PLT-SI-001 – Política de Segurança da Informação

Data: 15/09/2025

Revisão: 04

Classificação: Público

1. OBJETIVO

Estabelecer e regulamentar padrões seguros para manipulação e uso da informação, seja através de uso de recursos digitais, origem falada ou escrita e os meios utilizados para transmissão da informação, através de recursos computacionais disponibilizados pela Compwire aos seus colaboradores e clientes, dentro de sua rede corporativa, bem como prover Segurança no acesso destes.

Como premissa, esta Política tem também como objetivo: orientar sobre a adoção de controles e processos para atender aos requisitos de Segurança da Informação; resguardar as informações da Compwire, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade; prevenir possíveis causas de incidentes e responsabilidade legal da empresa e seus colaboradores, clientes e parceiros; minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da Compwire como resultado de falhas de segurança.

2. APLICAÇÃO

Esta Política se aplica a todos os colaboradores, ex-colaboradores, prestadores de serviço, ex. prestadores de serviço, clientes, qualquer pessoa com poderes de representação da organização respeitando os acordos operacionais estabelecidos, que possuíram, possuem ou virão a possuir acesso às informações da Compwire Informática e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura.

3. DEFINIÇÕES E ABREVIATURAS

- SGSI - Sistema de Gestão de Segurança da Informação (SGSI): Conjunto de controles, políticas, práticas e procedimentos que visam proteger a informação.

4. REFERÊNCIAS

- ISO/IEC 27001:2022 - Sistemas de Gestão da Segurança da Informação (Requisitos).
- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.

5. DESCRIÇÃO

5.1. Papéis e Responsabilidades

5.1.1. Todos os colaboradores

- Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis e procedimentos estabelecidos no SGSI;
- Ser responsável pelo acesso realizado com a sua identificação e autenticação;
- Deve acessar a informação para desempenhar profissionalmente suas funções relacionadas à Compwire ou para outras situações formalmente permitidas;

- Garantir a confidencialidade, integridade e disponibilidade das informações recebidas na execução das atividades da Compwire;
- Comunicar a equipe de Segurança da Informação sobre qualquer evento que viole ou possa violar esta Política;
- Preservar os ativos da organização;
- Assinar as políticas e normas aplicáveis, formalizando a ciência e o aceite integral das disposições da Política/Norma em questão;
- Compreender e seguir os princípios do Código de Ética e Conduta;
- Ser exemplo de conduta ética, representando um dos fatores críticos de sucesso para o aumento da consistência ética na empresa;
- Evitar qualquer ação que, direta ou indiretamente, tenha influência fraudulenta, enganosa ou coercitiva;
- Informar qualquer ato de violação ao Código de Ética e Conduta a Área de Compliance ou propor de forma anônima denuncia junto ao canal inserido no site: www.compwire.com.br/canal-de-denuncias/;
- Discutir com a área de Compliance os casos de dúvidas envolvendo questões éticas.

5.1.2. Alta Gestão

- Zelar pela manutenção do negócio, dentro de uma perspectiva de longo prazo e de sustentabilidade, que incorpore considerações de ordem econômica, social, ambiental e de boa governança corporativa na definição dos negócios e operações;
- Estabelecer e implementar as políticas e objetivos compatíveis com o contexto e planejamento estratégico da organização;
- Acompanhar os objetivos, indicadores e metas;
- Conduzir a análise crítica e melhoria do SGSI;
- Prover recursos para o SGSI através dos orçamentos corporativos;
- Apoiar no cumprimento das diretrizes de Segurança da Informação;
- Zelar pela adequação da estrutura de Segurança da Informação;
- Cumprir e promover o cumprimento desta Política e do Código de Ética e Conduta;
- Divulgar permanentemente a Política de Segurança da Informação e o Código de Ética e Conduta, assim como as demais políticas e legislações que regem o negócio, no intuito de esclarecer dúvidas e acolher sugestões, bem como submeter as suas práticas a processos de avaliação periódica;
- Obedecer à legislação e aos regulamentos trabalhistas (inclusive os aplicáveis a Pessoas Jurídicas – PJ – e cooperados), bem como às normas Municipais, Estaduais e Federais, e quaisquer outros dispositivos reguladores nacionais e internacionais, inclusive aqueles relativos ao controle de importações e exportações nos países em que atua;
- Assegurar a disponibilidade e transparência das informações que afetam os seus empregados, preservando os direitos de privacidade no manejo de informações médicas, funcionais e pessoais a eles pertinentes, de acordo com as diretrizes da LGPD;
- Garantir a segurança e saúde de seus colaboradores no trabalho, disponibilizando as condições e equipamentos necessários;

- Promover a igualdade de oportunidades para todos os empregados, em todas as políticas, práticas e procedimentos, assegurando a aplicação do princípio da isonomia nas relações de trabalho;
- Promover e respeitar a diversidade no ambiente de trabalho, e combater todas as formas de preconceito e discriminação;
- Desenvolver uma cultura organizacional que valoriza o intercâmbio e a disseminação de conhecimentos, promovendo a capacitação contínua de seus empregados.

5.1.3. Gestores

- Apoiar na condução de ações (incluindo gerenciamento de riscos) e aplicação de recursos para atingir os objetivos da Compwire;
- Manter um diálogo contínuo com o corpo administrativo e reportar resultados planejados, reais e esperados, vinculados aos objetivos da Compwire;
- Estabelecer e manter estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno);
- Promover os controles necessários às atividades sob responsabilidade de suas áreas, incluindo o monitoramento dos respectivos riscos de Segurança da Informação;
- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela Compwire;
- Garantir a observância da Política de Segurança da Informação e sua aplicabilidade para colaboradores e terceiros;
- Tomar as ações cabíveis para se fazer cumprir os termos desta política;
- Propagar a cultura de Segurança da Informação nos times sob sua gestão;
- Ser exemplo de conduta ética, representando um dos fatores críticos de sucesso para o aumento da consistência ética na empresa. As ações e os comportamentos dos líderes pesam significativamente mais que suas próprias palavras;
- Tomar as medidas necessárias para proteger a confidencialidade de informações restritas sobre a Compwire;
- Evitar qualquer ação que, direta ou indiretamente, tenha influência fraudulenta, enganosa ou coercitiva;
- Divulgar, orientar e garantir que o conteúdo do Código de Ética e Conduta seja compreendido e seguido pelos colaboradores;
- Informar qualquer ato de violação ao Código de Ética e Conduta a Área de Compliance ou propor de forma anônima denuncia junto ao canal inserido no site: www.compwire.com.br/canal-de-denuncias/;
- Em caso de necessidade, reunir-se com a Área de Compliance para conhecimento dos casos de violação do Código de Ética e Conduta ocorridos no período e as ações tomadas pela empresa;
- Reconhecer o mérito dos funcionários e propiciar igualdade de acesso às oportunidades de desenvolvimento, de acordo com o desempenho de cada funcionário.

5.1.4. Segurança da Informação

- Implementar e monitorar controles adequados para preservar a Segurança da Informação e o atendimento das políticas e normativos internos da Organização;
- Atuar para prevenir ou responder a riscos e ameaças de Segurança da Informação conforme as normativas estabelecidas;
- Elaborar e manter procedimentos técnicos de Segurança da informação com apoio das áreas da TI e Qualidade;
- Propor e administrar projetos e iniciativas relacionadas à Segurança da Informação;
- Estar presente nas áreas de TI e Negócio, atuando de maneira preventiva, sobre os riscos e ameaças de Segurança da Informação;
- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- Prover informações para a tomada de decisões estratégicas relacionadas à Segurança da Informação;
- Manter a estrutura normativa de Segurança da Informação alinhada com as diretrizes da empresa;
- Prover condições que assegurem a adequada identificação, classificação, avaliação, mitigação, gerenciamento e reporte dos riscos de Segurança da Informação e a efetividade dos controles associados considerando também os resultados dos testes de controles.

5.1.5. Tecnologia da Informação

- Prover condições que assegurem a adequada identificação, classificação, avaliação, mitigação, gerenciamento e reporte dos riscos de Segurança da Informação e a efetividade dos controles associados considerando também os resultados dos testes de controles;
- Garantir a observância da Política de Segurança da Informação e sua aplicabilidade para colaboradores e terceiros;
- Propagar a cultura da Segurança da Informação nos times sob sua gestão;
- Monitorar e atentar a desvios e rotinas que possam causar a exposição da organização no cenário de Segurança da Informação;
- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;
- Atender a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela organização;
- Realizar as cópias de segurança do ambiente tecnológico;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta política e adicionais;
- Verificar os riscos relativos ao acesso pelos subcontratados, parceiros às instalações da Empresa e seus colaboradores seguirão o procedimento de controle de acesso, para controle e proteção pertinentes dessas instalações.

5.1.6. Qualidade e Auditoria

- Desenvolver, implementar e melhorar continuamente as práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e entidades;

- Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno);
- Reportar à gestão e ao corpo executivo sobre a adequação e eficácia da governança e do gerenciamento de riscos, para apoiar o atingimento dos objetivos da Compwire e promover e facilitar a melhoria contínua;
- Controlar e apoiar no cumprimento do objetivo de melhoria contínua através do monitoramento e ações para o atingimento das métricas definidas;
- Gerenciar e controlar o processo de auditoria interna para cumprir as exigências das normas e certificações necessárias;
- Gerenciar junto as equipes o tratamento de não conformidades, oportunidades de melhorias e recomendações realizadas em auditoria.

5.1.7. Área Jurídica e Compliance

- Requerer a inserção de cláusulas que obriguem o cumprimento desta Política de Segurança da Informação e demais leis, regulamentos e normas aplicáveis aos prestadores de serviços, cujos contratos tenham sua análise requerida ao departamento, assegurando que as informações sejam utilizadas apenas para sua finalidade dentro da organização e preservando sua confidencialidade;
- Garantir a conformidade com as expectativas legais, regulatórias e éticas;
- Interpretar as leis e regulamentos relevantes para as operações da empresa e garantir sua implementação efetiva em todas as áreas;
- Desenvolver e manter políticas e procedimentos internos que estejam alinhados com as exigências legais e éticas, bem como com as melhores práticas do setor;
- Fornecer treinamento contínuo e educação para todos os colaboradores sobre questões de compliance relevantes ao seu trabalho, garantindo o entendimento das políticas e procedimentos da empresa;
- Realizar monitoramento regular das atividades da empresa para garantir conformidade com políticas, procedimentos e regulamentos aplicáveis;
- Identificar, avaliar e mitigar os riscos de compliance associados às operações da empresa, implementando controles adequados para reduzir a probabilidade de violações legais ou éticas;
- Manter e promover canais de comunicação confidenciais e acessíveis para que os colaboradores possam relatar preocupações ou violações de compliance sem medo de retaliação;
- Investigar prontamente quaisquer denúncias de violações de compliance de forma imparcial e tomar medidas corretivas apropriadas, conforme necessário;
- Preparar relatórios regulares sobre atividades de compliance e comunicar proativamente às partes interessadas relevantes sobre questões significativas de compliance;
- Fomentar uma cultura de ética e integridade em toda a empresa, promovendo o comportamento ético e responsável em todos os níveis organizacionais.

5.1.8. Recursos Humanos

- Orientar quanto a política e as normas de Segurança da Informação para todos os colaboradores e assegurar que estejam cientes das diretrizes, normas e procedimentos internos;
- Notificar as alterações dos colaboradores a equipe de TI para tomar medidas relativas à segurança da informação, com relação liberação ou bloqueios, exclusão ou transferência de direitos relativos a sessões/contas;
- Garantir que os ex-colaboradores devolvam todos os ativos de Tecnologia e Segurança da Informação à Empresa.

5.1.9. Fornecedores

- Estar ciente e cumprir as regras estabelecidas nos contratos;
- Garantir a confidencialidade, integridade e disponibilidade das informações recebidas na execução das atividades.

5.1.10. Parceiros de Negócio

- Estar ciente e cumprir as regras estabelecidas nos contratos;
- Garantir a confidencialidade, integridade e disponibilidade das informações recebidas na execução das atividades.

5.1.11. Comitê de Segurança da Informação e Privacidade de Dados

Constituído por um conjunto multidisciplinar de participantes da corporação, formado por membros de áreas selecionadas da empresa.

Cada área selecionada, deverá ter ao menos um membro neste comitê, ou um suplente, para casos de ausência. O comitê tem a responsabilidade de analisar assuntos relacionados à Segurança da Informação e Privacidade de Dados, propor novas iniciativas a respeito do assunto e aprovar revisões de documentos (considerando que o documento só será publicado, com ao menos 70% de aprovação das áreas).

Recomenda-se a reunião deste comitê, com periodicidade mínima de 3 meses de intervalo, e participação de 70% das áreas selecionadas. Ou, diante de uma convocação extraordinária, para discussões emergenciais

Cabe ao Comitê de Segurança da Informação e Privacidade de Dados, com o auxílio do setor de Tecnologia da Informação:

- Analisar, revisar e propor a aprovação de políticas, normas e demais documentos instruções de trabalho, relacionadas à Segurança da Informação;
- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;
- Garantir que as atividades de Segurança da Informação sejam executadas em conformidade com a PSI;
- Promover a divulgação da PSI e adotar as medidas necessárias para disseminar uma cultura de Segurança da Informação no ambiente;

- Identificar e avaliar as principais ameaças à Segurança da Informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- Tomar as ações cabíveis para se fazer cumprir os termos desta Política;
- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado;
- Aprovar a elaboração, divulgação e revisão do Código de Ética e Conduta;
- Compreender e seguir os princípios do Código de Ética e Conduta;
- Orientar-se pelas disposições deste Código e de observarem seu conteúdo em seu âmbito de atuação, além de promover sua divulgação, seu entendimento e sua internalização, norteando as ações e relações com os públicos interno e externo.

5.2. Princípios de Segurança

Segurança da Informação pode ser definida como uma série de atividades designadas para garantir a continuidade dos negócios em sistemas de informação, utilizando computadores e redes de computador visando manter a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações garantindo assim um ambiente seguro de sistemas de informação. Segurança da Informação também significa todas as medidas preventivas, tangíveis e intangíveis, tomadas para que informações sigilosas da Compwire, dados pessoais e ativos relativos à segurança da informação não sejam divulgadas a pessoas não autorizadas ou empresas concorrentes, e proteger informações valiosas da Empresa e de clientes de todos os possíveis vazamentos de informações e ameaças diversas.

- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

5.3. Estrutura

A estrutura de documentos de Segurança da Informação da Compwire é composta por diretrizes contempladas nas rotinas de Segurança da Informação e outras áreas, as quais são complementares à presente Política. Existem documentos que detalham as diretrizes corporativas a serem cumpridas por todos os colaboradores e terceiros associados à Organização para atingir o objetivo proposto.

5.4. Gestão de Continuidade do Negócio

Os serviços de atendimento ao cliente possuem disponibilidade 24X7, quando contratado, com a gestão dos serviços de telefonia hospedados em nuvem. Para garantir a plena operação sem interrupções foi elaborado no **Plano de Continuidade de Negócios – PCN**.

5.5. Disposições Gerais

A Compwire está comprometida com a proteção das informações sob sua responsabilidade, garantindo confidencialidade, integridade e disponibilidade em todas as suas atividades e na prestação de seus serviços. Esse compromisso inclui a conformidade com a legislação, assegurando a confiança de clientes, parceiros, colaboradores e demais partes interessadas. A segurança da informação é tratada de forma estratégica e contínua, sendo responsabilidade de todos os colaboradores na manutenção de um ambiente seguro e confiável.

O estabelecimento do Sistema de Gestão de Segurança da Informação é um compromisso da direção da Compwire, com foco na proteção dos ativos de informação contra acesso não autorizado, uso indevido, divulgação, modificação ou destruição.

A manutenção e melhoria contínua do Sistema de Gestão de Segurança da Informação também é objetivo da Compwire, conscientizando a todos e contando com a participação e colaboração de todos.

Periodicamente são realizadas análises críticas pela direção visando acompanhar, rever e melhorar o Sistema de Gestão de Segurança da Informação.

Os casos não previstos nesta política ou as dúvidas porventura existentes, poderão ser tratados pelo interessado junto à Gerência de Segurança da Informação

5.6. Penalidades

O descumprimento da política pode ocasionar medidas disciplinares, violações e sanções.

6. DOCUMENTOS RELACIONADOS

- PLT-RH-020 - Código de Ética e Conduta.