Segurança da Informação:** A GTI é responsável por revisar e atualizar periodicamente a Política de Segurança da Informação (PSI) e as Normas de Segurança da Informação, submetendo as alterações à aprovação do Comitê de Segurança da Informação e garantindo a divulgação das versões atualizadas a todos os colaboradores.
- **Propor metodologias e processos de Segurança da Informação:** A GTI deve desenvolver e implementar metodologias e processos para garantir a segurança das informações da empresa, como a avaliação de riscos, a gestão de vulnerabilidades, a resposta a incidentes e a recuperação de desastres.
- **Gerenciar o acesso aos sistemas e informações:** A GTI deve implementar e gerenciar os controles de acesso aos sistemas e informações da empresa, garantindo que apenas pessoas autorizadas tenham acesso aos recursos necessários para o desempenho de suas funções.
- **Monitorar e auditar o uso dos recursos tecnológicos:** A GTI deve monitorar o uso dos recursos tecnológicos da empresa, como computadores, redes, sistemas e aplicativos, a fim de identificar e prevenir atividades suspeitas ou não autorizadas.
- **Investigar e responder a incidentes de segurança:** A GTI deve investigar e responder a incidentes de segurança, como ataques cibernéticos, vazamento de dados e perda de informações, tomando as medidas necessárias para minimizar os impactos e evitar a recorrência do problema.
- **Conscientizar e treinar os colaboradores:** A GTI deve promover a conscientização e o treinamento dos colaboradores sobre a importância da segurança da informação, fornecendo informações e orientações sobre as melhores práticas de segurança.
- **Gerenciar fornecedores de tecnologia:** A GTI deve gerenciar os contratos e o relacionamento com fornecedores de tecnologia, garantindo que eles cumpram os requisitos de segurança da informação da empresa.

8.9 Do Comitê Consultivo

O Comitê Consultivo de Segurança da Informação é um órgão de apoio à GTI, responsável por auxiliar na definição de estratégias e diretrizes de segurança da informação, além de acompanhar a implementação e o cumprimento da PSI.

Composição:

O Comitê Consultivo deve ser composto por membros de diferentes áreas da Pirelli, com o objetivo de garantir uma visão multidisciplinar e abrangente sobre os desafios e as necessidades de segurança da informação. A participação de gestores de diversas áreas permite a troca de experiências e o desenvolvimento de soluções mais eficazes para proteger os ativos da empresa.

Responsabilidades:

Cabe ao Comitê Consultivo:

- **Analisar e aprovar as atualizações da PSI e das Normas de Segurança da Informação:** O Comitê deve revisar as propostas de atualização da GTI, avaliando sua adequação aos objetivos da empresa e às melhores práticas de segurança da informação.
- **Acompanhar a implementação da PSI:** O Comitê deve monitorar a implementação da PSI, verificando se as medidas de segurança estão sendo adotadas de forma correta e eficaz.
- **Avaliar os riscos de segurança da informação:** O Comitê deve analisar periodicamente os riscos de segurança da informação da empresa, identificando possíveis vulnerabilidades e propondo medidas de mitigação.
- **Propor melhorias para a segurança da informação:** O Comitê deve identificar oportunidades de melhoria na segurança da informação da empresa, propondo novas soluções e práticas para fortalecer a proteção dos ativos.
- **Atuar como canal de comunicação:** O Comitê deve servir como canal de comunicação entre a GTI e as demais áreas da empresa, facilitando o diálogo e a colaboração em questões relacionadas à segurança da informação.

Funcionamento:

O Comitê Consultivo deve se reunir periodicamente para discutir os assuntos relacionados à segurança da informação, analisar relatórios e indicadores, e tomar decisões sobre as medidas a serem adotadas. As reuniões devem ser registradas em atas, que devem ser disponibilizadas para consulta pelos membros do Comitê e pela GTI.

Ao contar com um Comitê Consultivo atuante e representativo, a Pirelli garante uma gestão mais eficiente e participativa da segurança da informação, fortalecendo a cultura de segurança e minimizando os riscos de incidentes.

8.10 Da Assessoria Jurídica

A Assessoria Jurídica (AJ) da Pirelli prestará apoio à Gerência de Tecnologia da Informação (GTI), quando solicitado, em questões relacionadas à segurança da informação. Esse apoio incluirá:

- **Análise de casos:** A AJ analisará casos específicos relacionados à segurança da informação, como incidentes de segurança, vazamento de dados, violações da PSI e outras situações que possam ter implicações legais.
- **Elaboração de pareceres:** A AJ emitirá pareceres jurídicos sobre questões de segurança da informação, orientando a GTI sobre as melhores práticas e os procedimentos a serem adotados para garantir a conformidade com a legislação vigente e proteger os interesses da empresa.
- **Estudo de casos:** A AJ realizará estudos aprofundados sobre temas relevantes para a segurança da informação, como a Lei Geral de Proteção de Dados (LGPD), a legislação sobre crimes cibernéticos e outras normas que possam impactar as atividades da empresa.

A colaboração entre a GTI e a AJ é fundamental para garantir que as medidas de segurança da informação adotadas pela empresa estejam em conformidade com a legislação e protejam os interesses da empresa e de seus clientes.

8.11 Da Gerência de Pessoal

Cabe à Gerência de Pessoal (GEP):

- **Incluir cláusulas de segurança da informação nos contratos de trabalho:** Na fase de contratação de funcionários, prestadores de serviços, estagiários e afins, a GEP deve incluir nos contratos individuais de trabalho cláusulas que formalizem a responsabilidade de cada colaborador em relação ao cumprimento da Política de Segurança da Informação (PSI) e à proteção de dados pessoais.
- **Conscientizar os colaboradores sobre a importância da segurança da informação:** A GEP deve promover ações de conscientização para que os colaboradores compreendam a importância da segurança da informação e a necessidade de seguir as normas e procedimentos estabelecidos pela empresa.
- **Informar os colaboradores sobre as consequências do descumprimento da PSI:** A GEP deve deixar claro aos colaboradores que o descumprimento da PSI e das normas de proteção de dados pessoais pode resultar em medidas disciplinares, incluindo a rescisão do contrato de trabalho.
- **Manter registros atualizados das autorizações de acesso:** A GEP deve manter registros atualizados das autorizações de acesso de cada colaborador aos sistemas e informações da empresa, garantindo que apenas pessoas autorizadas tenham acesso aos recursos necessários para o desempenho de suas funções.
- **Realizar treinamentos periódicos sobre segurança da informação:** A GEP deve promover treinamentos periódicos sobre segurança da informação para os colaboradores, abordando temas como a criação de senhas fortes, a identificação de phishing e outras ameaças, e o uso seguro de dispositivos móveis e redes sociais.
- **Comunicar as atualizações da PSI aos colaboradores:** A GEP deve informar os colaboradores sobre as atualizações da PSI e das normas de segurança da informação, garantindo que todos estejam cientes das novas regras e procedimentos.

Ao desempenhar essas responsabilidades, a GEP contribui para a criação de uma cultura de segurança da informação na empresa, protegendo os dados pessoais dos colaboradores e clientes, e garantindo a integridade e a confidencialidade das informações da empresa.

9. Da Inovação e Uso de Novas Tecnologias

A Pirelli reconhece a importância da inovação e do desenvolvimento de novas tecnologias para o seu crescimento e competitividade. Por isso, incentiva a busca por soluções inovadoras e o uso de novas tecnologias em seus processos e atividades, desde que estejam alinhadas com os objetivos da empresa e com os princípios da segurança da informação.

Incentivo à Inovação:

A Pirelli incentiva seus colaboradores a:

- **Pensar fora da caixa:** Buscar novas ideias e soluções criativas para os desafios da empresa.
- **Experimentar novas tecnologias:** Testar e avaliar novas tecnologias que possam trazer benefícios para a empresa, como aumento da produtividade, redução de custos e melhoria da qualidade dos produtos e serviços.
- **Compartilhar conhecimentos:** Trocar experiências e conhecimentos sobre novas tecnologias com outros colaboradores, promovendo um ambiente de aprendizado e colaboração.
- **Participar de projetos de inovação:** Colaborar em projetos de inovação da empresa, contribuindo com suas ideias e habilidades.

Segurança da Informação e Novas Tecnologias:

Ao adotar novas tecnologias, a EMPRESA deve garantir que elas sejam implementadas de forma segura, considerando os riscos e as vulnerabilidades que podem surgir. Para isso, é fundamental:

- **Avaliar os riscos de segurança:** Antes de implementar uma nova tecnologia, a EMPRESA deve realizar uma avaliação de riscos para identificar as possíveis ameaças e vulnerabilidades que ela pode trazer.
- **Implementar medidas de segurança adequadas:** A Pirelli deve implementar medidas de segurança adequadas para proteger seus sistemas e informações contra as ameaças identificadas na avaliação de riscos.
- **Monitorar e atualizar as tecnologias:** A Pirelli deve monitorar continuamente as novas tecnologias adotadas, aplicando as atualizações de segurança necessárias para garantir a proteção contra novas ameaças.
- **Treinar os colaboradores:** A Pirelli deve fornecer treinamento aos colaboradores sobre o uso seguro das novas tecnologias, conscientizando-os sobre os riscos e as medidas de proteção necessárias.

Ao incentivar a inovação e o uso de novas tecnologias de forma segura e responsável, a EMPRESA garante sua competitividade e o crescimento sustentável, ao mesmo tempo em que protege seus ativos de informação e seus negócios.

10. *Da Proteção de Dados Pessoais*

- **Disponibilidade:** Os dados pessoais estarão disponíveis para acesso e utilização pelos colaboradores autorizados, sempre que necessário para o cumprimento das finalidades para as quais foram coletados.
- **Integridade:** Os dados pessoais serão mantidos íntegros, completos e atualizados, garantindo sua exatidão e confiabilidade.
- **Confidencialidade:** Os dados pessoais serão protegidos contra o acesso não autorizado, uso indevido, divulgação, alteração ou destruição, garantindo a privacidade dos titulares dos dados.

Para garantir a proteção dos dados pessoais, a Pirelli adotará as seguintes medidas:

- **Mapeamento dos dados pessoais:** A Pirelli realizará um mapeamento completo dos dados pessoais que coleta e trata, identificando a origem, a finalidade, a base legal e os responsáveis pelo tratamento de cada dado.
- **Consentimento do titular:** A Pirelli solicitará o consentimento do titular dos dados pessoais para o tratamento de seus dados, informando de forma clara e transparente sobre a finalidade do tratamento, os direitos do titular e a possibilidade de revogar o consentimento a qualquer momento.
- **Medidas de segurança:** A Pirelli implementará medidas de segurança técnicas e administrativas adequadas para proteger os dados pessoais contra o acesso não autorizado, uso indevido, divulgação, alteração ou destruição.
- **Treinamento dos colaboradores:** A Pirelli promoverá o treinamento dos colaboradores sobre a LGPD e as boas práticas de proteção de dados pessoais, conscientizando-os sobre a importância da privacidade e da segurança das informações.
- **Canal de comunicação:** A Pirelli disponibilizará um canal de comunicação para que os titulares dos dados possam exercer seus direitos, como o acesso, a correção, a portabilidade e a exclusão de seus dados.
- **Revisão periódica:** A Pirelli revisará periodicamente suas políticas e procedimentos de proteção de dados pessoais, adaptando-os às mudanças na legislação e às novas tecnologias.

11. *Das Disposições Finais*

O descumprimento da Política de Segurança da Informação (PSI) e das Normas de Segurança da Informação da Pirelli, por parte de qualquer colaborador, prestador de serviço, estagiário ou afins, acarretará em sanções disciplinares. As penalidades serão aplicadas de acordo com a gravidade da infração e poderão variar desde uma advertência verbal ou escrita até a demissão por justa causa, conforme previsto na legislação trabalhista e nas normas internas da empresa.

A Pirelli se reserva o direito de revisar e atualizar a PSI e as Normas de Segurança da Informação periodicamente, a fim de garantir sua adequação às novas tecnologias, ameaças e legislações. As alterações serão comunicadas aos colaboradores por meio dos canais de comunicação internos da empresa.

12. *Documentos Relacionados*

Documentos administrativos:

- **Norma de Acesso Remoto:** Define as regras e procedimentos para o acesso remoto aos sistemas e informações da empresa, garantindo a segurança e a privacidade dos dados.
- **Norma de Acesso e Uso do Correio Eletrônico:** Estabelece as diretrizes para o uso seguro e adequado do correio eletrônico corporativo, incluindo regras para o envio e recebimento de mensagens, anexos e informações confidenciais.
- **Norma de Gestão de Usuários e Direitos de Acesso a Sistemas:** Define os processos para a criação, gerenciamento e desativação de contas de usuários, bem como a atribuição de permissões de acesso aos sistemas e informações da empresa.
- **Norma de Monitoramento de Ativos:** Estabelece os procedimentos para o monitoramento dos ativos de informação da empresa, incluindo computadores, dispositivos móveis, redes, sistemas e aplicativos, a fim de identificar e prevenir atividades suspeitas ou não autorizadas.
- **Norma de Uso e Acesso à Internet e às Redes Sociais:** Define as regras e diretrizes para o uso da internet e das redes sociais pelos colaboradores da empresa, visando garantir a segurança das informações e a proteção da imagem da empresa.
- **Norma de Uso de Ativos:** Estabelece as regras para o uso adequado dos ativos de informação da empresa, como computadores, dispositivos móveis, softwares e dados, a fim de garantir sua integridade, confidencialidade e disponibilidade.
- **Norma de Uso de Dispositivos Móveis:** Define as regras e procedimentos para o uso seguro de dispositivos móveis corporativos e pessoais, incluindo smartphones, tablets e laptops, para acessar os sistemas e informações da empresa.
- **Norma de Gestão de cópias de Segurança (Backup):** Estabelece os procedimentos para a realização de backups periódicos dos dados e informações da empresa, garantindo a recuperação em caso de perda, roubo ou desastre.
- **Norma de Gestão do Datacenter:** Define as regras e procedimentos para a gestão do datacenter da empresa, garantindo a segurança física e lógica dos equipamentos e informações armazenados.

Outras Políticas:

- **Política de Mídias Sociais da Pirelli:** Estabelece as diretrizes para o uso das mídias sociais pelos colaboradores da empresa, visando proteger a imagem da empresa e evitar a divulgação de informações confidenciais.
- **Política de Privacidade da Pirelli:** Define como a empresa coleta, utiliza, armazena e protege os dados pessoais de seus clientes, colaboradores e parceiros, em conformidade com a LGPD.
- **Política de Cookies da Pirelli:** Informa sobre o uso de cookies no site da empresa, explicando sua finalidade e como o usuário pode gerenciar suas preferências.

- **Política de Segurança da Informação Educacional:** Define as diretrizes para a segurança da informação em ambientes educacionais, como escolas e universidades, que utilizam os produtos e serviços da Pirelli.
- **Código de Conduta da Pirelli:** Estabelece os princípios éticos e as normas de conduta que devem ser seguidos por todos os colaboradores da empresa em suas atividades profissionais.

Anexo III - CÓDIGO DE ÉTICA

Código de Ética

Premissa

O Grupo Pirelli realiza suas operações internas e externas de acordo com os princípios estabelecidos neste Código de Ética (o "**Código**"), na crença de que a ética empresarial deve ser perseguida juntamente com o sucesso dos negócios.
Cada diretor, revisor oficial de contas, gerente, funcionário do Grupo Pirelli e, em geral, qualquer pessoa que trabalha em Itália e no estrangeiro para ou por conta do Grupo Pirelli, ou que tem relações de negócios com este ("**Destinatários do Código**") devem, cada qual no âmbito de suas funções e responsabilidades, respeitar os princípios e regras deste Código.

Princípios de Conduta

Integridade, transparência, honestidade e seriedade em conformidade à atividade do Grupo Pirelli. Principalmente, o Grupo Pirelli:
– Visa a excelência e a competitividade dentro do mercado, oferecendo aos seus clientes produtos e serviços de qualidade, que atendem de forma eficiente às suas necessidades.
– Garante a todas as partes interessadas (stakeholders) transparência em suas ações, mantendo a exigência de confidencialidade necessária na condução dos negócios e na garantia da competitividade. Para tal, os Destinatários do Código devem garantir a máxima confidencialidade a respeito das informações obtidas ou utilizadas em função ou por ocasião do desempenho de suas tarefas.
– Compromete-se em promover uma concorrência leal, considerada fundamental ao próprio interesse e de todos os que operam no mercado, dos clientes e das demais partes interessadas (stakeholders).
– Declara-se contrário e condena as condutas ilícitas e incorretas usadas para atingir objetivos econômicos estabelecidos, que só poderão ser alcançados por meio da excelência do desempenho quanto à qualidade, sustentabilidade econômica, social e ambiental.
– Apoia e valoriza seus recursos humanos.
– Busca o respeito do princípio de iguais oportunidades no ambiente de trabalho, sem discriminação de sexo, estado civil, orientação sexual, credo religioso, opiniões políticas e sindicais, cor, raça, nacionalidade, idade ou estado de saúde.
– Busca e apoia a proteção dos direitos humanos reconhecidos internacionalmente;
– Busca e promove a garantia dos direitos humanos declarados em nível internacional.
– Usa os recursos de forma responsável, visando alcançar um desenvolvimento sustentável, respeitando o meio ambiente e os direitos das gerações futuras. Não aceita a corrupção de qualquer natureza, em qual quer jurisdição, até mesmo onde tal atividade seja admitida, tolerada ou não perseguida por lei. Para tal, os Destinatários do Código não poderão oferecer presentes ou prestar outras gentilezas que possam representar violação de normas que infrinjam o Código, ou que ainda possam, se públicos, constituírem prejuízo mesmo que apenas à imagem do Grupo Pirelli.
– Defende e protege seus bens corporativos, e procurará os meios para evitar atos de apropriação indébita, roubo e fraude contra o Grupo.

– Protege e salvaguarda a reputação corporativa, que é um ativo intangível da empresa e do Grupo, e a reputação de todos os seus trabalhadores externos, exigindo de si mesmo uma conduta condizente com esses objetivos, para preservar também a cultura corporativa representada pelo conjunto de valores que refletem a natureza específica do Grupo Pirelli;
– Condena a busca de interesses pessoais e/ou de terceiros em detrimento dos interesses da Empresa.
– Como componente ativo e responsável das comunidades nas quais opera, tem um comprometimento com o respeito, dentro do Grupo e nas relações com o mundo externo, das leis vigentes nos Países onde desempenha a própria atividade.
– Implementa os instrumentos organizacionais destinados a prevenir a violação de normas e princípios de transparência, seriedade e lealdade por parte de seus empregados e colaboradores, e vigia seu cumprimento e a sua concreta implementação.

Sistema de Controle Interno

A eficiência e a eficácia do sistema de controle interno são uma condição fundamental para operar as atividades empresariais em conformidade com as regras e os princípios deste Código. O sistema de controle interno é o conjunto de ferramentas, atividades, procedimentos e estruturas organizacionais, voltado a garantir, mediante um processo integrado de identificação, medição, gestão e monitoramento dos principais riscos, os seguintes objetivos:

– A eficácia e a eficiência das atividades empresariais, garantindo a rastreabilidade de ações e decisões.
– A confiabilidade das informações relativas à contabilidade e à gestão.
– O respeito às leis e regulamentos.
– A garantia da integridade do patrimônio empresarial.

Para tal, os Destinatários do Código são chamados a contribuir com o contínuo melhoramento do sistema de controle interno. Os órgãos de controle e de fiscalização, a Auditoria Interna e a Auditoria Externa, no desempenho de suas atividades e no que for de sua competência, têm acesso direto, completo e incondicional a todas as pessoas, atividades, operações, documentos, arquivos e bens empresariais.

Partes Interessadas

O Grupo Pirelli adota uma abordagem “multi-stakeholders”, isto é, busca um crescimento sustentável e duradouro, visando atender às expectativas de todos aqueles que interagem com o Grupo e suas Empresas.

→ ACIONISTAS, INVESTIDORES E COMUNIDADE FINANCEIRA

O diálogo e as relações do Grupo Pirelli com todas as categorias de acionistas, investidores institucionais e privados, analistas financeiros, agentes de mercado e, de modo geral, com a comunidade financeira, apoiam-se na máxima transparência, no

respeito dos princípios de precisão, presteza e igualdade de acesso à informação, tendo em vista favorecer uma correta avaliação dos ativos do Grupo.

→ MEIO AMBIENTE

O Grupo Pirelli administra suas atividades no respeito ao Meio Ambiente e à Saúde Pública. Suas opções, quanto aos investimentos e aos negócios, estão em conformidade com o respeito ao meio ambiente, numa perspectiva de crescimento eco-compatível mesmo mediante a adoção de tecnologias específicas e métodos de produção que – se sustentáveis do ponto de vista financeiro e ope racional – sejam aptos a reduzir o impacto ambiental de suas atividades, mesmo além dos limites estabelecidos pelas normas vigentes.
O Grupo governa as suas atividades com o auxílio de Sistemas de Gestão Ambiental certificados; adota métodos e tecnologias produtivas visando reduzir os desperdícios e preservar os recursos naturais; e avalia os impactos ambientais diretos e indiretos de seus produtos e serviços.
O Grupo colabora ainda com as principais organizações nacionais e internacionais, com o intuito de promover a sustentabilidade ambiental, local e global.

→ CLIENTES

A excelência dos produtos e dos serviços oferecidos do Grupo Pirelli baseiase na constante inovação, com o objetivo de antecipar as necessidades de seus clientes e atender a seus pedidos com uma resposta imediata e competente, com uma conduta honesta, amável e de grande colaboração.

→ RECURSOS HUMANOS

O Grupo Pirelli reconhece a importância dos recursos humanos, com a certeza de que o elemento principal de sucesso de cada empresa é constituído pela contribuição profissional das pessoas que nela trabalham, num clima de lealdade e confiança entre as duas partes.
O Grupo Pirelli preserva a saúde, a segurança e a higiene nos locais de trabalho, mediante sistemas de gestão em constante melhoramento e evolução, e mediante a promoção de uma cultura da segurança e da saúde apoiada na lógica da prevenção e na exigência de administrar, de maneira eficaz, os riscos profissionais.
O Grupo Pirelli considera o respeito pelos direitos dos trabalhadores como um elemento fundamental para os negócios.
Da mesma forma, o Grupo Pirelli exige um comportamento baseado no respeito mútuo, integridade e dignidade das pessoas.
As relações de trabalho são geridas com ênfase especial na igualdade de oportunidades, favorecendo o crescimento profissional de cada pessoa e valorizando as diferenças para criar um ambiente de trabalho inclusivo.

→ FORNECEDORES E COLABORADORES EXTERNOS

Os fornecedores e os colaboradores externos desempenham um papel fundamental no melhoramento da competitividade geral da Empresa.

As relações do Grupo com os fornecedores e os colaboradores externos, tendo em vista a máxima vantagem competitiva, apoiam-se na lealdade, na imparcialidade e no respeito das iguais oportunidades para todos os envolvidos.
Os fornecedores e colaboradores externos do Grupo Pirelli deverão respeitar as disposições e os princípios previstos neste Código.

→ COMUNIDADE EXTERNA
O Grupo Pirelli mantém com as autoridades públicas locais, nacionais e supranacionais, relações baseadas na plena e eficiente colaboração, transparência, respeito às mútuas autonomias, aos objetivos econômicos e aos valores que constam do Código.
O Grupo Pirelli deseja contribuir para o bem-estar econômico e para o crescimento das comunidades nas quais atua, oferecendo serviços eficientes e tecnologicamente avançados.
O Grupo Pirelli defende e, se necessário, patrocina iniciativas sociais, culturais e educacionais voltadas para a valorização das pessoas e o melhoramento de suas condições de vida.
O Grupo Pirelli não oferece contribuições, vantagens ou presta gentilezas a partidos políticos ou organizações sindicais dos trabalhadores, ou a seus representantes ou candidatos, mantendo-se o cumprimento das normas eventualmente aplicáveis.

→ CONCORRENTES
O Grupo Pirelli reconhece que uma concorrência correta e leal constitui elemento fundamental para o desenvolvimento da Empresa e do mercado e administra as próprias atividades promovendo uma competição baseada na inovação, na qualidade e no desempenho dos próprios produtos. As Empresas e todos os empregados do Grupo deverão evitar quaisquer práticas comerciais incorretas e, de modo algum, a convicção de que agir em vantagem do Grupo possa justificar a adoção de uma conduta contrária a estes princípios.

Respeito do Código

O Grupo Pirelli exige que a conduta de todos os Destinatários do Código seja coerente com os princípios gerais que estabelece. Todos os Destinatários do Código deverão, portanto, evitar qual quer conduta contrária aos princípios que constam do Código.
O Grupo Pirelli também exige que todos os destinatários do Código de Ética, incluindo os trabalhadores externos, relatem imediatamente qualquer violação conhecida deste Código de Ética, de acordo com os procedimentos estabelecidos.
O Grupo compromete-se a adotar procedimentos apropriados, regulamentos ou disposições voltadas a garantir que os valores aqui afirmados se reflitam na conduta concreta do Grupo e de seus empregados e colaboradores.
Uma violação dos princípios e conteúdo deste Código pode constituir um descumprimento das obrigações primárias de acordo com o contrato de trabalho do infrator e / ou seu contrato, com a possibilidade que possam enfrentar medidas disciplinares previstas na legislação, em acordos coletivos ou em contratos.