Política de Segurança da Informação

Pirelli

Aluno1: Luiz Felipe

Aluno2: Luiz Otávio

Aluno3: Diego Queiroz

Aluno4: Marcus Vinícius

Histórico de revisões

Versão	Data	Alteração
Versão 1.0	29/05/2024	Lançamento da Primeira versão

Este documento deve:

1. Estar sempre atualizado;
2. Ter cópia controlada e somente gerada pela área responsável pela divulgação dos Instrumentos Normativos;
3. Ser divulgado a todos os funcionários, prestadores de serviços, estagiários e afins da instituição.

Sumário

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.