

# **Política de Segurança da Informação Eco Cleaning**

## **1. Introdução**

A segurança da informação é essencial para garantir a confidencialidade, integridade e disponibilidade dos dados da empresa Eco Cleaning. Esta política estabelece diretrizes e procedimentos para proteger as informações contra ameaças internas e externas.

## **2. Missão**

Nossa missão é criar soluções de limpeza eficazes e sustentáveis que respeitem e preservem o meio ambiente. Comprometemo-nos a desenvolver produtos inovadores, seguros e biodegradáveis, que minimizem o impacto ambiental e promovam um futuro mais saudável para o nosso planeta e para as próximas gerações. Valorizamos a transparência, a ética e a responsabilidade em todas as etapas de nossa cadeia produtiva, desde a seleção de matérias-primas até a entrega final aos nossos clientes. Trabalhamos continuamente para educar e inspirar a sociedade a adotar práticas de limpeza mais verdes e conscientes, contribuindo para um mundo mais limpo e sustentável.

## **3. Visão**

Ser reconhecida como a líder global em soluções de limpeza ecológicas, promovendo a transformação do mercado de produtos de limpeza com inovação, sustentabilidade e ética. Aspiramos a criar um mundo onde todas as práticas de limpeza sejam seguras para o meio ambiente, contribuindo para um planeta mais limpo, saudável e sustentável. Nosso objetivo é inspirar outras empresas e consumidores a adotarem alternativas ecológicas, estabelecendo novos padrões de responsabilidade ambiental e promovendo um futuro em que a harmonia entre a atividade humana e a natureza seja uma realidade.

## **4. Questões estratégicas**

A respeito de questões estratégicas temos em vista a proteção de dados sensíveis para proteger informações confidenciais, como fórmulas de produtos, dados de fornecedores e informações financeiras. Para garantir a proteção dos dados implementamos diversos sistemas robustos de criptografia para proteger dados em trânsito e em repouso, além de políticas rigorosas de acesso baseado em permissões. Além disso, a empresa Eco Cleaning está em conformidade com as regulamentações de proteção de dados como a LGPD (Lei Geral de Proteção de Dados) no Brasil e o GDPR (General Data Protection Regulation) na Europa. Para isso, desenvolvemos um programa de conformidade que inclua auditorias

regulares, treinamentos aos funcionários e monitoramento contínuo. Para mitigar riscos associados a ameaças internas, implementamos uma política de segurança rigorosa, incluindo controle de acesso, monitoramento de atividades e programas de conscientização para educar os funcionários sobre a importância da segurança da informação. Para garantir a segurança dos ambientes de produção industrial e dispositivos de internet das coisas usados na produção contra ataques cibernéticos, segmentamos redes de TI e OT (tecnologia operacional), adotamos a utilização de firewalls e monitoramento contínuo as atividades das redes de manufatura para detectar e responder rapidamente a ameaças.

## **5. Diretrizes**

### **5.1 Confidencialidade**

Acesso Restrito: As informações devem ser acessadas somente por indivíduos autorizados com necessidade legítima de uso.

Criptografia: Utilizar criptografia para proteger dados sensíveis em trânsito e em repouso.

### **5.2 Integridade**

Controle de Alterações: Implementar mecanismos de controle de versões para documentos críticos.

Verificação Regular: Realizar auditorias e verificações periódicas para garantir que os dados não foram alterados de maneira não autorizada.

### **5.3 Disponibilidade**

Backup: Manter backups regulares de dados críticos e assegurar que eles possam ser restaurados rapidamente.

Planos de Contingência: Desenvolver e manter um plano de recuperação de desastres para garantir continuidade operacional.

## **6. Papeis e Responsabilidades**

### **6.1 Diretor de TI**

Desenvolver, implementar e manter a política de segurança da informação.

Realizar auditorias periódicas e responder a incidentes de segurança.

### **6.2 Equipe de TI**

Implementar controles de segurança, realizar backups regulares e monitorar a rede para detectar atividades suspeitas.

Fornecer suporte técnico e treinamento aos funcionários sobre práticas de segurança.

### **6.3 Colaboradores**

Cumprir as diretrizes de segurança estabelecidas.

Realizar todos os cursos obrigatórios dentro do prazo informado.

Reportar imediatamente qualquer atividade suspeita ou incidente de segurança ao Diretor de TI.

## **7. 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.

## **8. Procedimentos e Instruções Operacionais**

### **8.1 Controle de Acesso**

Utilizar autenticação multifator (MFA) para acessar sistemas críticos.

Revisar e atualizar regularmente as permissões de acesso dos usuários.

### **8.2 Manutenção de Sistemas**

Aplicar atualizações e patches de segurança assim que estiverem disponíveis.

Desativar contas de usuários imediatamente após a saída da empresa.

### **8.3 Gestão de Incidentes**

Estabelecer um plano de resposta a incidentes com etapas claras para identificação, contenção, erradicação, recuperação e comunicação de incidentes.

Realizar simulações de incidentes de segurança periodicamente para testar a eficácia do plano de resposta.

### **8.4 Treinamento e Conscientização**

Oferecer programas regulares de treinamento de segurança para todos os funcionários.

Implementar campanhas de conscientização sobre phishing, engenharia social e outras ameaças comuns.

## **8.5 Gestão de Backup**

Realizar backups completos dos dados críticos semanalmente e backups incrementais diariamente.

Testar a restauração de backups mensalmente para garantir a integridade e disponibilidade dos dados.

## **8.6 Manuseio de Informações Confidenciais**

Evitar a transmissão de informações confidenciais por e-mail sem criptografia.

Utilizar ferramentas de compartilhamento seguro para a transferência de arquivos sensíveis.

Esta política deve ser revisada anualmente e atualizada conforme necessário para garantir que continue alinhada com as melhores práticas de segurança da informação e com as necessidades da empresa da Eco Cleaning.

## **Glossário**

**Autenticação:** Processo de verificar a identidade de um usuário, sistema ou entidade antes de permitir o acesso aos recursos.

**Autenticação de Dois Fatores (2FA):** Método de autenticação que requer duas formas diferentes de verificação para acessar um sistema, geralmente algo que o usuário sabe (senha) e algo que o usuário possui (token de segurança).

**Autorização:** Processo de conceder ou negar permissões a usuários ou sistemas após a autenticação.

**Backup:** Cópia de segurança de dados importantes para recuperação em caso de perda de dados.

**Confidencialidade:** Garantia de que a informação é acessível somente a pessoas autorizadas.

**Criptografia:** Processo de codificação de informações para impedir acesso não autorizado.

**Disponibilidade:** Garantia de que a informação esteja acessível quando necessária.

**Engenharia Social:** Técnica utilizada por hackers para manipular indivíduos a fim de obter informações confidenciais ou acesso a sistemas protegidos.

**Integridade:** Garantia de que a informação não foi alterada ou destruída de maneira não autorizada.

**Incidente de Segurança:** Evento que compromete a confidencialidade, integridade ou disponibilidade de informações, sistemas ou serviços e que exige resposta imediata para mitigar danos.

**Malware:** Software malicioso projetado para causar danos a um computador, servidor ou rede, incluindo vírus, worms, trojans, spyware, entre outros.

**Patch:** Atualização de software projetada para corrigir vulnerabilidades de segurança ou problemas de funcionalidade em um sistema operacional ou aplicativo.

**Phishing:** Técnica de engenharia social utilizada para enganar usuários e obter informações confidenciais, como senhas e números de cartões de crédito, fingindo ser uma entidade confiável.

**Ransomware:** Tipo de malware que criptografa os dados de um sistema e exige um pagamento (geralmente em criptomoedas) para restaurar o acesso aos arquivos.

**Sniffing:** Técnica de monitoramento de tráfego de rede para capturar informações sensíveis, como senhas, através da análise de pacotes de dados.

**Token de Segurança:** Dispositivo físico ou aplicativo móvel que gera códigos de acesso temporários e únicos para autenticação de dois fatores.

**Vulnerabilidade:** Fraqueza ou falha em um sistema, rede ou aplicação que pode ser explorada por ameaças para comprometer a segurança e causar danos.

## **Anexo Procedimentos**

### **Procedimento para Configuração do Wi-Fi para funcionários**

**Objetivo:** Este procedimento visa orientar os funcionários da empresa Eco Cleaning sobre como configurar a conexão Wi-Fi em dispositivos da empresa, garantindo uma conexão segura e estável.

#### **1. Verificação Inicial**

1.1 Certifique-se de que o dispositivo está ligado.

1.2 Verifique se o dispositivo tem o adaptador Wi-Fi habilitado.

- Nos computadores, isso pode ser feito através das configurações de rede.
- Em dispositivos móveis, verifique nas configurações de Wi-Fi.

#### **2. Localização das Credenciais de Wi-Fi**

2.1 Obtenha o nome da rede (SSID) e a senha (Key) do Wi-Fi.

- Essas informações podem ser fornecidas pelo departamento de TI ou estarem disponíveis em um local seguro e autorizado na empresa.

#### **3. Conexão ao Wi-Fi no Windows**

3.1 Clique no ícone de rede na bandeja do sistema (geralmente no canto inferior direito).

3.2 Selecione a rede Wi-Fi da empresa (SSID) na lista de redes disponíveis.

3.3 Clique em "Conectar".

3.4 Digite a senha (Key) fornecida e clique em "Avançar".

3.5 Aguarde a conexão ser estabelecida.

- Certifique-se de marcar a opção "Conectar automaticamente" se desejar que o dispositivo se conecte à rede sempre que estiver disponível.

#### **4. Conexão ao Wi-Fi no macOS**

4.1 Clique no ícone de Wi-Fi na barra de menus (canto superior direito).

4.2 Selecione a rede Wi-Fi da empresa (SSID) na lista de redes disponíveis.

4.3 Digite a senha (Key) fornecida e clique em "Conectar".

4.4 Aguarde a conexão ser estabelecida.

## 5. Conexão ao Wi-Fi em Dispositivos Android

- 5.1 Abra o aplicativo "Configurações".
- 5.2 Toque em "Wi-Fi" ou "Conexões".
- 5.3 Certifique-se de que o Wi-Fi está ligado.
- 5.4 Selecione a rede Wi-Fi da empresa (SSID) na lista de redes disponíveis.
- 5.5 Digite a senha (Key) fornecida e toque em "Conectar".
- 5.6 Aguarde a conexão ser estabelecida.

## 6. Conexão ao Wi-Fi em Dispositivos iOS (iPhone/iPad)

- 6.1 Abra o aplicativo "Configurações".
- 6.2 Toque em "Wi-Fi".
- 6.3 Certifique-se de que o Wi-Fi está ligado.
- 6.4 Selecione a rede Wi-Fi da empresa (SSID) na lista de redes disponíveis.
- 6.5 Digite a senha (Key) fornecida e toque em "Conectar".
- 6.6 Aguarde a conexão ser estabelecida.

## 7. Verificação da Conexão

- 7.1 Após a conexão, abra um navegador de internet ou aplicativo que utilize a internet para verificar se a conexão está funcionando.
- 7.2 Se não conseguir se conectar, repita os passos anteriores ou entre em contato com o departamento de TI para assistência.

## 8. Segurança e Boas Práticas

- 8.1 Nunca compartilhe a senha do Wi-Fi da empresa com pessoas não autorizadas.
- 8.2 Desconecte-se da rede Wi-Fi da empresa quando não estiver em uso prolongado ou fora do horário de trabalho.
- 8.3 Informe qualquer atividade suspeita ou problemas de conexão ao departamento de TI imediatamente.

## 9. Suporte Técnico

- 9.1 Em caso de dificuldades, entre em contato com o departamento de TI através do [suporte@ecocleaning.com.br](mailto:suporte@ecocleaning.com.br).
- 9.2 Forneça detalhes do problema, incluindo quaisquer mensagens de erro e os passos já realizados.

## **Procedimento para Adicionar uma Máquina ao Active Directory (AD)**

Objetivo: Este procedimento visa orientar os funcionários sobre como adicionar uma máquina (computador) ao Active Directory (AD) da empresa, garantindo que a máquina seja integrada corretamente ao domínio da rede corporativa.

### 1. Verificação Inicial

- 1.1 Certifique-se de que você possui as credenciais de administrador de domínio.
- 1.2 Verifique se a máquina está conectada à rede corporativa (cabo Ethernet ou Wi-Fi).
- 1.3 Anote o nome da máquina que será adicionada ao AD para evitar duplicações e conflitos de nomes.

## 2. Configuração do Nome da Máquina

### 2.1 Acesse as configurações de sistema da máquina.

- No Windows, clique com o botão direito em "Este Computador" (ou "Meu Computador") e selecione "Propriedades".
- Em seguida, clique em "Configurações avançadas do sistema".

### 2.2 Clique na aba "Nome do Computador" e, em seguida, clique em "Alterar".

### 2.3 Digite o nome da máquina (certifique-se de seguir o padrão de nomenclatura da empresa, se houver).

### 2.4 Clique em "OK" e reinicie a máquina, se solicitado.

## 3. Adição ao Domínio

### 3.1 Após a reinicialização, acesse novamente as configurações do sistema (conforme o passo 2.1).

### 3.2 Clique na aba "Nome do Computador" e, em seguida, clique em "Alterar".

### 3.3 Selecione a opção "Domínio" e digite o nome do domínio da empresa (por exemplo, "empresa.local").

### 3.4 Clique em "OK".

## 4. Autenticação no Domínio

### 4.1 Uma janela pop-up solicitará as credenciais de administrador do domínio.

### 4.2 Digite o nome de usuário e a senha do administrador do domínio.

### 4.3 Clique em "OK" e aguarde a máquina ser adicionada ao domínio.

## 5. Confirmação e Reinicialização

### 5.1 Uma mensagem de boas-vindas ao domínio deve aparecer. Clique em "OK".

### 5.2 Reinicie a máquina para aplicar as alterações.

## 6. Verificação de Conectividade

### 6.1 Após a reinicialização, faça login na máquina usando uma conta de usuário do domínio para verificar a conectividade.

### 6.2 Acesse "Este Computador" (ou "Meu Computador") e verifique se as unidades de rede mapeadas e outros recursos do domínio estão acessíveis.

## 7. Configuração Adicional (Se Necessário)

### 7.1 Verifique se as políticas de grupo (GPOs) foram aplicadas corretamente.



- Isso pode ser feito executando o comando "gpupdate /force" no prompt de comando. 7.2 Instale qualquer software necessário que seja padronizado pela empresa, se ainda não estiver instalado.

## 8. Documentação

8.1 Documente o nome da máquina, o nome do usuário e a data em que a máquina foi adicionada ao domínio.

8.2 Envie essas informações ao departamento de TI para registro e manutenção de inventário.

## Procedimento para Uso do Outlook Corporativo

Objetivo: Este procedimento visa orientar os funcionários sobre como configurar e utilizar o Microsoft Outlook para gerenciar emails, compromissos, contatos e tarefas no ambiente corporativo.

### 1. Configuração Inicial do Outlook

#### 1.1 Instalação do Microsoft Outlook

- Verifique se o Microsoft Outlook está instalado no seu computador.
- Se não estiver instalado, entre em contato com o departamento de TI para realizar a instalação.

#### 1.2 Abrindo o Outlook pela Primeira Vez

- Clique no ícone do Outlook na área de trabalho ou no menu iniciar.
- Se esta for a primeira vez que está abrindo o Outlook, o assistente de configuração será iniciado automaticamente.

#### 1.3 Configurando a Conta de Email

- Na tela de boas-vindas do assistente, clique em "Próximo".
- Selecione "Configurar minha conta automaticamente" e clique em "Próximo".
- Digite seu endereço de email corporativo e clique em "Conectar".
- Digite sua senha de email quando solicitado e clique em "Conectar".

- Se for solicitado, digite seu nome de usuário e senha novamente e clique em "OK".
- Clique em "Concluir" para finalizar a configuração.

## 2. Navegação Básica no Outlook

### 2.1 Interface do Outlook

- Pannel de Navegação: Localizado à esquerda, permite acessar emails, calendário, contatos e tarefas.
- Lista de Mensagens: Mostra uma lista de emails na pasta selecionada.
- Pannel de Leitura: Exibe o conteúdo do email selecionado.

### 2.2 Enviando e Recebendo Emails

- Para enviar um novo email, clique em "Novo Email" na barra de ferramentas.
- Digite o endereço do destinatário no campo "Para", adicione um assunto no campo "Assunto" e escreva sua mensagem no corpo do email.
- Clique em "Enviar" para enviar a mensagem.
- Para verificar novos emails, clique em "Enviar/Receber" na barra de ferramentas.

### 2.3 Gerenciando Emails

- Para abrir um email, clique duas vezes sobre ele na lista de mensagens.
- Para responder a um email, clique em "Responder" ou "Responder a todos".
- Para encaminhar um email, clique em "Encaminhar".
- Para excluir um email, selecione o email e pressione "Delete" ou clique em "Excluir" na barra de ferramentas.
- Use pastas e categorias para organizar seus emails. Clique com o botão direito em um email e selecione "Mover" para mover para uma pasta ou "Classificar" para adicionar uma categoria.

## 3. Usando o Calendário

### 3.1 Acessando o Calendário

- Clique em "Calendário" no Pannel de Navegação.

### 3.2 Criando um Novo Compromisso

- Clique em "Novo Compromisso" na barra de ferramentas.
- Digite o assunto, local e detalhes do compromisso.
- Selecione a data e hora de início e término.
- Clique em "Salvar e Fechar" para adicionar o compromisso ao seu calendário.

### 3.3 Criando uma Reunião

- Clique em "Nova Reunião" na barra de ferramentas.
- Digite o assunto, local e detalhes da reunião.
- Adicione os participantes nos campos "Para".

- Selecione a data e hora de início e término.
- Clique em "Enviar" para enviar o convite para os participantes.

## 4. Gerenciando Contatos

### 4.1 Acessando Contatos

- Clique em "Pessoas" no Painel de Navegação.

### 4.2 Adicionando um Novo Contato

- Clique em "Novo Contato" na barra de ferramentas.
- Digite o nome, endereço de email, telefone e outras informações do contato.
- Clique em "Salvar e Fechar" para adicionar o contato à sua lista de contatos.

### 4.3 Editando e Excluindo Contatos

- Para editar um contato, clique duas vezes no contato para abrir e faça as alterações necessárias.
- Clique em "Salvar e Fechar" para salvar as alterações.
- Para excluir um contato, selecione o contato e pressione "Delete" ou clique em "Excluir" na barra de ferramentas.

## 5. Gerenciando Tarefas

### 5.1 Acessando Tarefas

- Clique em "Tarefas" no Painel de Navegação.

### 5.2 Criando uma Nova Tarefa

- Clique em "Nova Tarefa" na barra de ferramentas.
- Digite o assunto e detalhes da tarefa.
- Selecione a data de início e término, se aplicável.
- Clique em "Salvar e Fechar" para adicionar a tarefa à sua lista de tarefas.

### 5.3 Acompanhamento de Tarefas

- Marque tarefas como concluídas clicando na caixa de seleção ao lado da tarefa.
- Edite tarefas clicando duas vezes nelas para abrir e fazer as alterações necessárias.

## 6. Suporte Técnico

### 6.1 Problemas Comuns e Soluções

- Não consigo enviar/receber emails: Verifique sua conexão com a internet e tente novamente. Se o problema persistir, reinicie o Outlook e verifique as configurações de conta.
- Erro de senha/credenciais: Verifique se está digitando corretamente suas credenciais. Se você esqueceu sua senha, entre em contato com o departamento de TI para redefini-la.
- Outlook está lento: Tente fechar e reabrir o programa. Certifique-se de que não há muitas tarefas em execução ao mesmo tempo no seu computador.

## 6.2 Contato com o Suporte de TI

- Em caso de dificuldades técnicas, entre em contato com o departamento de TI através do [suporte@ecocleaning.com.br](mailto:suporte@ecocleaning.com.br).
- Forneça detalhes do problema, incluindo quaisquer mensagens de erro e os passos já realizados.