Eco Cleaning

PSI: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ECO CLEANING

Bem-vindo à cartilha de segurança da informação da Eco Cleaning. A segurança da informação é fundamental para proteger os dados da empresa, dos nossos colaboradores e dos nossos clientes. Esta cartilha visa fornecer orientações claras e práticas para garantir a proteção das informações contra ameaças internas e externas.

Pilares da Segurança da Informação

Confidencialidade

O que é: Garantir que a informação seja acessada apenas por pessoas autorizadas.
Como garantir: Não compartilhe senhas, utilize criptografia para dados sensíveis e controle rigorosamente quem pode acessar as informações.

Integridade

O que é: Assegurar que a informação não seja alterada ou destruída de maneira não autorizada.
Como garantir: Use verificações regulares de integridade de dados, mantenha backups atualizados e controle de versão dos documentos.

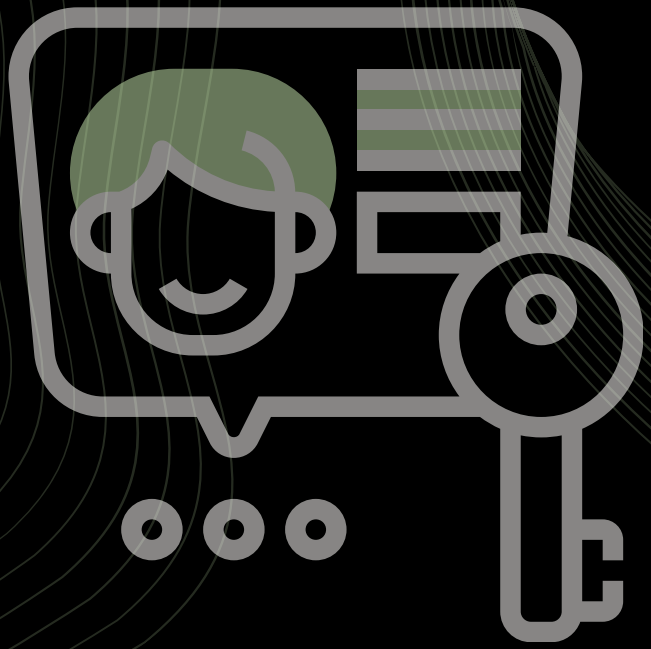
Disponibilidade

O que é: Garantir que a informação esteja disponível quando necessário.
Como garantir: Mantenha sistemas atualizados, implemente planos de recuperação de desastres e evite interrupções desnecessárias.

Eco Cleaning

Missão

Garantir a proteção e a confidencialidade das informações e dados da empresa e dos clientes, promovendo um ambiente seguro que permita a continuidade dos negócios e o crescimento sustentável da Eco Cleaning, alinhado com os princípios de limpeza ecológica e responsabilidade ambiental.



Visão

Ser reconhecida como líder em segurança da informação no setor de limpeza ecológica, adotando práticas inovadoras e sustentáveis que protejam os ativos digitais da empresa, assegurando a confiança dos clientes e a integridade dos serviços prestados.

Classificação da Informação

Pública: Informações que podem ser divulgadas sem restrições.

Interna: Informações que são restritas aos funcionários da empresa.

Confidencial: Informações sensíveis que requerem proteção contra acesso não autorizado e são acessíveis somente por pessoas *autorizadas.*

Secreta: Informações altamente sensíveis, críticas para a operação da empresa, acessíveis apenas por indivíduos específicos com permissões especiais.

Proteção de Dados dos Clientes

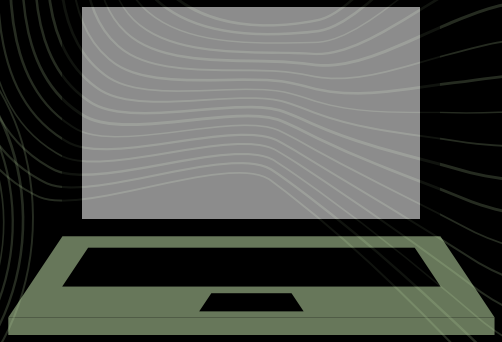
Desafio: Garantir a confidencialidade e integridade dos dados dos clientes, incluindo informações pessoais e detalhes de contratos de serviço.

Estratégia: Implementar criptografia de ponta a ponta, políticas de acesso restrito, e treinamentos regulares para funcionários sobre a importância da proteção de dados.

Conformidade com Regulamentações

Desafio: Cumprir com todas as legislações e regulamentações relevantes, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

Estratégia: Manter um programa de conformidade atualizado que inclui auditorias regulares, análise de impacto de proteção de dados (DPIA) e a nomeação de um Encarregado de Proteção de Dados (DPO).



Prevenção de Ameaças Cibernéticas

Desafio: Mitigar riscos associados a ataques cibernéticos, como malware, phishing e ransomware.

Estratégia: Implementar soluções robustas de segurança de rede e endpoint, realizar testes de penetração periódicos, e estabelecer um plano de resposta a incidentes para minimizar danos em caso de violações.

Eco Cleaning

Segurança na Cadeia de Suprimentos

Desafio: Assegurar que todos os fornecedores e parceiros cumpram com os padrões de segurança da informação da Eco Cleaning.
Estratégia: Desenvolver políticas de segurança para terceiros, exigir contratos que incluam cláusulas de segurança e realizar avaliações regulares de riscos e conformidade dos fornecedores.

Continuidade dos Negócios e Recuperação de Desastres

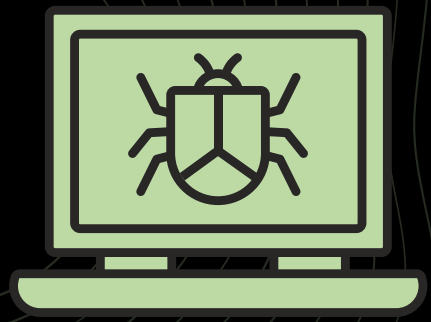
Desafio: Garantir que a empresa possa continuar operando mesmo diante de desastres naturais, falhas de sistema ou ataques cibernéticos.
Estratégia: Implementar e testar regularmente um plano de continuidade de negócios (BCP) e um plano de recuperação de desastres (DRP), incluindo backups regulares e redundância de dados.

Eco Cleaning

Práticas de Segurança

Senhas

Criação de Senhas: Utilize senhas fortes com, pelo menos, 8 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais.
Alteração Regular: Altere suas senhas regularmente, pelo menos a cada 90 dias.
Confidencialidade: Nunca compartilhe suas senhas com ninguém.



E-mails

Cuidado com Anexos e Links: Não abra anexos ou clique em links de e-mails de remetentes desconhecidos.
Phishing: Esteja atento a e-mails que solicitam informações pessoais ou confidenciais.

Eco Cleaning

Dispositivos

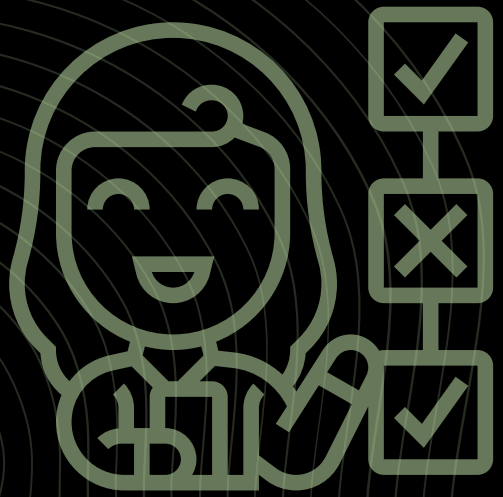
Uso Seguro de Dispositivos: Mantenha dispositivos de trabalho seguros, não os deixe desacompanhados e use senhas de bloqueio.

Atualizações: Mantenha todos os softwares e sistemas operacionais atualizados com as últimas versões e patches de segurança.

Acesso Remoto

VPN: Utilize a VPN da empresa para acessar recursos internos de fora do escritório.

Ambiente Seguro: Certifique-se de que o ambiente de trabalho remoto é seguro e privado.



Dados e Documentos

Backup Regular: Realize backups regulares dos dados importantes e armazene-os em local seguro.

Compartilhamento de Informações: Compartilhe informações sensíveis somente por meios seguros e com pessoas autorizadas.

Uso da Internet

Sites Confiáveis: Acesse apenas sites confiáveis e evite downloads de fontes não verificadas.

Redes Sociais: Evite compartilhar informações corporativas em redes sociais.

Penalidades e Infrações

Na Eco Cleaning, levamos a segurança das informações muito a sério. As penalidades para violações incluem:

Advertência Verbal: Para infrações menores ou incidentes acidentais.

Advertência Escrita: Para reincidências ou infrações mais sérias.

Suspensão: Para infrações graves ou contínuas.

Demissão: Para violações severas ou repetidas que coloquem a empresa em risco significativo. Todas as penalidades são aplicadas de acordo com a gravidade da infração e o histórico do colaborador.

Papel dos Colaboradores

Cada colaborador tem um papel fundamental na proteção das informações da Eco Cleaning:
Cumprimento das Políticas: Seguir rigorosamente as políticas e procedimentos de segurança da informação.
Educação e Treinamento: Participar ativamente dos programas de treinamento oferecidos pela empresa.
Relatório de Incidentes: Reportar imediatamente qualquer suspeita de violação de segurança ou comportamento inadequado.
Confidencialidade: Manter a confidencialidade das informações e evitar a divulgação não autorizada.

Conclusão

A segurança da informação é uma responsabilidade compartilhada. Ao seguir as diretrizes desta cartilha, todos na Eco Cleaning contribuem para um ambiente mais seguro e protegido. Agradecemos sua cooperação e empenho em manter a segurança da informação em nossa empresa.

Eco Cleaning

Eco Cleaning

Para mais informações acesse:

Eco Cleaning - Limpeza com Responsabilidade e Segurança