

Política Segurança da Informação - Fornecedores

1. Objetivo

A Política de Segurança da Informação para Terceiro visa estabelecer as regras e diretrizes que guiam o relacionamento com os fornecedores, e/ou prestadores de serviço juntos as Empresas do Grupo Ipiranga (“Empresas”), sendo a base para o estabelecimento de todos os padrões e procedimentos de segurança.

A Política se aplica a todo terceiro que forneça ou desenvolva algum tipo de sistema ou serviço para as Empresas do Grupo Ipiranga, sendo os gestores de cada sistema responsáveis pela correta adequação dos pontos de segurança que não estejam atendidos pelo seu Terceiro.

2. Público-Alvo

Este documento aplica-se a todos os fornecedores e/ou prestadores de serviços que estabelecem contrato com as Empresas do Grupo Ipiranga.

3. Papéis e Responsabilidades

Todos os fornecedores e/ou prestadores de serviços, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação. Em atenção especial ao compromisso com os critérios legais e éticos que envolvam as Empresas do Grupo Ipiranga. É de inteira responsabilidade do Terceiro qualquer prejuízo ou dano sofrido ou causado alguma das Empresas do Grupo Ipiranga ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.

4. Termos e Definições

Ativos de Informação: dados, sistemas, infraestrutura, softwares, documentos e outros recursos que possuem valor para a organização.

Incidente de Segurança – Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores, bem como toda situação em que uma entidade de informação está sob risco.

Integridade: capacidade de garantir que a informação esteja mantida em seu estado original, conforme foi concebida, a fim de protegê-la contra alterações indevidas, intencionais ou acidentais na guarda ou transmissão.

Lei Geral de Proteção de Dados Pessoais (LGPD): Lei n.º 13.709/2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da Lei (arts. 1º e 17, LGPD).

Mesa Limpa: Política que ajuda a prevenir o acesso não autorizado a informações sensíveis e a proteger os dados da organização.

5. Descrição das Regras Gerais

5.1. Geral

Os prestadores de serviços, fornecedores e/ou parceiros devem cumprir com todos os requisitos das legislações aplicáveis, e devem comprometer-se a seguir integralmente os itens a seguir:

- Assegurar a confidencialidade, integridade e disponibilidade das informações da Empresa, mediante utilização de mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- Assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Empresa, estando sujeitos à monitoração, rastreabilidade e auditoria;
- Assegurar a participação do quadro de pessoal da organização na Conscientização em Segurança da Informação;
- Assegurar a existência de processos para continuidade de negócios e gestão de incidentes de segurança para proteção, detecção, resposta e recuperação contra ataques cibernéticos;
- Garantir o cumprimento desta Política, Procedimentos e Padrões de Segurança da Informação e Privacidade da Empresa;
- Garantir que todos os incidentes de segurança da informação e/ou suspeitas de fraquezas serão reportados e tratados;
- Identificar os riscos de segurança da informação, que permanentemente serão avaliados, controlados e se possível reduzidos;
- Atender às leis que regulamentam as atividades da Empresa e seu mercado de atuação;
- Assegurar a existência de um programa anual de treinamento e conscientização em Segurança da Informação para todos os seus colaboradores.
- Prestadores de serviço/fornecedores devem passar por processo de qualificação de Segurança da Informação na pré-contratação ou contratação;

- Em caso de subcontratação pelo fornecedor e/ou prestador de serviço, este deverá garantir que a empresa subcontratada siga todos os requisitos de segurança da informação estabelecidos neste documento e nas legislações aplicáveis.

5.2. Responsabilidades específicas

5.2.1. Conscientização Sobre Segurança da Informação

A educação em segurança da informação deve ser um processo contínuo e praticado regularmente a fim de reduzir riscos. Todos os colaboradores do fornecedor e/ou do prestador de serviço que tenham acesso aos sistemas de informação devem anualmente participar de um programa de conscientização em segurança da informação.

5.2.2. Acordos de confidencialidade

Contratos de não-divulgação firmados pelos colaboradores e fornecedores/prestadores de serviço devem permanecer em vigor após a rescisão ou mudança na relação trabalhista.

5.2.1. Para todos os fins, serão consideradas informações confidenciais Informações Confidenciais (i) toda e qualquer informação relativa ao negócio da Contratante, bem como qualquer informação que seja revelada, fornecida, comunicada ou adquirida (verbalmente, por escrito, em forma eletrônica, textos, desenhos, fotografias, gráficos, projetos, plantas ou qualquer outra forma) pela Contratada na pessoa de seus sócios, administradores, diretores, empregados ou prepostos ou subcontratados; e (ii) qualquer segredo de negócio ou know-how, documento, croqui, desenho, fita de vídeo, reproduções, traduções, tabelas, gráficos, documentos financeiros, demonstrações financeiras, documentos contábeis, relatórios de auditoria, fórmulas, estudos, pareceres, métodos de elaboração, métodos analíticos, pesquisas, banco de dados, dados técnicos, dados operacionais, dados de engenharia, especificações técnicas, especificações de equipamentos, requerimentos escritos e qualquer outra forma de comunicação ou documentação da Contratante, escrita ou não (através de meios audiovisuais, mídia eletrônica ou qualquer outra forma), relacionados às informações supra mencionadas.

5.2.3. Classificação da Informação

Os dados devem ser tratados com base nas exigências de confidencialidade, integridade e disponibilidade das informações

5.2.4. Tratamento de Mídia

O fornecedor e/ou prestador de serviços deverá estabelecer um procedimento seguro para o tratamento das mídias (discos rígidos internos/externos, drives de memória etc.), considerando o descarte de forma segura, ou então a completa migração para o ambiente da Ipiranga, com a devida expurgação de sua propriedade exclusiva, a fim de prevenir a divulgação não autorizada de dados. Após a expurgação dos dados o fornecedor e/ou

prestador devem apresentar um laudo sobre o processo de expurgo, emitido por uma empresa especializada.

Caso seja impossível expurgar os dados, o fornecedor e/ou prestador de serviços devem garantir a proteção de todos os dados contra acesso não autorizado e/ou vazamentos.

5.2.5. Controle de Acesso

O acesso aos ativos deve ser gerenciado pelo proprietário dos ativos. Em particular, a norma de controle de acesso deve ser estabelecidas, documentada e revisada periodicamente, de forma a refletir a realidade de acessos pertinente.

O acesso aos dados, sistemas e aplicativos deve ser controlado por um procedimento seguro de autenticação.

Os processos de gestão de acesso de usuário devem ser definidos e formalizados, incluindo as etapas de provisionamento, alteração e exclusão. O acesso de usuário deve ser atribuído conforme necessário.

O processo deve garantir a responsabilização pelas ações de gestão de acesso de usuário. Revisões formais de direitos de acesso de usuário devem ser realizadas periodicamente, dependendo da criticidade do ativo, semestralmente, a fim de identificar qualquer acesso não autorizado e garantir a devida segregação de atribuições.

5.2.6. Política mesa e tela limpa

Deve ser estabelecida uma política de mesa e tela limpa nas instalações de processamento de informações, levando em conta as classificações de informação, a disponibilidade e integridade das informações, as exigências legais e contratuais e os riscos presentes nas circunstâncias concretas.

5.2.7. Segurança de Serviços de Rede

Cada serviço de rede, seja local ou terceirizado, deve incluir mecanismos de segurança (proteção, detecção e reação) adaptados à sensibilidade dos dados sendo transmitidos. Esses mecanismos de segurança devem ser implementados na rede ou diretamente nos sistemas, aplicativos, estações de trabalho e/ou banco de dados.

Todas as transferências de dados devem ser realizadas por ferramentas explicitamente validadas por equipe tecnicamente qualificada.

5.2.8. Trabalho Remoto

Deve ser estabelecido uma política de trabalho remoto, visando assegurar a confidencialidade, a integridade e a disponibilidade das informações tratadas fora do ambiente de trabalho.

5.2.9. Backup de Informações e Sistemas

Os [Procedimentos de Backup e Restore](#) são provenientes do Grupo Ultra. Esses procedimentos devem ser definidos para os dados, softwares e sistemas que tratam informações.

5.2.10. Relações com Terceiros

Os serviços entregues por terceiros devem seguir as diretrizes estabelecidas nesta política, sendo de total responsabilidade do fornecedor de serviços a garantia pelo cumprimento dos serviços e de todas as obrigações contratuais e legais.

5.2.11. Aquisição, Desenvolvimento e Manutenção de Sistemas

Todos os fornecedores de softwares, desenvolvimento ou manutenção de sistemas, sempre iniciar um novo projeto de TI ou mudança substancial em sistema de informação existente, recomendamos que os itens obrigatórios de segurança sejam documentados.

5.2.12. Gestão de Incidentes

Os incidentes de Segurança da Informação devem ser identificados e gerenciados por processos consistentes, disciplinados e compartilhados.

Assim que identificados, o mais rápido possível, todos os incidentes de segurança devem ser notificados e comunicados a área de Segurança da Informação da Ipiranga.

O fornecedor deverá ter um plano de emergência para a gestão de continuidade dos serviços, incluindo aspectos de segurança da informação, com o objetivo de garantir a disponibilidade dos recursos em caso de incidente de Segurança da Informação. O plano de emergência deve ser previamente aprovado pela Ipiranga.

A equipe responsável deve investigar a causa raiz do incidente a fim de mitigar impactos futuros.

5.3. Observância de Leis e Normas

As atividades da Empresa devem garantir a observância das obrigações contratuais para assegurar que as devidas exigências de segurança sejam levadas em conta em seus processos.

Ao Terceiro que trata dados pessoais, a este deve garantir que os dados pessoais sejam gerenciados de acordo com a Lei 13.709 de 14 de agosto de 2019 – Lei Geral de Proteção de Dados Pessoais, quando nenhuma outra orientação for passada.

As atividades do fornecedor, prestador de serviços e parceiros devem garantir a observância das obrigações estatutárias e regulatórias para assegurar que as devidas exigências de segurança sejam levadas em conta em seus processos. Todas as exigências legais, estatutárias e regulatórias relevantes devem ser explicitamente definidas e documentadas.

5.4. Violações

Qualquer violação das diretrizes constantes nesta política constitui-se em incidentes de segurança da informação e será devidamente registrado e analisado pelo Comitê de Segurança da Informação da Ipiranga.

Após análise do Comitê de Segurança, serão deliberadas medidas disciplinares ao fornecedor, que podem incluir:

- Advertência formal ou informal;
- Cancelamento do contrato de prestação de serviço;
- Multas previstas em contrato;
- Ações judiciais ou abertura de boletim de ocorrência.

5.5. Adesão e Atualização da Política

Ao aderir a presente política o fornecedor concorda que este documento poderá ser atualizado a qualquer momento pela Ipiranga, devendo o fornecedor se adequar a eventuais alterações no prazo estipulado pela Ipiranga.

Atualizado pela última vez em 13 de novembro de 2025.