1. OBJETIVO

Definir diretrizes de Segurança da Informação para que os prestadores de serviço do Grupo Fasitec adotem práticas seguras, visando proteger as informações da empresa, atender aos requisitos de confidencialidade, integridade e disponibilidade, prevenir incidentes e responsabilidades legais, mitigar riscos ao negócio, controlar acessos e transferências de dados, além de promover a conscientização sobre o uso adequado e a classificação da informação.

2. DEFINIÇÕES

- **SGI:** Sistema de Gestão Integrado
- **Grupo Fasitec:** Conjunto de produtos e serviços desenvolvidos e oferecidos pela Fasitec, englobando, os sistemas SICON e SiconCard.
- **SGSI:** Sistema de Gestão de Segurança da Informação
- **CID:** Confidencialidade, disponibilidade e integridade.
- **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.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **CPD:** Centro de Processamento de Dados. É uma estrutura física e/ou lógica onde são concentrados os recursos necessários para o processamento e armazenamento de informações em uma organização.

3. RESPONSABILIDADES

Usuários da informação

- Ler, compreender e cumprir integralmente os termos da Política Corporativa de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Encaminhar para o CSI quaisquer dúvidas sobre este documento e/ou qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais;
- Cumprir esta política, sob pena de incorrer nas sanções ou punições disciplinares e legais cabíveis;
- Preservar a CID das informações de que fazem uso.

Gestores da informação (cargos de liderança)

- Apoiar o Comitê de Segurança da Informação em suas decisões;
- Identificar e avaliar as ameaças à SI, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações e tomar ações cabíveis quando isso não ocorrer;
- Proteger, no nível físico e lógico, os ativos de informação e de processamento do Grupo Fasitec relacionados com a sua área de atuação;
- Solicitar ao CSI apoio para restringir acesso de prestadores de serviço, quando necessário, aos ativos de informação.

Comitê de Segurança da Informação

- Analisar, revisar e propor a aprovação junto à Diretoria das políticas e normas relacionadas à segurança da informação;
- Garantir a disponibilidade dos recursos necessários para uma efetiva gestão da Segurança da Informação;
- Garantir que as atividades de Segurança da Informação sejam executadas em conformidade com esta política;
- Realizar a gestão dos incidentes de SI, garantindo tratamento adequado;
- Promover a divulgação da PCSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do Grupo Fasitec;

- Avaliar a eficácia e a adequação desta política, a quantidade de incidentes relacionados ao acesso não autorizado das informações;
- Validar a eficácia e revisar o PCN, se necessário, toda vez que for ativado;
- Atualizar e manter listagem com as autoridades relevantes às atividades do SGSI.

4. APLICAÇÃO

Esta política se aplica a todos os locais de trabalho, todas as instalações e todos os equipamentos do escopo do SGI, além de todos os usuários que utilizam a informação da empresa.

5. EXECUÇÃO

5.1. Uso aceitável dos ativos de informação

Os ativos da informação do SGSI do Grupo Fasitec, bem como suas características, localização e backup estão descritos no DO-003SGI - Inventário de Ativos da Informação do Grupo Fasitec.

As diretrizes para o uso de equipamentos concedidos aos prestadores de serviço estão detalhadas no documento DO-013/INFRA – TERMO DE RESPONSABILIDADE DE USO DE EQUIPAMENTOS, assinado pelos usuários, e complementadas pelos pontos descritos a seguir:

- Os equipamentos fornecidos pela Fasitec destinam-se exclusivamente ao desempenho de atividades profissionais, sendo proibido seu uso para fins pessoais.
- A manutenção ou qualquer alteração nos equipamentos é de responsabilidade da equipe de Infraestrutura; os demais usuários não estão autorizados a realizar intervenções.
- Os equipamentos devem ser utilizados com zelo, visando sua preservação e funcionamento adequado.
- Computadores devem ser desligados ao final do expediente ou em ausências prolongadas, salvo justificativas operacionais.
- Os dispositivos possuem mecanismos de bloqueio automático para reforçar a política de mesa e tela limpas.

- Ao término da relação de prestação de serviço, os equipamentos devem ser devolvidos em condições adequadas de conservação.
- Danos causados por mau uso ou negligência serão analisados e poderão resultar em responsabilização do usuário.
- É proibida a conexão de equipamentos particulares à rede da Fasitec (cabeada ou sem fio) sem autorização da equipe de Infraestrutura.

5.2. Armazenamento em Nuvem

A Fasitec disponibiliza espaço para armazenamento remoto de arquivos em nuvem, por meio da plataforma oficial SharePoint.

É proibido o uso de qualquer outra solução de armazenamento em nuvem que não tenha sido oficialmente adotada e homologada pela equipe de Infraestrutura da Fasitec.

5.3. Equipamentos de Impressão

O uso de equipamentos de impressão e fotocópias deve ser restrito à impressão/reprodução de documentos que sejam de interesse da Fasitec ou que estejam diretamente relacionados ao desempenho das atividades profissionais do usuário.
Documentos contendo informações restritas e confidenciais devem ser removidos imediatamente de impressoras, scanners e copiadoras, e armazenados de forma segura.
O reaproveitamento de páginas já impressas, contendo informações classificadas como internas, restritas ou confidenciais, é proibido, devendo elas serem descartadas de acordo com o item 5.15 deste documento.

5.4. Segurança Física

O usuário deve observar as seguintes disposições específicas quanto à segurança física:

- A porta principal possui controle de acesso, liberado por meio de leitura digital, ou liberação de entrada realizada por prestador de serviço autorizado.
- O acesso de pessoas externas às dependências da Fasitec só será permitido após o preenchimento do anexo Cadastro de Visitantes, sob responsabilidade do prestador

de serviço alocado na recepção. Caso o visitante tenha acesso a informações restritas da Fasitec, deverá ser acompanhado de um responsável interno.

- Em áreas sensíveis, como o CPD, o acesso de prestador de serviços e terceiros só será permitido com autorização prévia.
- Pessoas externas devem sempre estar acompanhadas nas instalações da Fasitec, inclusive durante manutenções prediais.
- A Fasitec se reserva o direito de monitorar seus ambientes físicos, utilizando sistema de circuito fechado de televisão (CFTV) nas áreas comuns. As imagens são armazenadas e protegidas contra manipulação indevida.
- Quando um prestador de serviço não estiver em seu local de trabalho, todos os documentos em papel e mídias classificadas como confidenciais ou restritas devem ser removidos de sua mesa.

As instalações de processamento de informações da Fasitec serão mantidas em áreas seguras, com perímetro fisicamente isolado para proteger contra acessos não autorizados, danos e interferências de origem humana ou natural.

5.5. Controle de Acesso Lógico

A Fasitec fornece acesso a redes e sistemas (internos e externos) para o desempenho exclusivo das atividades profissionais de seus usuários.

Cadastros em sites externos devem ser vinculados ao nome e e-mail do prestador de serviço, exceto quando o site exigir uso por CNPJ — nesse caso, o gestor deve gerenciar as credenciais.

O Financeiro é responsável por gerenciar acessos a sites bancários em caso de movimentações de pessoal.

A Fasitec pode auditar, monitorar e acessar informações trafegadas e equipamentos usados, por se tratar de ativos corporativos.

5.6. Acesso a Redes e Serviço

Documentos e projetos devem ser armazenados em locais seguros e homologados (como pastas de rede, sistemas corporativos ou Share Point), com proteção técnica, administrativa e física garantida pela Fasitec.

Acesso a pastas e arquivos é controlado por grupos, com base nas funções dos usuários.

É proibido compartilhar arquivos diretamente entre estações de trabalho; devem ser usados os servidores da empresa ou e-mail corporativo para rastreabilidade.

A instalação de softwares utilitários sem justificativa e autorização da equipe de Infraestrutura não é permitida.

5.7. Uso da Internet

O acesso à Internet deve ser feito exclusivamente pela rede local da Fasitec, com infraestrutura e proteção adequada via firewall.

A equipe de Infraestrutura pode bloquear sites para grupos ou usuários; em caso de necessidade justificada, deve-se abrir um chamado no GLPI para análise e possível liberação.

Informações obtidas em sites não confiáveis só devem ser usadas após verificação de sua autenticidade.

O usuário é responsável pelas consequências de uso inadequado ou não autorizado da Internet.

5.8. Troca de Mensagens

Mensagens devem conter apenas informações verdadeiras e não podem ter conteúdo ofensivo, impróprio, ilegal ou inaceitável.

É proibido o envio de spam ou mensagens não solicitadas a pessoas sem vínculo comercial.

E-mails suspeitos ou que solicitem informações confidenciais devem ser reportados ao CSI.

Mensagens com dados relevantes para os negócios devem ser salvas.

Publicações em redes sociais ou fóruns devem deixar claro que não representam a opinião oficial da Fasitec.

5.9. Utilização de senha (autenticação secreta)

Senhas são de uso pessoal e não devem ser compartilhadas com ninguém, nem com superiores ou administradores.
O uso do TeamPass é recomendado para cadastro e gerenciamento de senhas. É a única ferramenta homologada pela equipe de Infraestrutura.
Senhas não devem ser transmitidas por nenhum meio a pessoas não autorizadas.
Devem ser alteradas imediatamente em caso de suspeita de comprometimento, sendo necessário reportar o incidente.

Recomenda-se que as senhas sigam os critérios abaixo:

- Mínimo de 8 caracteres;
- Pelo menos um número;
- Letras maiúsculas e minúsculas;
- Um caractere especial;
- Não usar palavras de dicionário ou informações pessoais.

Senhas pessoais não devem ser reutilizadas em contextos profissionais.
É recomendado trocar a senha no primeiro acesso ao sistema.

Sistemas internos do Grupo Fasitec (como Sicon e Sicon Card) exigem senhas conforme os critérios de segurança definidos e só permitem o uso após validação.
Para sistemas externos ou de terceiros, o Grupo Fasitec não define os critérios, mas incentiva fortemente o uso do TeamPass, que exige senhas classificadas como muito fortes.

5.10. Transferência de Informações

A troca de informações pode ocorrer por e-mail, downloads, sistemas, telefone, SMS, mensagens instantâneas, mídias portáteis, fóruns e redes sociais.

A transferência de informações no relacionamento com partes externas — como fornecedores de serviços, clientes e empresas de manutenção de hardware e software — deve seguir diretrizes:

- Deve haver contrato assinado (em papel ou eletrônico) antes de qualquer troca de informações restritas e de alto impacto a operação.

- Trocas de informações com terceiros devem manter a confidencialidade, exceto no caso de dados públicos.
- Informações de propostas de fornecedores não devem ser compartilhadas entre concorrentes durante cotações.

Contato com autoridades e grupos especiais

- O Grupo Fasitec mantém contato com autoridades legais (polícia, bombeiros, reguladores, etc.) para responder rapidamente a incidentes de segurança.
- O CSI também mantém relações com fóruns e grupos de discussão para acompanhar boas práticas, vulnerabilidades e alertas.
- A lista de contatos e orientações está no anexo **LISTA DE CONTATOS COM AUTORIDADES E GRUPOS ESPECIAIS**
- e deve ser usada por um membro do CSI quando necessário.

Uso de mídias removíveis

- É proibido armazenar informações corporativas em mídias externas pessoais (pendrives, HDs, celulares, etc.).
- Portas USB dos computadores são bloqueadas por padrão e só podem ser liberadas com autorização do CSI, após análise da necessidade.

5.11. Mesa e Tela Limpa

Todas as informações não públicas devem ser protegidas contra acesso não autorizado, independentemente do meio em que estejam armazenadas.

Mesa limpa:

- Evite deixar informações visíveis sobre a mesa.
- Proteja documentos quando pessoas não autorizadas se aproximarem.
- Guarde materiais ao final do expediente (documentos, cadernos, mídias, etc.).

Tela limpa:

- Não cole post-its com informações sensíveis na tela do computador.

- Bloqueie a tela ao se afastar do computador ou dispositivo móvel.
- Em reuniões, evite exibir documentos sensíveis na área de trabalho ou pastas visíveis.
- Desligue o computador ao final do expediente para prevenir acessos não autorizados.

5.12. Acesso Privilegiado

Exemplos de acessos privilegiados são:

- Acesso de administrador de máquinas ou redes;
- Acesso ao código-fonte dos sistemas próprios;
- Acesso a servidores e banco de dados;
- Acesso físico ao CPD/Data Center;
- Portas USB desbloqueadas;
- Acesso às imagens das câmeras internas do Grupo Fasitec.

Outros acessos podem ser classificados como privilegiados pelo CSI em futuras revisões.
Os acessos privilegiados são registrados e revisados periodicamente na planilha DO-002SGI - Controle de Acessos Privilegiados.

5.13. Inteligência de Ameaças

O Grupo Fasitec adota uma abordagem proativa para identificar, monitorar e mitigar ameaças cibernéticas, com as seguintes práticas:

Antivírus nas máquinas

- Utilização do Kaspersky em todos os dispositivos;
- Atualizações regulares para garantir a detecção de malwares e novas ameaças.

Proteção dos servidores em nuvem

- Servidores protegidos por fornecedor certificado na ISO/IEC 27001;
- Utilização do Anti Dos, Waf , IPS para bloquear tentativas de acesso não autorizado, com monitoramento em tempo real de padrões maliciosos.

Participação em fóruns de segurança

- Envolvimento ativo em comunidades como OWASP.
- Compartilhamento de informações sobre ameaças e vulnerabilidades, e adoção das melhores práticas do setor.

5.14. Propriedade Intelectual

As informações geradas e armazenadas na empresa são ativos de sua propriedade e devem ser preservadas e protegidas contra uso ou divulgação indevidos, salvo as seguintes exceções:

- Se o contrário for afirmado no copyright do documento;
- Se as informações tiverem sido previamente publicadas em meios de comunicação que podem ser acessados por qualquer público: jornais, revistas, redes sociais, entre outros.

5.15. Classificação da Informação

O Grupo Fasitec define critérios específicos para o manuseio de informações com base em sua classificação: pública, interna, restrita e confidencial. Para cada tipo de informação, são estabelecidas orientações quanto a:

- Autorização de acesso: quem pode acessar a informação e sob quais condições.
- Divulgação: em quais casos e para quem a informação pode ser compartilhada.
- Armazenamento seguro, incluindo: Rede interna; Documentos físicos; Mídias removíveis; SharePoint.
- Transporte: medidas para garantir a proteção da informação em trânsito.
- Descarte: métodos adequados para eliminar informações com segurança.
- Transferência: cuidados e permissões para envio de dados a outras partes.

Essas diretrizes estão organizadas em uma tabela, acessível por link divulgado pelo CSI, e são fundamentais para que todos os usuários mantenham um nível adequado de proteção das informações sob sua responsabilidade.

5.16. Rotulagem da Informação

Quando a rotulagem direta não for possível (por exemplo, devido ao tipo ou origem do documento), o usuário ou gestor da informação deve determinar a classificação e aplicar as medidas de proteção e armazenamento previstas na política.

Exemplos de documentos que não podem ser rotulados:

- Normas ISO;
- Documentos emitidos por órgãos governamentais;
- Mídias incompatíveis com rotulagem (ex: vídeos, áudios);
- Documentos antigos (anteriores à política) que não podem ser modificados sem comprometer sua integridade.

Quando possível, os documentos devem ser rotulados conforme sua classificação (pública, interna, restrita, confidencial), seguindo estas orientações:

- Documentos em papel: rodapé de todas as páginas, texto preferencialmente centralizado;
- Papel arquivado em pastas/envelopes: rotulagem na capa ou envelope, com proteção adequada durante transporte;
- Planilhas: parte superior (centralizada, à direita ou à esquerda), conforme layout;
- Planilhas com várias abas: rotulagem na parte superior da primeira aba;
- Apresentações: indicação logo no início da apresentação;
- E-mails: classificação padrão é “restrita”, e um aviso padrão é adicionado logo abaixo da assinatura;
- Informações orais: a classificação deve ser informada verbalmente ou por escrito antes da comunicação do conteúdo.

Nota: informações classificadas como públicas não exigem rotulagem.

5.17. Comunicação de Incidentes

O Grupo Fasitec conta com o apoio de todos os seus prestadores de serviços para a melhoria contínua do seu Sistema de Gestão de Segurança da Informação (SGSI). Além de seguir os requisitos estabelecidos nesta e em outras políticas, espera-se que os prestadores de serviços comuniquem imediatamente qualquer vulnerabilidade ou incidente ao Comitê de Segurança da Informação (CSI), para que providências possam ser tomadas de forma ágil e eficaz.

São exemplos de incidentes que devem ser comunicados (sem se limitar aos listados):

- Datas e horários incorretos em sistemas computacionais;
- Acessos não autorizados, tanto físicos quanto lógicos;
- Computadores sem antivírus ativo ou atualizado;
- Indisponibilidade de informações necessárias para o trabalho;
- Informações corrompidas ou não íntegras;
- Informações de classificação não pública acessíveis ou expostas a pessoas não autorizadas.

O contato com o CSI pode ser feito pessoalmente, ou por meio do endereço de e-mail oficial: segurancainformacao@grupofasitec.com.br

6. SANÇÕES OU PUNIÇÕES:

Infrações e/ou desvios conducentes às diretrizes constantes no presente documento poderão incorrer na aplicação de medidas disciplinares, ou até mesmo instauração de processos judiciais cíveis e criminais, conforme as legislações pertinentes.

7. DOCUMENTOS

7.1. DO-003/SGSI - Inventário de Ativos da Informação
7.2. DO-002/SGSI - Controle de Acessos Privilegiados
7.3. DO-004/SGSI - Tabela de classificação da Informação
7.4. DO-0013/INFRA – TERMO DE RESPONSABILIDADE DE USO DE EQUIPAMENTOS

8. HISTÓRICO DAS ALTERAÇÕES

DATA	VERSÃO	ALTERAÇÕES
16/05/2025	01	Aprovação da política