f

Manual de uso

MINDAWARE 360º

powered by HSC

Sumário

1. Introdução

2. Cadastro da Empresa
    - Ativação da Empresa
    - Acesso a Plataforma MindAware
    - Editar Perfil
    - Alterar a Senha
    - Configurações de segurança

3. Menu Administração
    - Configuração Geral
        - Logo da Empresa
        - Recomendação de Cursos
        - Autenticação de dois fatores
        - E-mail Remetente das Mensagens de Notificação
        - Domínios da Empresa
        - Notificações
        - Configurações de Ranking
    - Usuários
        - Criação de Usuários Manual
        - Definição de Perfil do Usuário
        - Importação de Usuários
        - Pesquisar Usuários
        - Editar Usuários
        - Ativação de Usuários
        - Desativação de Usuários
        - Exclusão de Usuários
    - Grupos
        - Criação de Grupos
        - Editar Grupos
        - Ativar Grupos de Usuários
        - Exclusão de Grupos

- Termos e Políticas
  - Cadastro de Termos e Políticas
  - Visualizar evidências dos Termos e Políticas
  - Editar Termos e Políticas

4. Menu Cursos
   - Cursos da Plataforma
     - Direcionar Cursos para Grupos de Usuários
   - Cursos Customizados
     - Como Criar um Curso Customizado

5. Menu Campanhas
   - Campanhas Comportamentais
     - Orientação sobre Campanhas de Phishing
     - Como Criar uma Campanha
   - Campanhas Educacionais
     - Orientação sobre Campanhas Educacionais
     - Como Criar uma Campanha

6. Dashboard
   - Dashboard Comportamental
     - Métricas das campanhas
     - Rankings
   - Dashboard Educacional
     - Métricas dos cursos
     - Métricas de usuários por curso
     - Rankings
     - Métricas de campanhas educacionais
   - Dashboard de Cursos Personalizados
     - Métricas dos cursos
     - Métricas de usuários por curso
     - Rankings
     - Métricas de campanhas educacionais
   - Dashboard por Grupo
   - Dashboard de Usuário

7. Ranking
    - Ranking Institucional
    - Ranking de Grupos
    - Ranking de Usuários

8. Quadrante MindAware
    - Visão Geral do Quadrante
    - Dashboard por Status de Quadrante
    - Dashboard do Usuário
        - Métricas Educacionais
        - Métricas Comportamentais

9. Relatórios
    - Como criar um Relatório
    - Consultar Relatórios Criados
    - Ações do Relatório

10. Insígnias e Conquistas
    - Visualização das Insígnias

11. Segurança
    - Violação de dados
    - Vulnerabilidade

12. Integrações
    - Microsoft
    - Serviço de diretório

13. Liberação de Filtragem de Campanhas de Phishing em Sistemas de Proteção de Email

14. Liberação em Sistemas Microsoft Office 365
    - Premissas
    - Procedimento
        - Primeira Etapa: Criação de Conector de Entrada
        - Segunda Etapa: Criando Regras para o email

        - Terceira Etapa: Criando Regras para Microsoft Defender

15. Liberação
    - Motivos Técnicos para Falsos Positivos
    - Recomendações

Esse sumário deve ajudar a navegar facilmente pelo manual do administrador MindAware, facilitando o acesso às informações específicas que você precisa.

Introdução

Bem-vindo ao **Manual do Administrador MindAware 360ª**, seu guia essencial para gerenciar e otimizar a plataforma de Conscientização MindAware 360ª.

Aqui você encontrará instruções detalhadas e práticas para configurar, administrar e utilizar todas as funcionalidades da plataforma de maneira eficiente.

A plataforma **MindAware 360º** e todos os seus conteúdos estão disponíveis integralmente em **português (pt-BR)**, garantindo uma comunicação adequada ao público brasileiro. Os treinamentos são apresentados de forma clara e compreensível, permitindo que todos os colaboradores participem das ações de conscientização com autonomia e segurança. O **MindAware 360º** também pode ser acessado por meio de computadores e dispositivos móveis, oferecendo maior flexibilidade.

Além disso, a plataforma oferece uma **formação completa — do Essencial ao Profissional** — estruturada para desenvolver e validar o conhecimento dos colaboradores em segurança da informação. De maneira evolutiva permite que cada usuário avance de acordo com seu nível de maturidade, garantindo aprendizado contínuo e comprovado através de certificações da própria plataforma.

Este manual foi projetado para ser sua referência completa no uso do MindAware 360ª, ajudando-o a administrar e otimizar todos os aspectos da plataforma de forma eficaz.

Consulte este guia sempre que precisar de orientação ou suporte para **maximizar o potencial da sua implementação do MindAware 360ª**.

Cadastro da Empresa

Ativação da Empresa

Para configurar a empresa dentro da plataforma MindAware 360ª e realizar a ativação do perfil inicial de administrador, você precisará seguir um processo que inclui a validação das informações abaixo:

- **Razão Social:** Nome legal da empresa.
- **CNPJ:** Número de Cadastro Nacional da Pessoa Jurídica da empresa.
- **Endereço:** Endereço físico da sede da empresa.
- **Domínios registrados para abrangência do processo de conscientização**: Lista de domínios de e-mail da empresa que serão utilizados para receber comunicações dentro da plataforma MindAware.

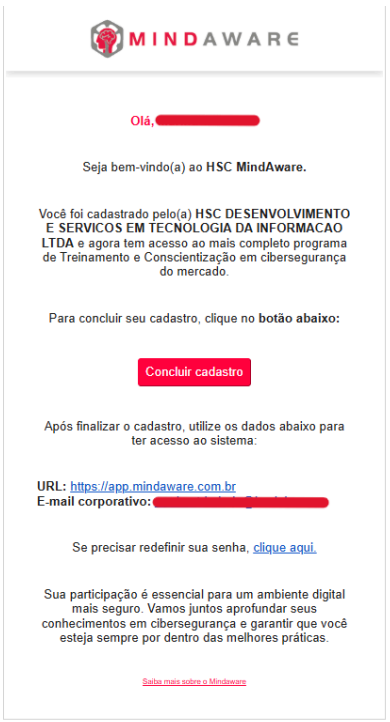
Este processo garante que a empresa esteja devidamente configurada na plataforma MindAware e que o administrador tenha acesso imediato para começar a configurar e gerenciar as funcionalidades conforme necessário.

Acesso plataforma

O acesso pode ser feito de mais de um jeito, seja por convite, conta da Microsoft ou conta do Google. Lembrando que o usuário já deve existir na plataforma com o mesmo e-mail da conta da Microsoft ou do Google para que o usuário consiga concluir o cadastro.

- **Acesso por convite:**

O usuário receberá um e-mail de ativação para concluir seu cadastro, conforme tela abaixo:



MINDAWARE

Olá, [redacted]

Seja bem-vindo(a) ao **HSC MindAware.**

Você foi cadastrado pelo(a) **HSC DESENVOLVIMENTO E SERVICOS EM TECNOLOGIA DA INFORMACAO LTDA** e agora tem acesso ao mais completo programa de Treinamento e Conscientização em cibersegurança do mercado.

Para concluir seu cadastro, clique no **botão abaixo:**

Concluir cadastro

Após finalizar o cadastro, utilize os dados abaixo para ter acesso ao sistema:

URL: https://app.mindaware.com.br
E-mail corporativo: [redacted]

Se precisar redefinir sua senha, clique aqui.

Sua participação é essencial para um ambiente digital mais seguro. Vamos juntos aprofundar seus conhecimentos em cibersegurança e garantir que você esteja sempre por dentro das melhores práticas.

Saiba mais sobre o Mindaware

Ao clicar no botão **concluir cadastro,** será solicitado os dados abaixo:

Nome completo, país, estado, cidade e a criação de sua senha.

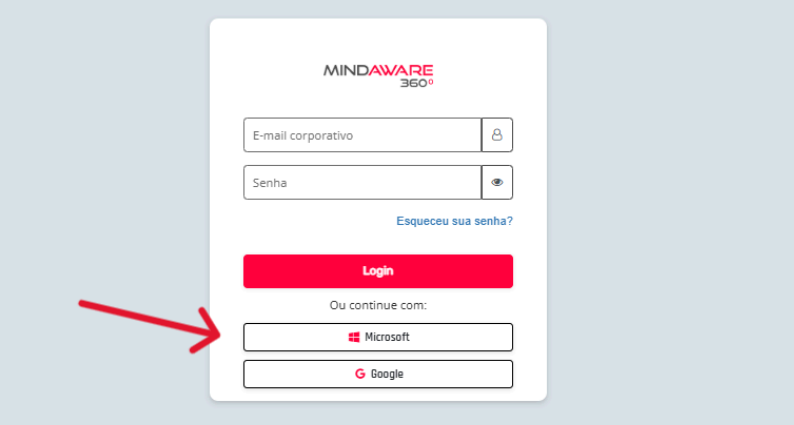


Logo após deve marcar a opção, **Li e aceito a política de privacidade e botão cadastrar.**

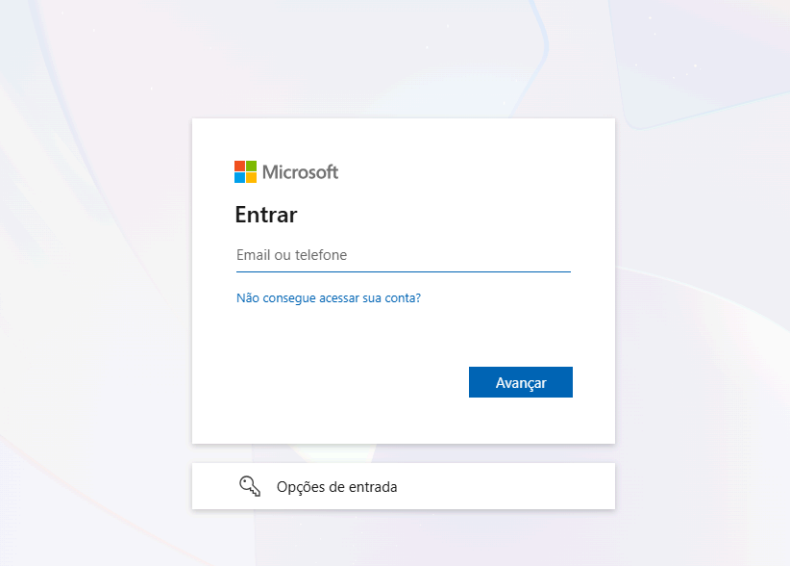
E então terá acesso à plataforma MindAware 360° de conscientização.

- **Acesso pela Microsoft**

Para acessar utilizando sua conta do Microsoft, clique no botão correspondente na tela de login.



Em seguida, um menu será exibido para você realizar o login com sua conta Microsoft. Lembre-se de utilizar sua conta profissional, não sua conta pessoal.



Após o login, uma nova tela será aberta solicitando os seguintes dados para completar seu cadastro:

Nome completo, país, estado, cidade e a criação de sua senha.

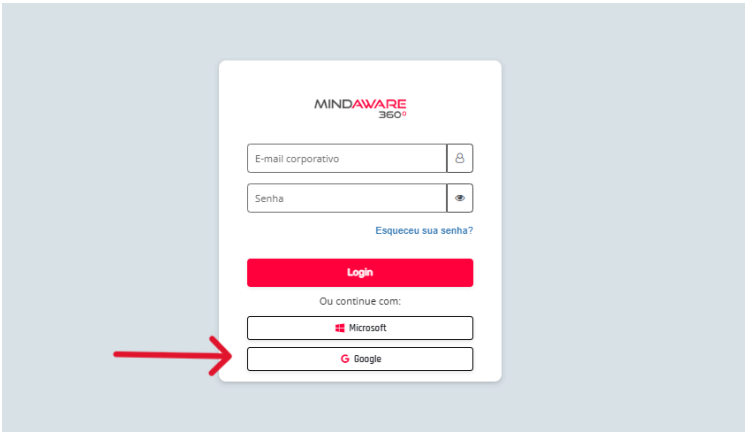


Após preencher as informações, marque a opção "Li e aceito a política de privacidade" e clique em "Cadastrar".

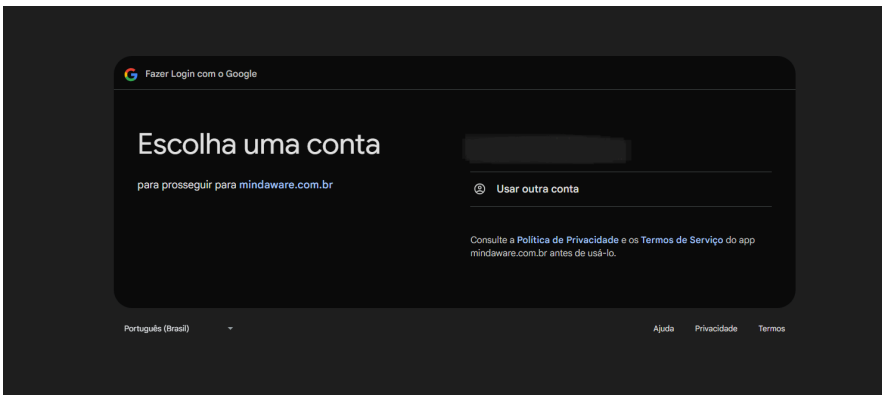
Pronto! Agora você terá acesso à plataforma MindAware 360º.

- **Acesso pelo Google**

Para acessar utilizando sua conta do Google, clique no botão correspondente na tela de login.



Em seguida, um menu será exibido para você realizar o login com sua conta Google. Lembre-se de utilizar sua conta profissional, não sua conta pessoal.



Após o login, uma nova tela será aberta solicitando os seguintes dados para completar seu cadastro:

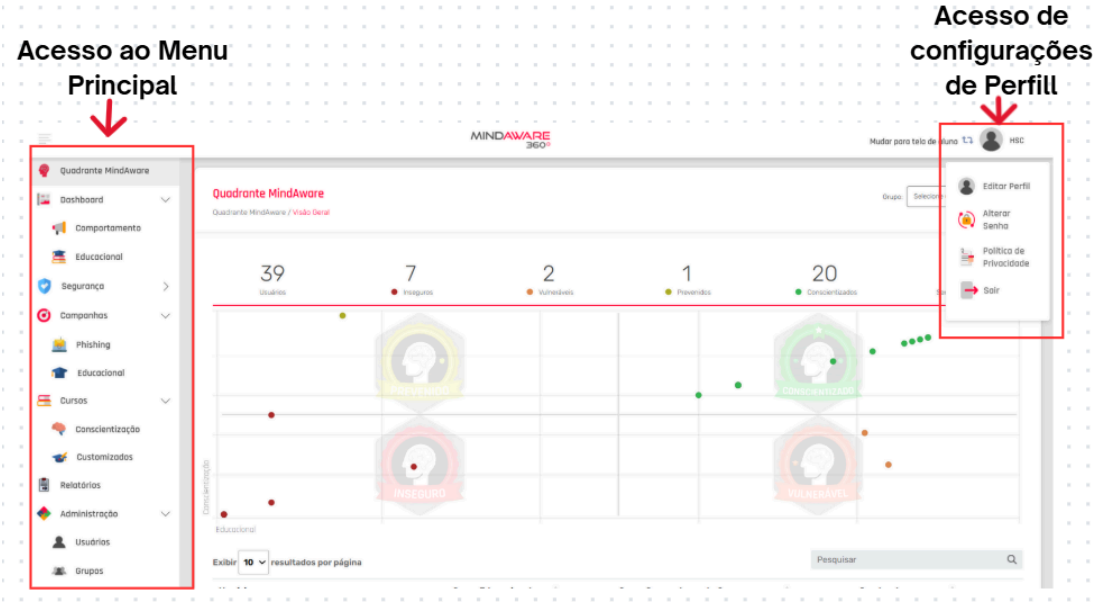
Nome completo, país, estado, cidade e a criação de sua senha.



Após preencher as informações, marque a opção "Li e aceito a política de privacidade" e clique em "Cadastrar".

Pronto! Agora você terá acesso à plataforma MindAware 360º.

Logo após o primeiro acesso, o usuário já poderá ver cursos e ter interação com toda a plataforma de acordo com seu perfil.

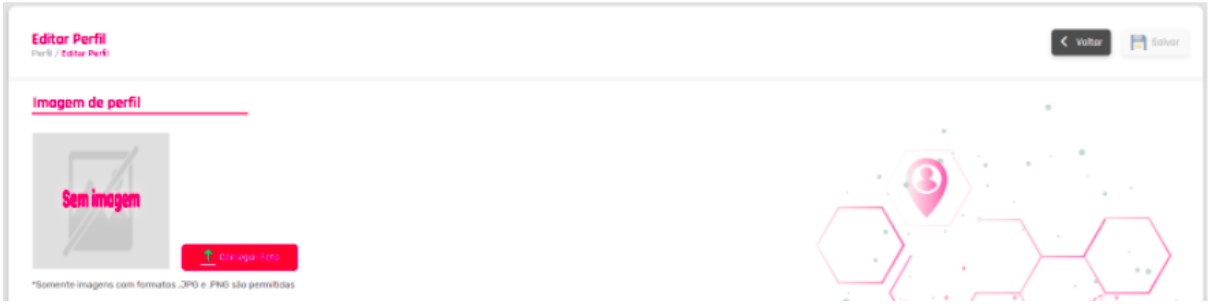


Podendo através do Menu ao lado do seu NOME, ter acesso às configurações de segurança do seu perfil tal como:

Editar Perfil:

- **Carregar uma foto para seu perfil**

Na opção **Imagem do Perfil → Click na Opção de carregar foto → Escolha foto → Salvar**



- **Atualizar dados de cadastro:**

Na opção **Dados de cadastro**, é possível manter as informações atualizadas com relação ao seu cadastro.



- **<u>Autenticação de dois fatores (MFA):</u>** Considere habilitar a autenticação de dois fatores para uma camada extra de segurança ao fazer login na plataforma.

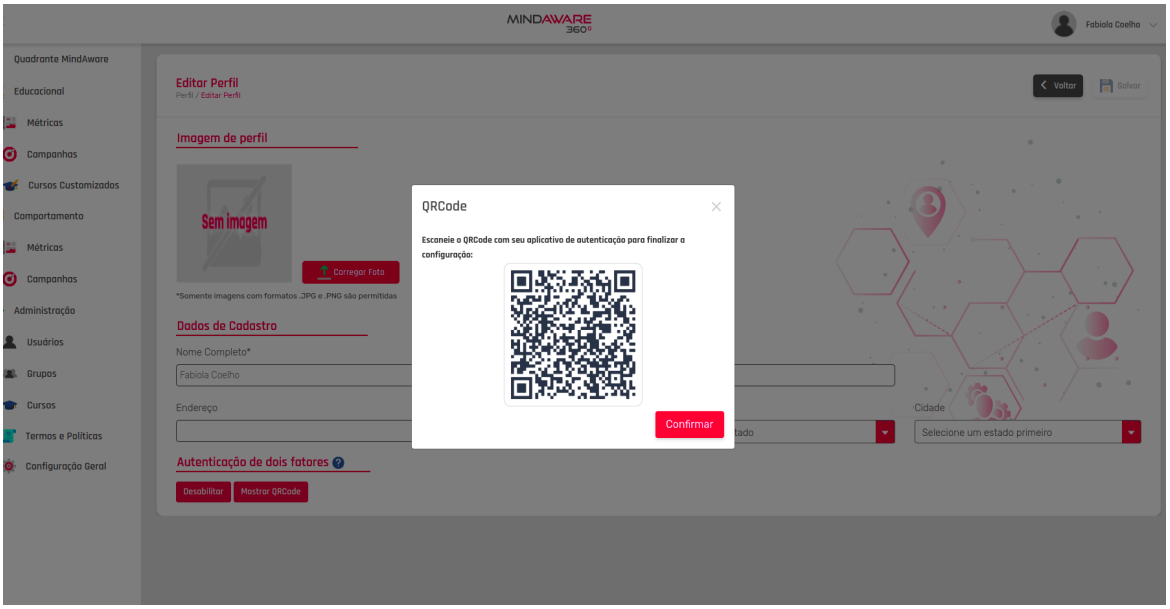
  Na opção **Autenticação de dois fatores** clicar em **ativar**



Será solicitado a **confirmação de sua senha:**

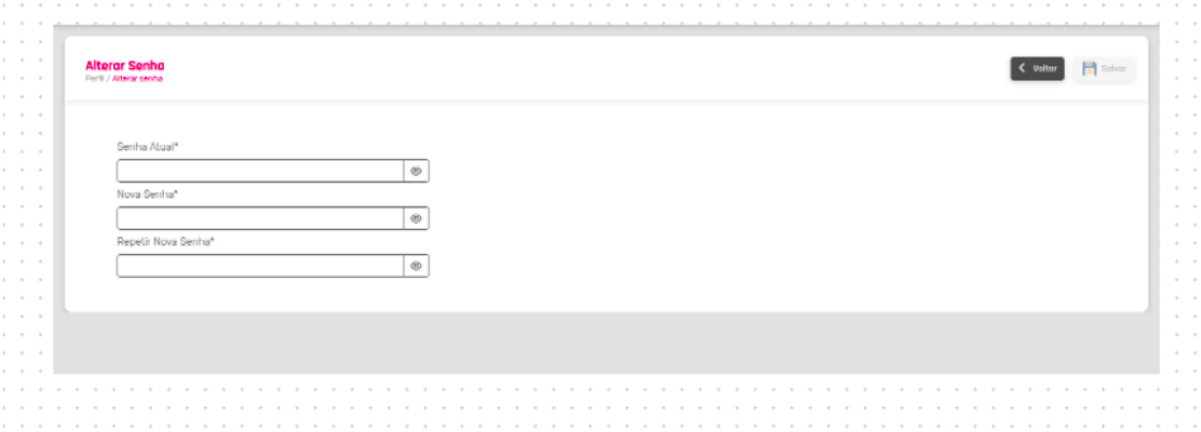


Ao confirmar a sua senha, **abrirá o QRCODE** (conforme tela abaixo) para escanear e assim fazer a autenticação em seu celular.



Alterar a Senha

Considere esta opção para alterar a senha do seu usuário.



Siga os passos:

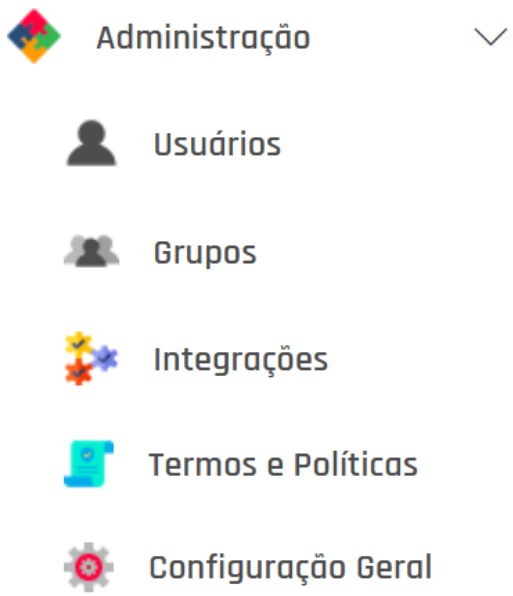
Confirme sua senha atual → digite uma nova senha → Repita a nova senha → Clicar em Salvar

Dicas de Segurança:

- **Senha Forte**: Use uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais para criar uma senha forte e segura.

Menu Administração

Nesta seção, será possível personalizar, configurar e administrar a plataforma MindAware 360.



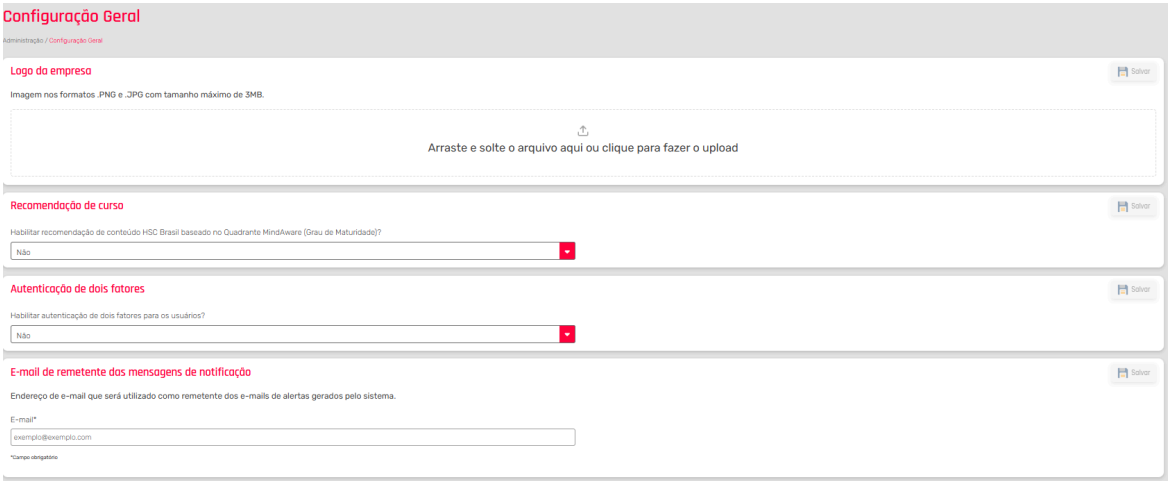
Neste menu, vamos realizar a **configuração geral de administração** como **Usuários, Grupos, Integrações, Termos e Políticas e Configuração Geral.**

Vamos realizar a **carga de usuários**, **gerenciar os grupos** para já iniciar as atividades de ação dentro da plataforma.

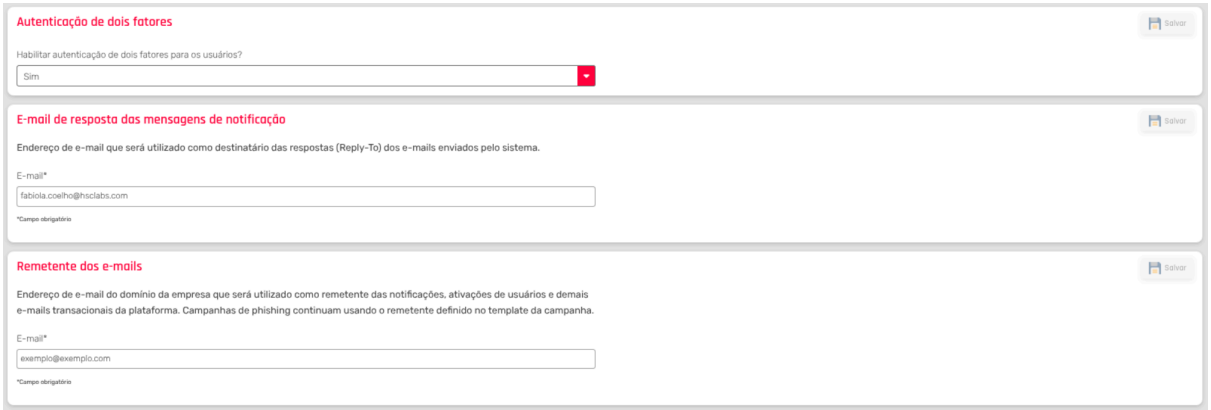
Temos nele também a possibilidade de incluir **Termos e políticas** para disponibilizar aos colaboradores, assim como visualizar seus registros de aceite.

Configuração Geral

No Menu **Configuração Geral** teremos a possibilidade de realizarmos as seguintes ações:



- **Logo da Empresa:** Permite configurar o logotipo que representa a empresa dentro da plataforma.
- **Recomendação de Cursos:** Define se é possível ou não liberar cursos que serão recomendados aos usuários, promovendo uma experiência personalizada de aprendizado de acordo com seu status no quadrante.
- **Autenticação de Dois Fatores:** Define se os usuários vão poder ter a opção de habilitar a autenticação de dois fatores.
- **E-mail de Resposta das Mensagens de Notificação:** Endereço de e-mail que será utilizado como destinatário das respostas (Reply-To) dos e-mails enviados pelo sistema.
- **E-mail Remetente das Mensagens:** Configura o endereço de e-mail que será utilizado para receber as mensagens de notificação dos usuários em caso de identificação de um possível ataque da plataforma.
- **Domínios da Empresa:** Relação dos domínios cadastrados na ativação da Empresa, oferecendo controle sobre os endereços utilizados para acessar a plataforma e seus serviços.
- **Conteúdos Opcionais:** Define se os cursos identificados como opcionais, realizados voluntariamente pelos usuários, serão contabilizados no Score Educacional e no Quadrante MindAware. Quando desabilitada, os cursos poderão ser realizados normalmente, porém não contribuirão para esses indicadores.



Notificações

O Menu de Notificações permite ao administrador controlar o envio de notificações da plataforma, definindo se elas estarão ativas, quais tipos de notificações serão enviadas, a frequência de envio e o conteúdo das mensagens.

Na tela de configurações clique em “Notificações“ para abrir as configurações de notificações.



Na parte superior da tela, encontra-se a seção Ativação das Notificações.

Nessa seção, o administrador pode ativar ou desativar globalmente o envio de notificações para todos os usuários da plataforma

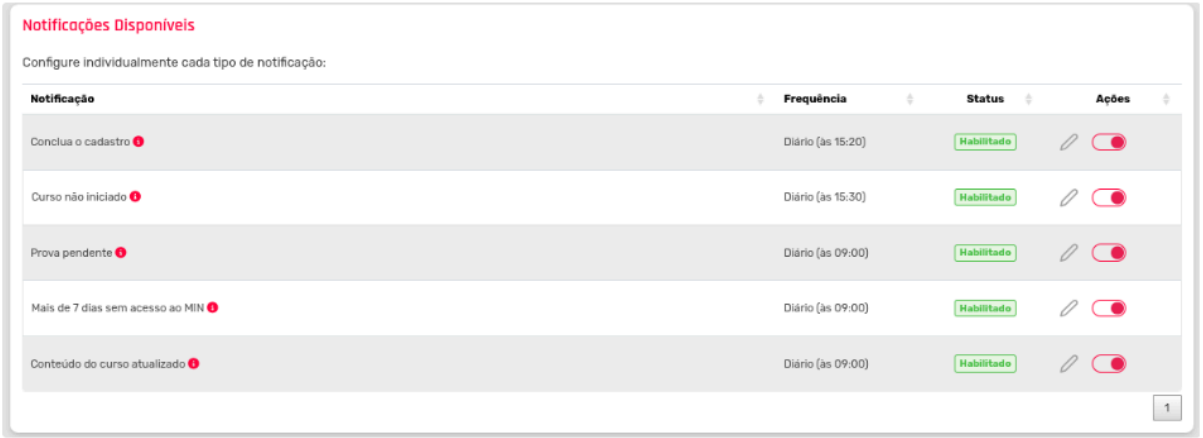
Quando essa opção estiver:

- **Ativada:** a plataforma enviará notificações automáticas conforme as configurações definidas
- **Desativada:** nenhuma notificação será enviada, independentemente das configurações individuais

Essa opção funciona como um controle geral do envio de notificações.

Notificações Disponíveis

Logo abaixo, é exibida a seção Notificações Disponíveis, onde o administrador pode configurar cada tipo de notificação individualmente.



Nessa lista, são exibidas notificações como, por exemplo:

- Concluir o cadastro
- Curso não iniciado
- Prova pendente
- Mais de 7 dias sem acesso à plataforma
- Conteúdo do curso atualizado

Cada notificação representa um evento específico que pode gerar um aviso ao usuário.

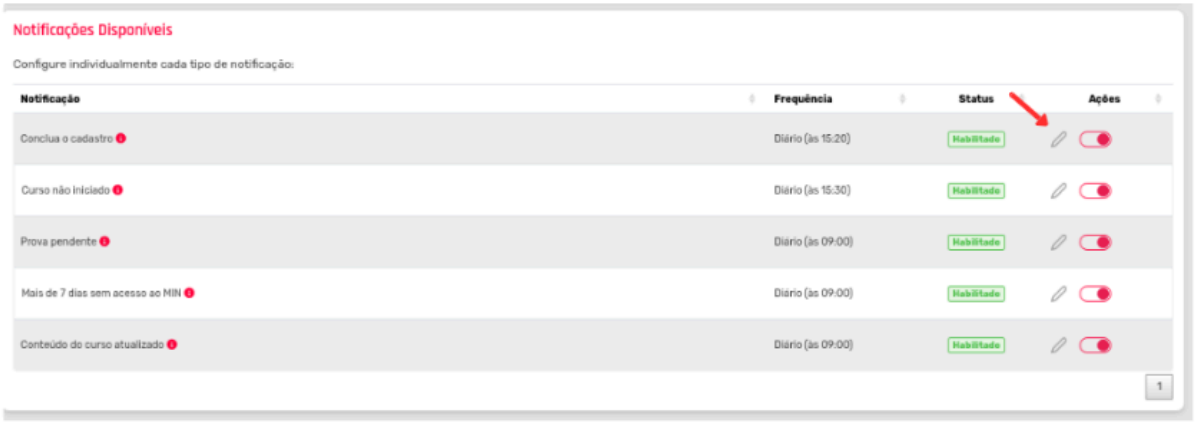
Status:
Cada notificação possui um status individual, indicando se está:

Habilitada
Desabilitada

Mesmo com as notificações globais ativadas, uma notificação específica só será enviada se estiver habilitada individualmente.

Edição da mensagem da notificação:

Clicando no ícone indicado abrirá um painel de edição, onde é possível:



- Definir a frequência de envio, como:
    - Diária

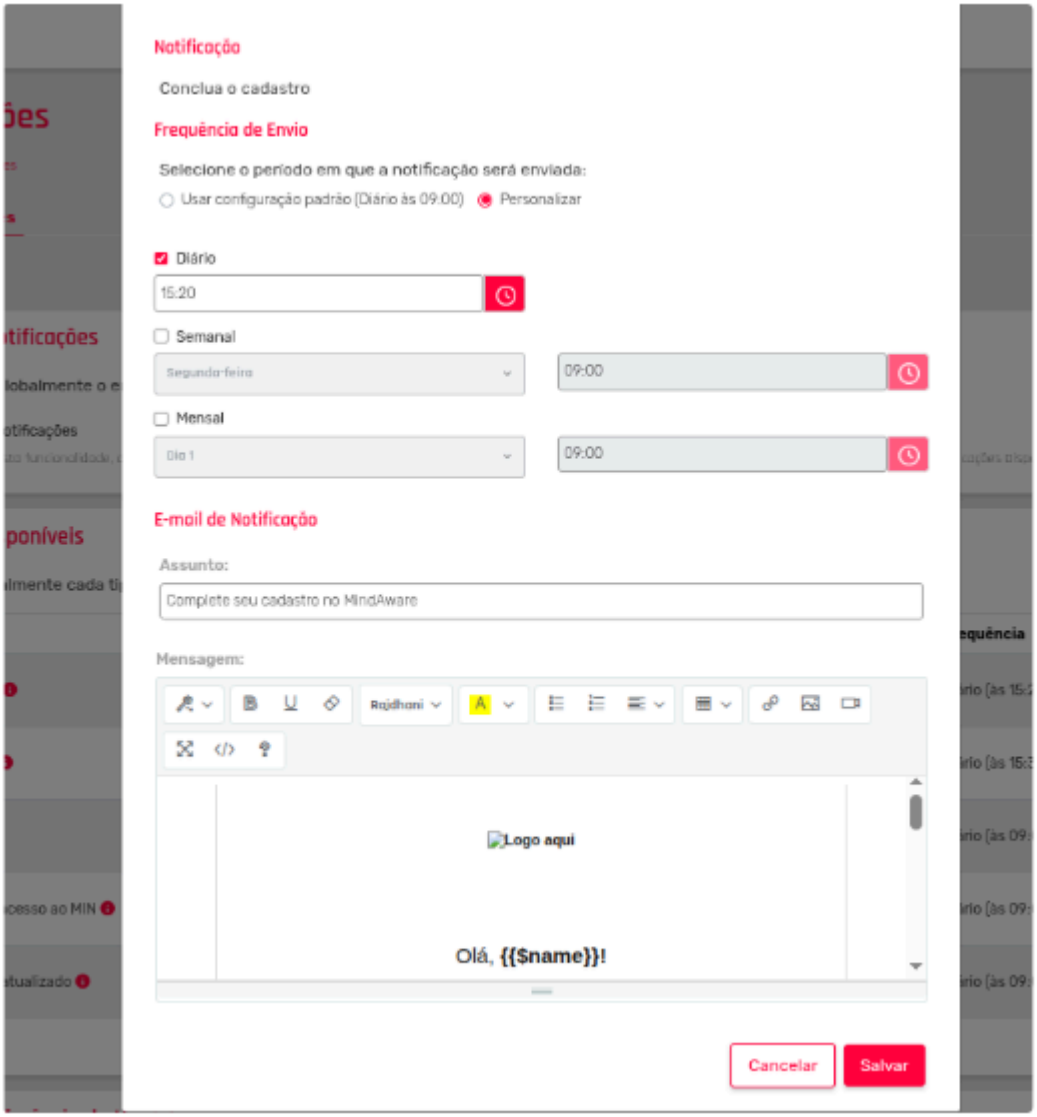
- Semanal
- Em horários específicos

- Definir o dia e horário exato:

Se as notificações forem semanais deve escolher o dia da semana, e se forem mensais deve escolher o dia do mês que elas serão enviadas.

- Editar a mensagem de cada notificação

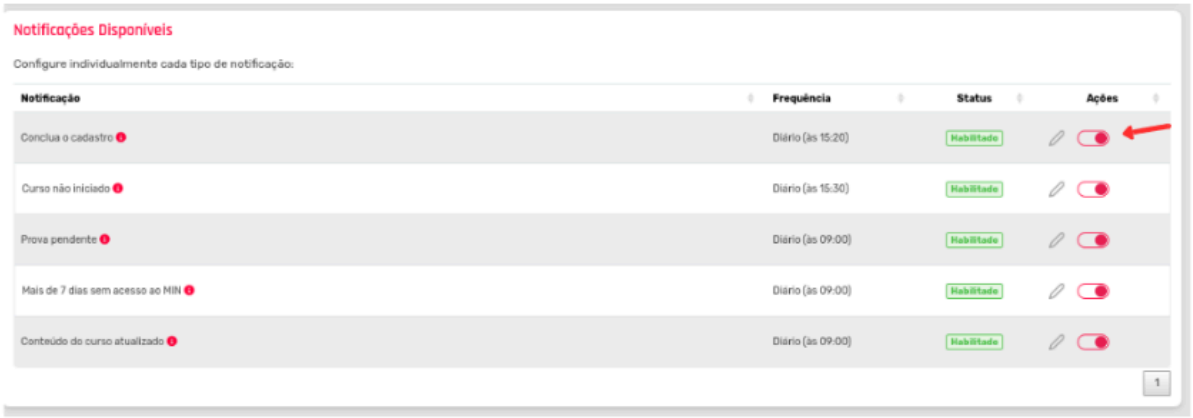
- Adicionar sua logo a mensagem



Essa edição permite personalizar o texto enviado aos usuários e seus períodos, adequando a comunicação ao tom institucional da organização, mantendo as variáveis obrigatórias do sistema.

Ativar ou desativar notificações individualmente

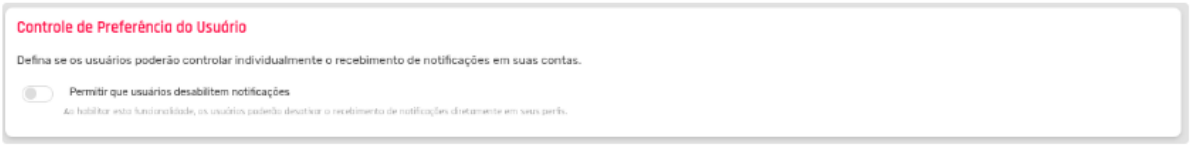
No ícone indicado, é possível ativar ou desativar cada notificação de forma independente



Isso permite controle total sobre quais comunicações serão enviadas pela plataforma.

4. Controle de Preferência do Usuário

Na parte inferior da tela, encontra-se a seção Controle de Preferência do Usuário.



Nessa seção, o administrador pode definir se:

- Os usuários poderão decidir individualmente se desejam ou não receber notificações

Quando essa opção estiver:

- Ativada: cada usuário poderá habilitar ou desabilitar notificações em seu próprio perfil
- Desativada: as notificações seguirão exclusivamente as configurações definidas pelo administrador

5. Restaurar Padrões

No canto superior da tela, está disponível a opção Restaurar Padrões.



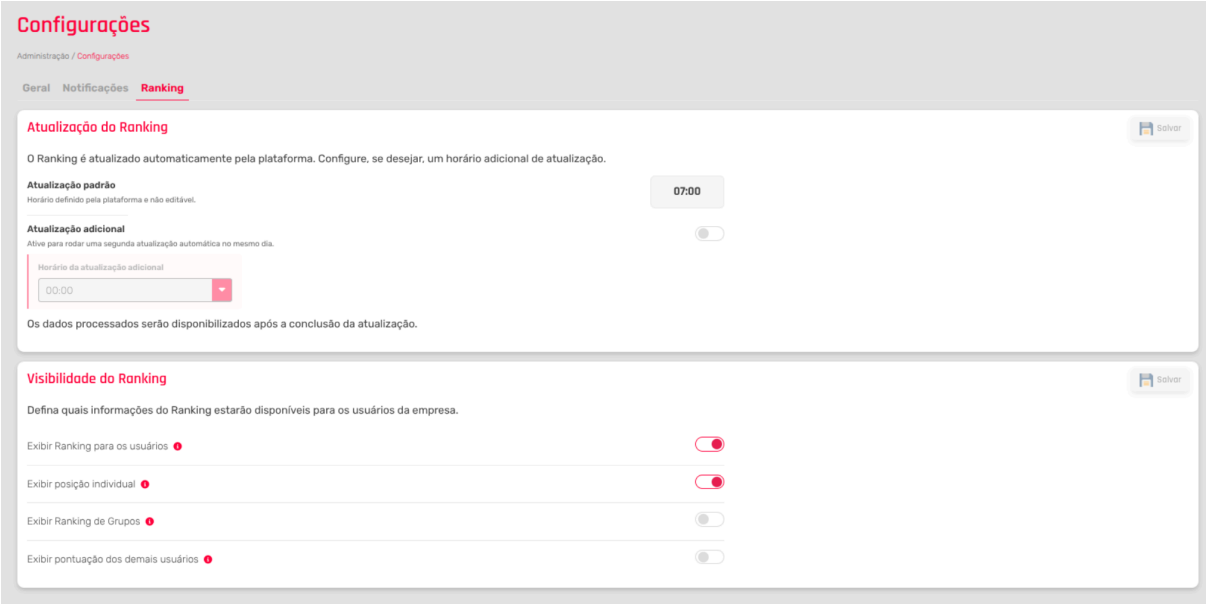
Ao utilizar essa opção:

- Todas as configurações de notificações retornam aos valores padrão da plataforma
- Frequências, mensagens e status são redefinidos conforme o padrão original

---

Configuração do Ranking

A plataforma permite ao administrador definir parâmetros relacionados à **atualização e visibilidade do Ranking**.



Atualização padrão

A plataforma possui um horário padrão para processamento e atualização das informações do Ranking.

O horário padrão apresentado é definido pela plataforma e **não pode ser alterado pelo administrador**.

Atualização adicional

Caso seja necessário atualizar o Ranking mais de uma vez ao dia, o administrador poderá habilitar a opção **Atualização adicional**.

Essa funcionalidade permite configurar um segundo horário de atualização automática no mesmo dia.

Para configurar:

1. Ative a opção **Atualização adicional**;
2. Selecione o horário desejado no campo **Horário da atualização adicional**;
3. Clique em **Salvar**.

Após a conclusão do processamento, os novos dados serão disponibilizados nas telas do Ranking.

Visibilidade do Ranking

Na seção **Visibilidade do Ranking**, o administrador poderá definir quais informações relacionadas ao Ranking estarão disponíveis para os usuários da empresa.

As opções podem ser ativadas ou desativadas conforme a política e estratégia de conscientização adotada pela organização.

Exibir Ranking para os usuários

Define se o Ranking estará disponível para visualização pelos usuários.

Ao habilitar essa opção, os participantes poderão ter acesso às informações de Ranking disponibilizadas pela plataforma.

Exibir posição individual

Define se cada usuário poderá visualizar sua própria posição no Ranking.

Essa opção permite disponibilizar ao participante sua colocação individual de acordo com a pontuação registrada pela plataforma.

Exibir Ranking de Grupos

Define se as informações relacionadas ao **Ranking de Grupos** poderão ser apresentadas aos usuários.

Quando habilitada, a classificação dos grupos poderá ser disponibilizada para consulta conforme as configurações da plataforma.

Exibir pontuação dos demais usuários

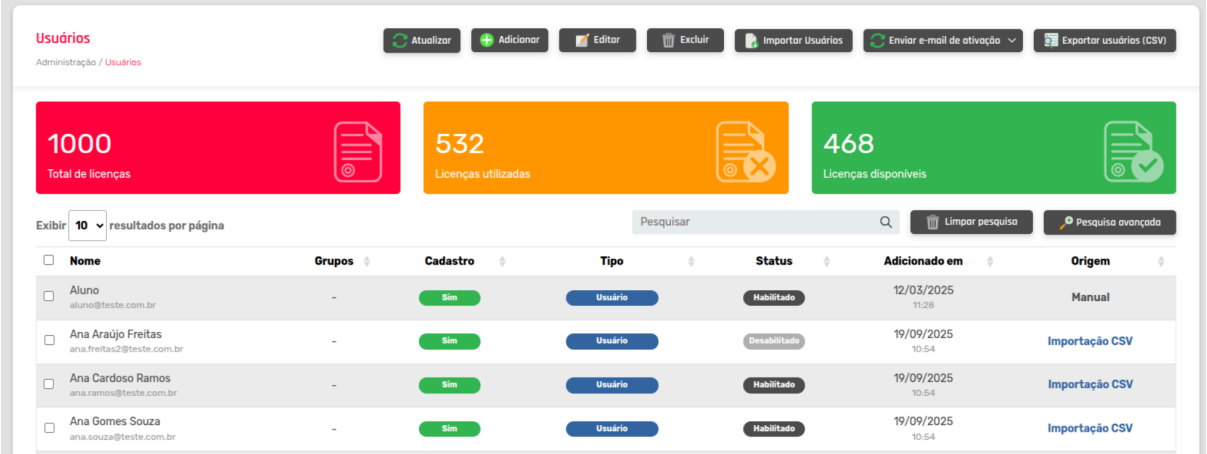
Define se os usuários poderão visualizar a pontuação dos demais participantes apresentada no Ranking.

Ao desabilitar essa opção, a organização pode restringir a exposição das pontuações individuais dos outros usuários.

Após configurar as opções desejadas, clique em **Salvar** para aplicar as definições.

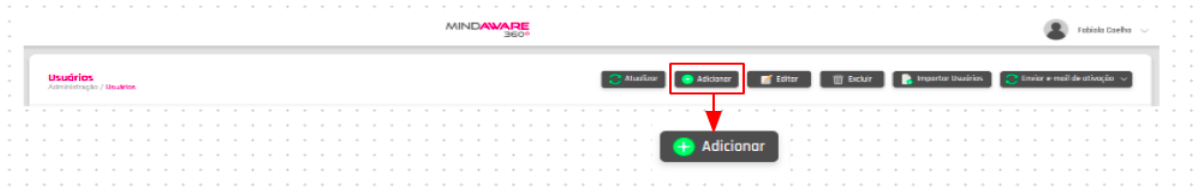
Usuários

No **Menu Usuário,** é possível realizar toda administração com relação à base de usuários da plataforma, assim como visibilizar a disponibilidade de Licenças contratadas, utilizadas e disponibilizadas para uso da plataforma.

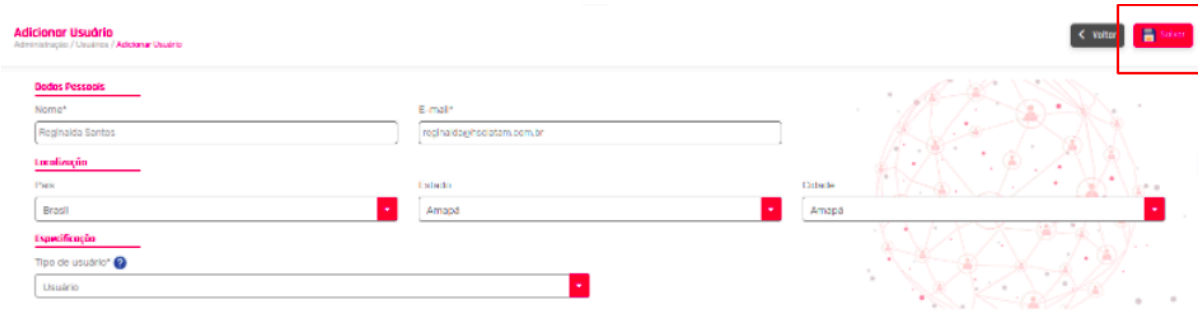


Criação de Usuários Manual

- Instruções de como adicionar novos usuários individualmente:
    - No Menu usuários **clicar no botão adicionar:**



    - Preencher os dados do formulário (**Nome, e-mail, Localização**, **Especificação: usuário, Grupos (podendo ser cargo e setor**),

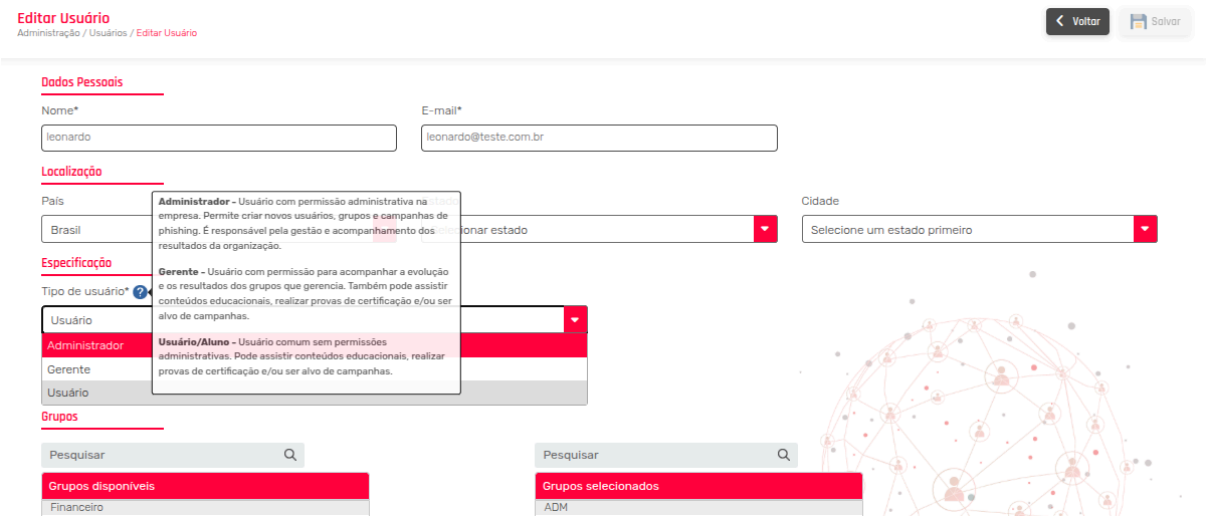


Definição de Especificação do Usuário:

Permite a configuração de diferentes perfis de usuário de acordo com suas funções e responsabilidades dentro da plataforma. Cada perfil possui níveis de acesso específicos, garantindo a segmentação adequada dos dados e o acesso seguro às informações, conforme as permissões atribuídas a cada usuário.

Existem três tipos de perfil de usuário:

- **Administrador:** Tem total gerência sobre a plataforma, pode realizar cargas de usuários, edições e exclusões, criar campanhas de simulação no menu Comportamento e construir cursos no menu Educacional para toda a organização.
- **Gerente:** Tem ação somente ao grupo na qual ele está destinado, pode criar campanhas educacionais através de cursos customizados e ser alvo em campanhas de phishing, por esta razão, não têm privilégios para criar campanhas no Menu Comportamento.
- **Usuário:** Tem interações somente como aluno, como por exemplo: acesso à cursos, certificados e ser alvo em campanhas de simulação de phishing.



Seleção do Perfil de Permissões:

Durante a criação manual de um usuário, na seção **Permissões e Acesso**, é possível selecionar o Perfil de Permissões que será associado ao usuário cadastrado.

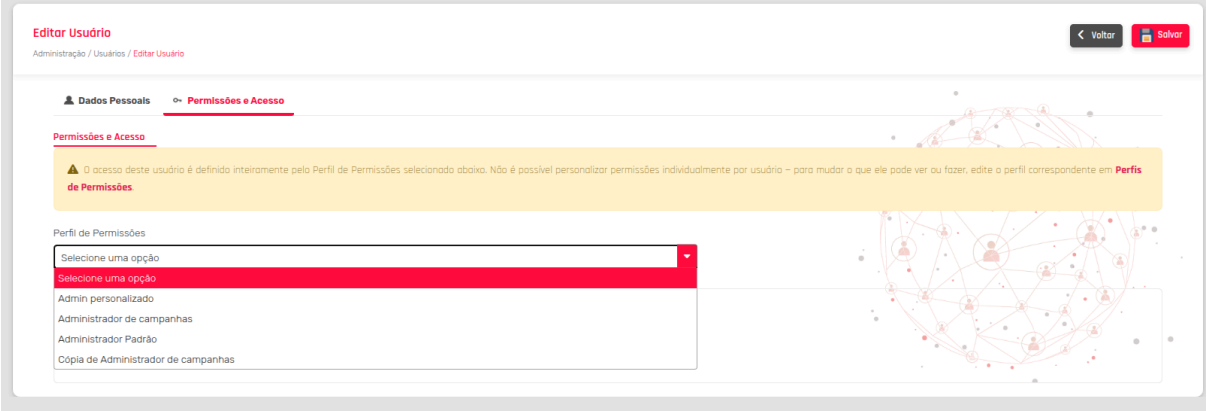
Os perfis disponíveis para seleção serão apresentados de acordo com o tipo de usuário escolhido:

- **Gerente:** Permite selecionar um Perfil de Permissões do tipo Gerente.
- **Administrador:** Permite selecionar um Perfil de Permissões do tipo Administrador.

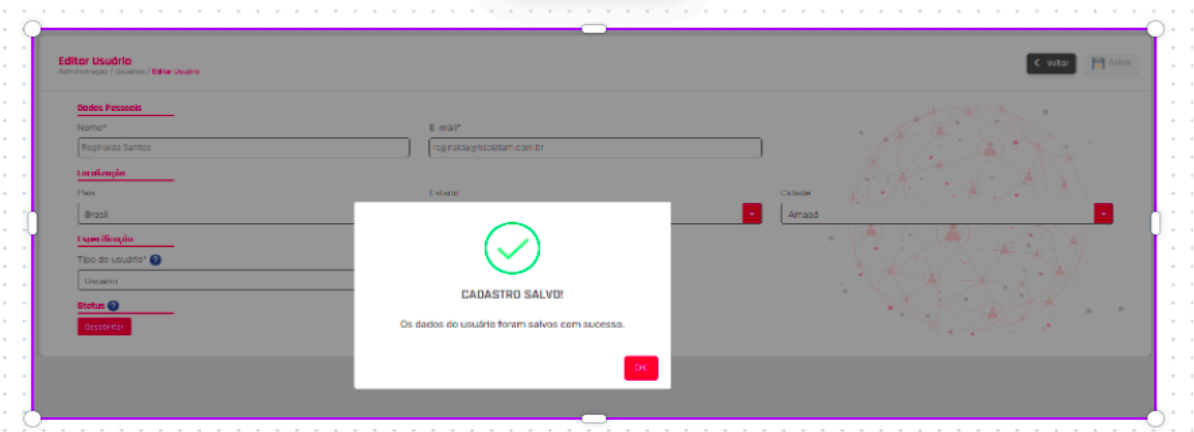
O Perfil de Permissões define quais módulos, funcionalidades e ações o usuário poderá acessar dentro da plataforma.

Caso não seja selecionado um perfil personalizado, o usuário utilizará as permissões padrão correspondentes ao seu tipo de usuário.

Após selecionar o perfil desejado, clique em **Salvar** para concluir o cadastro do usuário.



E clicar em **Salvar.**



Então, o cadastro **do usuário** será realizado, e a plataforma fará a notificação do Cadastro salvo.

Importação de Usuários:

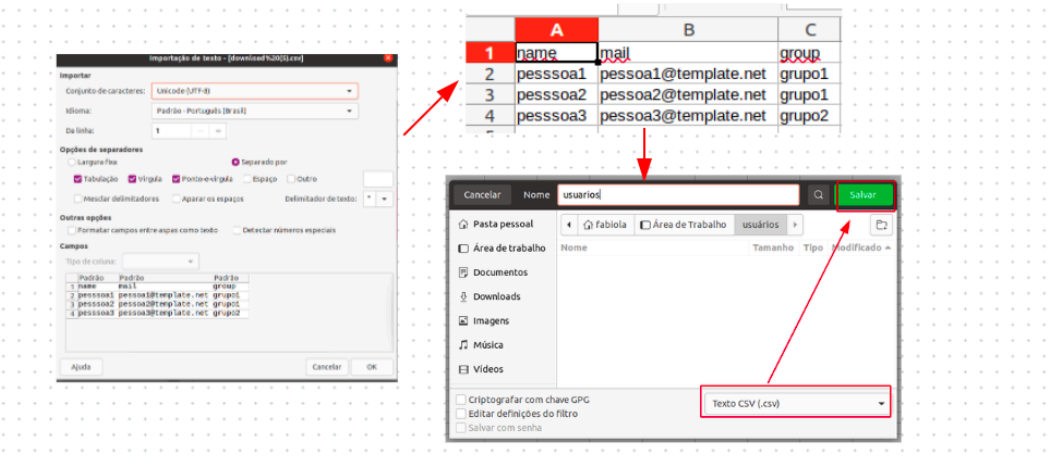
- Instruções para importar múltiplos usuários para a plataforma através de um arquivo .CSV:



Ao clicar no Menu Importar usuários , abrirá a tela abaixo:



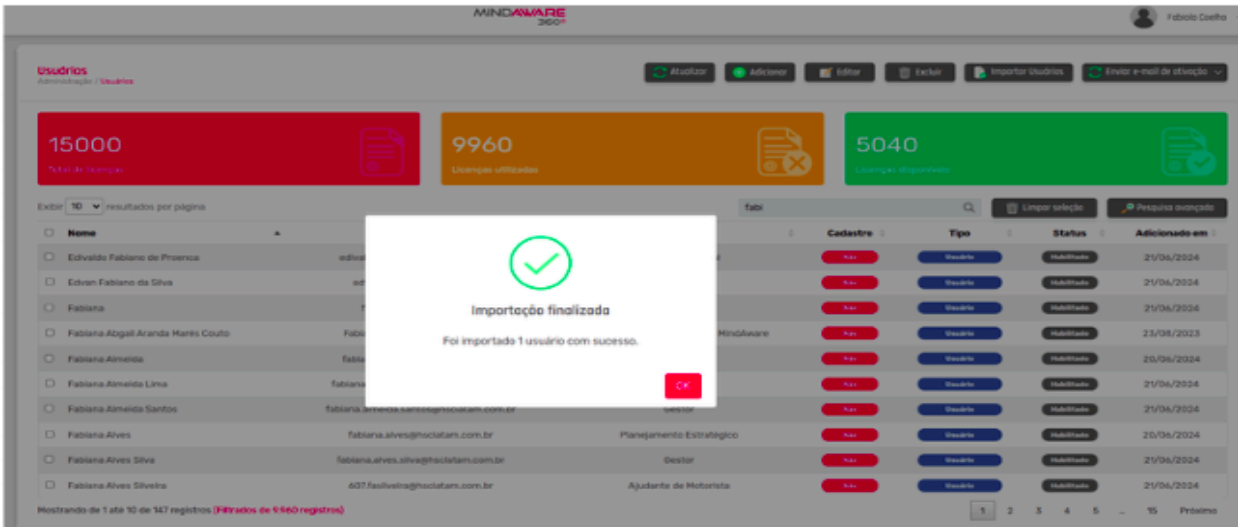
Caso não tenha o template, pode **clicar e fazer o download do template** para seguir o exemplo preenchendo os dados de **Nome, E-mail e grupo**, e salvar como este arquivo como .CSV



Logo após salvar o arquivo .csv podes então importar este na plataforma, escolhendo através do botão **Escolher arquivo** e **clicar em Importar.**



Então, a **carga dos usuários** será realizada, e a plataforma faŕa a notificação da **Importação finalizada.**

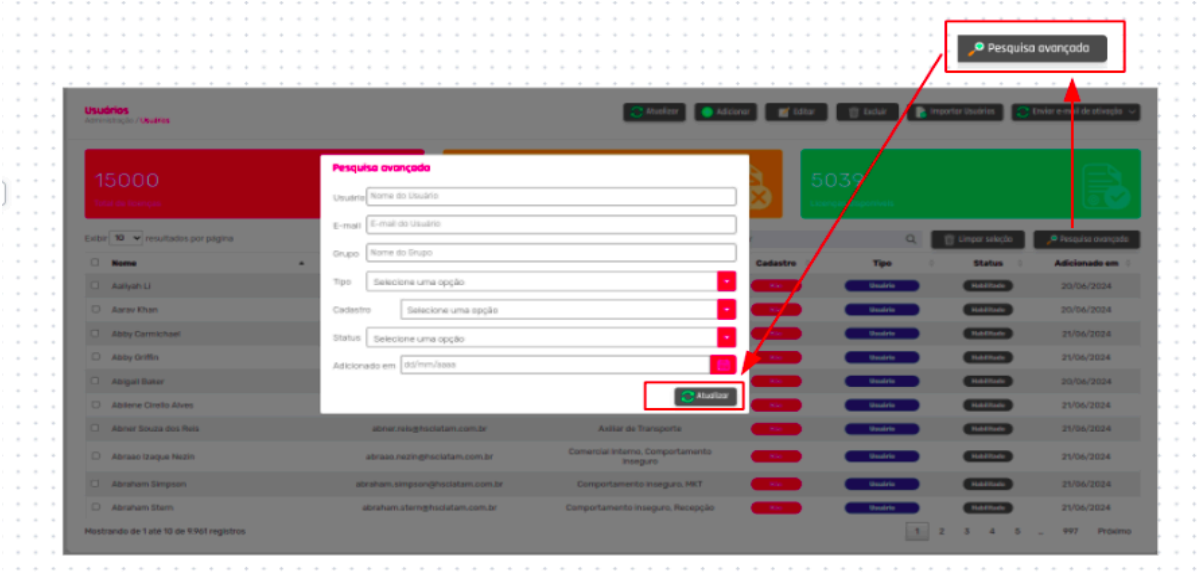


Pesquisar Usuários: Instruções que permitem realizar pesquisas de usuários

cadastrados na plataforma:



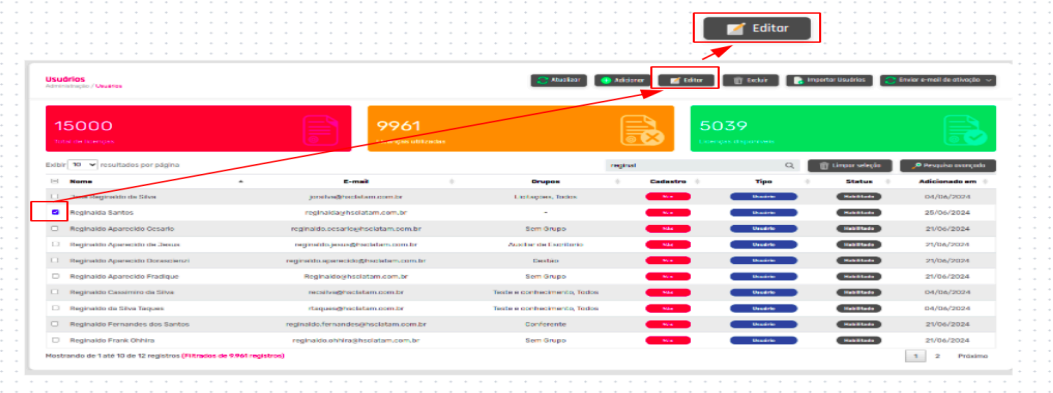
- **Pesquisa simples:** É possível realizar uma pesquisa simples, através da digitação de uma única informação.
- **Pesquisa Avançada:** É possível realizar pesquisa avançada, através de combinações de dados como, após clicar em atualizar



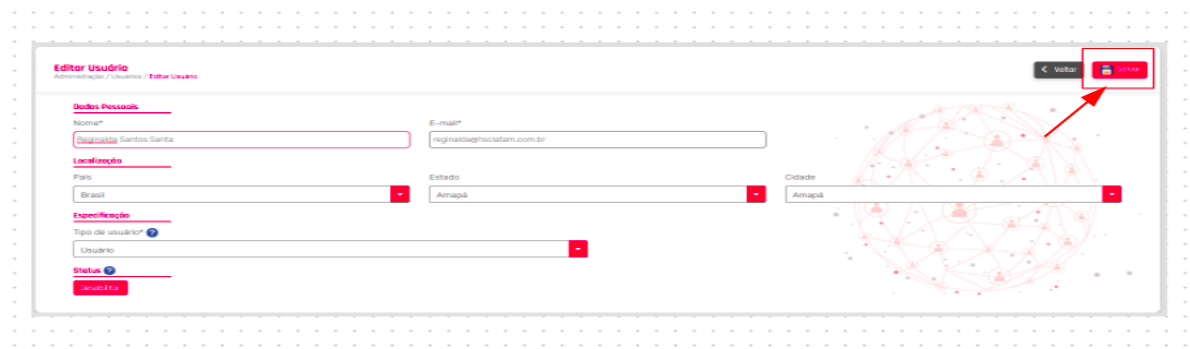
Editar Usuários:

Esta é uma ação que permite modificar as informações dos usuários existentes, para isso, basta seguir as seguintes instruções:.

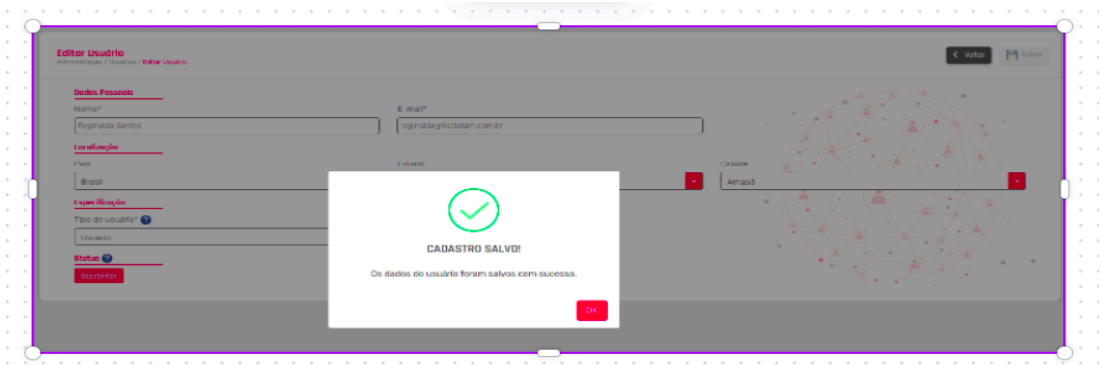
- **Selecione o usuário** que deseja editar os dados → após clique no **botão editar**



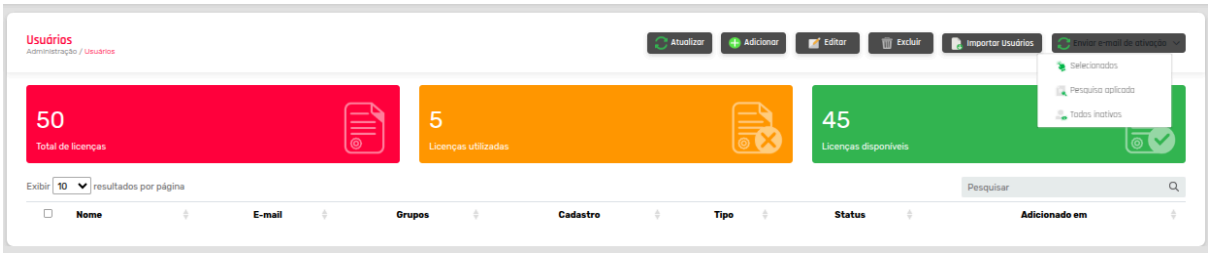
- Após edição da informação, clicar no salvar.



- E a plataforma trará a notificação do **Cadastro salvo.**

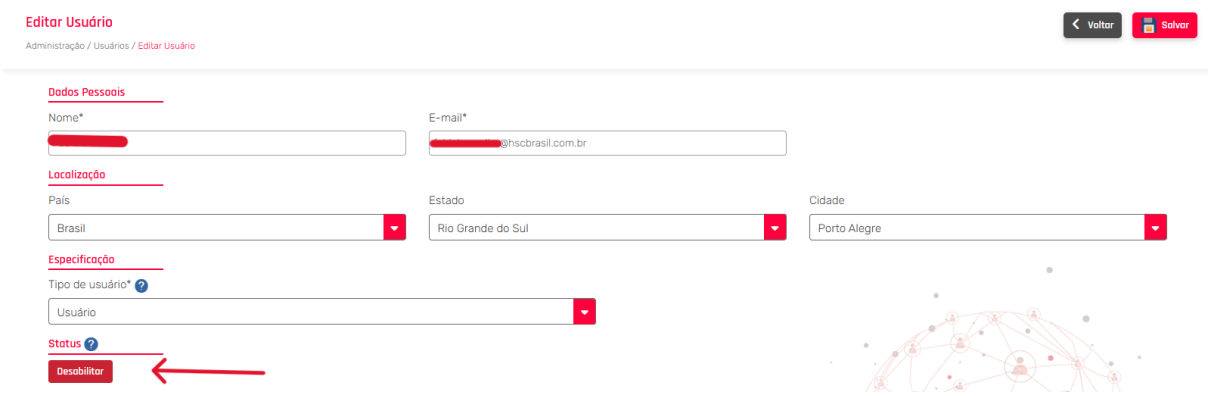


Ativação de Usuários: Utiliza-se este botão basicamente para ativar contas de usuários recém criadas ou contas de usuários que estão inativos.

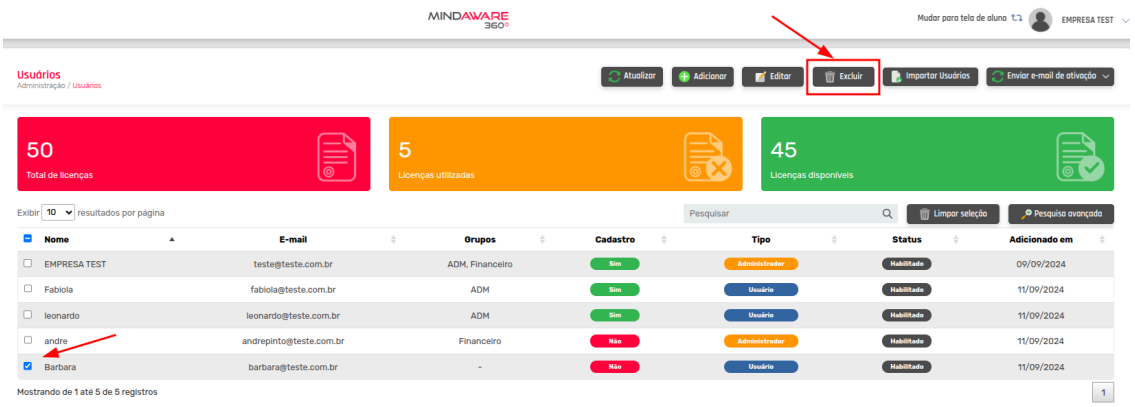


Desativação de Usuários: Quando um usuário é desabilitado não se tem perda no histórico, apenas o acesso da plataforma será restrito. O usuário não poderá efetuar login, recuperar senha, participar de campanha, será removido dos grupos e não receberá notificações por e-mail.

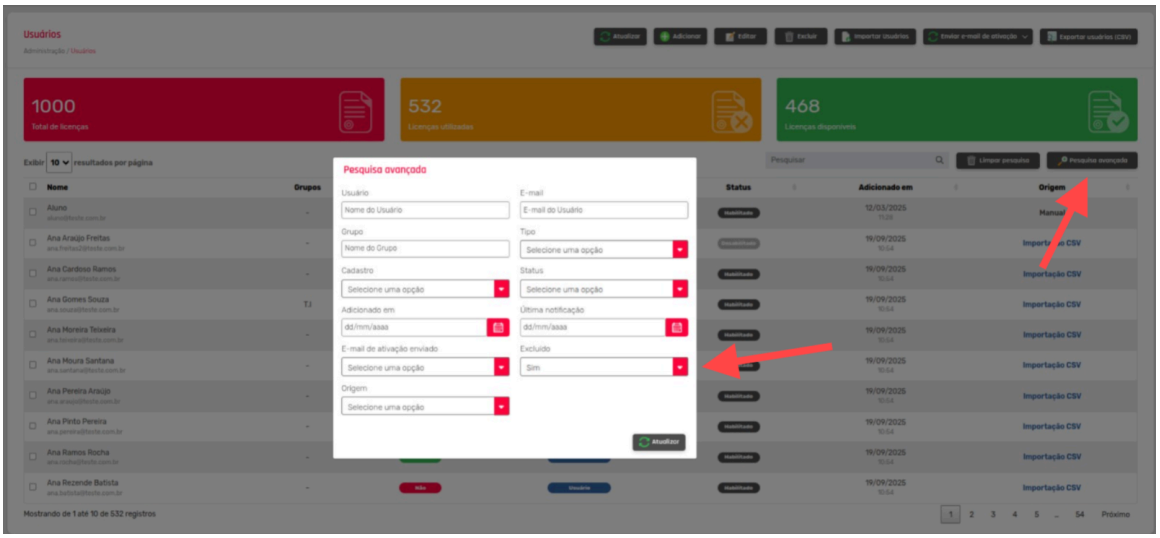
Para desativar um usuário escolha o usuário, vá em **Editar** e aperte no botão indicado. Assim que confirmar a desativação o usuário já estará desabilitado.



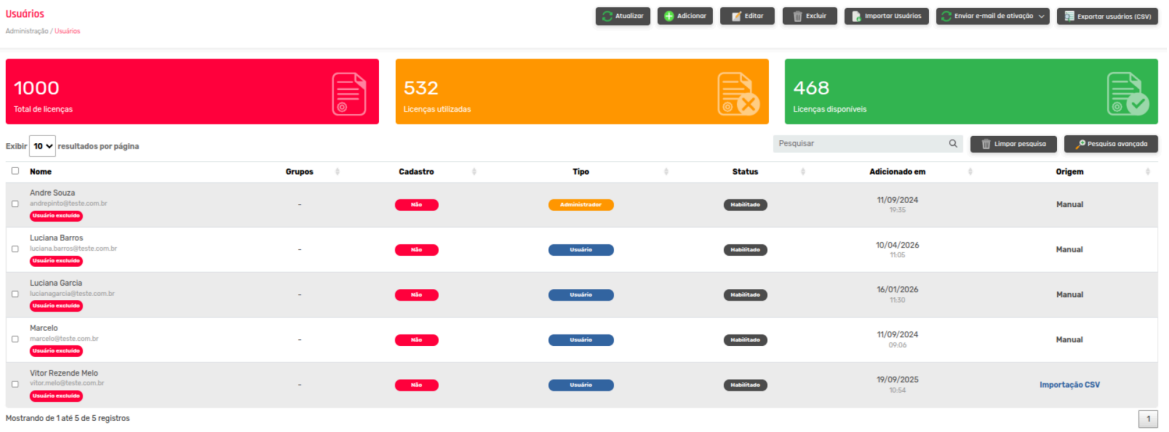
Excluir Usuários: Para excluir contas de usuários que não são mais necessárias, basta selecionar o(s) usuário(s) desejado(s) e realizar a remoção permanente clicando no botão **-> Excluir** e confirmando em seguida.



<u>Ver Usuários Excluídos:</u> É possível visualizar os usuários que foram excluídos da plataforma utilizando os filtros da **Pesquisa Avançada**. Para isso, acesse a **Pesquisa Avançada**, localize o filtro **Excluído** e selecione a opção **Sim**.

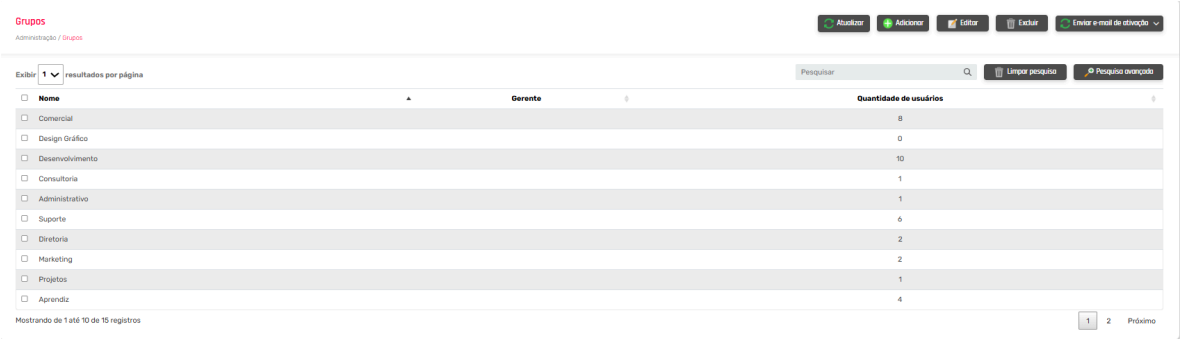


Após aplicar o filtro, serão exibidos todos os usuários que foram excluídos da plataforma.

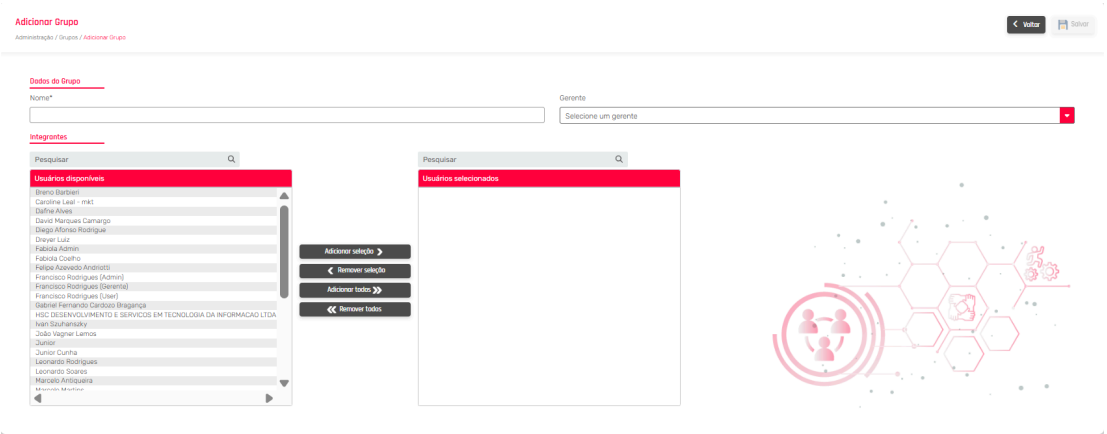


Grupos

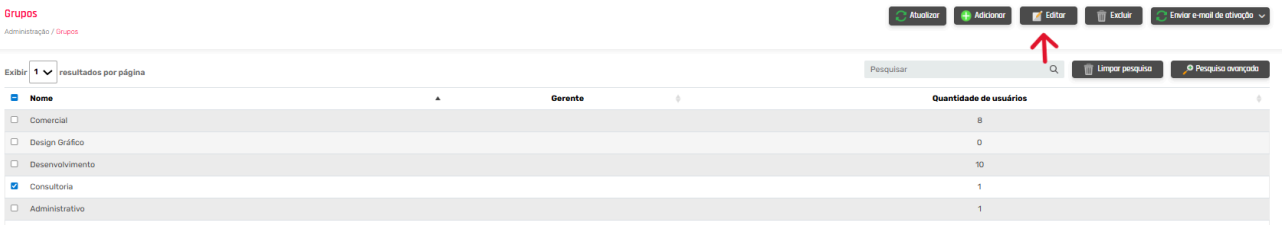
A plataforma possibilita o gerenciamento de grupos de usuários, nesta opção, teremos as seguintes ações:



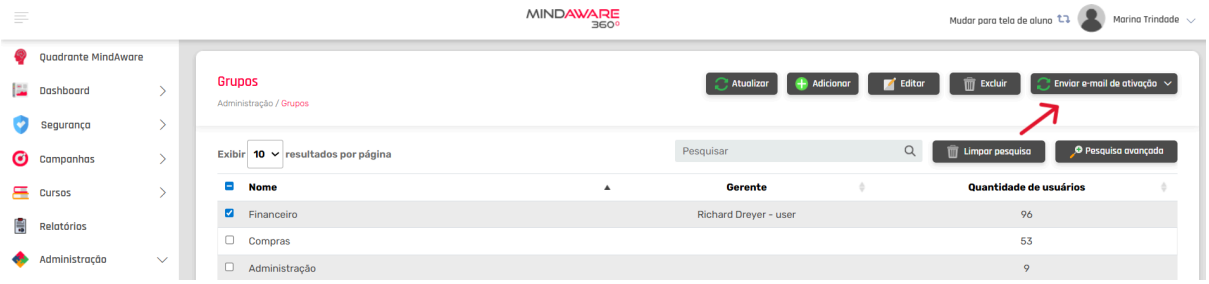
- **<u>Criação de Grupos:</u>** Como vimos acima, os usuários, assim como os grupos, podem ser importados através de uma planilha CSV obedecendo a estrutura do seu servidor AD, LDAP ou Zimbra. Além disso, podemos criar grupos manualmente, basta clicar no **Menu Administração -> Grupos** e no **botão Adicionar**. Em seguida preencha as informações e clique em **Salvar**.



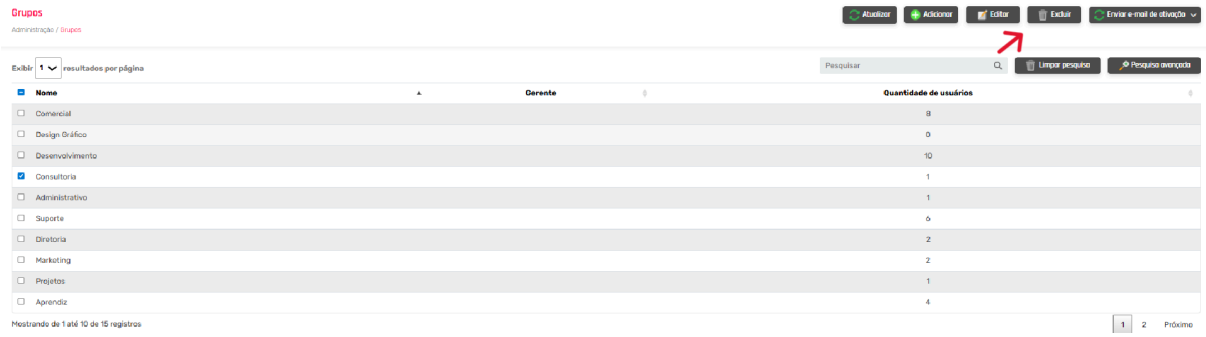
- **<u>Editar Grupos:</u>** Para editar um grupo, basta selecionar o grupo desejado na lista e clicar em "Editar". Isso abrirá a mesma tela utilizada na criação do grupo, porém já preenchida com as informações existentes. Faça as alterações necessárias e, em seguida, clique em **Salvar** para atualizar os dados do grupo.



- **<u>Ativar Grupos de Usuários:</u>** Você pode criar um grupo de usuários que ainda não foram ativados para enviar o email de ativação. Assim que criar o grupo normalmente, selecione e aperte em **Enviar e-mail de ativação.**

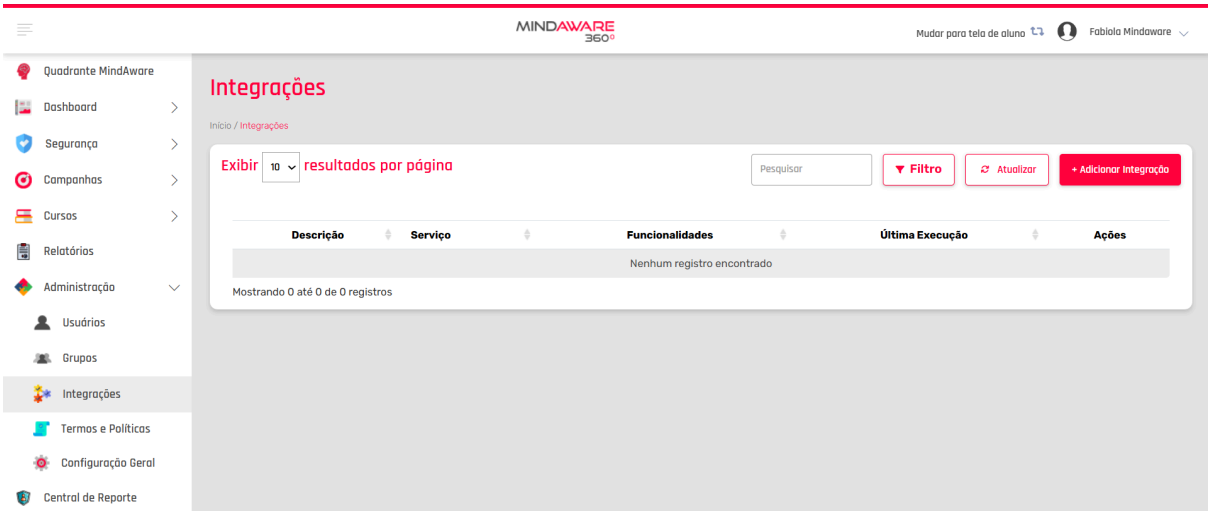


- **<u>Exclusão de Grupos:</u>** Para excluir grupos quando não são mais necessários, basta selecionar o grupo e clicar em Excluir e em seguida confirmar a ação.

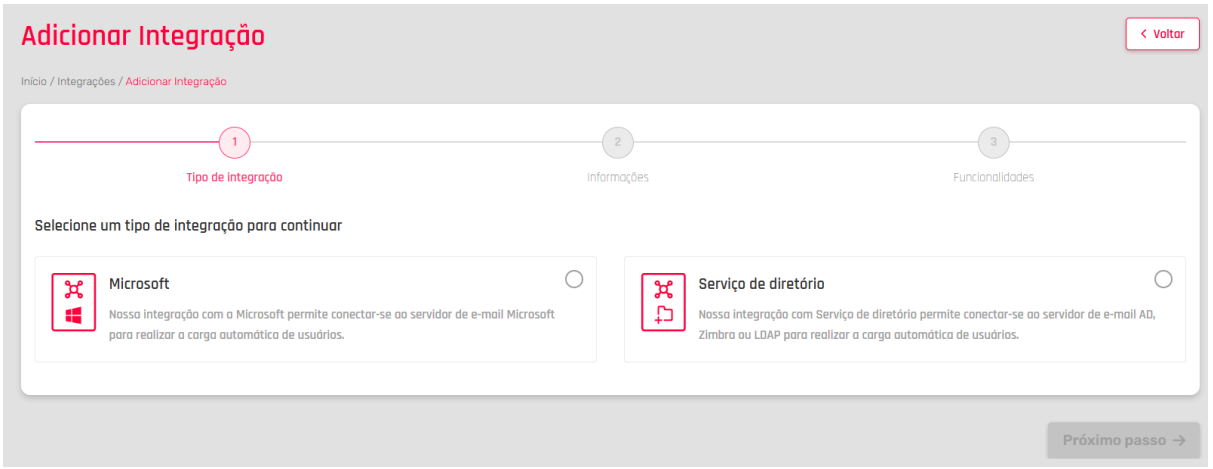


Integrações

A integração com o Mindaware 360° tem como objetivo receber e aplicar automaticamente as alterações realizadas nos cadastros de usuários. Para adicionar uma integração é necessário ir em **Integrações** no menu e ir em "Adicionar uma nova integração".



Após é preciso escolher se a integração vai ser com a Microsoft ou com um Serviço de diretório, como E-mail AD, Zimbra ou LDAP.

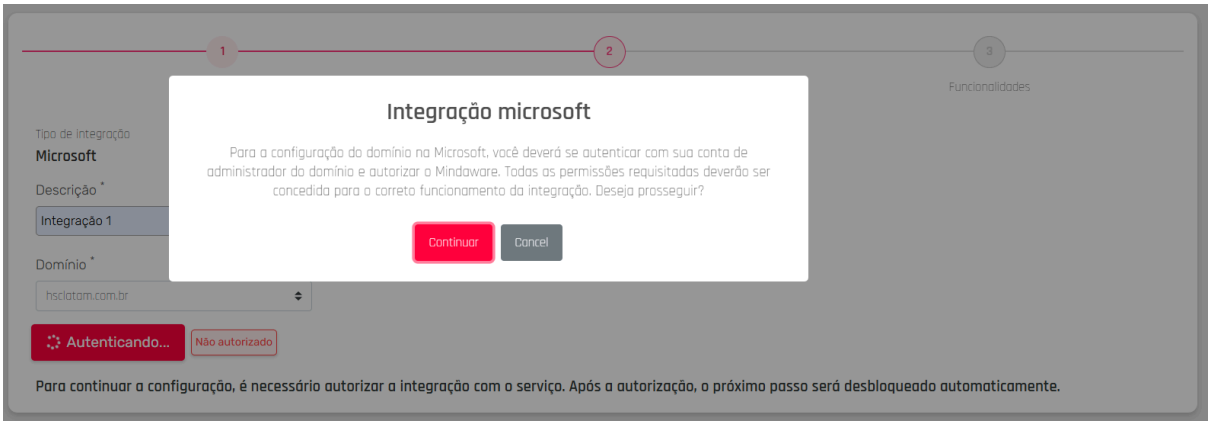


Microsoft

Informações: Ao selecionar a opção **Integrar com a Microsoft**, será exibida uma nova tela solicitando uma descrição da integração e para selecionar um domínio da empresa que será o de integração.



Você deverá autorizar a autenticação da sua conta de administrador do domínio e autorizar o Mindaware.



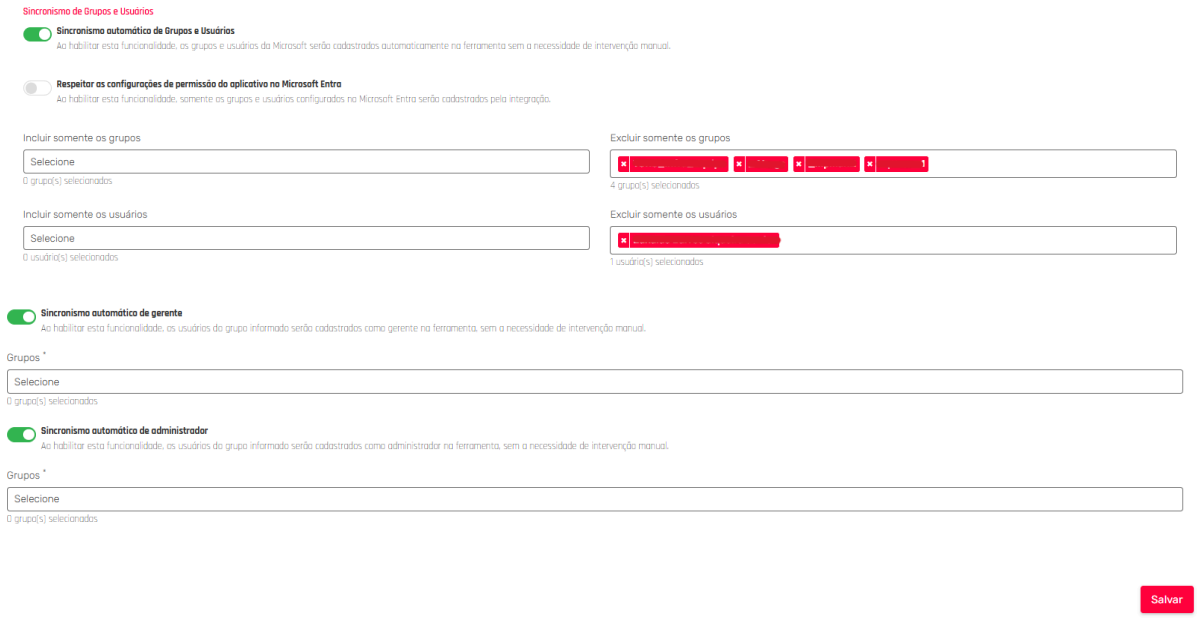
Ao apertar em continuar ele irá autenticar sua conta, e ao concluir passará para próxima tela.

Funcionalidades: Na segunda tela terão as seguinte funcionalidades:

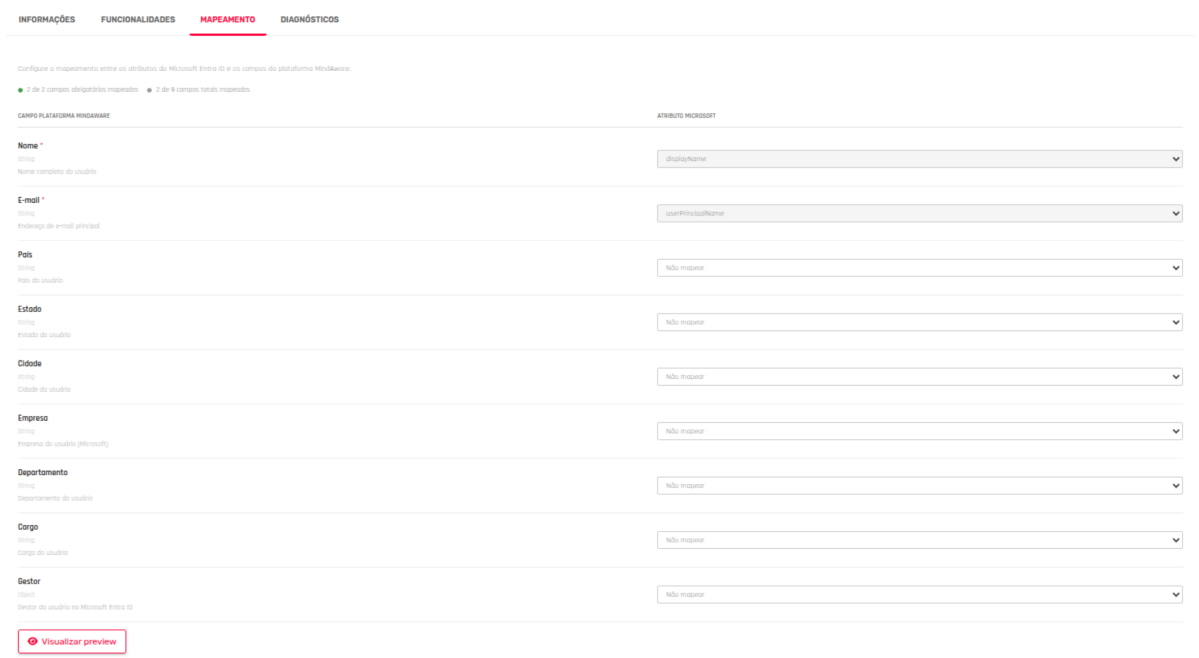
- **Sincronismo automático de Grupos e Usuários:** Ao habilitar esta funcionalidade, os grupos e usuários da Microsoft serão cadastrados automaticamente na ferramenta sem a necessidade de intervenção manual.

- **Respeitar as configurações de permissões do aplicativo no Microsoft entra:** Ao habilitar esta funcionalidade, somente os grupos e usuários configurados no Microsoft Entra serão cadastrados pela integração.
- **Incluir somente os grupos:** Caso a sincronização esteja configurada para incluir todos os usuários, esta opção permite definir grupos cujos membros **não** deverão ser sincronizados. Se o campo for deixado em branco, nenhum grupo será excluído da sincronização.
- **Excluir somente os grupos:** Se estiver configurado para incluir todos os usuários, pode escolher grupos específicos para que os usuários que pertencem aos grupos selecionados não façam parte da sincronização. Se deixar esse campo em branco nenhum usuário será excluído.
- **Incluir somente os usuários:** Permite que você selecione usuários específicos para fazer a sincronização. Se nenhum usuário for selecionado, todos serão incluídos conforme as demais regras de sincronização (como inclusão de grupos).
- **Excluir somente os usuários:** Permite definir usuários que **não** devem ser incluídos na sincronização, mesmo que façam parte de grupos permitidos. Se o campo for deixado em branco, nenhum usuário será excluído.
- **Sincronismo automático de gerente:** Ao habilitar esta funcionalidade, os usuários do grupo informado serão cadastrados como gerente na ferramenta, sem a necessidade de intervenção manual.
- **Sincronismo automático de administrador:** Ao habilitar esta funcionalidade, os usuários do grupo informado serão cadastrados como administrador na ferramenta, sem a necessidade de intervenção manual. Para essa funcionalidade, é necessário ter um grupo na Microsoft apenas com os usuários que serão administradores.

Após definir clique em **Salvar**.



Mapeamento: Nesta tela, é possível definir quais informações do Active Directory / Microsoft Entra ID serão enviadas para o MindAware. Também é possível escolher qual informação será associada a cada campo disponível na plataforma. Após realizar o mapeamento desejado, clique em **Salvar** para aplicar as configurações.



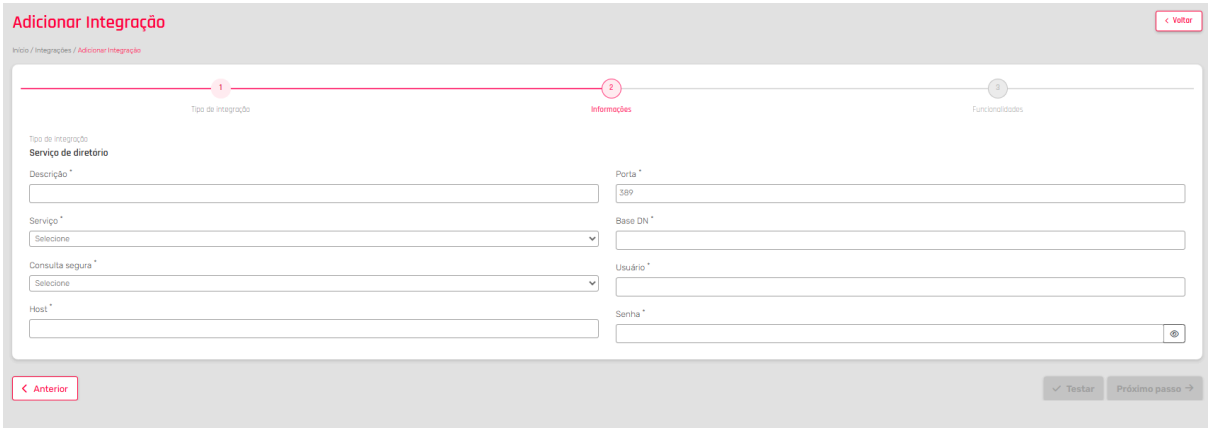
Diagnóstico:

Essa tela permite verificar e diagnosticar a integração com o **Active Directory / Microsoft Entra ID**.

- **Validar Conexão:** verifica se a conexão com o ambiente Microsoft está funcionando corretamente.
- **Listar Grupos:** exibe os grupos disponíveis no ambiente integrado.
- **Membros do Grupo:** permite consultar quais usuários fazem parte de um determinado grupo.
- **Buscar Usuário:** permite localizar um usuário pelo e-mail e visualizar os grupos aos quais ele pertence.

Serviços de diretório

Ao selecionar Serviços de diretório abrirá uma tela pedindo as seguintes informações:

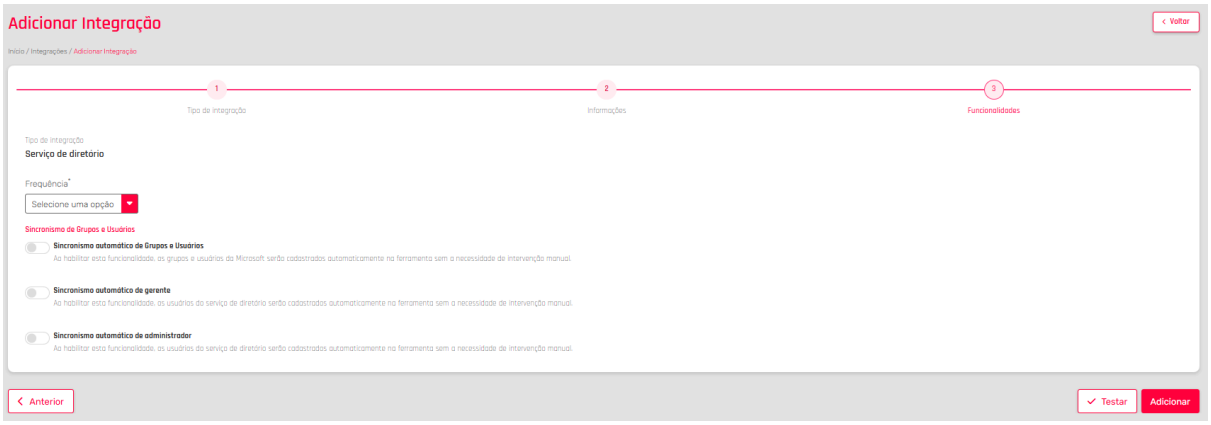


Após preencher e avançar terá algumas funcionalidades para ativar ou não.

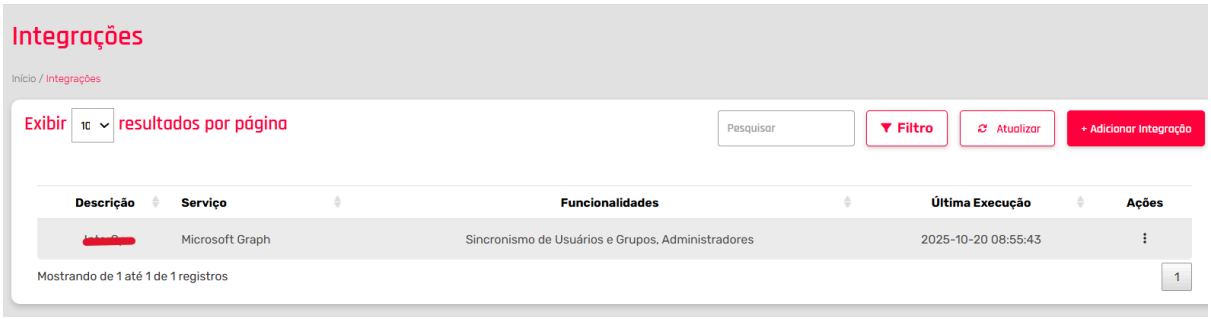
- **Frequência:** Permite configurar o intervalo de tempo entre cada sincronização automática.
- **Sincronismo automático de Grupos e Usuários:** Ao habilitar esta funcionalidade, os grupos e usuários da Microsoft serão cadastrados automaticamente na ferramenta sem a necessidade de intervenção manual.
- **Sincronismo automático de gerente:** Ao habilitar esta funcionalidade, +__os usuários do serviço de diretório serão cadastrados

automaticamente na ferramenta sem a necessidade de intervenção manual.

- **Sincronismo automático de administrador:** Ao habilitar esta funcionalidade, os usuários do serviço de diretório serão cadastrados automaticamente na ferramenta sem a necessidade de intervenção manual.

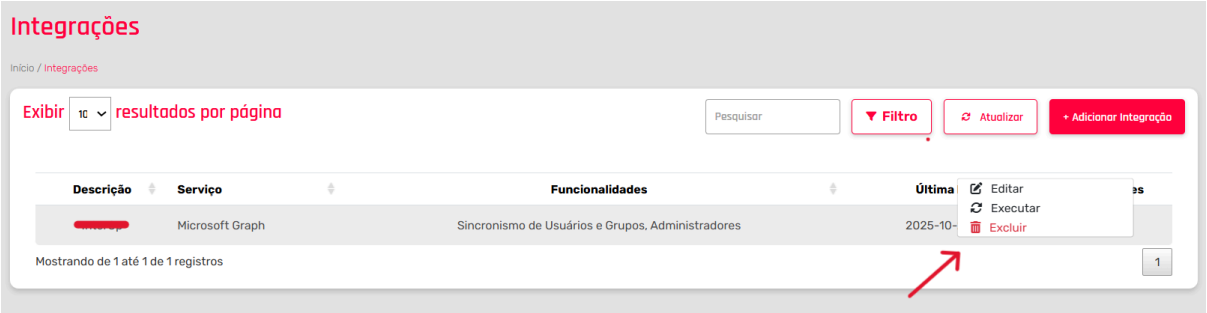


Após definir as funcionalidades clique em Adicionar e será realizada a sincronização.



Ao clicar nos três pontos (menu de ações) ao lado da integração configurada, é possível editar, executar manualmente ou excluir a integração.

- **Editar:** permite alterar as configurações existentes.
- **Executar:** realizar imediatamente uma nova sincronização, sem aguardar o intervalo.
- **Excluir:** remove permanentemente a integração, interrompendo futuras sincronizações automáticas.

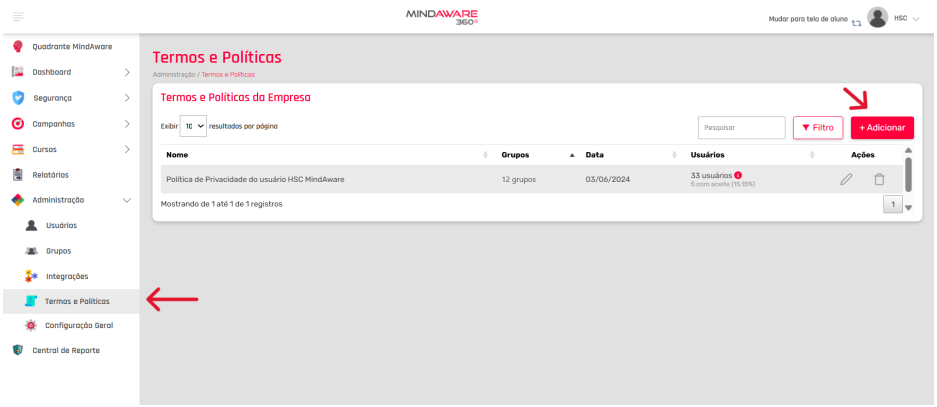

Integrações
Início / Integrações
Exibir 10 resultados por página
Pesquisar
Filtro
Atualizar
+ Adicionar Integração
Descrição
Serviço
Funcionalidades
Última
Microsoft Graph
Sincronismo de Usuários e Grupos, Administradores
2025-10-
Editar
Executar
Excluir
Mostrando de 1 até 1 de 1 registros
1

Termos e Políticas

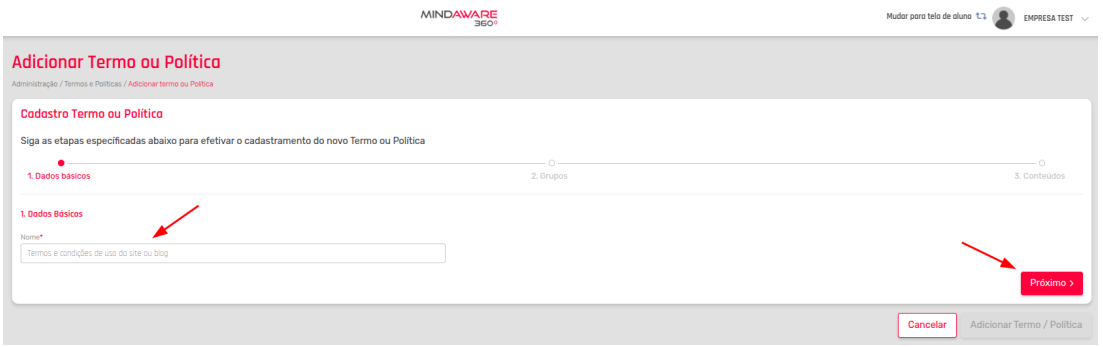
A seção Termos e Políticas foi criada para que a empresa possa informar de forma efetiva, seus colaboradores visando seus processos internos, pois possibilita a documentação do aceite do colaborador, ou seja, a ciência do recebimento de uma documentação. Nesta seção veremos:

- **<u>Cadastro de Termos e Políticas</u>**:
  Para adicionar um Termo ou Política:

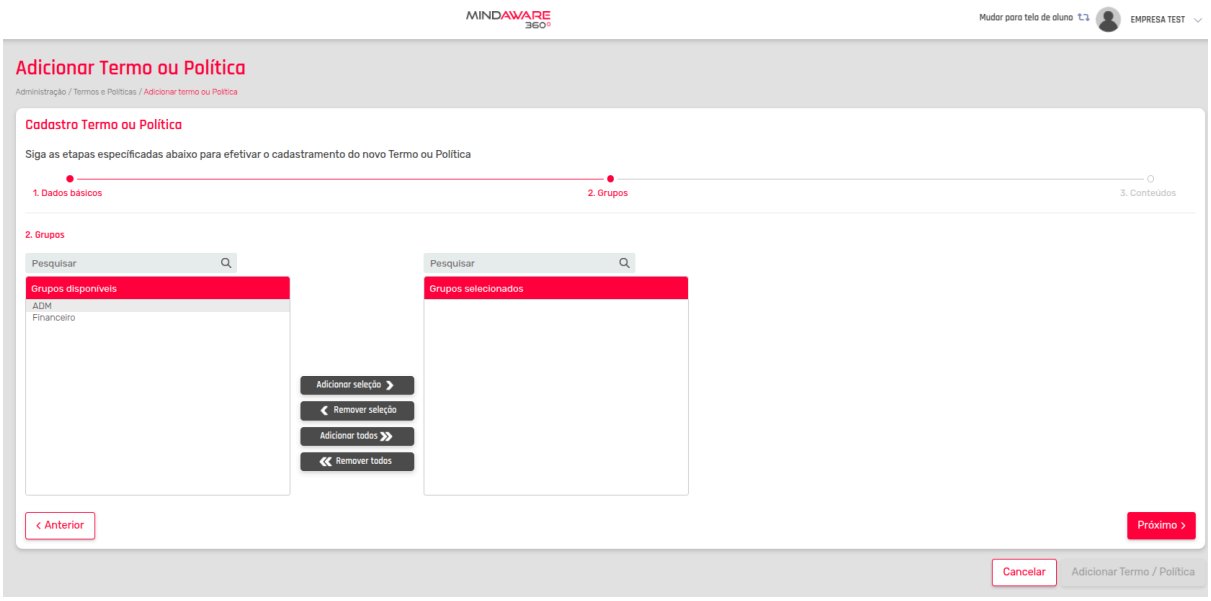
1) Clique no **Menu Administração -> Termos e Políticas** e no **botão Adicionar**.



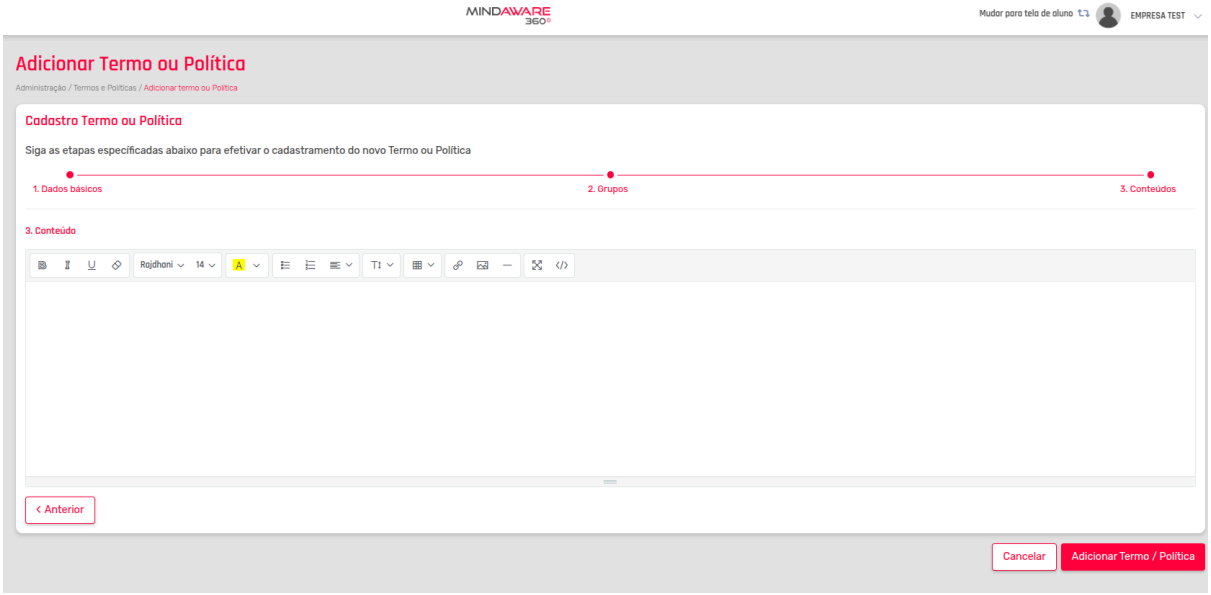
2) Coloque o nome correspondente ao Termo ou Política e após clique no **botão -> Próximo**.



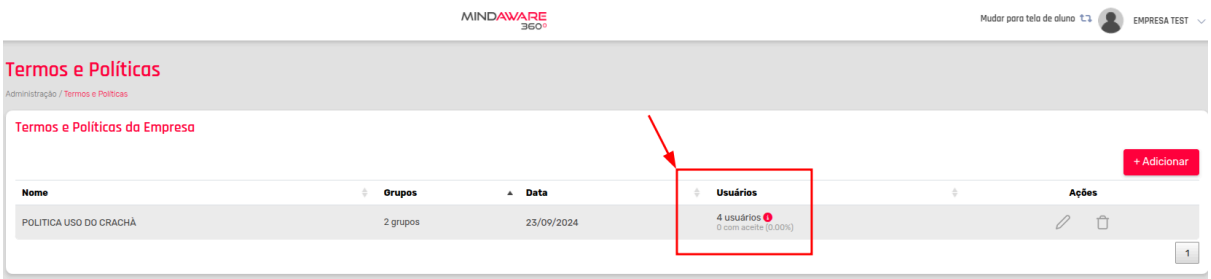
3) Na próxima etapa selecione o(s) grupo(s) que receberão o documento e clique no **botão -> Próximo**.



4) Nesta última etapa, crie o seu documento e clique no **botão -> Adicionar Termo / Política**.

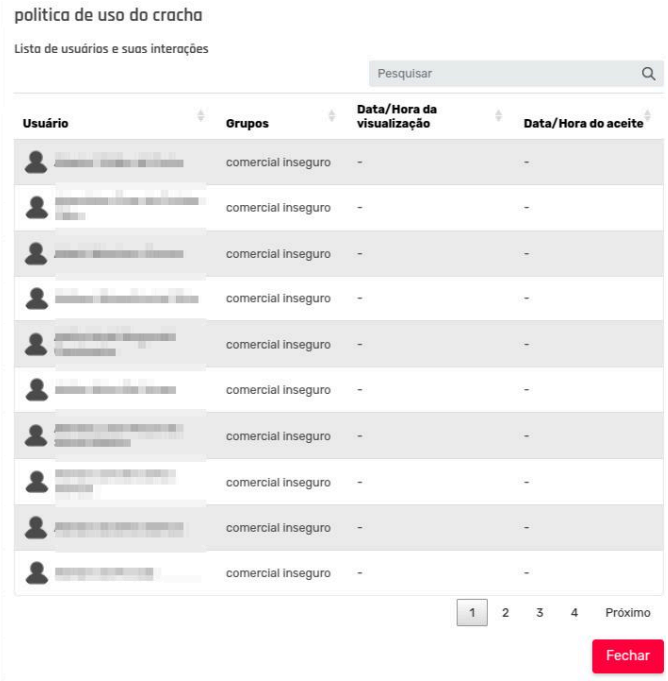


Para visualizar os aceites basta clicar sobre os usuários conforme imagem abaixo:



Serão exibidas a lista de usuários e suas interações em cada Termo ou Política criada, como:

- Nome
- Grupo
- Data e Hora da Visualização
- Data e Hora do Aceite

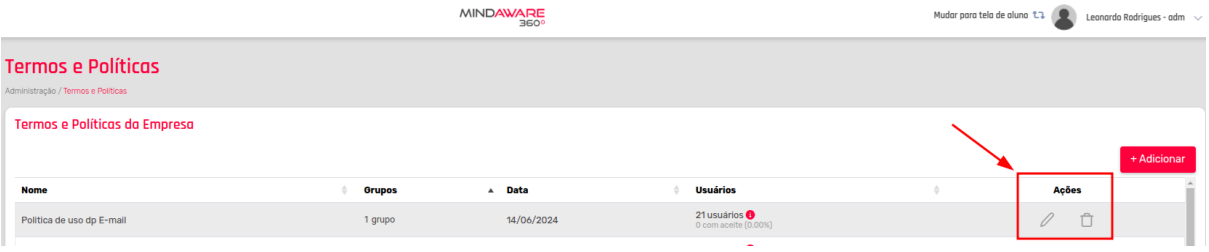


- **<u>Editar termo:</u>**

Para editar um Termo ou Política basta clicar no **ícone do lápis** na linha do Termo ou Política desejado e seguir as etapas igualmente quando se cria.

- **<u>Excluir termo:</u>**

Para excluir um Termo ou Política, basta clicar no ícone da lixeira na linha do Termo ou Política desejada.



Auditoria

A Auditoria permite ao administrador consultar e acompanhar as principais ações realizadas na plataforma, proporcionando maior controle, segurança e rastreabilidade das atividades administrativas e operacionais.

Por meio da **Central de Auditoria**, é possível identificar os usuários responsáveis pelas ações, a data e hora em que ocorreram, o módulo em que foram realizadas e, quando aplicável, quais informações foram modificadas.

Para acessar esta funcionalidade, vá até o menu **Administração → Auditoria**

O acesso às informações de Auditoria respeita as permissões de cada perfil, garantindo que somente usuários autorizados possam visualizar os registros disponíveis de sua empresa.

Central de Auditoria

Na Central de Auditoria, o administrador poderá visualizar o histórico das principais ações realizadas na plataforma.

Os registros são apresentados de forma organizada, permitindo identificar as seguintes informações:

- **Data e Hora:** Indica quando a ação foi realizada.
- **Usuário:** Identifica o responsável pela ação.
- **Empresa:** Apresenta a empresa relacionada ao registro.
- **Módulo:** Identifica em qual área da plataforma a ação foi executada.
- **Ação:** Informa qual operação foi realizada.
- **Registro Afetado:** Identifica o item ou informação relacionada à ação.
- **Resultado:** Apresenta o resultado da operação.
- **Detalhes:** Permite consultar informações complementares sobre a ação realizada.

Essas informações permitem ao administrador acompanhar as atividades da plataforma e identificar eventuais alterações realizadas em seus módulos.



Ações Registradas

A plataforma permite consultar diferentes tipos de ações realizadas pelos usuários, facilitando o acompanhamento das operações administrativas.

Entre as principais ações registradas estão:

- **Criou:** Indica que um novo registro ou configuração foi adicionado à plataforma.
- **Editou:** Indica que uma informação existente foi modificada.
- **Excluiu:** Indica que um registro foi removido da plataforma.

Cada ação fica associada ao usuário responsável, à data e hora da ocorrência e ao módulo em que foi realizada.

Detalhamento das Alterações

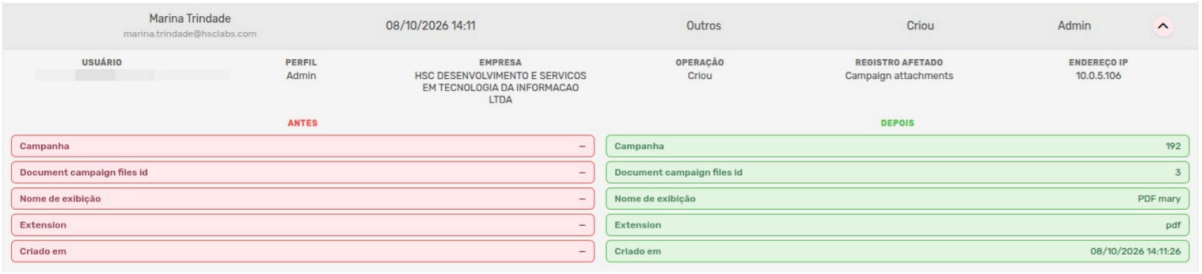
Ao consultar um registro de Auditoria, o administrador poderá visualizar informações adicionais sobre a ação realizada.

Quando houver alterações em informações existentes, a plataforma poderá apresentar os dados anteriores e os novos dados, permitindo identificar exatamente o que foi modificado.

Por exemplo:

- **Antes:** Perfil do usuário = Usuário.
- **Depois:** Perfil do usuário = Gerente.

Essa funcionalidade facilita a identificação de mudanças em cadastros, configurações e outras informações administrativas, permitindo um acompanhamento mais detalhado das operações.



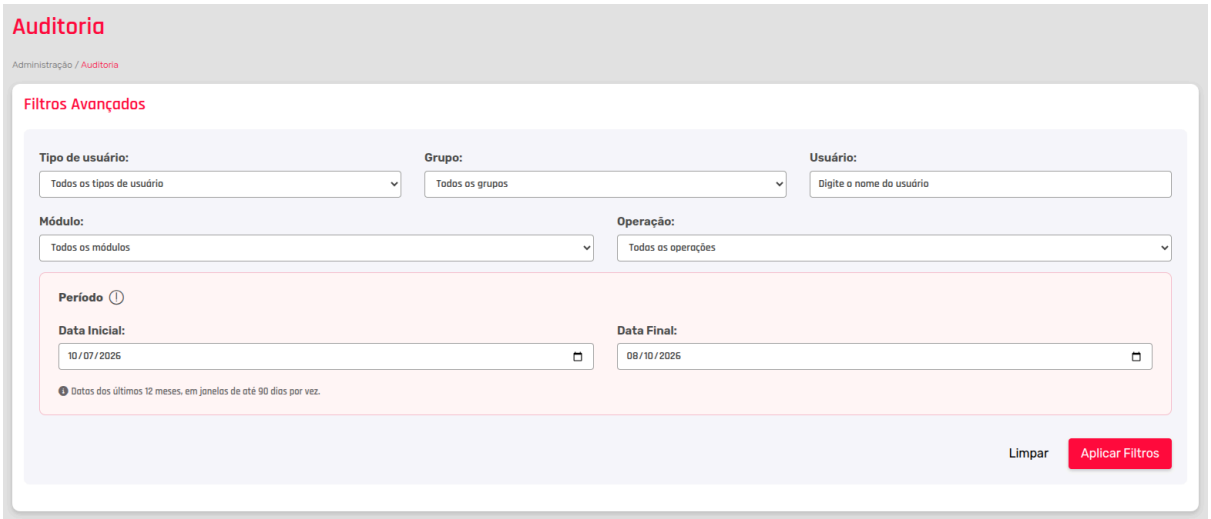
Pesquisa e Filtros

A Central de Auditoria disponibiliza opções de pesquisa e filtros para facilitar a localização dos registros.

O administrador poderá realizar consultas utilizando informações como:

- **Período:** Permite consultar ações realizadas em um intervalo de datas.
- **Módulo:** Permite selecionar a área da plataforma que deseja consultar.
- **Usuário:** Permite localizar ações realizadas por determinado usuário.
- **Ação:** Permite filtrar os registros pelo tipo de operação realizada.
- **Resultado:** Permite consultar os registros conforme o resultado da operação.

Após selecionar os filtros desejados, a plataforma apresentará os registros correspondentes, respeitando as permissões de acesso do usuário.



Módulos Auditados

A Auditoria permite acompanhar ações realizadas nas principais funcionalidades administrativas do MindAware 360°.

Entre os módulos que possuem registros de Auditoria estão:

- **Usuários e Grupos:** Acompanhamento de ações relacionadas aos cadastros e alterações de usuários e grupos.
- **Campanhas:** Registro das principais ações realizadas no gerenciamento das campanhas.
- **Cursos:** Acompanhamento de alterações relacionadas aos cursos da plataforma.
- **Integrações:** Registro de ações realizadas nas configurações e no gerenciamento das integrações.
- **Termos e Políticas:** Acompanhamento das alterações realizadas nos termos e políticas cadastrados.
- **Configurações:** Registro das principais alterações nas configurações administrativas.
- **Ranking:** Acompanhamento de ações relacionadas às configurações do Ranking.
- **Central de Reportes:** Registro das ações relacionadas às funcionalidades de reporte disponíveis na plataforma.

Os registros são associados aos respectivos módulos, facilitando a identificação e a consulta das operações realizadas.

Exportação dos Registros

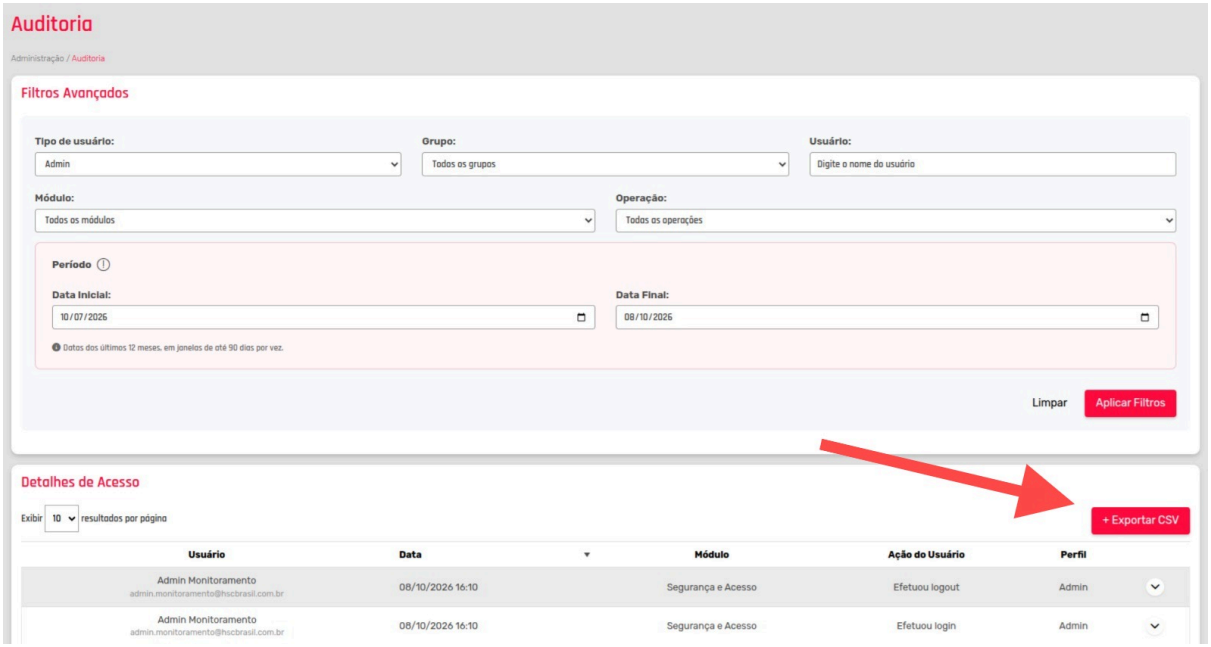
A Central de Auditoria também permite exportar os registros disponíveis, conforme as opções disponibilizadas pela plataforma.

Para realizar a exportação, o administrador deverá selecionar os filtros desejados e utilizar a opção de exportação disponível na tela.

Os dados exportados considerarão:

- O período selecionado.
- Os filtros aplicados na consulta.
- A empresa relacionada ao usuário.
- As permissões de acesso do perfil.

Essa funcionalidade permite utilizar os registros em processos de acompanhamento administrativo, análises de segurança e atividades de conformidade.



Perfis de Permissões

A funcionalidade **Perfis de Permissões** do MindAware 360° permite ao administrador configurar e gerenciar os acessos administrativos da plataforma, definindo quais módulos, funcionalidades e ações estarão disponíveis para os usuários com perfil de Gerente e Administrador.

Por meio dessa funcionalidade, é possível criar perfis personalizados de permissões e associá-los aos usuários conforme suas funções e responsabilidades dentro da organização.

Essa configuração proporciona maior controle sobre os acessos à plataforma, permitindo que cada usuário utilize somente as funcionalidades necessárias para suas atividades.

Para acessar esta funcionalidade, vá até o menu **Administração → Perfis de Permissões**.



Tipos de Usuário

A plataforma MindAware 360° possui três tipos de usuários, cada um com características e níveis de acesso específicos.

- **Usuário:** Possui acesso às funcionalidades disponíveis na Home, como cursos, termos e políticas, campanhas educacionais, campanhas de phishing simulado e Central de Reporte. Esse tipo de usuário não utiliza Perfis de Permissões administrativas.
- **Gerente:** Possui acesso às funcionalidades administrativas disponibilizadas para o seu tipo de usuário, incluindo os Dashboards de Quadrante, Educacional e Comportamental dos grupos sob sua responsabilidade. Quando um Perfil de Permissões personalizado é

associado, o Gerente passa a utilizar as funcionalidades autorizadas pelo perfil, mantendo o acesso restrito aos grupos que gerencia.

- **Administrador:** Possui acesso às funcionalidades administrativas da plataforma conforme o perfil associado. Quando não possui um perfil personalizado, utiliza o Administrador Padrão. Ao receber um perfil específico, passa a acessar somente os módulos e ações autorizados por esse perfil.

Central de Perfis de Permissões

No menu Perfis de Permissões, o administrador poderá visualizar e gerenciar os perfis cadastrados na plataforma.

Nesta tela, são apresentadas informações como:

- **Nome:** Identifica o Perfil de Permissões cadastrado.
- **Descrição:** Apresenta as informações sobre a finalidade do perfil.
- **Tipo:** Identifica se o perfil pertence ao tipo Gerente ou Administrador.
- **Usuários Associados:** Apresenta a quantidade de usuários vinculados ao perfil.
- **Status:** Indica se o perfil está ativo ou desativado.
- **Data de Criação:** Informa quando o perfil foi cadastrado.
- **Ações:** Permite visualizar, editar e realizar outras operações disponíveis para o perfil.

A plataforma também disponibiliza opções de pesquisa simples e avançada, permitindo localizar perfis por nome, tipo, status e data de criação.



Criação de Perfil de Permissões

Para criar um novo Perfil de Permissões, acesse o **Perfis de Permissões** e clique no botão **Novo Perfil**.

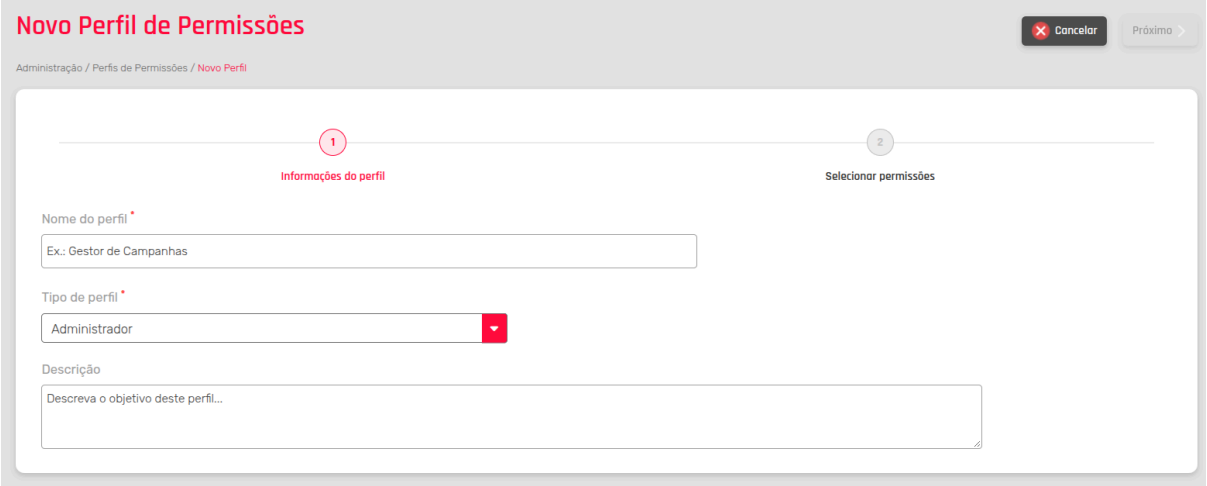
O cadastro será realizado em duas etapas:

1. Informações do Perfil

Nesta etapa, o administrador deverá preencher as informações de identificação do perfil:

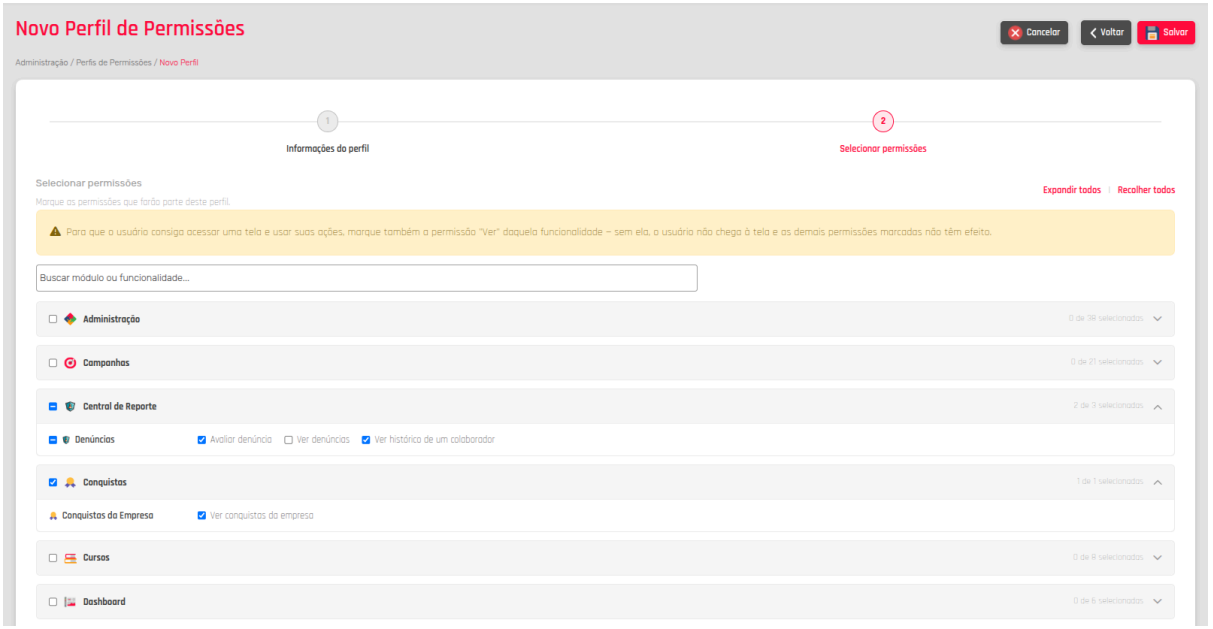
- **Nome:** Informe um nome para identificar o Perfil de Permissões.
- **Tipo:** Selecione se o perfil será destinado aos usuários Gerente ou Administrador.
- **Descrição:** Informe a finalidade do perfil e quais responsabilidades serão atribuídas aos usuários que o utilizarão.

O tipo selecionado determinará para quais usuários o perfil poderá ser disponibilizado.



2. Selecionar Permissões

Nesta etapa, o administrador poderá selecionar os módulos, funcionalidades e ações que estarão disponíveis para os usuários associados ao perfil.



As permissões são organizadas por áreas da plataforma, facilitando a identificação e seleção dos acessos desejados.

Após configurar as permissões necessárias, conclua o cadastro para disponibilizar o novo perfil.

Configuração das Permissões

A plataforma permite configurar as permissões de acordo com as funcionalidades disponíveis em cada módulo.

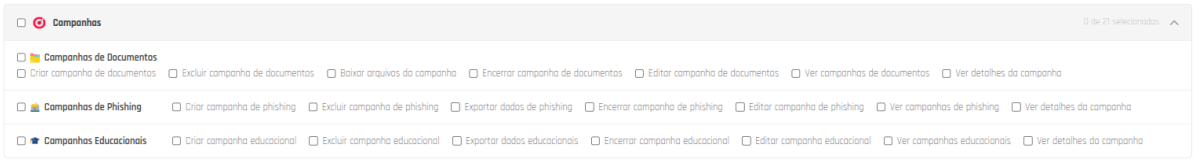
Entre os módulos que podem ser configurados estão:

- Administração.
- Campanhas.
- Central de Reporte.
- Conquistas.
- Cursos.
- Dashboard.
- Métricas.
- Ranking.
- Relatórios.

Cada módulo poderá apresentar diferentes permissões, de acordo com as ações disponíveis na funcionalidade.

Entre as principais permissões estão:

- **Ver:** Permite acessar e visualizar a funcionalidade.
- **Criar:** Permite cadastrar novos registros.
- **Editar:** Permite modificar informações existentes.
- **Excluir:** Permite remover registros.
- **Exportar:** Permite realizar a exportação de informações.
- **Encerrar:** Permite finalizar operações nas funcionalidades que disponibilizam essa ação.
- **Ver Detalhes:** Permite consultar informações detalhadas dos registros.



Importante: Para que o usuário consiga acessar uma funcionalidade e executar suas ações, é necessário que a permissão **Ver** esteja habilitada.

Caso essa permissão não esteja selecionada, o usuário não poderá acessar a funcionalidade, mesmo que outras ações estejam autorizadas no perfil.

Gerenciamento dos Perfis

Após a criação, os Perfis de Permissões poderão ser administrados por meio das ações disponíveis na listagem.

Entre as opções estão:

- **Ver Detalhes:** Permite consultar as informações do perfil e todas as permissões configuradas.
- **Duplicar:** Permite criar um novo Perfil de Permissões utilizando as configurações de um perfil existente como base.
- **Editar:** Permite alterar as informações e permissões de um perfil cadastrado.
- **Desativar:** Permite tornar um perfil indisponível, conforme as regras da plataforma.
- **Excluir:** Permite remover um perfil quando essa operação estiver disponível.



Essas funcionalidades facilitam a manutenção dos acessos administrativos e permitem adequar as permissões conforme as necessidades da organização.

Associação do Perfil ao Usuário

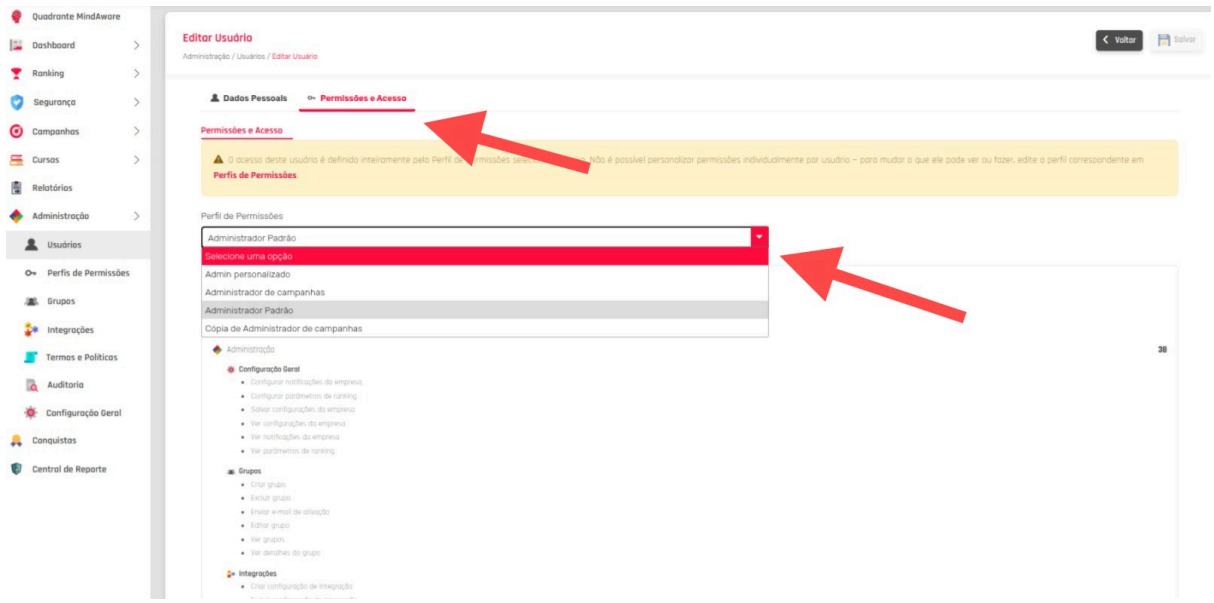
Após criar um Perfil de Permissões, o administrador poderá associá-lo aos usuários cadastrados na plataforma.

Para realizar essa configuração, acesse **Administração → Usuários → Adicionar/Editar Usuário → Permissões e Acesso**.

Nesta opção, será possível selecionar um Perfil de Permissões compatível com o tipo de usuário.

- **Gerente:** Poderá receber Perfis de Permissões cadastrados para o tipo Gerente.
- **Administrador:** Poderá receber Perfis de Permissões cadastrados para o tipo Administrador.

As permissões são definidas diretamente no perfil e não individualmente no cadastro do usuário.



Caso seja necessário modificar os acessos de um usuário, o administrador poderá editar as permissões do perfil associado ou selecionar outro perfil compatível.

Permissões de Acesso do Gerente

Os Perfis de Permissões também permitem definir quais funcionalidades estarão disponíveis para os usuários do tipo Gerente.

Entretanto, mesmo quando um perfil disponibiliza permissões adicionais, o Gerente continuará tendo acesso somente às informações relacionadas aos grupos sob sua responsabilidade.

Por exemplo, caso um Gerente possua permissão para visualizar campanhas, dashboards ou informações de usuários, os dados apresentados estarão limitados aos grupos dos quais ele é gerente.

Essa configuração garante que as permissões administrativas sejam aplicadas sem ampliar o acesso às informações de outros grupos da organização.

Permissões Relacionadas aos Grupos

Algumas funcionalidades da plataforma utilizam informações relacionadas aos grupos de usuários.

Para permitir o acesso a essas funcionalidades, o Perfil de Permissões deverá possuir as permissões necessárias no módulo **Grupos**.

Entre elas estão:

- **Ver grupos:** Permite acessar informações relacionadas aos grupos.
- **Ver Detalhes:** Permite consultar informações detalhadas dos grupos, quando exigido pela funcionalidade.

Para usuários do tipo Gerente, essas permissões continuarão respeitando os grupos sob sua responsabilidade.

Perfis Padrão do Sistema

O MindAware 360° possui Perfis de Permissões padrão para os tipos Gerente e Administrador.

Esses perfis são disponibilizados pela plataforma e representam os conjuntos de permissões definidos para cada tipo de usuário.

Gerente Padrão

Possui as permissões administrativas padrão destinadas aos usuários do tipo Gerente, mantendo o acesso restrito aos dados dos grupos sob sua responsabilidade.

Administrador Padrão

Possui o conjunto padrão de permissões administrativas da plataforma, permitindo o gerenciamento das funcionalidades disponíveis para o tipo Administrador.

Além dos perfis padrão, o administrador poderá criar novos Perfis de Permissões personalizados, de acordo com as necessidades da organização, sem alterar as definições dos perfis padrão do sistema.

Menu Cursos

A partir das métricas obtidas nas campanhas de comportamento, e com base na metodologia aplicada na estratégia de uma campanha comportamental, o próximo passo é dar continuidade ao processo educacional dos colaboradores.

Nesta etapa, o foco é promover a conscientização por meio dos treinamentos disponíveis na plataforma, ou ainda, pela aplicação de Cursos Customizados desenvolvidos conforme as necessidades da empresa.

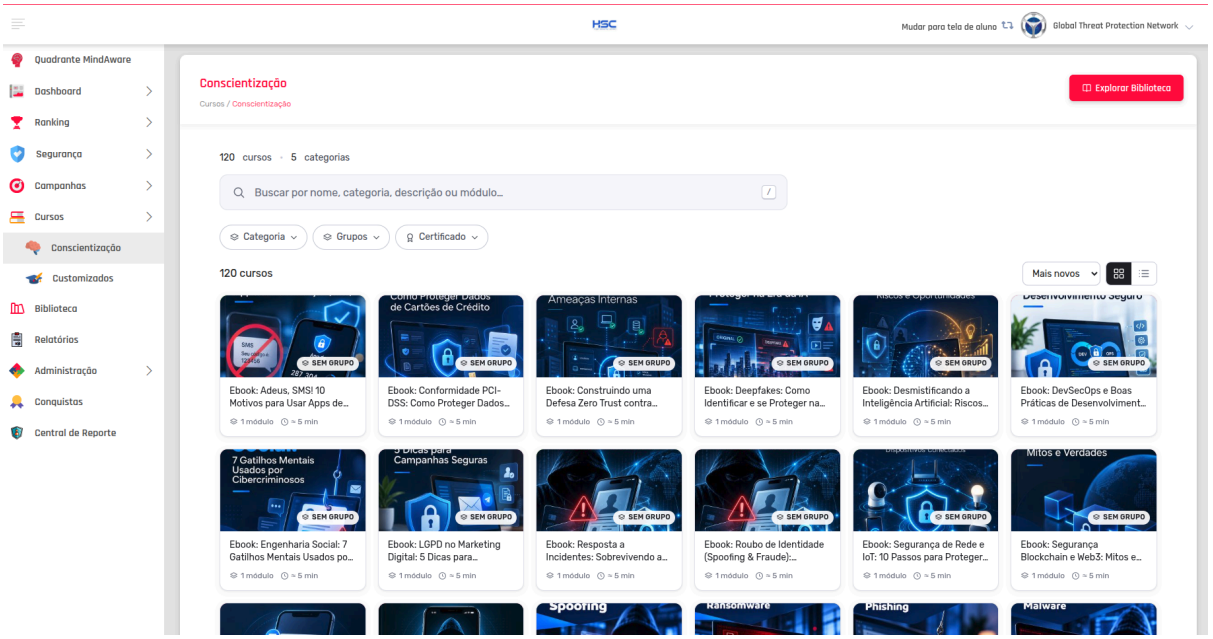
Além disso, a plataforma oferece uma trilha de formação completa — do Essencial ao Profissional — permitindo validar de forma progressiva o conhecimento do usuário. Ao concluir os módulos e alcançar a média mínima de 60% (podendo esta ser configurada conforme necessidade do cliente) de acertos nas avaliações, o colaborador é automaticamente certificado, reforçando seu aprendizado e evolução contínua dentro do programa.

A plataforma também envia diariamente um e-mail aos usuários notificando caso possuam cursos pendentes ou indisponíveis.

Cursos da Plataforma

A plataforma MindAware 360 disponibiliza cursos que vão desde o nível básico ao avançado, incluindo boas práticas e uma biblioteca de conteúdos prontos para iniciar os treinamentos e campanhas de conscientização dos colaboradores da sua empresa. São diversos cursos que podem ser enviados para as equipes de cada departamento, bastando marcar o grupo correspondente para que o conteúdo fique visível na área do colaborador. Todos os vídeos são dublados e legendados em português (Brasil) e no formato MP4 com alta resolução.

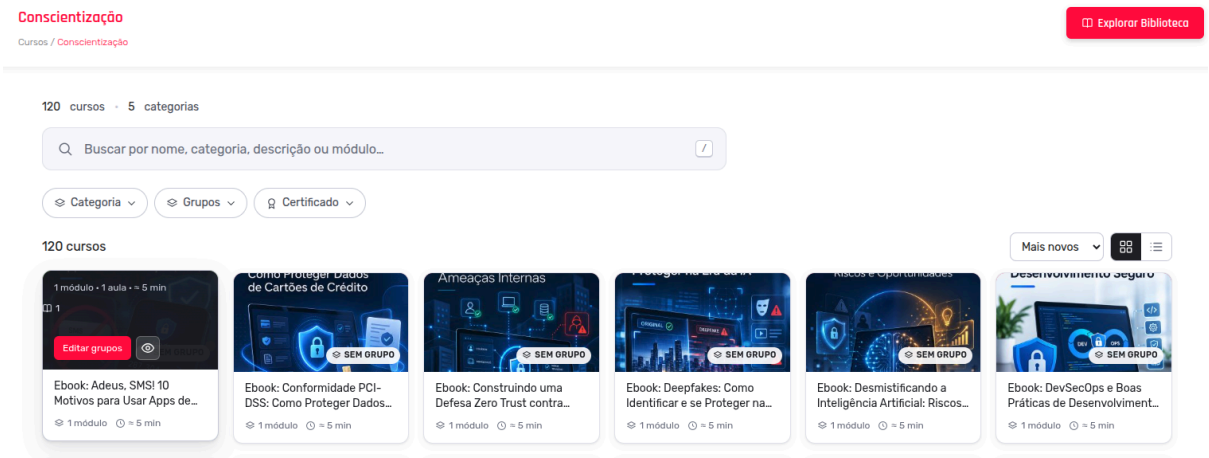
Além disso, a plataforma conta com uma formação completa — do Essencial ao Profissional — permitindo validar o conhecimento do usuário por meio de avaliações estruturadas. Ao atingir a média mínima de 60% de respostas corretas, o colaborador é automaticamente certificado, garantindo reconhecimento formal de sua evolução no programa.



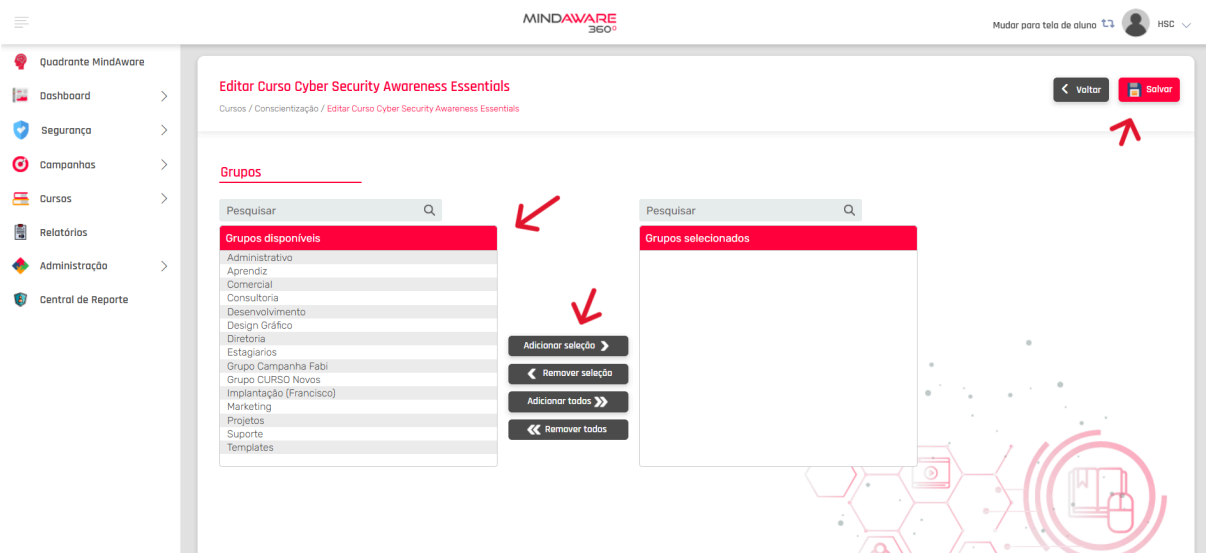
- **<u>Direcionar Cursos para Grupos de Usuários</u>:**

  Para configurar cursos específicos para grupos de usuários selecionados, siga os passos abaixo:

  1) Coloque o cursor em cima do curso escolhido
  2) Clique em “Editar grupos”



  3) Selecione o(s) grupo(s) que realizarão o curso e clique em -> Salvar:

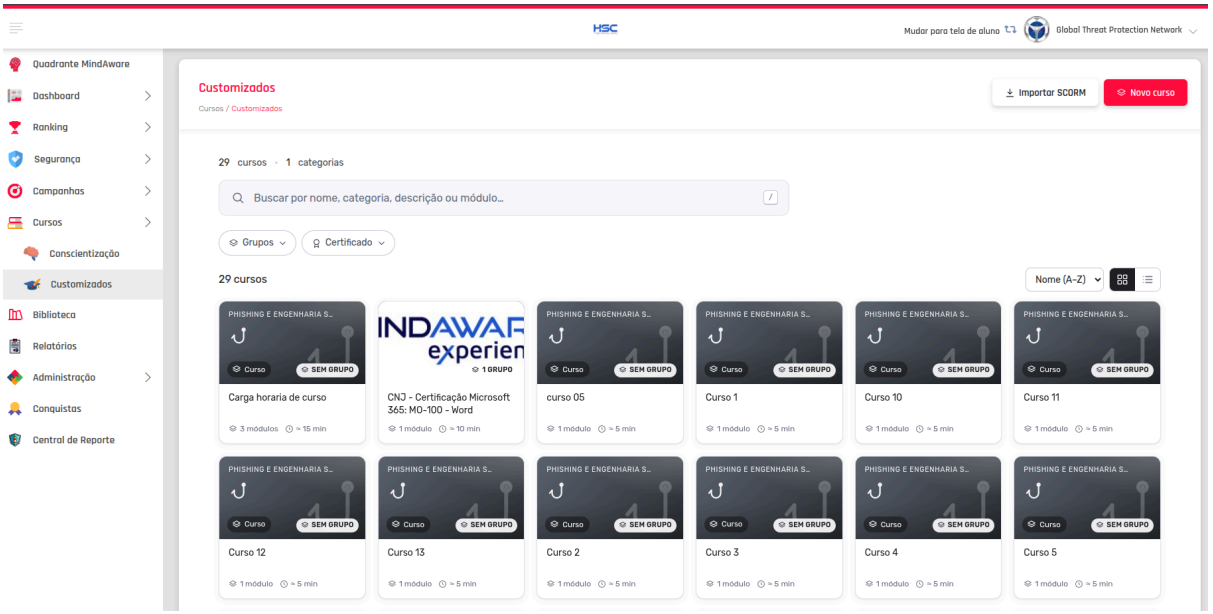


Cursos Customizados

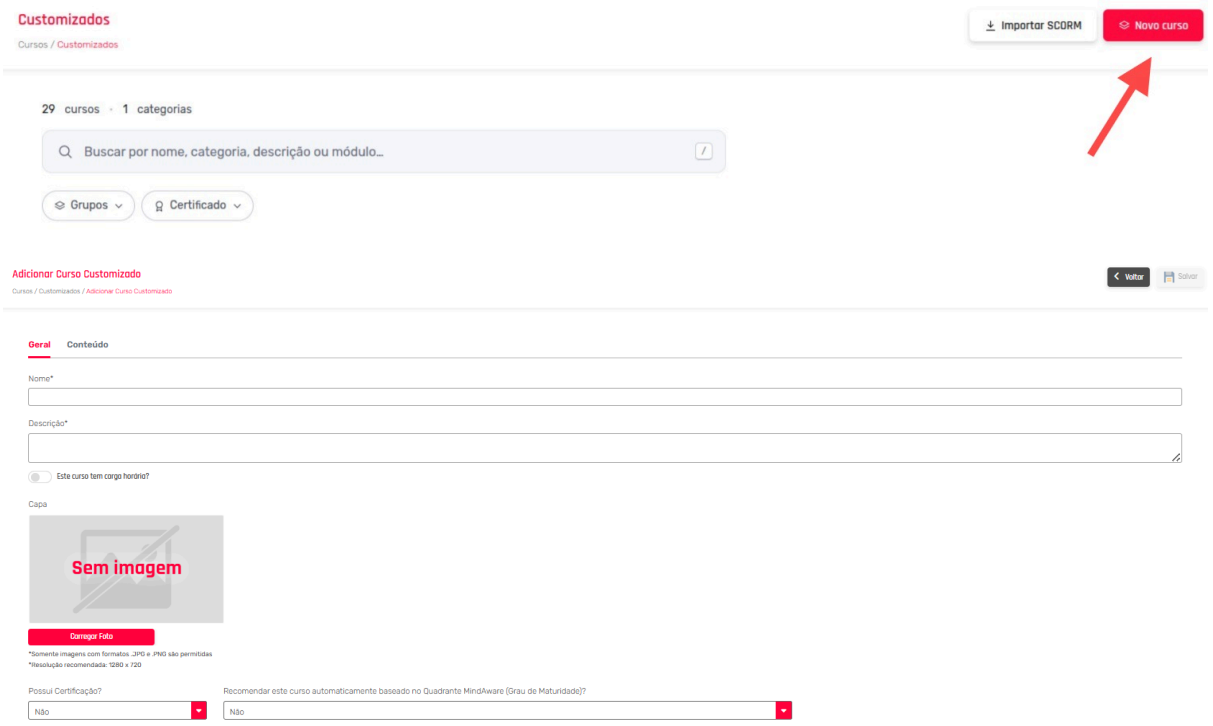
Nesta seção, é possível criar diversos treinamentos, como, por exemplo, um curso específico, o reforço de uma política da empresa, funções de um departamento ou até mesmo uma certificação.

- **<u>Como Criar um Curso Customizado:</u>**

Acessando o menu **Cursos -> Cursos Customizados**, a plataforma possibilita criar qualquer curso de forma customizada com certificação, contendo variados tipos de conteúdos, tais como: Questões dissertativas, objetivas, inclusões de vídeos, imagens, Jogos, Textos HTML e Documentos diversos.

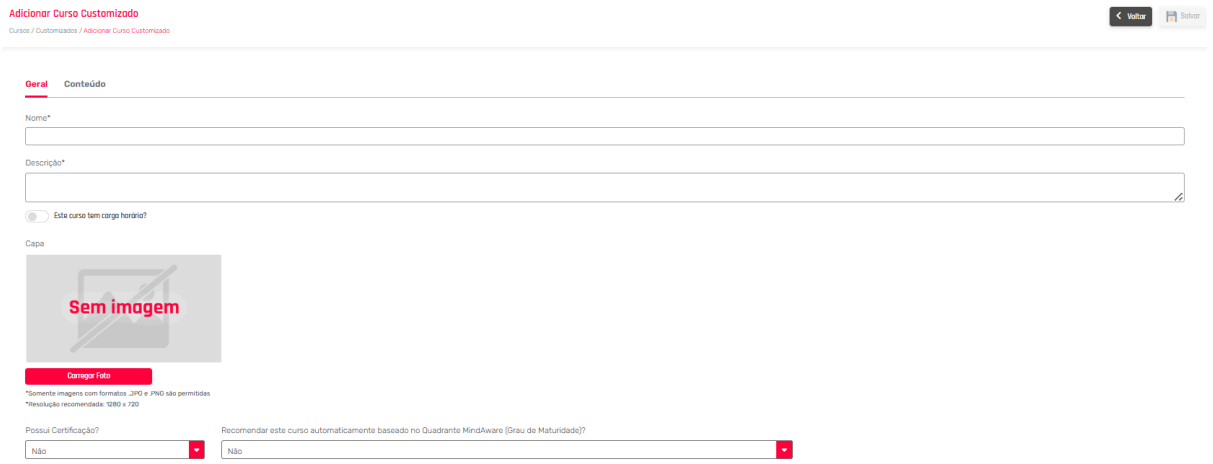


1) Para criar um um curso customizado basta clicar no botão **Adicionar** e preencher os campos conforme imagem abaixo:



2) Escolha um nome para o curso e, se desejar, preencha também a descrição e selecione uma foto de capa. Você pode definir se o curso oferecerá certificação — nesse caso, uma etapa extra será exibida para criação da prova e exportação do certificado. Além disso, é possível

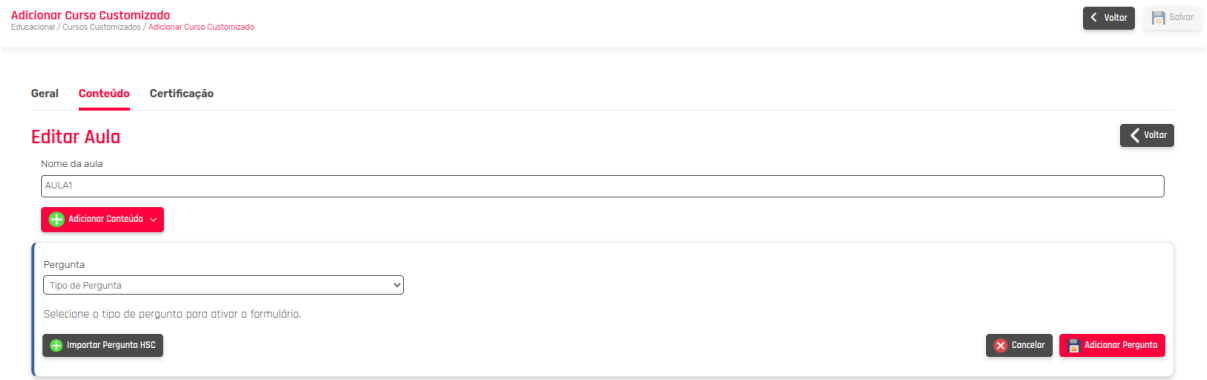
indicar se o curso será recomendado para alunos de um quadrante específico e, se sim, qual deles.



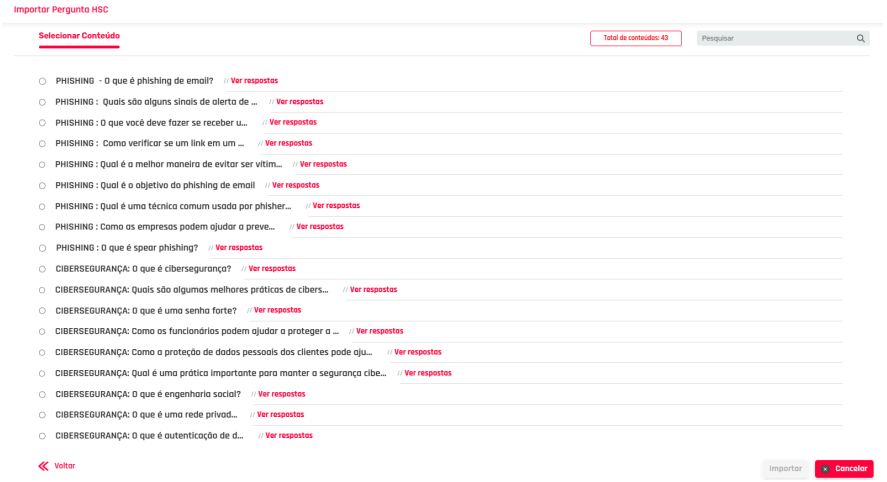
3) Após preencher os campos e selecionar as opções, clique em Conteúdo e comece a adicionar as aulas criando seus respectivos conteúdos utilizando o botão - > **Adicionar Conteúdo**.



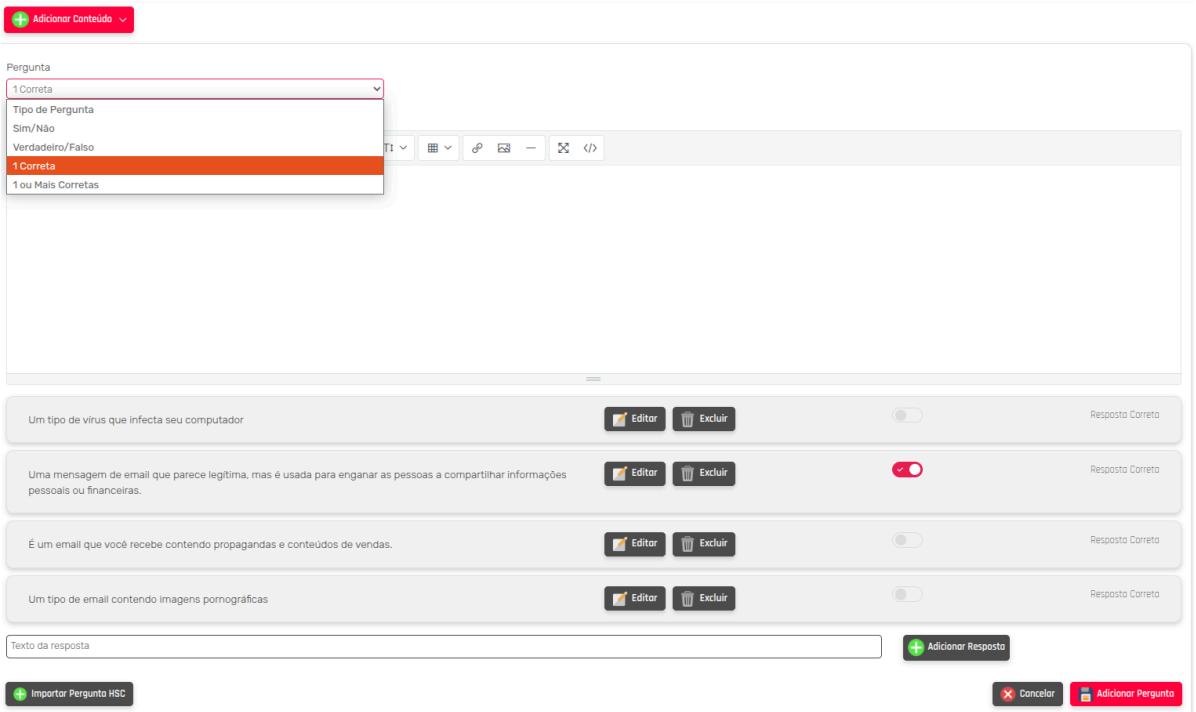
4) Como por exemplo, vamos adicionar uma pergunta que poderá ser importada dos conteúdos já existentes na biblioteca de conteúdos da HSC ou importar uma outra qualquer.



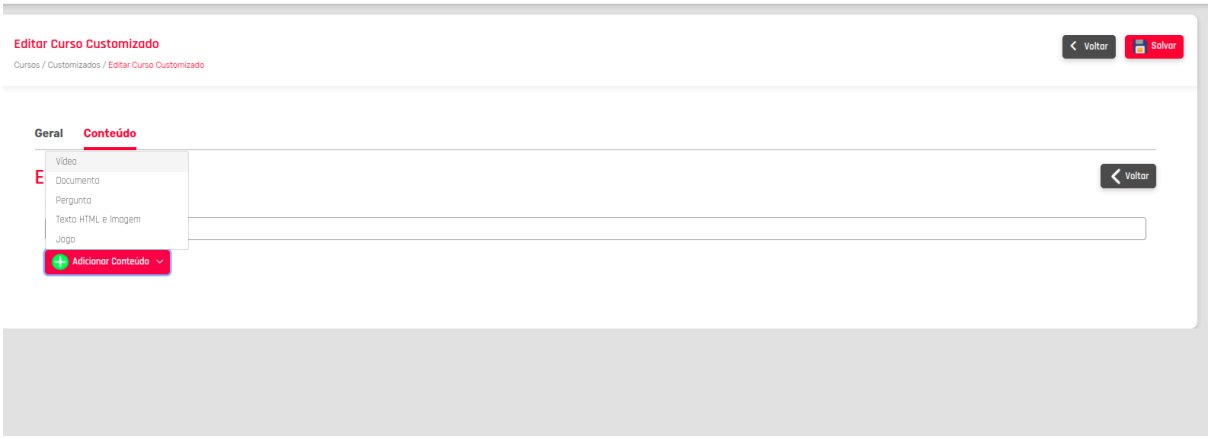
5) Na biblioteca de conteúdo da HSC existe uma lista com diversas questões, inclusive com suas respectivas respostas:



6) Ao importar uma pergunta da biblioteca de conteúdo da HSC, já irá carregar as respostas e pode-se optar pelo tipo de questão, no exemplo conforme abaixo será uma questão de múltipla escolha com apenas uma correta. Após isso, basta clicar no botão -> Adicionar Pergunta.



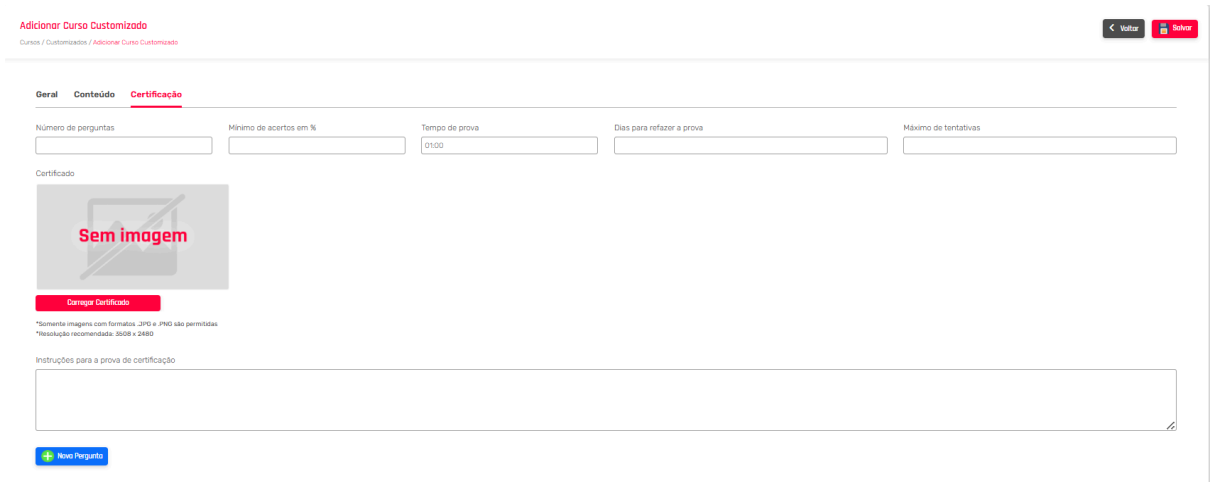
Dentre as opções de formato de conteúdo temos: Vídeos (formatos MP4; AVI; MOV; ou WMV), documentos, pergunta, Textos HTML, Jogos.



Após adicionar todas as aulas desejadas, clique no botão **Salvar**. Se o curso **não tiver certificação**, ele estará pronto para ser vinculado a grupos ou campanhas educacionais.

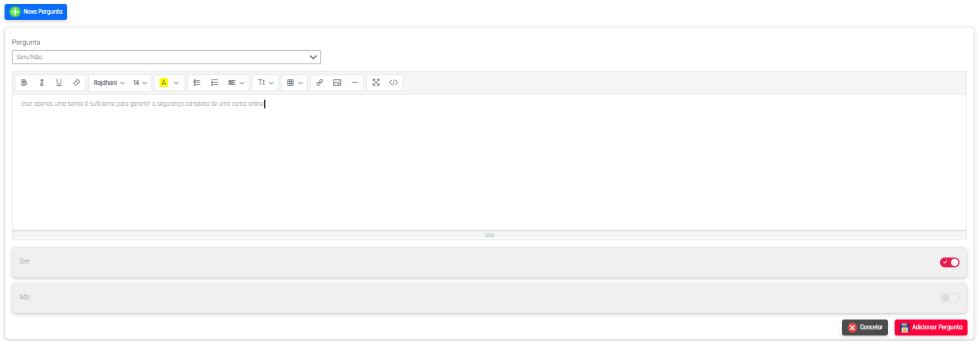
Caso tenha optado por incluir **certificação**, você será direcionado automaticamente para a próxima etapa, onde poderá configurar a prova e o certificado.

7) Nessa etapa, defina os parâmetros da prova: escolha o número de perguntas, a porcentagem mínima de acertos necessária para aprovação, o tempo disponível para realização da prova, o intervalo (em dias) para uma nova tentativa e o número máximo de tentativas permitidas por usuário.



8) Em seguida, exporte o certificado apertando em **Carregar Certificado.**
9) Na etapa da prova, você poderá escrever instruções para o usuário.
10) Clique em **Nova Pergunta**, selecione o **tipo de pergunta** desejado e escreva o enunciado. Defina também as **opções de resposta** e marque

qual delas será considerada **correta**. Aperte em **Adicionar Pergunta** para salvar.

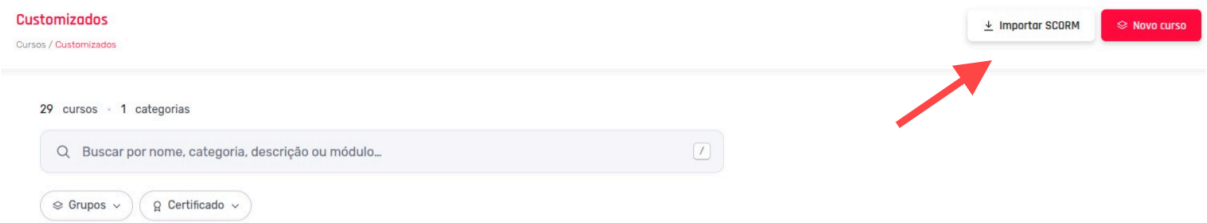


11) Após ter adicionado todas as perguntas, aperte em **Salvar** e seu curso estará pronto para ser direcionado ao grupo de usuários.

- **<u>Como Criar um Curso Customizado formato SCORM</u>**

Também é possível criar um curso importando através do formato **SCORM.**

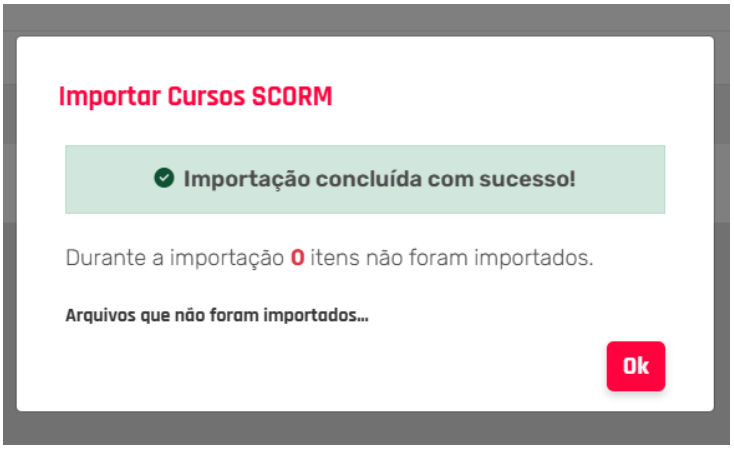
Na tela inicial de Cursos Customizados, clique em “Importar”.



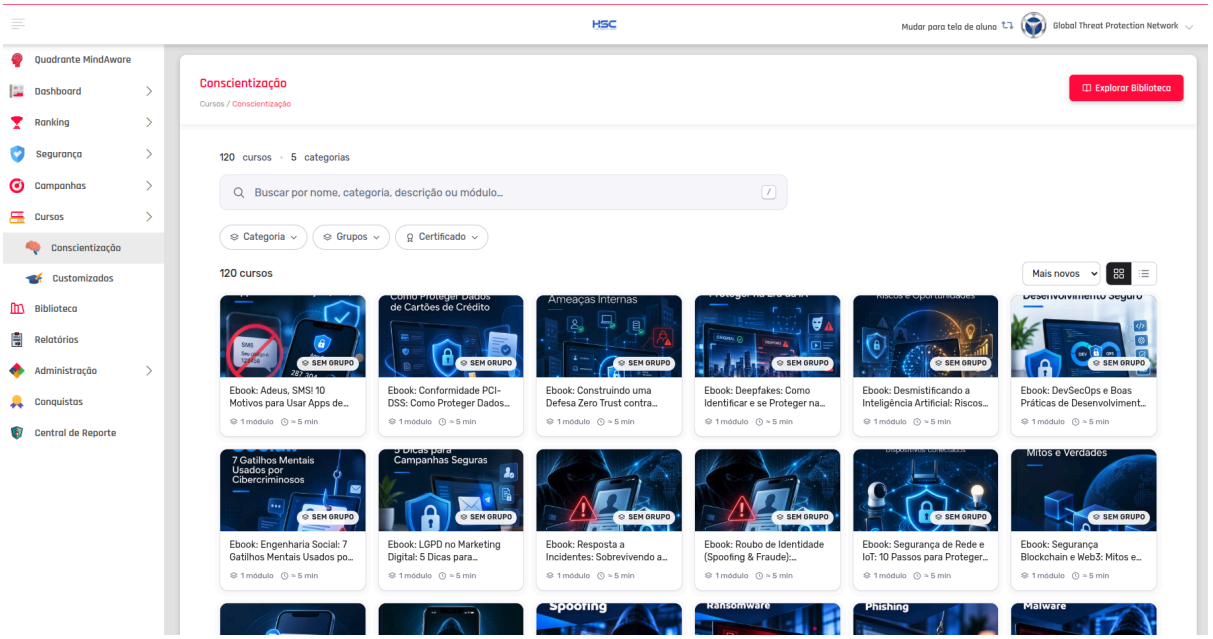
Aparecerá uma janela, aperte em “Escolher Arquivo”, escolha o arquivo desejado e depois vá em “Importar”.



Mostrará essa tela após e o curso já estará criado.



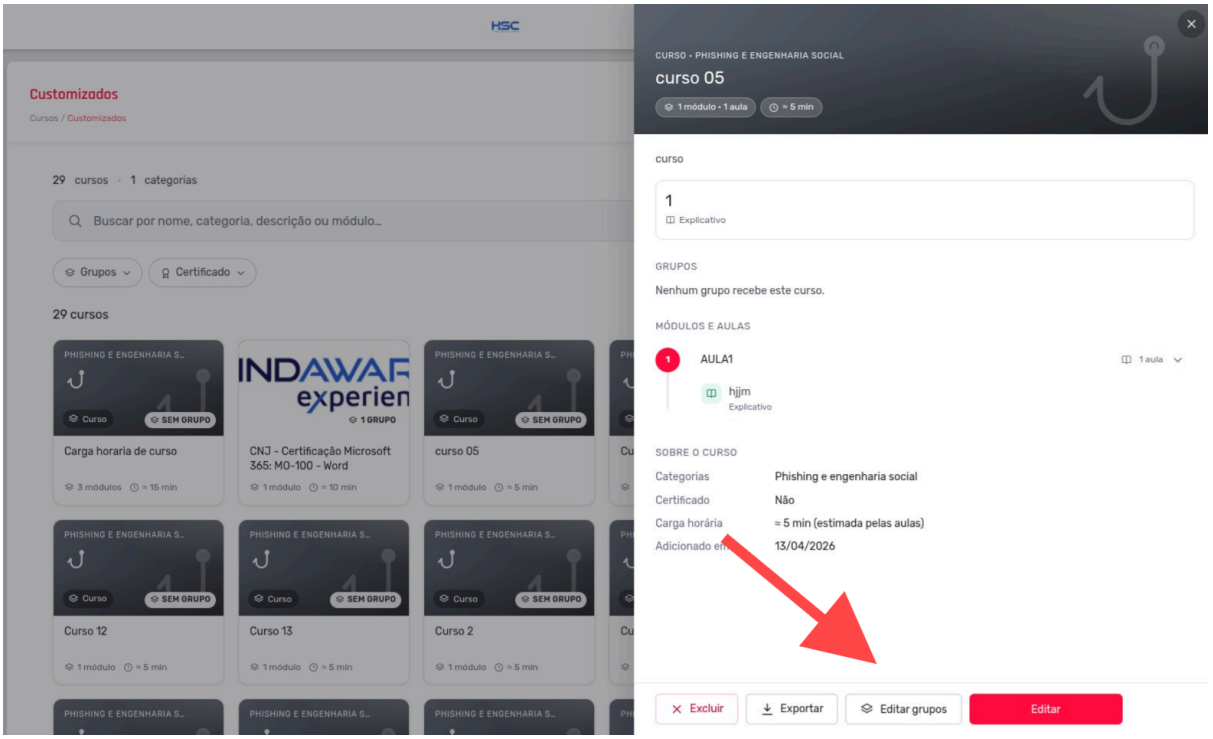
É possível exportar um curso customizado se necessário. Escolha o curso e vá em “Exportar”, assim já será feito o Download do curso.



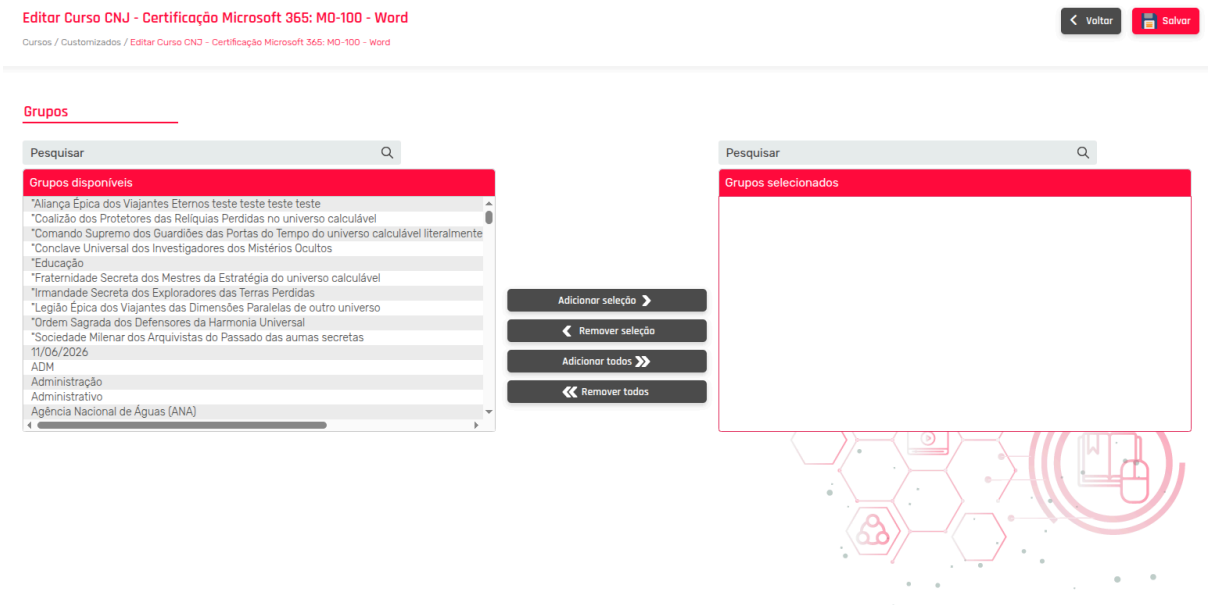
- **<u>Direcionar Cursos para Grupos de Usuários</u>**:

  Para configurar cursos específicos para grupos de usuários selecionados, siga os passos abaixo:

  1. Clique no curso escolhido
  2. Clique em “Editar grupos”



3. Selecione o(s) grupo(s) que realizarão o curso e clique em “Salvar”:

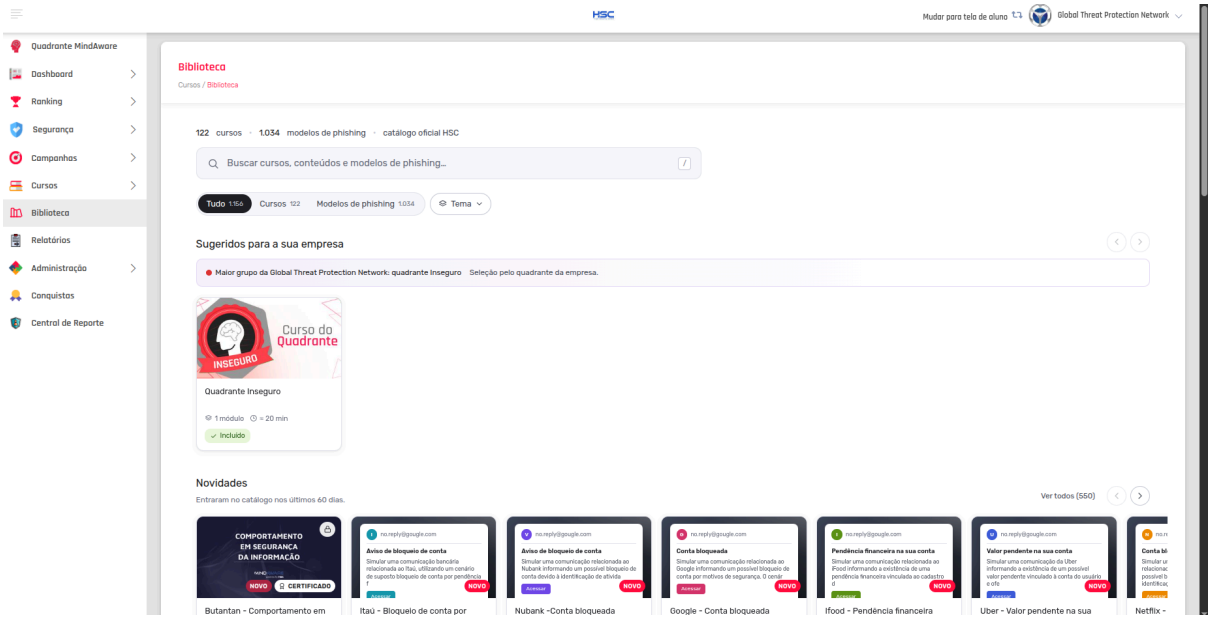


Biblioteca

A Biblioteca da plataforma MindAware 360° foi desenvolvida para facilitar o acesso dos administradores aos conteúdos disponíveis, reunindo em um único ambiente os **cursos, conteúdos educacionais e modelos de phishing** disponibilizados pela plataforma.

Nesta seção, o administrador poderá consultar os materiais disponíveis, visualizar suas informações, identificar conteúdos incluídos no plano da empresa e utilizar os cursos e modelos de phishing na criação de campanhas educacionais e comportamentais.

A Biblioteca possui um **campo de pesquisa e filtros**, permitindo localizar conteúdos de maneira rápida e prática, de acordo com suas características e categorias.



Recomendações de Conteúdos

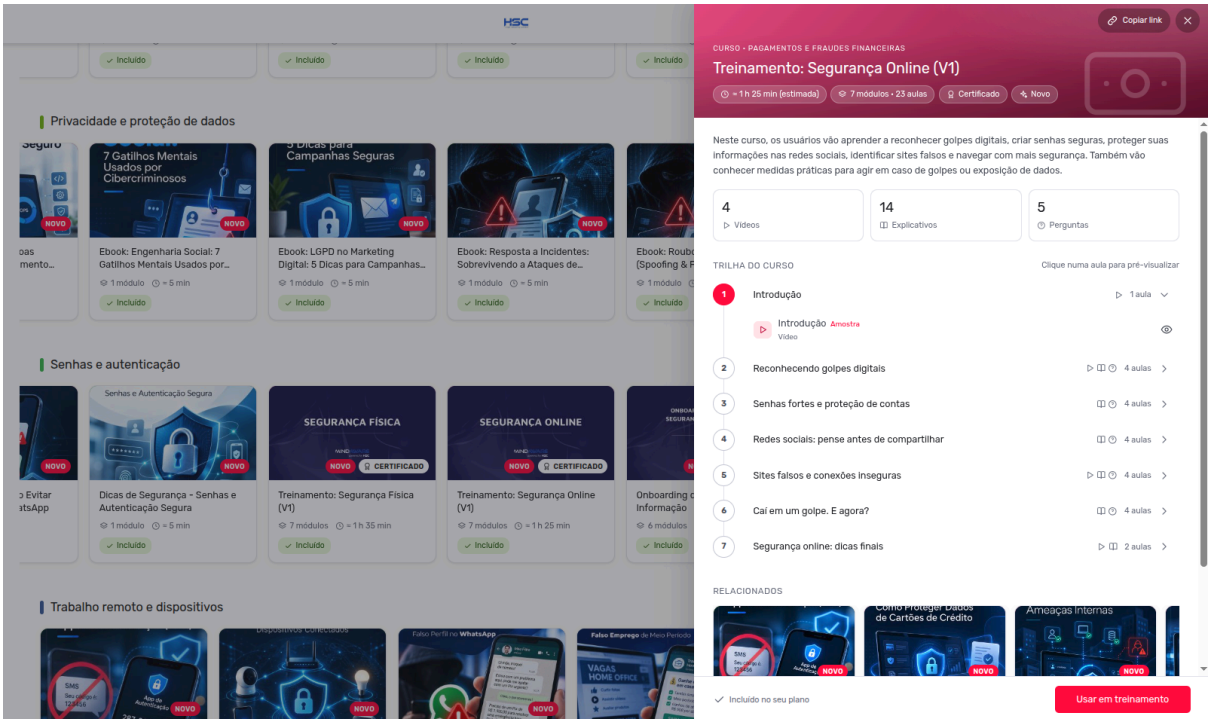
A plataforma disponibiliza uma seção de **conteúdos recomendados por Inteligência Artificial (IA)**, que analisa o cenário dos usuários da empresa e seu posicionamento no Quadrante MindAware.

Com base nessas informações, são apresentados cursos e conteúdos recomendados de acordo com as necessidades de conscientização identificadas,

auxiliando o administrador na escolha dos treinamentos mais adequados para a organização.

Visualização dos Cursos

Ao clicar em um curso disponível na Biblioteca, será aberto um **painel lateral** contendo as principais informações sobre o treinamento.



Nesse painel, será possível visualizar:

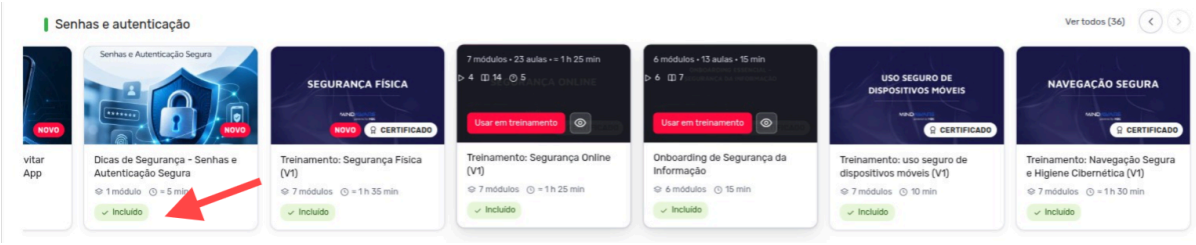
- **Nome do curso:** Identificação do treinamento selecionado.
- **Categoria:** Tema ao qual o curso pertence.
- **Descrição:** Apresentação dos objetivos e assuntos abordados no treinamento.
- **Duração:** Tempo estimado para conclusão do curso.
- **Quantidade de módulos e aulas:** Estrutura do treinamento e número de aulas disponíveis.
- **Conteúdos:** Relação das aulas e materiais que compõem o curso.
- **Cursos relacionados:** Sugestões de outros treinamentos associados ao conteúdo selecionado.

O administrador também poderá visualizar a estrutura do curso e acessar a prévia das aulas disponíveis.

Na parte inferior do painel, estará disponível o botão **Usar em treinamento**, que direciona o administrador para a tela de criação de uma campanha educacional, permitindo utilizar o curso selecionado.

Disponibilidade dos Cursos

Os cursos apresentados na Biblioteca possuem uma identificação que informa se o conteúdo está disponível para utilização pela empresa.



Os status apresentados são:

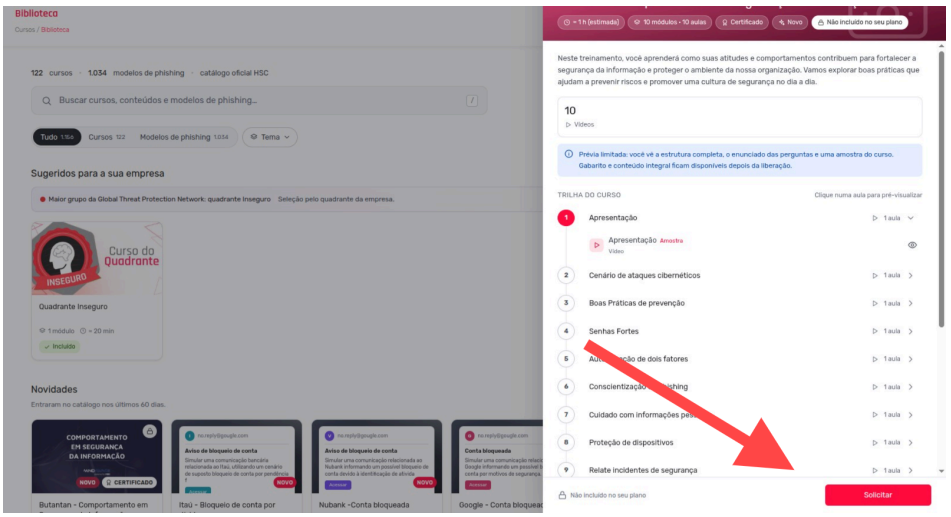
- **Incluído:** Indica que o curso está disponível no plano da empresa e pode ser utilizado na criação de campanhas educacionais.
- **Não incluído:** Indica que o curso ainda não está disponível para utilização pela empresa, sendo necessário solicitar sua liberação.

Solicitação de Liberação de Cursos

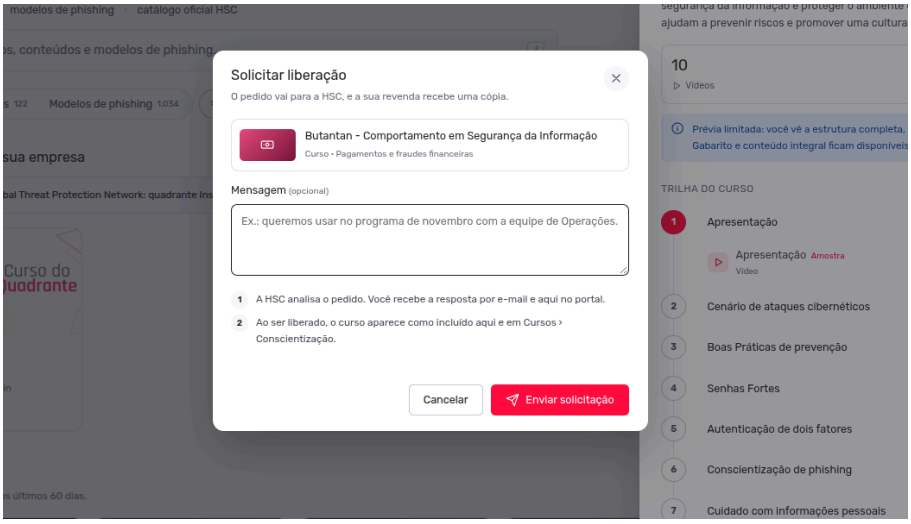
Caso o administrador tenha interesse em utilizar um curso que não esteja incluído no plano da empresa, poderá realizar uma solicitação de liberação diretamente pela Biblioteca.

Para solicitar a liberação, siga os passos:

1. Localize o curso desejado utilizando a pesquisa, os filtros ou as categorias disponíveis.
2. Clique no curso identificado como **Não incluído**.
3. No painel lateral, clique no botão **Solicitar**.



4. Será aberta uma janela de solicitação, na qual será possível adicionar uma mensagem justificando o pedido, caso necessário.



5. Clique em **Enviar solicitação** para concluir.

Após o envio, a HSC receberá uma notificação com a solicitação de liberação do curso, podendo realizar a análise e **aprovar ou rejeitar o pedido**.

O administrador responsável pela solicitação receberá uma notificação por e-mail informando o resultado da análise, incluindo o motivo apresentado para a aprovação ou rejeição.

Caso a solicitação seja aprovada, o curso passará a ser identificado como **Incluído** e ficará disponível para utilização nas campanhas educacionais da empresa.

Cursos Opcionais

Na Biblioteca da plataforma MindAware 360°, alguns cursos são identificados com a tag **Opcional**, indicando que são conteúdos complementares de conscientização, que podem ser realizados pelos usuários sem a obrigatoriedade de participação em uma campanha educacional.



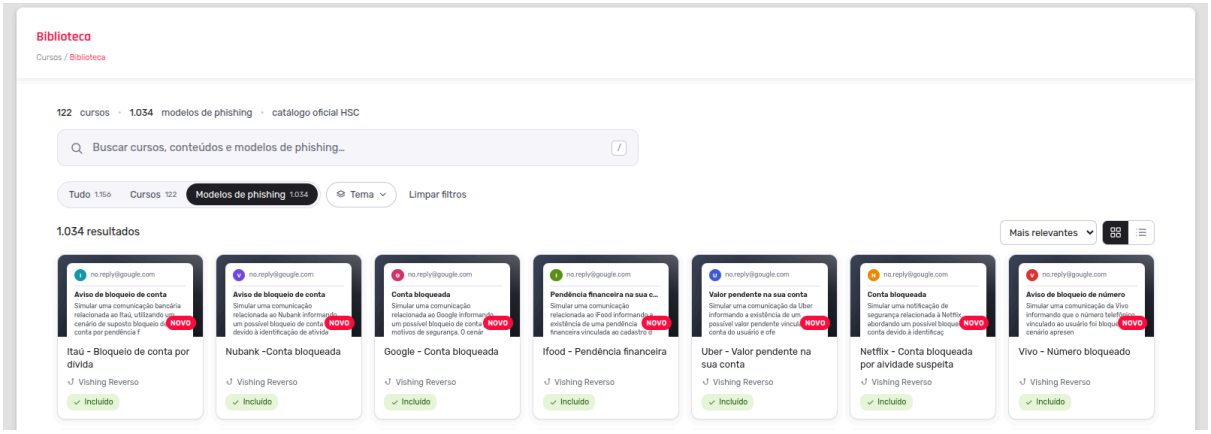
Esses cursos têm como objetivo ampliar as oportunidades de aprendizado dos colaboradores, permitindo que desenvolvam seus conhecimentos em segurança da informação de forma voluntária.

A contabilização dos cursos opcionais no **Score Educacional e no Quadrante MindAware** dependerá das configurações definidas pelo administrador da empresa.

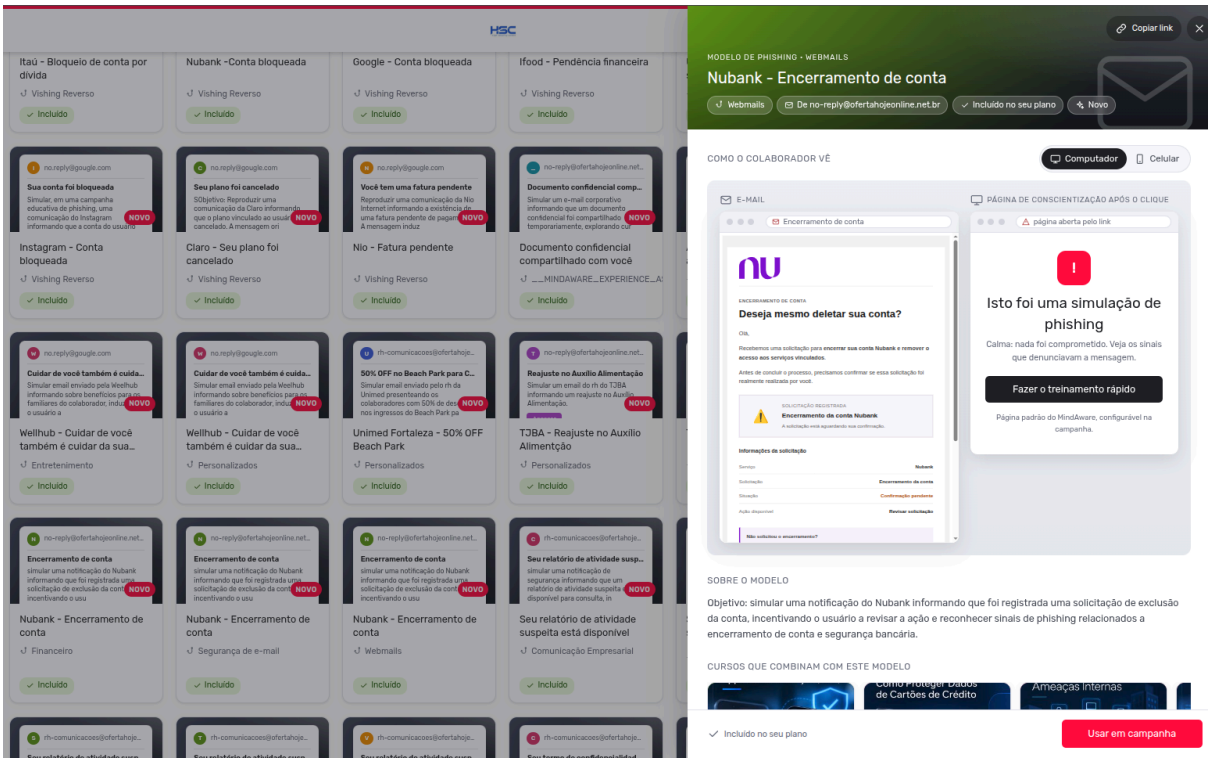
Dessa forma, os cursos opcionais podem ser utilizados como um recurso adicional de conscientização, sem a necessidade de torná-los obrigatórios para os colaboradores.

Visualização dos Modelos de Phishing

Além dos cursos e conteúdos educacionais, a Biblioteca disponibiliza os **modelos de phishing** que podem ser utilizados nas campanhas comportamentais.



Ao selecionar um modelo de phishing, será aberto um painel lateral com suas informações e uma prévia da comunicação que será apresentada aos colaboradores.



Nesse painel, será possível visualizar: nome do modelo, categoria, descrição, prévia do e-mail, prévia página web e conteúdos relacionados.

Pré-visualização dos Modelos de Phishing

A Biblioteca permite que o administrador visualize como o modelo de phishing será apresentado aos colaboradores antes de utilizá-lo em uma campanha.

Na seção **Como o colaborador vê**, estarão disponíveis as opções:

- **Computador:** Apresenta a visualização do modelo de phishing em uma tela de desktop.
- **Celular:** Apresenta a visualização adaptada para dispositivos móveis.

Quando o modelo possuir uma página Web associada, também será possível visualizar a mensagem de e-mail e a página que será apresentada ao colaborador após a interação com o link da simulação.



Essa funcionalidade permite ao administrador verificar a aparência e a estrutura do modelo antes de sua utilização.

Boletins e Comunicados

A plataforma MindAware 360º permite ao administrador criar, personalizar e enviar boletins e comunicados aos colaboradores, facilitando a divulgação de informações importantes, orientações de segurança e conteúdos de conscientização.

Além da criação de comunicados próprios, a plataforma disponibiliza uma biblioteca de boletins produzidos pela HSC, que podem ser utilizados e personalizados conforme as necessidades da empresa.

Também é possível configurar assinaturas para o envio automático de boletins, definir públicos específicos e acompanhar os resultados das comunicações realizadas.

Para acessar essa funcionalidade, no menu lateral, clique em Comunicação → Boletins e Comunicados.

Visualização dos Comunicados

Na tela de Boletins e comunicados, o administrador poderá visualizar todas as comunicações criadas pela empresa, consultar suas situações e acompanhar os resultados dos envios.

Na parte superior, estarão disponíveis três abas:

- Comunicados: Permite visualizar, criar e gerenciar as comunicações da empresa.
- Biblioteca HSC: Disponibiliza os boletins produzidos pela HSC para utilização nas comunicações.
- Assinaturas: Permite configurar o envio automático dos boletins das séries disponíveis.

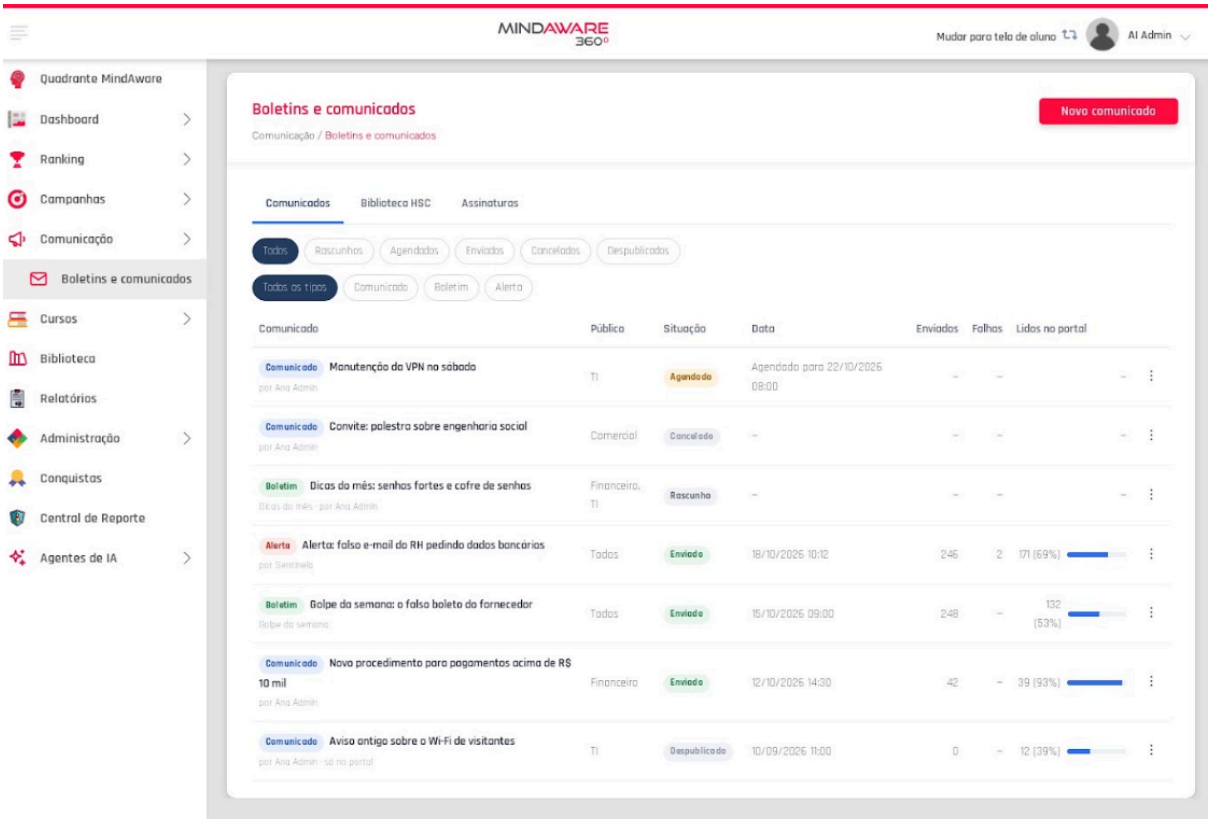
Na aba Comunicados, é possível utilizar filtros para localizar as mensagens de acordo com sua situação e tipo.

As situações disponíveis são:

- Rascunho: Comunicados criados que ainda não foram enviados ou agendados.

- Agendado: Comunicados programados para envio em uma data e horário definidos.
- Enviado: Comunicados cujo processo de envio foi concluído.
- Cancelado: Comunicados que tiveram o agendamento cancelado.
- Despublicado: Comunicados retirados da disponibilização no portal.

Cada comunicado apresenta informações como tipo, autor, público, data e indicadores de envio, permitindo acompanhar as comunicações realizadas pela organização.



Ações dos Comunicados

Ao clicar no menu de ações, representado pelos três pontos ao lado de cada comunicado, serão apresentadas as opções disponíveis conforme sua situação.

- Editar: Permite modificar as informações e o conteúdo de um comunicado.
- Pré-visualizar: Exibe como a mensagem será apresentada aos destinatários.

- Duplicar: Permite criar um novo comunicado utilizando as informações de outro já existente.
- Cancelar agendamento: Interrompe o envio programado de um comunicado.
- Despublicar: Retira do portal um comunicado que já foi enviado.

As opções disponíveis variam conforme a situação do comunicado. Os rascunhos podem ser editados, pré-visualizados e duplicados. Os agendados também permitem cancelar o agendamento. Já os enviados podem ser pré-visualizados, duplicados ou despublicados.

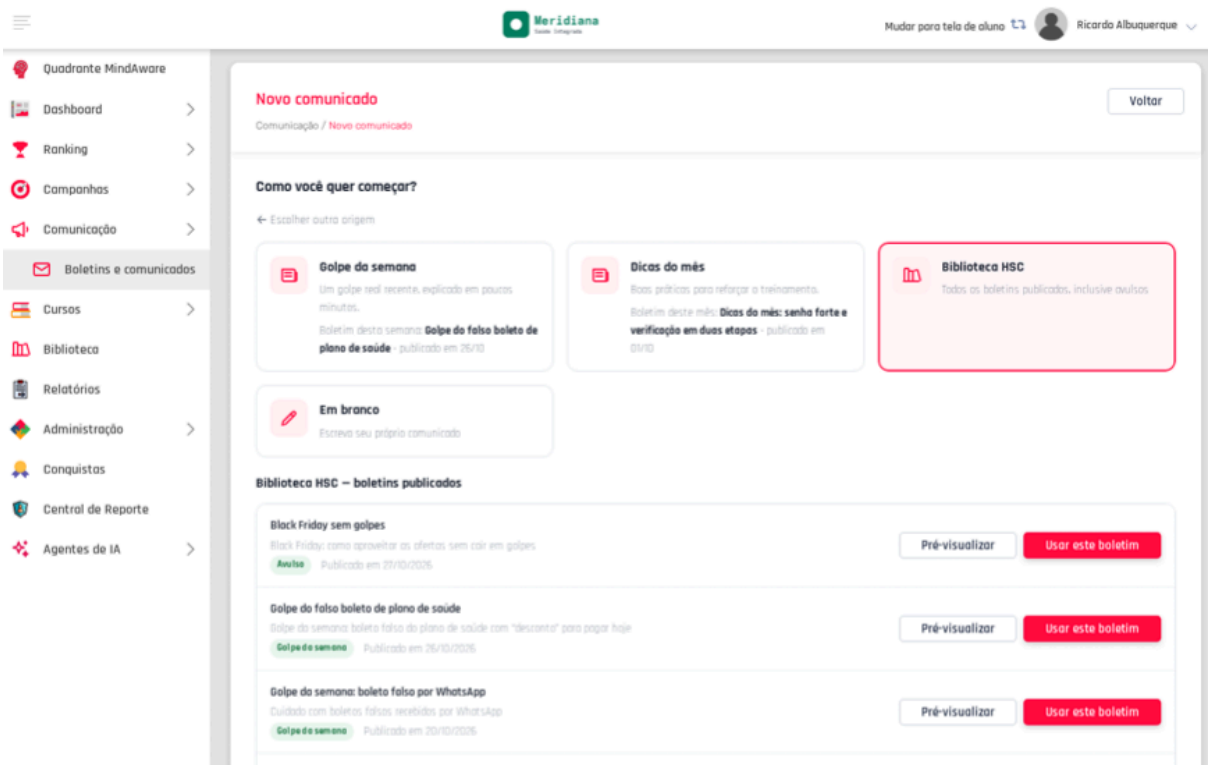
Criação de Comunicados

Para criar uma nova comunicação, vá na aba Comunicados e clique no botão Novo comunicado.

Será apresentada uma janela com as opções disponíveis para iniciar a criação.

O administrador poderá escolher entre:

- Golpe da semana: Permite utilizar o boletim mais recente da série, publicado pela HSC na semana atual.
- Dicas do mês: Permite utilizar o boletim mais recente da série, publicado pela HSC no mês atual.
- Biblioteca HSC: Permite consultar os boletins publicados, incluindo conteúdos avulsos, e selecionar aquele que deseja utilizar.
- Em branco: Permite criar um comunicado próprio, sem utilizar um conteúdo previamente disponibilizado.



Biblioteca HSC

Ao selecionar a opção Biblioteca HSC, será apresentada uma relação dos boletins disponibilizados pela HSC.

O administrador poderá consultar os conteúdos e utilizar a opção Pré-visualizar para verificar as informações antes de selecionar o boletim desejado.

Após a seleção, o conteúdo será carregado no editor, permitindo realizar as alterações necessárias antes do envio.

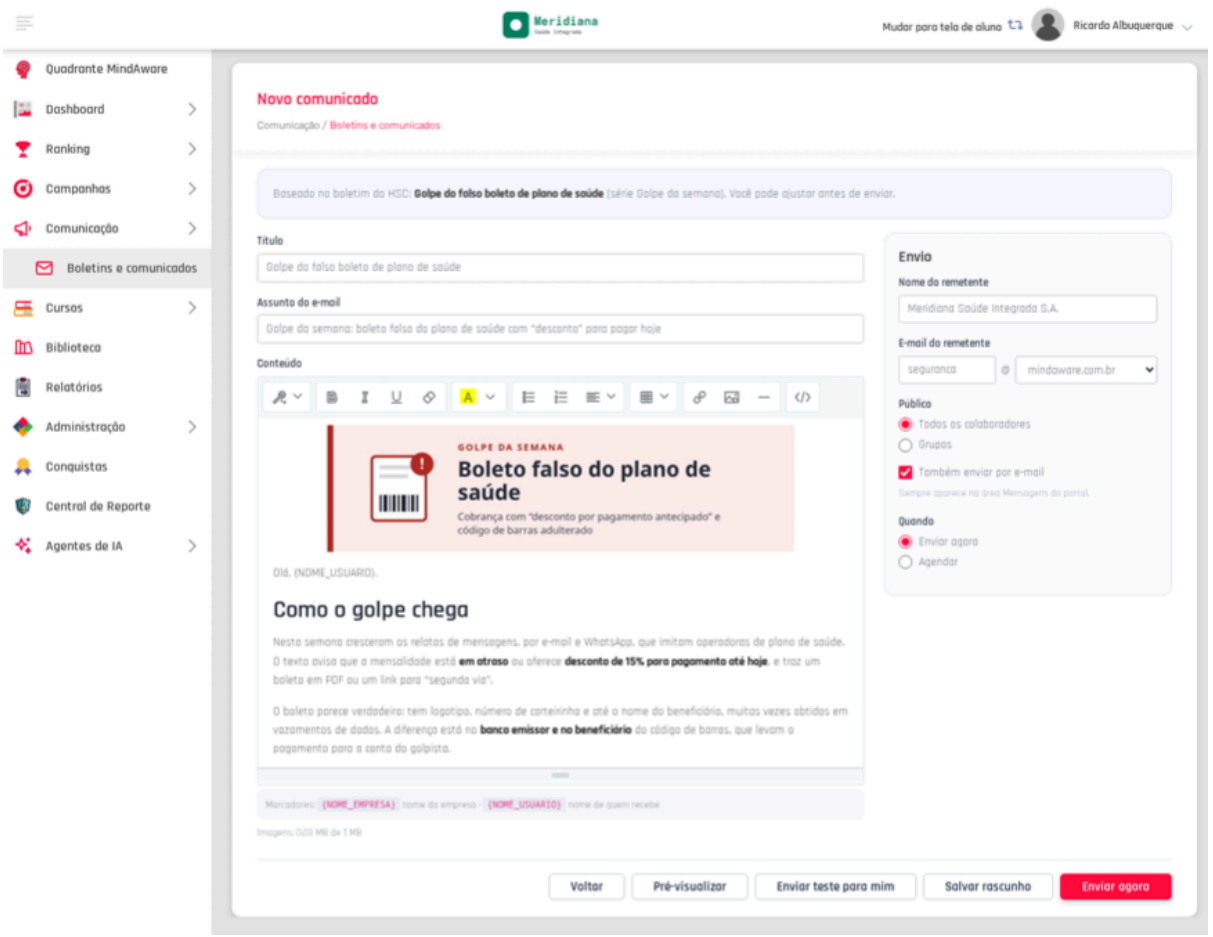
Quando um comunicado for criado a partir de um boletim da biblioteca, a plataforma apresentará uma identificação de sua origem.

Edição e Personalização dos Comunicados

Após selecionar a origem do comunicado, será apresentada a tela de edição, onde o administrador poderá preencher as informações e personalizar o conteúdo.

Nesta tela, estarão disponíveis os seguintes campos:

- Título: Permite definir o nome do comunicado para identificação na plataforma.
- Assunto do e-mail: Define o assunto apresentado aos destinatários quando a comunicação for enviada por e-mail.
- Conteúdo: Permite elaborar ou modificar a mensagem que será disponibilizada aos colaboradores.



O editor disponibiliza recursos de formatação de texto, inserção de imagens, links e outros elementos visuais, permitindo adequar a comunicação à identidade e às necessidades da organização.

Também é possível utilizar marcadores de personalização no assunto e no conteúdo da mensagem:

- `{NOME_EMPRESA}`: Insere automaticamente o nome da empresa.
- `{NOME_USUARIO}`: Insere automaticamente o nome do colaborador destinatário.

Esses marcadores serão substituídos pelas informações correspondentes no momento da apresentação da mensagem.

Configuração do Envio

Na mesma tela de edição, o administrador poderá utilizar o painel Envio para configurar os destinatários, o remetente e o momento em que a comunicação será encaminhada.

As seguintes opções estarão disponíveis:

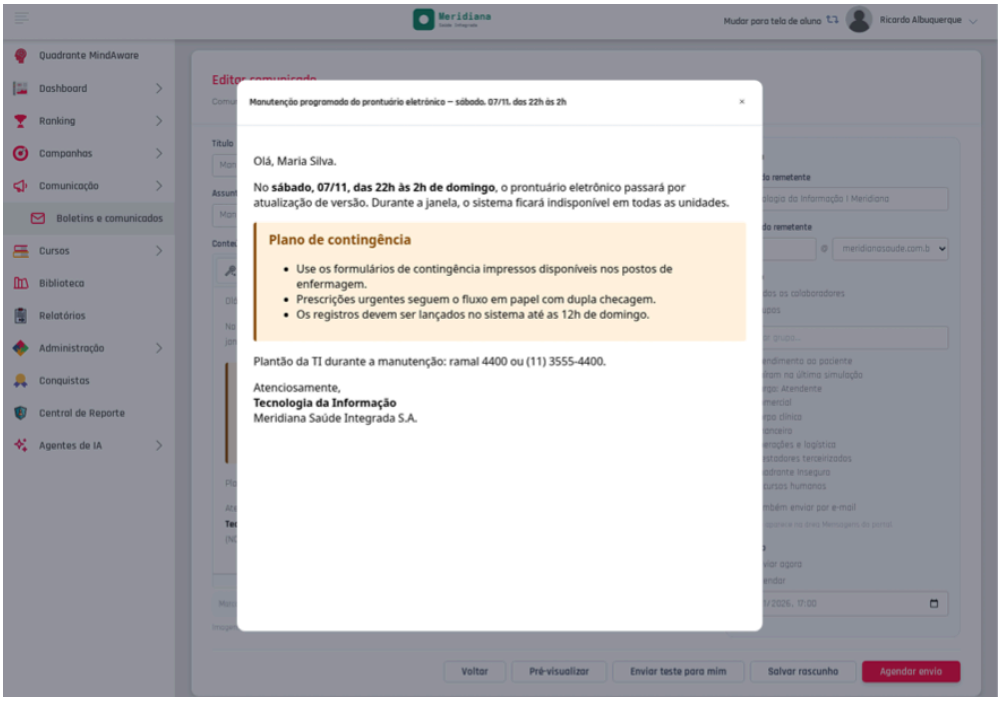
- Nome do remetente: Permite definir o nome que será apresentado como responsável pelo envio. Por padrão, será utilizado o nome da empresa.
- E-mail do remetente: Permite personalizar a parte inicial do endereço e selecionar um domínio autorizado, incluindo os domínios cadastrados da empresa e o domínio mindaware.com.br.
- Público: Permite direcionar a comunicação para todos os colaboradores ou selecionar grupos específicos, utilizando o campo de busca.
- Também por e-mail: Define se a comunicação será encaminhada por e-mail, além de ficar disponível na área de Mensagens da plataforma. Essa opção estará marcada por padrão.
- Quando: Permite definir se a comunicação será enviada imediatamente ou agendada para uma data e horário futuros.



Os agendamentos utilizam o horário de Brasília.

Pré-visualização e Envio de Teste

Antes de concluir o envio, o administrador poderá utilizar a opção Pré-visualizar para verificar como o comunicado será apresentado aos destinatários.



Também estará disponível a opção Enviar teste para mim, que permite encaminhar uma versão de teste para o endereço de e-mail do administrador que estiver conectado à plataforma.

O e-mail de teste será enviado imediatamente, com a identificação [Teste] no assunto.

Os testes não serão disponibilizados na área de Mensagens e não serão contabilizados nos indicadores dos comunicados.

Enviar ou Agendar Comunicado

Após preencher as informações e conferir o conteúdo, o administrador poderá concluir a configuração utilizando uma das opções:

- Enviar agora: Inicia imediatamente o processo de envio da comunicação.
- Agendar envio: Permite programar o envio para uma data e horário futuros.

Ao selecionar uma dessas opções, a plataforma apresentará uma confirmação com as informações do público destinatário.

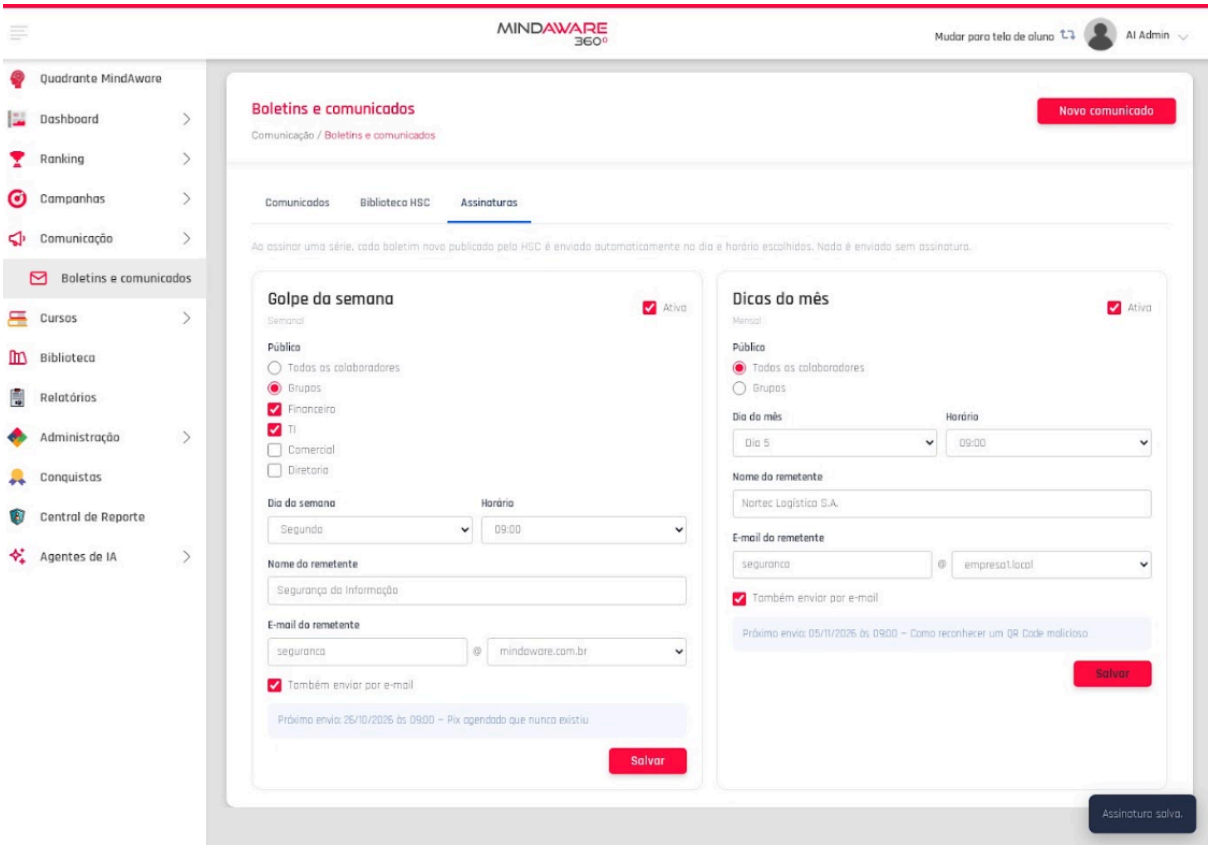
Após a confirmação, o comunicado será encaminhado ou permanecerá agendado conforme a opção selecionada.

Assinaturas de Boletins

A plataforma permite configurar assinaturas para automatizar o envio dos boletins publicados pela HSC, sem a necessidade de criar manualmente uma comunicação a cada nova publicação.

Para realizar essa configuração, acesse Comunicação → Boletins e comunicados e selecione a aba Assinaturas.

Nesta tela, o administrador poderá configurar as assinaturas das séries Golpe da semana e Dicas do mês, definindo os destinatários, a frequência e as informações de envio.



As seguintes configurações estarão disponíveis:

- Ativa: Permite ativar ou desativar o envio automático da série.
- Público: Define se os boletins serão enviados para todos os colaboradores ou para grupos específicos.

- Dia: Permite definir o dia do envio. Para Golpe da semana, será selecionado um dia da semana. Para Dicas do mês, será possível escolher um dia entre 1 e 28.
- Horário: Permite configurar o horário de envio, entre 00h00 e 23h30, com intervalos de 30 minutos.
- Remetente: Permite configurar o nome e o endereço de e-mail do remetente, respeitando os domínios autorizados.
- Também por e-mail: Define se os boletins serão encaminhados por e-mail, além de disponibilizados na plataforma.

Como funciona o envio automático

Quando uma assinatura estiver ativa, a plataforma verificará os boletins publicados pela HSC .

O envio será realizado automaticamente no dia e horário configurados, respeitando o público definido pelo administrador.

Caso não exista um novo boletim publicado no período, nenhum envio será realizado.

A tela também apresentará informações sobre o próximo envio programado ou o motivo pelo qual uma comunicação não foi realizada.

Importante: O envio automático dos boletins somente ocorrerá quando a assinatura correspondente estiver ativada e configurada pelo administrador.

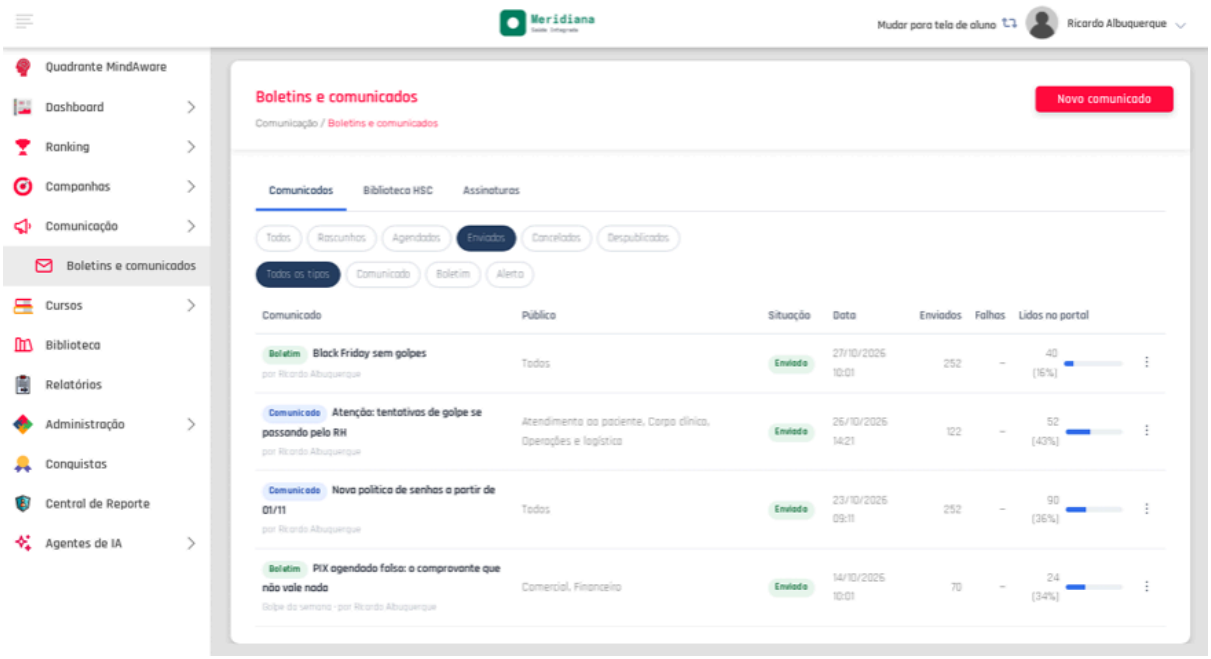
Acompanhamento dos Comunicados

Após realizar o envio, o administrador poderá acompanhar a situação e os indicadores de cada comunicado diretamente na aba Comunicados.

Quando a opção Enviar agora for utilizada, o comunicado passará inicialmente pela situação Enviando, enquanto a plataforma processa o encaminhamento das mensagens.

Após a conclusão do processamento, sua situação será alterada para Enviado. Normalmente, esse processo é concluído em até um minuto.

Durante o envio, o comunicado já estará disponível na área de Mensagens dos destinatários.



Na listagem, serão apresentados os seguintes indicadores:

- Enviados: Apresenta a quantidade de e-mails entregues ao servidor de envio.
- Falhas: Informa a quantidade de mensagens que não puderam ser encaminhadas após três tentativas ou devido à ausência de um endereço de e-mail válido.
- Lidos no portal: Apresenta a quantidade e o percentual de colaboradores que acessaram o comunicado na área de Mensagens da plataforma.

O percentual de leitura é calculado com base no público destinatário da comunicação.

A plataforma considera como leitura somente a abertura do comunicado na área de Mensagens. A abertura do e-mail não é utilizada para contabilizar esse indicador.

Essas informações permitem ao administrador acompanhar a distribuição das mensagens, identificar possíveis falhas e avaliar o alcance das comunicações realizadas, contribuindo para o aprimoramento das ações de conscientização da organização.

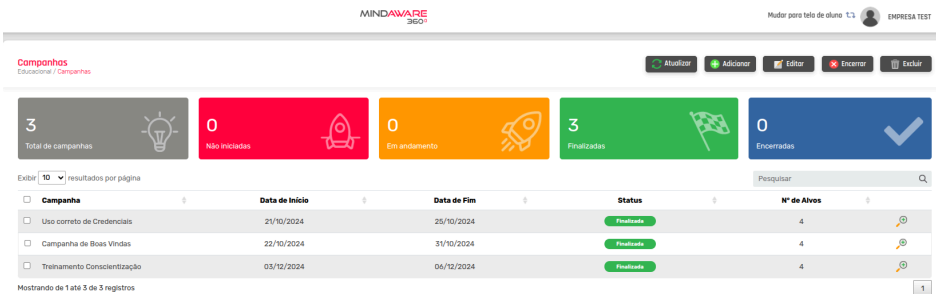
Menu Campanhas

“ PHISHING: Phishing é uma tentativa de golpe cibernético por meio de e-mail, induzindo a vítima à fornecer de forma ilegal, informações, tais como: Números de documentos, senhas bancárias, cartões de crédito e etc.”

Nesta seção, será possível a criação de campanhas educacionais e de simulação de phishing, onde será possível utilizar mais de 500 templates reais para o testar a maturidade dos colaboradores ao receber um e-mail malicioso. As campanhas podem ser disparadas a diversos grupos diferentes, com cursos ou templates diferentes à colaboradores distintos, adotando assim, estratégias variadas. Nesta seção veremos:

Campanhas Educacionais

Nesta seção, são criadas as Campanhas Educacionais para desenvolver a maturidade dos colaboradores. O número de campanhas que podem ser criadas é ilimitado, permitindo total flexibilidade na gestão dos treinamentos.

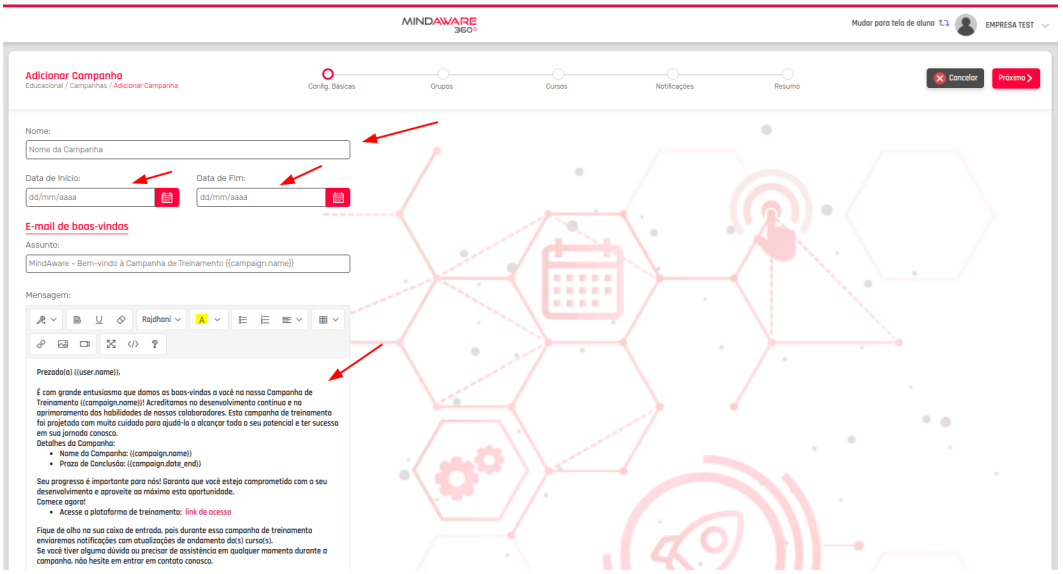


<u>Como criar uma campanha:</u> Para criar uma Campanha Educacional, siga as etapas abaixo:

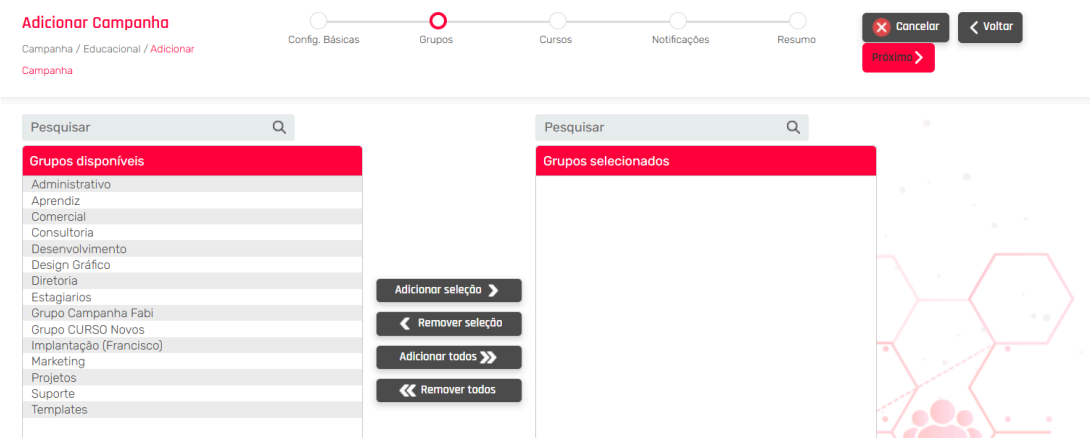
1) Acesse -> **Menu Educacional -> Campanhas** e clique em **-> botão Adicionar**



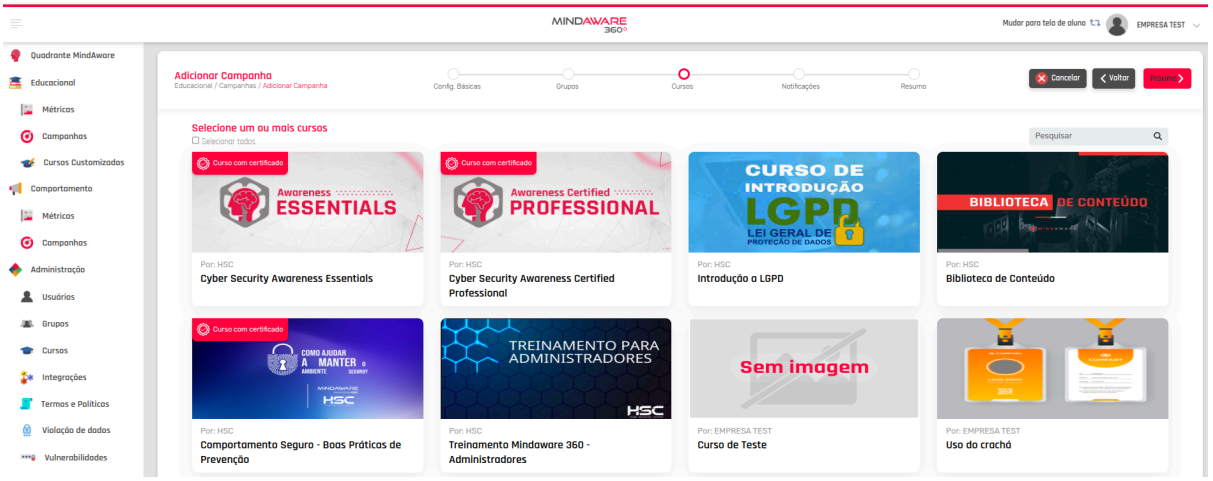
2) Preencha as informações atribuindo um nome para a campanha, data de início, data de fim e assunto. O MindAware traz um texto padrão para a mensagem de notificação que poderá ser alterada de acordo com o vocabulário da empresa, somente atentar para preservar os campos onde ficam a variável {{next}}. Além disso, a plataforma possui outras variáveis, como as de nome, sobrenome e email de usuário, nome da empresa, data do início e fim da campanha e mais algumas para auxiliar na escrita da notificação do email.



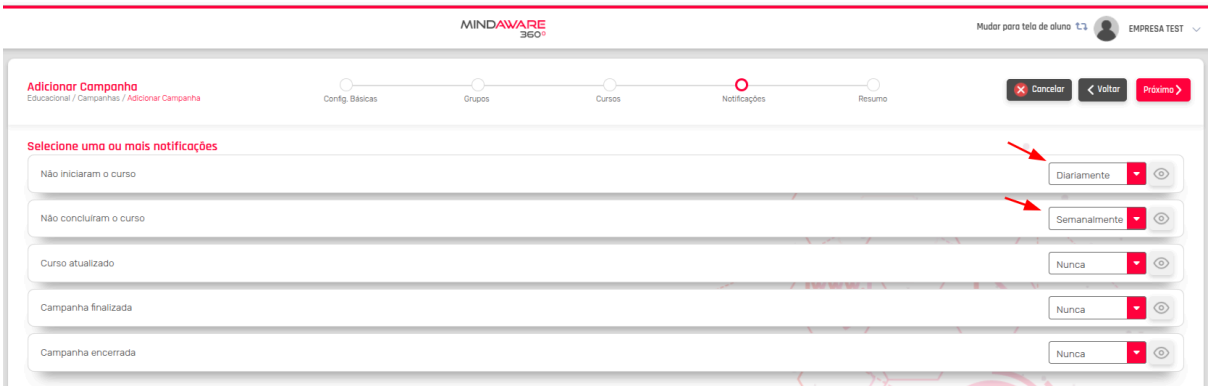
3) Selecione o(s) grupo(s) que irão participar do curso.



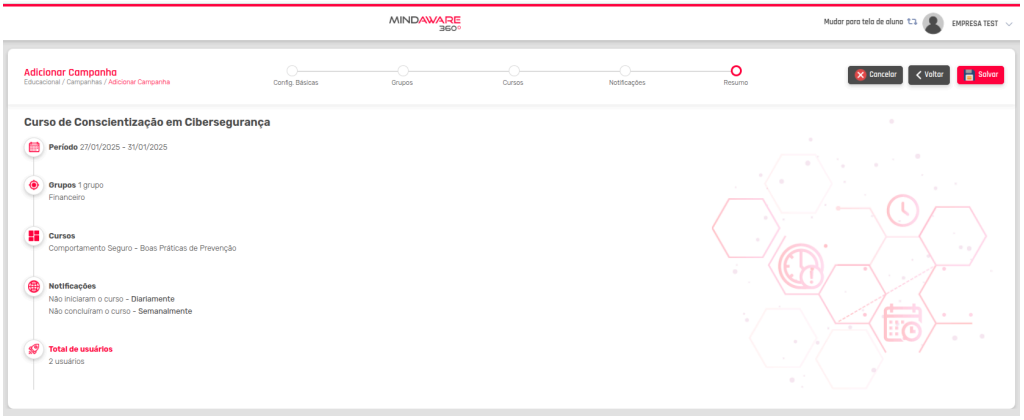
4) Nesta etapa, vamos selecionar o curso a ser aplicado:



5) Nesta etapa, é possível ativar as notificações, as notificações disponíveis são: para usuários que não concluíram o curso, para quando uma aula do curso for atualizada, para quando a campanha for finalizada ou encerrada. Todas as notificações podem ter a mensagem e o período de envio editados.



6) Nesta etapa, assim como na criação das campanhas de comportamento, também será apresentado um resumo contendo o Período da campanha, Grupos participantes, Notificações e o Total de usuários participantes, basta clicar em **botão -> Salvar.**



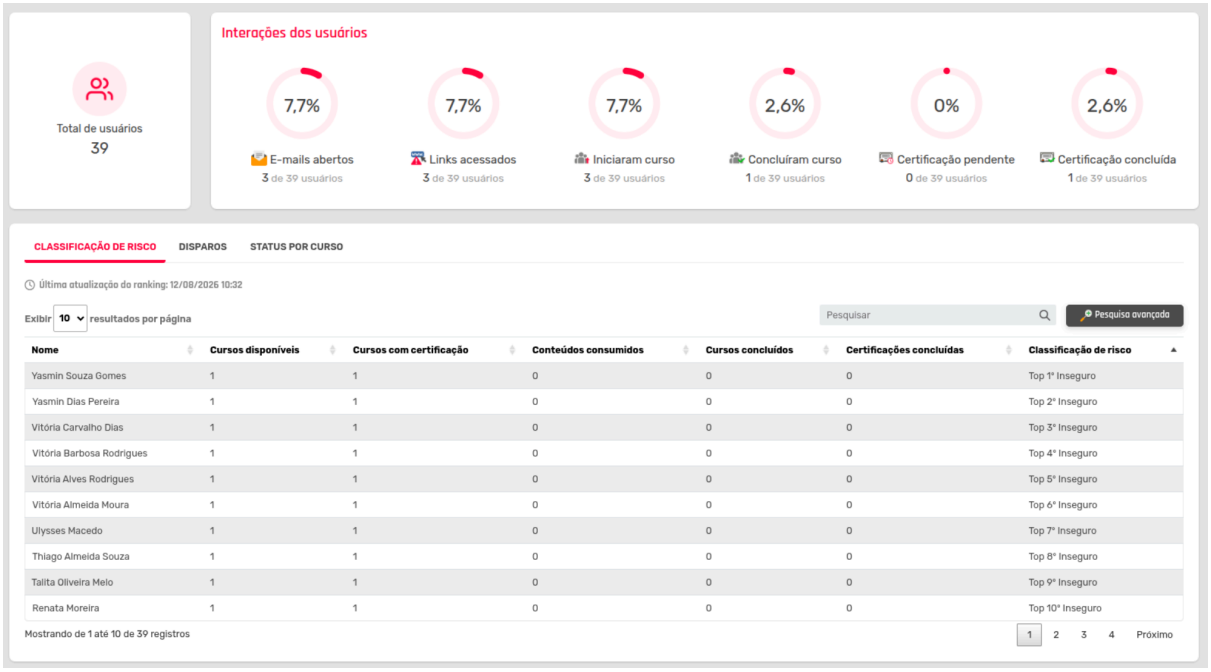
Após a criação da campanha é possível acompanhar as campanhas, basta aplicar um duplo clique sobre a campanha desejada e abrirá um painel trazendo informações tais como: Total de usuários em campanha, e-mails de notificação abertos, os links clicados, quantos iniciaram o curso e quantos finalizaram o curso.

Os usuários receberão notificações por e-mail evidenciando as ações e etapas realizadas na campanha.

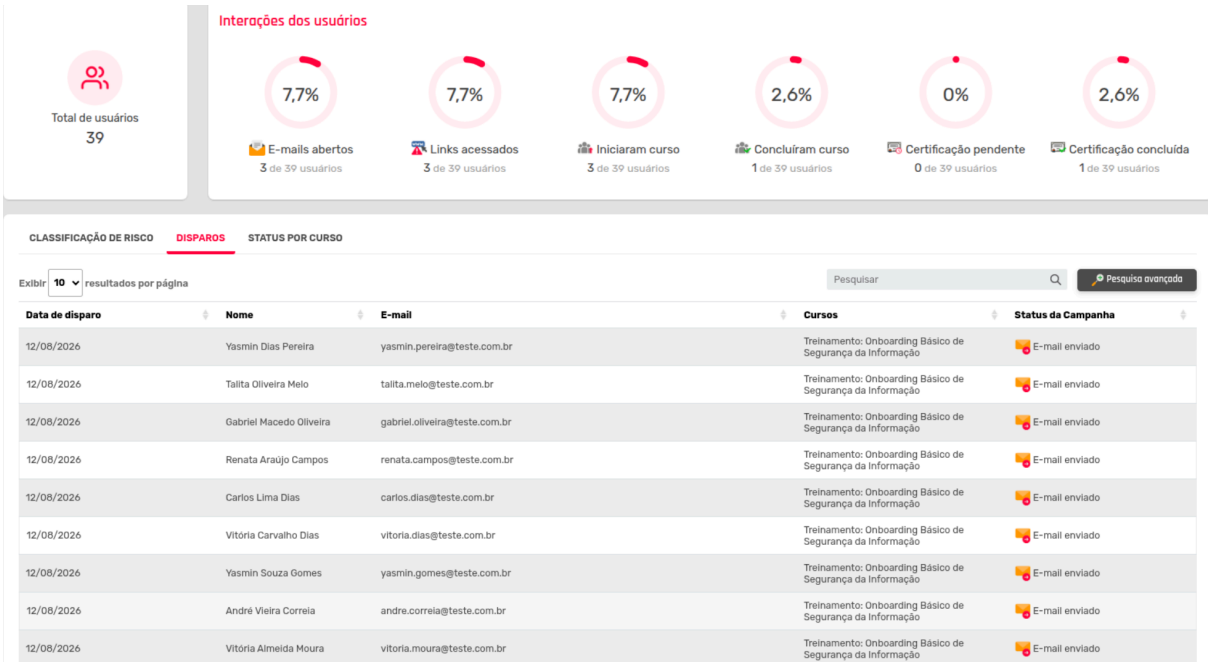
Quando um usuário concluir todas as etapas, receberá uma notificação de encerramento e deixará de receber novas notificações relacionadas àquela campanha.

Caso todos os usuários concluam integralmente suas respectivas etapas, o envio de notificações será automaticamente encerrado e a campanha será considerada finalizada.

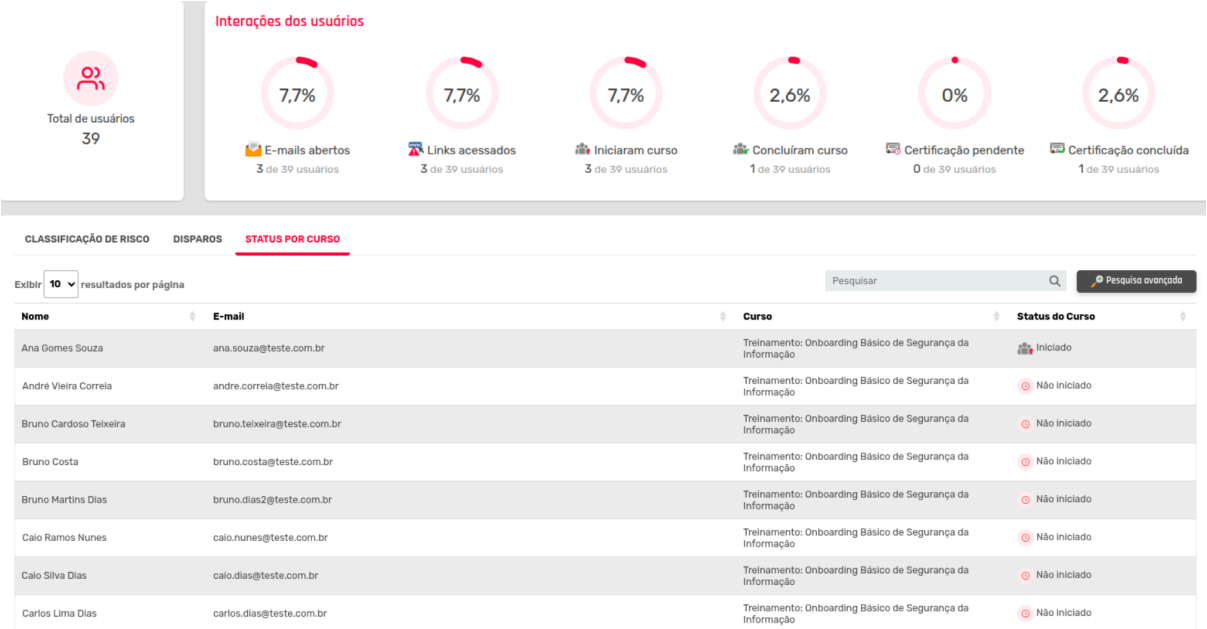
Em **Classificação de Risco**, é possível visualizar o nível de risco dos usuários de acordo com o andamento do treinamento. Os usuários classificados como mais inseguros são aqueles que ainda não iniciaram o curso ou que não concluíram todas as etapas. Já os usuários classificados como seguros são aqueles que concluíram o treinamento e realizaram a certificação.



Em **Disparos**, é possível visualizar o status individual de cada usuário na campanha, permitindo acompanhar de forma detalhada sua participação e evolução ao longo das ações realizadas.



Em **Status por Curso**, é possível consultar o andamento de cada usuário individualmente em cada curso disponibilizado. Essa visualização é especialmente útil em campanhas que possuem mais de um curso, pois permite acompanhar separadamente o status de conclusão de cada conteúdo.



Ao clicar **"Relatórios"**, você terá duas opções para gerar os relatórios da campanha selecionada:

- **Relatório Estratégico (PDF)** – Gera um documento em PDF com as principais métricas e análises da campanha.

- **Log de Disparos (CSV)** – Exportar um arquivo em formato CSV contendo o histórico detalhado de todos os disparos realizados, acessos únicos e totais e ações de cada usuário.



Campanhas Comportamental (Simulação de Phishing)

Uma Campanha de Simulação de Phishing é uma ação controlada criada pelos administradores com o objetivo de avaliar o nível de conscientização e o comportamento dos colaboradores diante de mensagens que reproduzem cenários reais de engenharia social.

Por meio dessas campanhas, a organização pode avaliar como os usuários reagem ao recebimento de mensagens potencialmente fraudulentas,

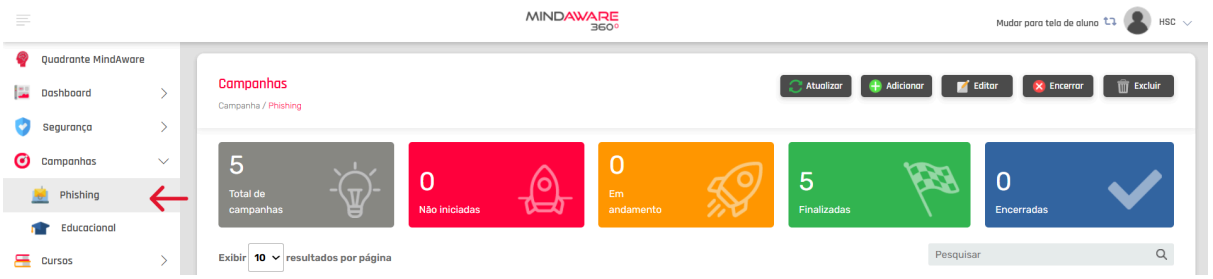
identificando comportamentos como abertura da mensagem, acesso a links e submissão de dados em páginas simuladas. Todas as ações são realizadas em ambiente controlado e registradas individualmente pela plataforma.

A plataforma MindAware 360° disponibiliza uma ampla biblioteca de modelos de phishing, permitindo a utilização de diferentes temas, remetentes, assuntos e abordagens para construir campanhas compatíveis com a realidade da organização.

Também é possível utilizar templates personalizados, permitindo maior flexibilidade na construção das simulações.

As campanhas podem ser direcionadas para um ou mais grupos de usuários e configuradas com diferentes períodos, templates, páginas de destino e métodos de disparo.

Como criar uma campanha: Para criar uma campanha de Simulação de Phishing deveremos acessar **Menu Campanhas -> Phishing**

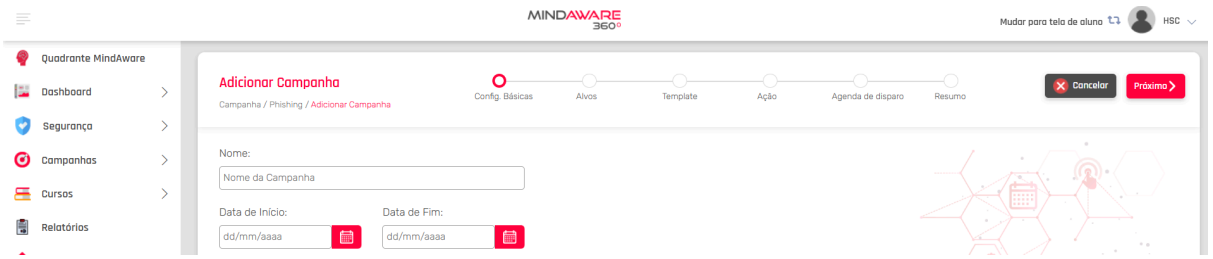


1) Clique no botão Adicionar. Na primeira etapa, serão definidas as informações básicas da campanha:

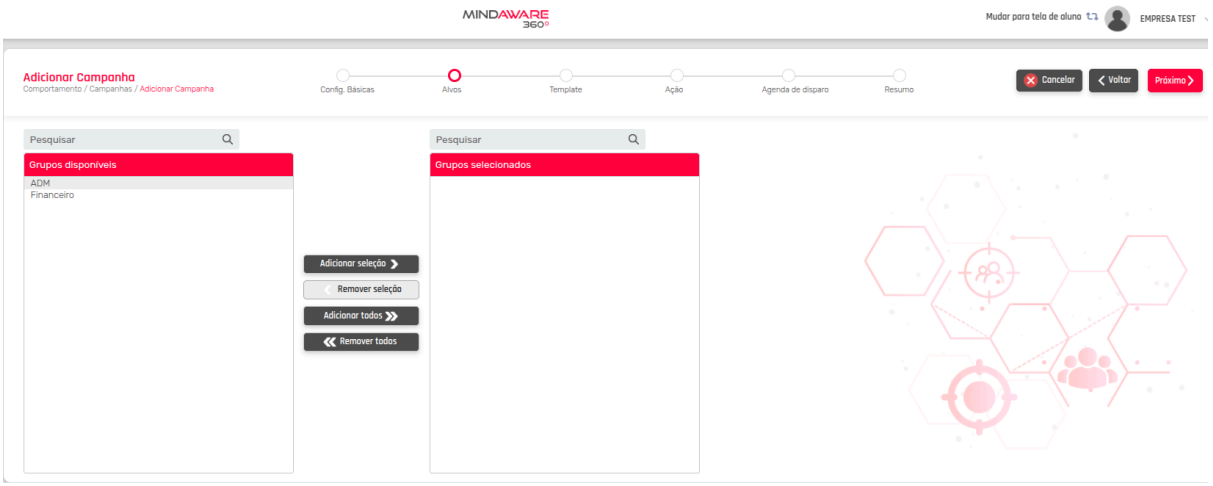
- Nome da Campanha;
- Data de Início;
- Data de Término.

Após preencher as informações, clique no botão Próximo.

O período definido será utilizado para determinar a janela de execução da campanha.



2) Após clicar no **botão -> Avançar**, nesta tela, iremos definir o(s) grupo(s) de usuários que irão participar:

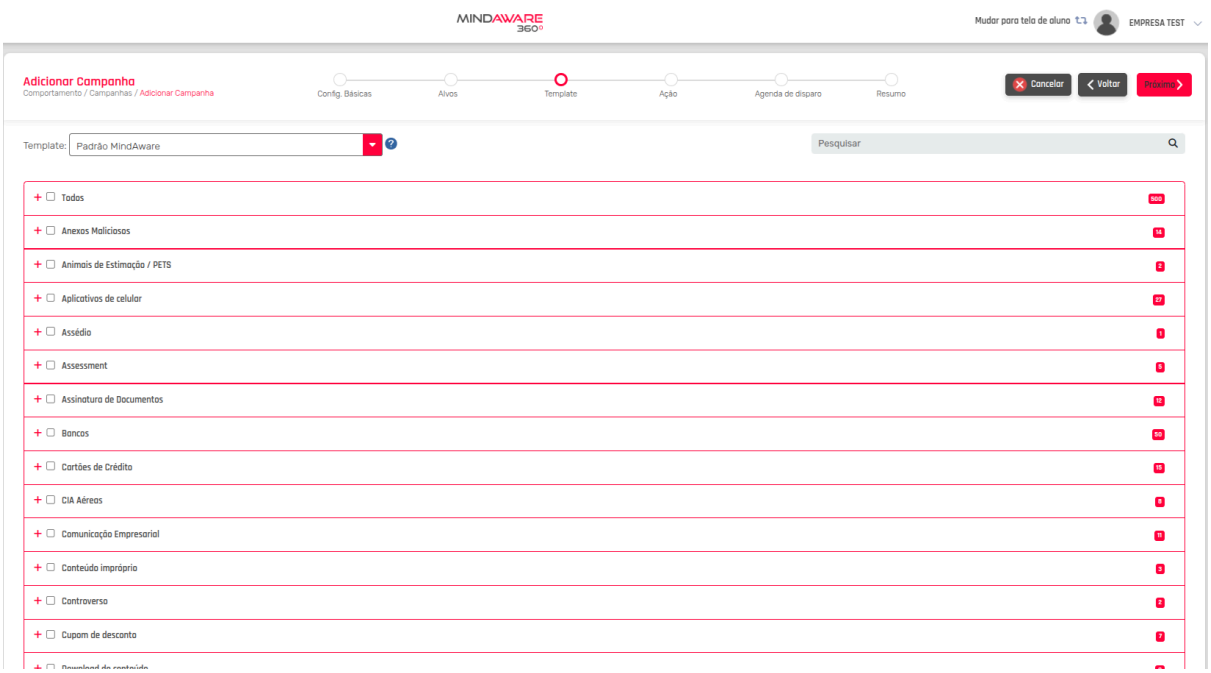


3) Definidos os grupos participantes, serão definidos os templates de phishing utilizados na campanha.

   É possível selecionar um ou mais templates conforme a estratégia definida para a campanha.

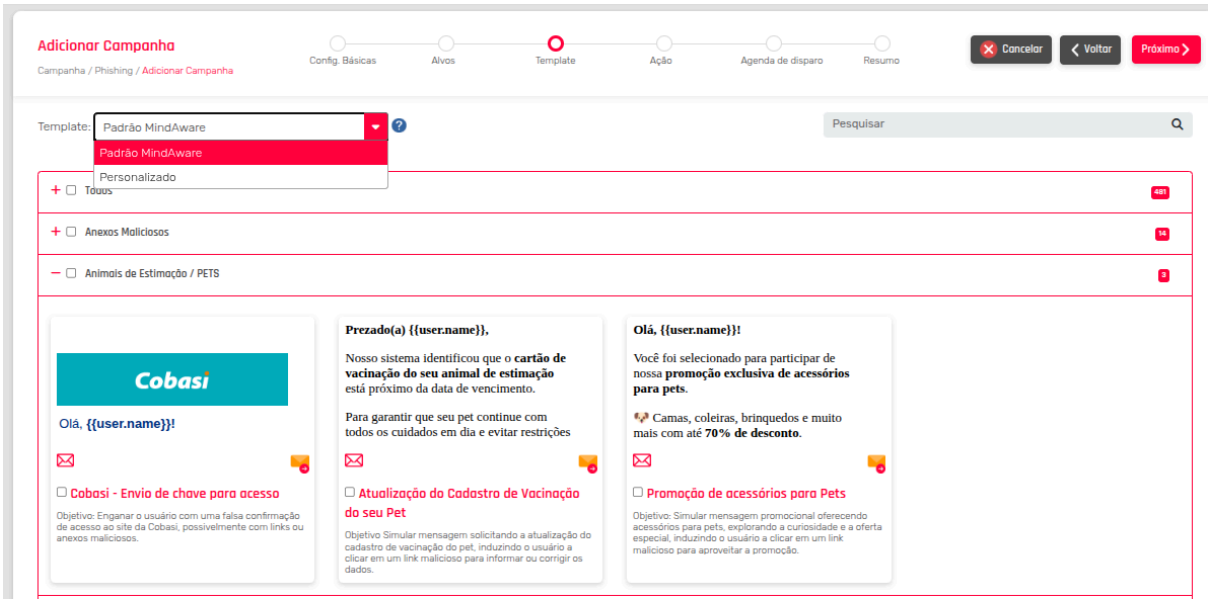
   A plataforma conta com mais de 1000 templates, entre eles existem templates com páginas web e timers.

   Após selecionar os templates desejados, clique em Próximo.

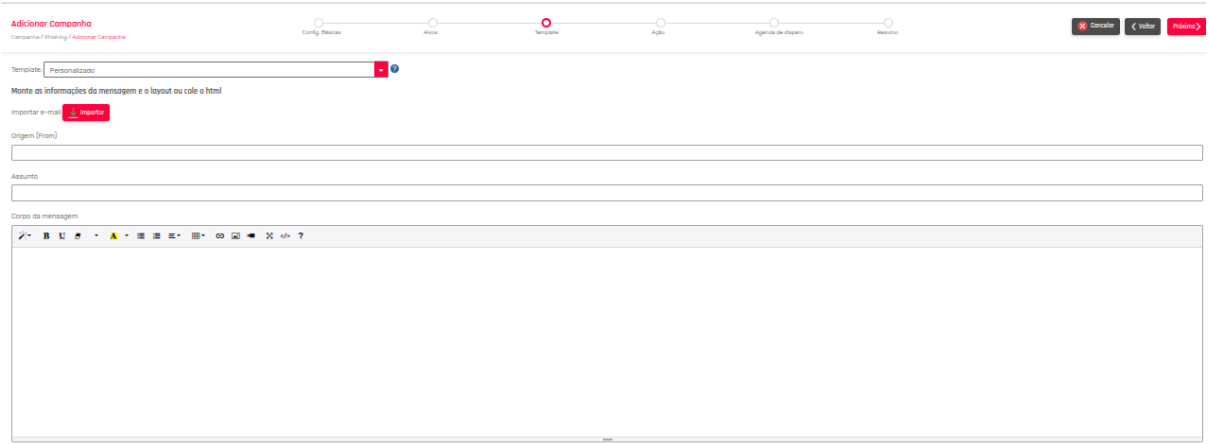


Além dos modelos disponibilizados pela plataforma, também é possível criar ou importar um **template personalizado**.

Para isso, selecione a opção **Personalizado**.



E então irá para essa tela, onde poderá importar um template ou criar um do zero.



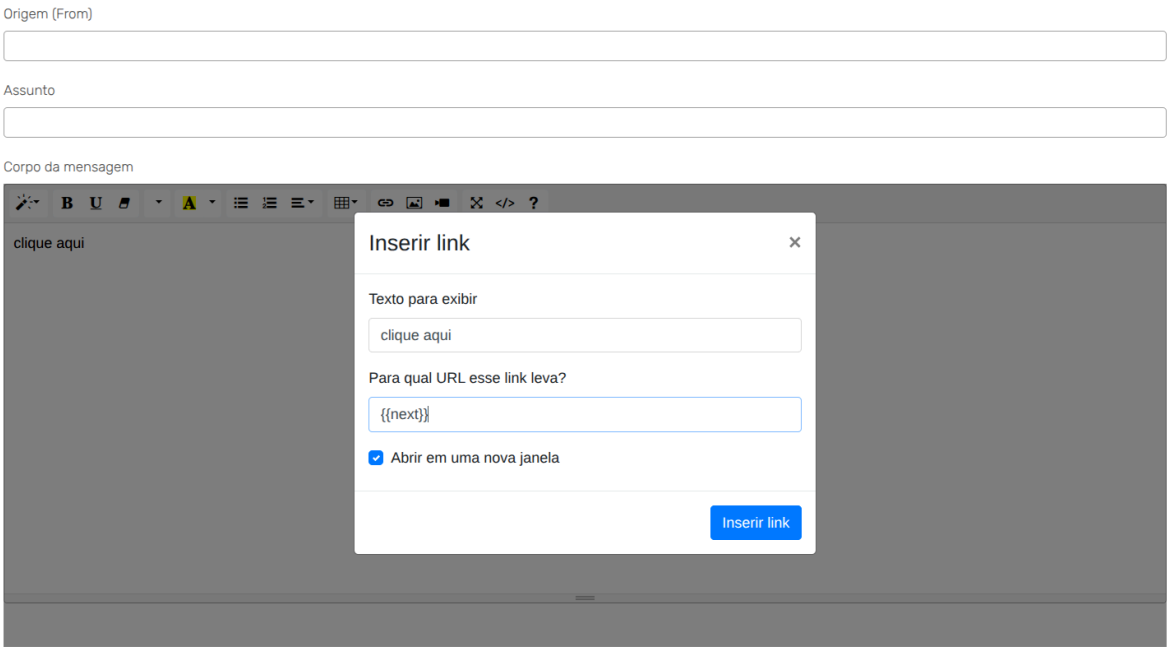
Para importar um template clique em **Importar** Clique em Importar e selecione o arquivo desejado. O arquivo utilizado para importação deverá estar no formato .eml.

Após a importação, as informações do template serão preenchidas para utilização e edição na campanha.

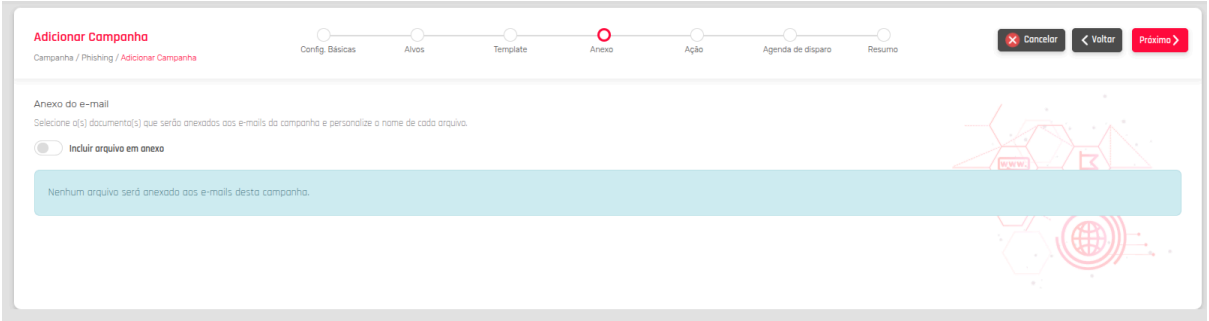
Também é possível criar um template do zero, preenchendo manualmente os campos conforme o necessário. Preencha a origem (deixe sem o domínio, pois ele será preenchido automaticamente), o assunto e o corpo da mensagem, onde é possível adicionar fotos, arquivos PDF, Word, Excel e colar códigos HTML.

Lembre-se de sempre adicionar um link com a variável **{{next}}**, da forma que está no print, para templates personalizados. Essa variável é responsável por contabilizar os cliques e redirecionar os usuários.

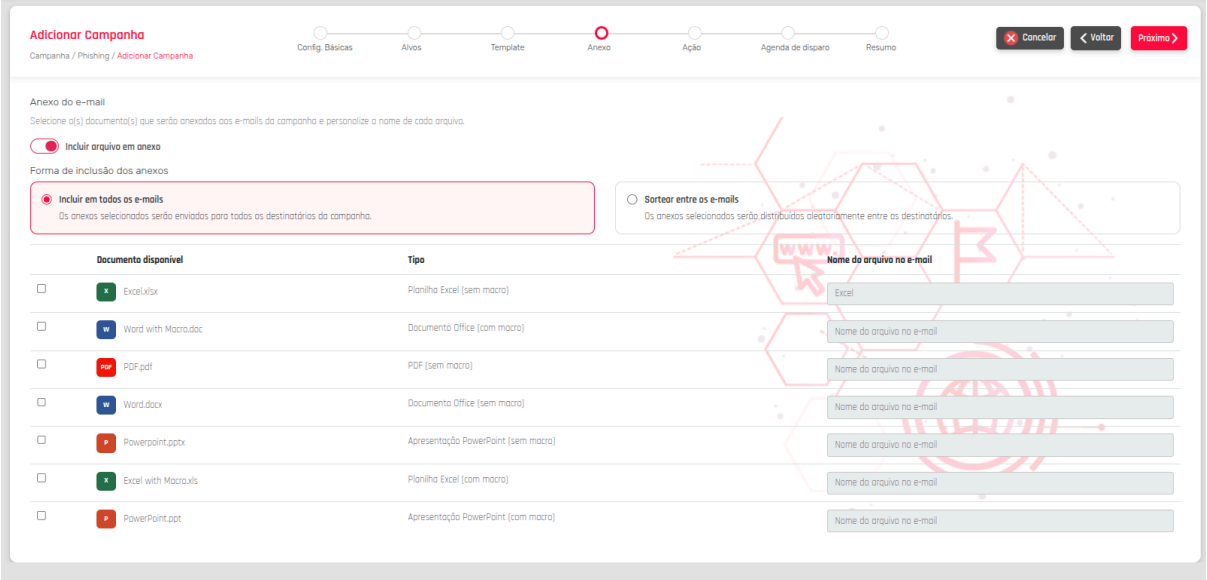
Também é possível utilizar a variável **{{qrcode}}**, que gera automaticamente um QR Code apontando para o mesmo link da variável **{{next}}** e o anexa à mensagem. Essa funcionalidade permite criar campanhas de simulação de phishing por meio da leitura de QR Codes (*Quishing*), avaliando o comportamento dos usuários diante desse tipo de ameaça.



4) Na etapa **Anexo**, durante a criação de uma campanha de simulação de phishing, o administrador poderá definir se os e-mails enviados aos usuários terão arquivos anexados.



Para incluir arquivos na campanha, habilite a opção **Incluir arquivo em anexo**. Ao ativar essa funcionalidade, serão apresentadas as opções de configuração e os documentos disponíveis para seleção.



A plataforma permite definir como os arquivos selecionados serão distribuídos aos destinatários da campanha, oferecendo duas opções:

- **Incluir em todos os e-mails:** Os arquivos selecionados serão enviados para todos os destinatários da campanha.
- **Sortear entre os e-mails:** Os arquivos selecionados serão distribuídos aleatoriamente entre os destinatários da campanha.

Logo abaixo, será apresentada uma lista com os documentos disponíveis para utilização na simulação.

Entre os tipos de arquivos disponíveis estão:

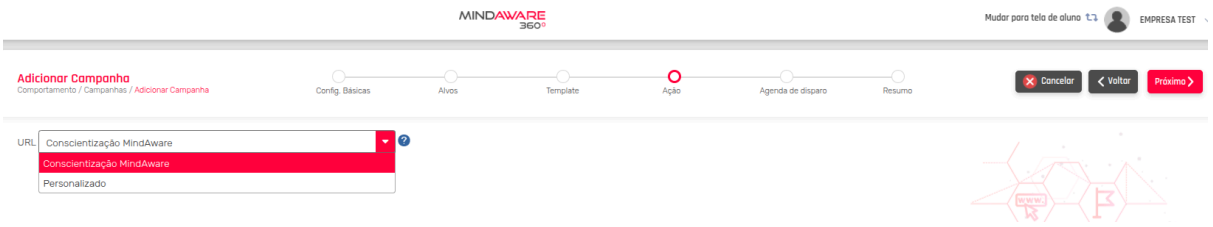
- **Excel (.xlsx):** Planilha Excel sem macro.
- **Word (.docx):** Documento Word sem macro.
- **PDF (.pdf):** Documento em formato PDF.
- **PowerPoint (.pptx):** Apresentação PowerPoint sem macro.
- **Excel com Macro (.xls):** Planilha Excel com macro.
- **Word com Macro (.doc):** Documento Word com macro.
- **PowerPoint com Macro (.ppt):** Apresentação PowerPoint com macro.

Para selecionar um documento, marque a caixa de seleção correspondente ao arquivo desejado. O administrador poderá personalizar o nome que será apresentado ao destinatário quando o documento for recebido como anexo.

Após selecionar os documentos, definir a forma de distribuição e informar os nomes desejados para os arquivos, clique em **Próximo** para continuar a configuração da campanha.

Caso não deseje utilizar arquivos anexados, mantenha a opção **Incluir arquivo em anexo** desabilitada e clique em **Próximo** para avançar para a etapa seguinte.

5) Selecionado os templates, na próxima etapa vamos definir a **Ação do Clique** do usuário, onde teremos duas opções para a escolha de direcionamento do clique para a sua devida URL:
    - **Personalizado:** Utilize esta opção quando for necessário direcionar o usuário para uma página específica ou personalizada de acordo com o objetivo da simulação.
    - **Conscientização MindAware:** Utilize esta opção para direcionar o clique do usuário para uma página padrão de aviso do MindWare.

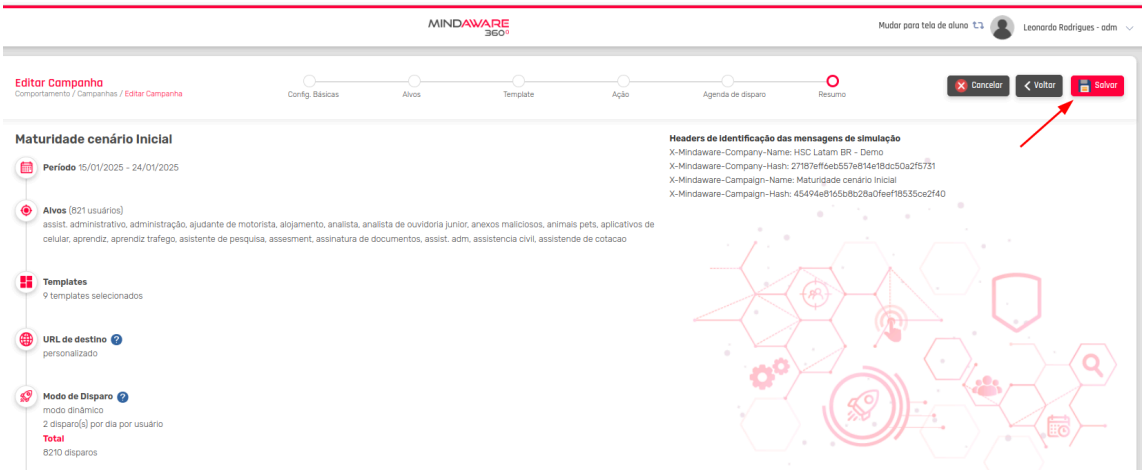


6) Na próxima etapa será definida a Agenda de Disparos, que poderá ser:

- **Modo Dinâmico:** Neste modo, os disparos serão feitos em intervalos regulares respeitando a configuração de disparos definida. Ao utilizar esta opção, são utilizadas técnicas para evitar disparos e templates similares entre os alvos aumentando a legitimidade da campanha.
- **Modo Estático:** Neste modo, os disparos seguem a agenda definida na configuração. Utilize esta opção quando as campanhas precisam ser disparadas em horários específicos. Esta opção utiliza apenas 01 template por agenda de disparo para todos usuários.



7) Na última etapa será exibido um resumo da campanha, ou seja, todas as configurações realizadas:
    - Período;
    - Alvos;
    - Templates;
    - URL de destino;
    - Modo de Disparo



Após a criação, é possível acompanhar a execução e os resultados diretamente pela plataforma.

Para acessar os detalhes, localize a campanha desejada e aplique um duplo clique sobre ela.

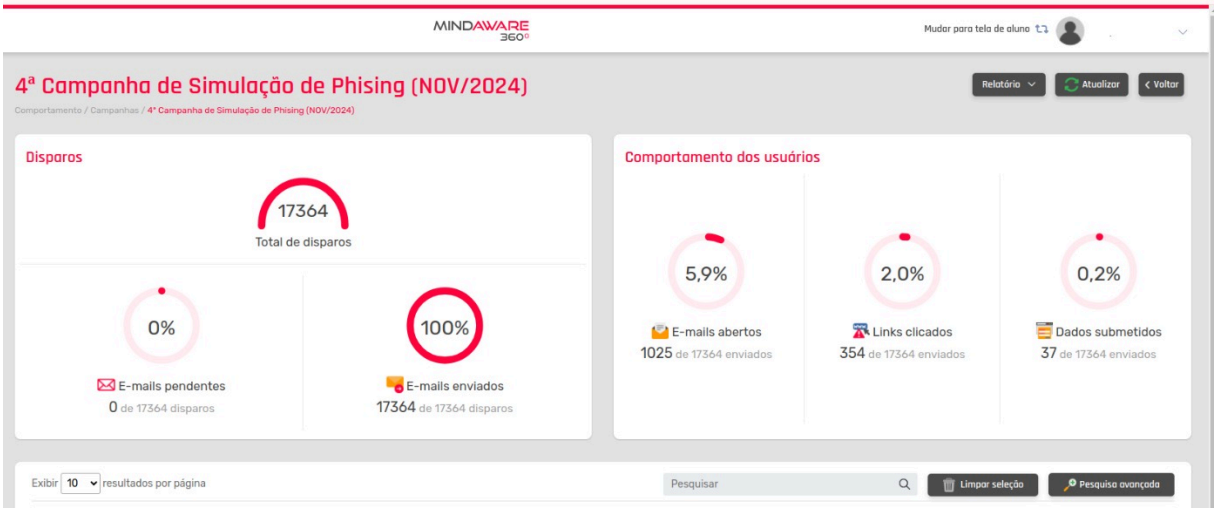
Será apresentado um painel com informações relacionadas aos disparos e às interações realizadas pelos usuários. É possível filtrar os usuários por departamento, cargo, localidade e demais informações pelo filtro.

Entre os indicadores que podem ser acompanhados estão:

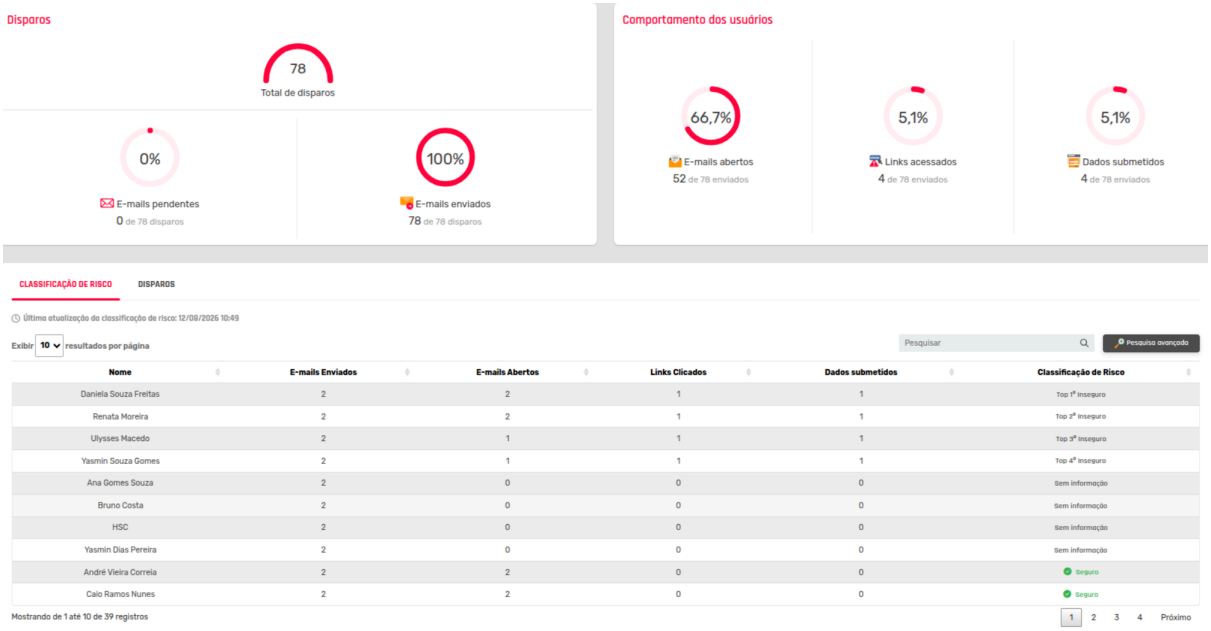
- total de usuários participantes;

- mensagens enviadas;
- mensagens abertas;
- links acessados;
- dados submetidos;
- demais eventos registrados durante a simulação.

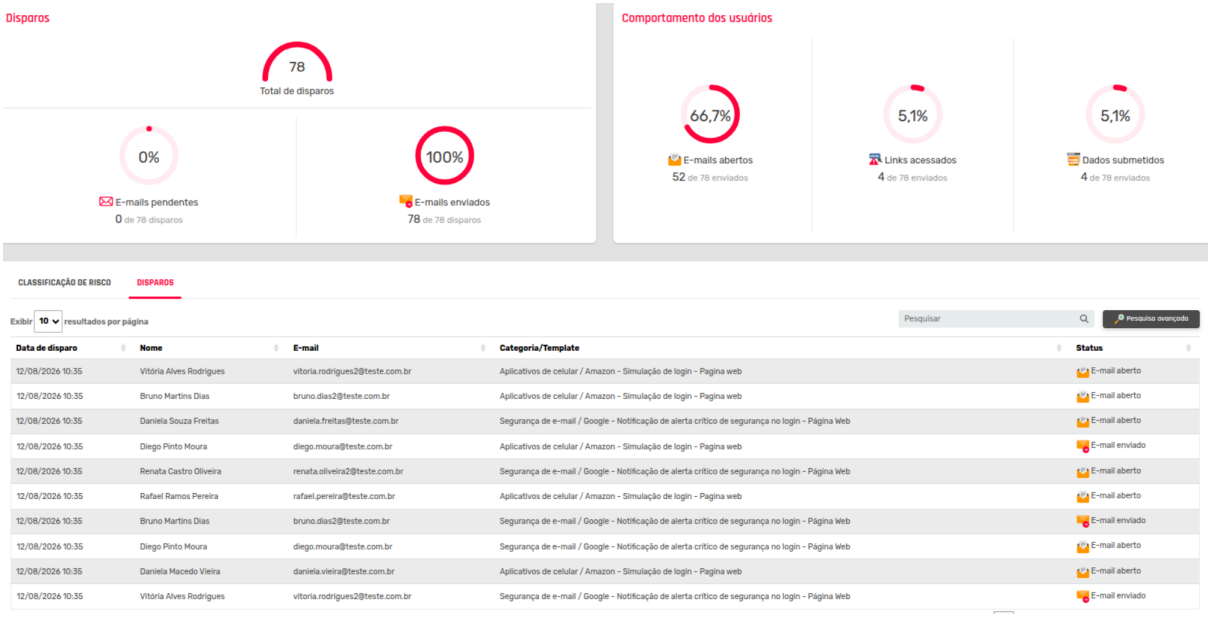
A solução registra individualmente as interações dos participantes, possibilitando avaliar a efetividade da campanha e identificar usuários que apresentaram comportamentos de maior risco.



Em **Classificação de Risco**, é possível visualizar os usuários de acordo com seu comportamento durante a campanha de phishing. Os usuários classificados como mais inseguros são aqueles que realizaram ações de risco, como clicar em links ou fornecer dados. Já os usuários seguros são aqueles que visualizaram o e-mail simulado, mas não realizaram nenhuma ação insegura. Os usuários classificados como **Sem Informação** são aqueles que ainda não visualizaram o e-mail da campanha. Esses dados são utilizados também para a seleção automática de templates com base no histórico do usuário.



Em **Disparos**, é possível visualizar o status individual de cada usuário, permitindo acompanhar de forma detalhada sua participação e as interações realizadas durante a campanha.



Nessa tela tem o botão **“Relatórios”** onde terá duas opções para gerar os relatórios da campanha selecionada:



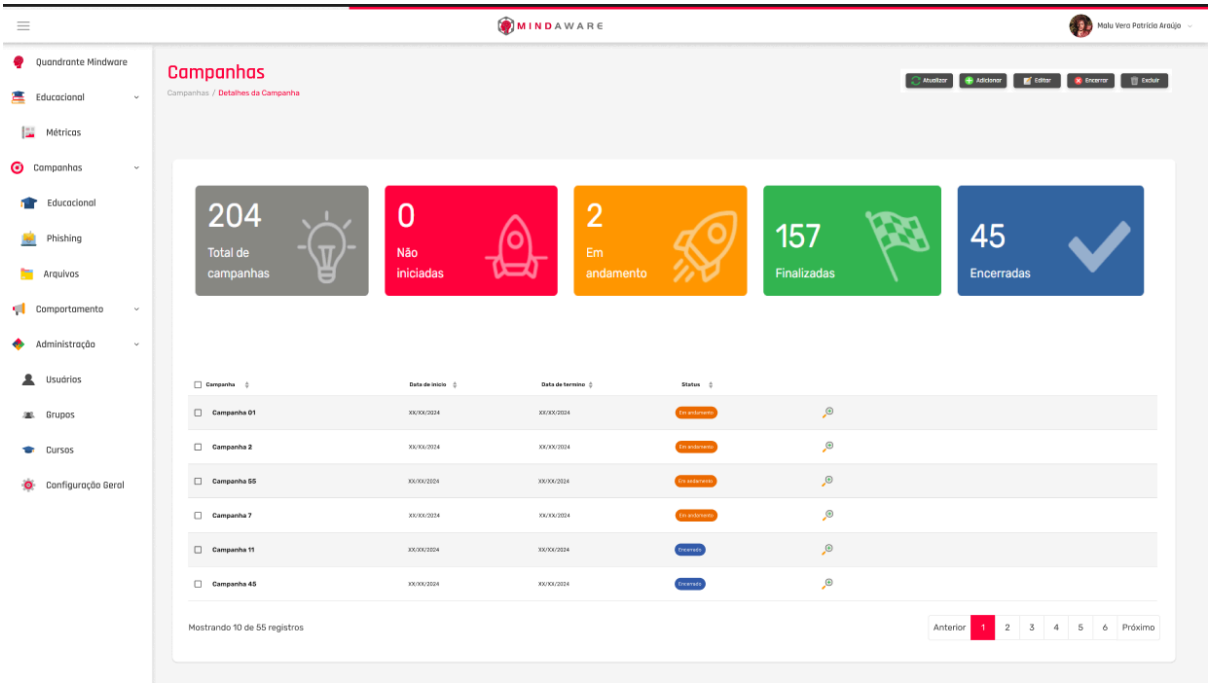
- **Relatório Estratégico (PDF)** – Gera um documento em PDF com as principais métricas e análises da campanha.

- **Log de Disparos (CSV)** – Exportar um arquivo em formato CSV contendo o histórico detalhado de todos os disparos realizados, acessos únicos e totais e ações de cada usuário.

Campanha de Documento

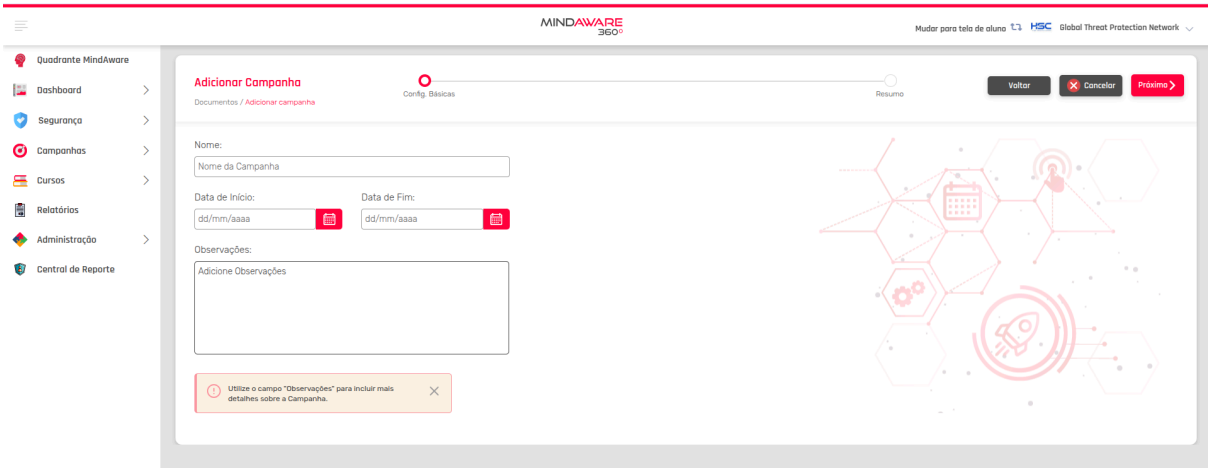
O objetivo é realizar simulações de ataques por meio de downloads em dispositivos USB ou arquivos enviados por qualquer canal, avaliando como os usuários reagem à abertura de documentos potencialmente maliciosos. Com isso, administradores conseguem configurar arquivos específicos, editar o nome dos arquivos, acompanhar o engajamento e analisar indicadores de segurança das ações realizadas.

Com acesso de Admin da empresa no Menu principal em **Campanhas > Arquivos.**

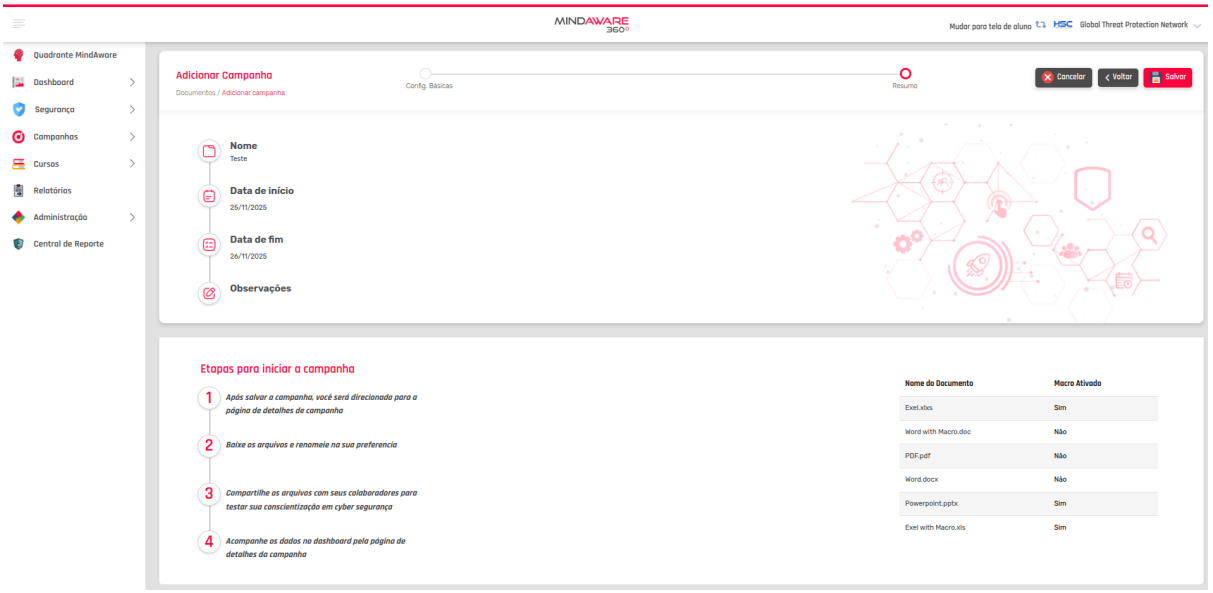


O administrador passa a contar com uma visão centralizada e detalhada do desempenho das campanhas de Arquivos e Documentos, garantindo maior controle, rastreabilidade e melhor análise do comportamento dos usuários.

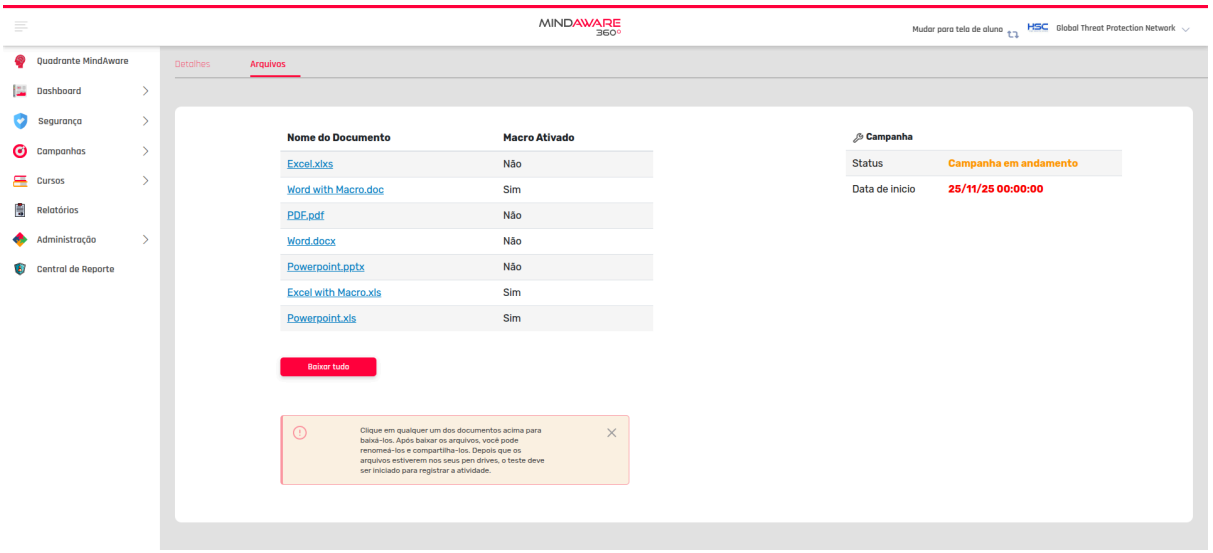
Na opção **Adicionar** Campanha, é possível configurar todas as informações necessárias, incluindo nome da campanha, datas de início e término e um campo de observações para registrar detalhes adicionais sobre o objetivo ou contexto da campanha.



Após o preenchimento das informações em **Próximo** vai mostrar o resumo e as indicações das etapas para iniciar a campanha.



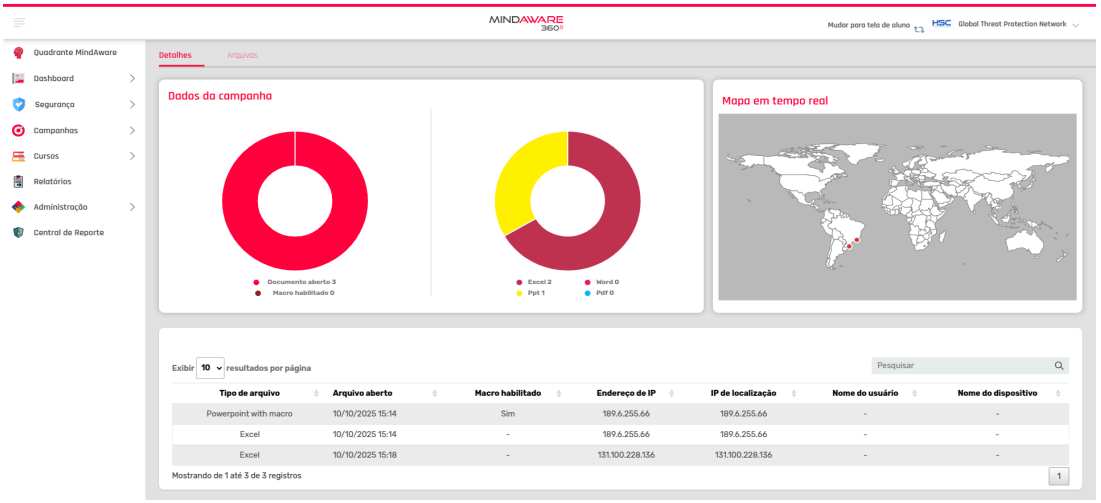
Após o preenchimento das informações, ao clicar em **Próximo**, será exibido um resumo da configuração e as etapas necessárias para iniciar a campanha.



Na aba Detalhes, é possível analisar todas as interações dos usuários com os arquivos da campanha, identificando se o documento foi apenas aberto ou se houve habilitação de macro. Também é possível visualizar quais arquivos receberam maior número de interações.

A tabela apresenta de forma detalhada:

- Tipo de arquivo
- Data e hora da abertura
- Indicação de macro habilitada
- Endereço IP e localização
- Nome do usuário
- Nome do Dispositivo (quando disponível)



Campanha de Vishing

A plataforma MindAware 360° permite realizar campanhas comportamentais de **Vishing**, uma modalidade de engenharia social que utiliza ligações telefônicas para simular tentativas de obtenção de informações dos colaboradores.

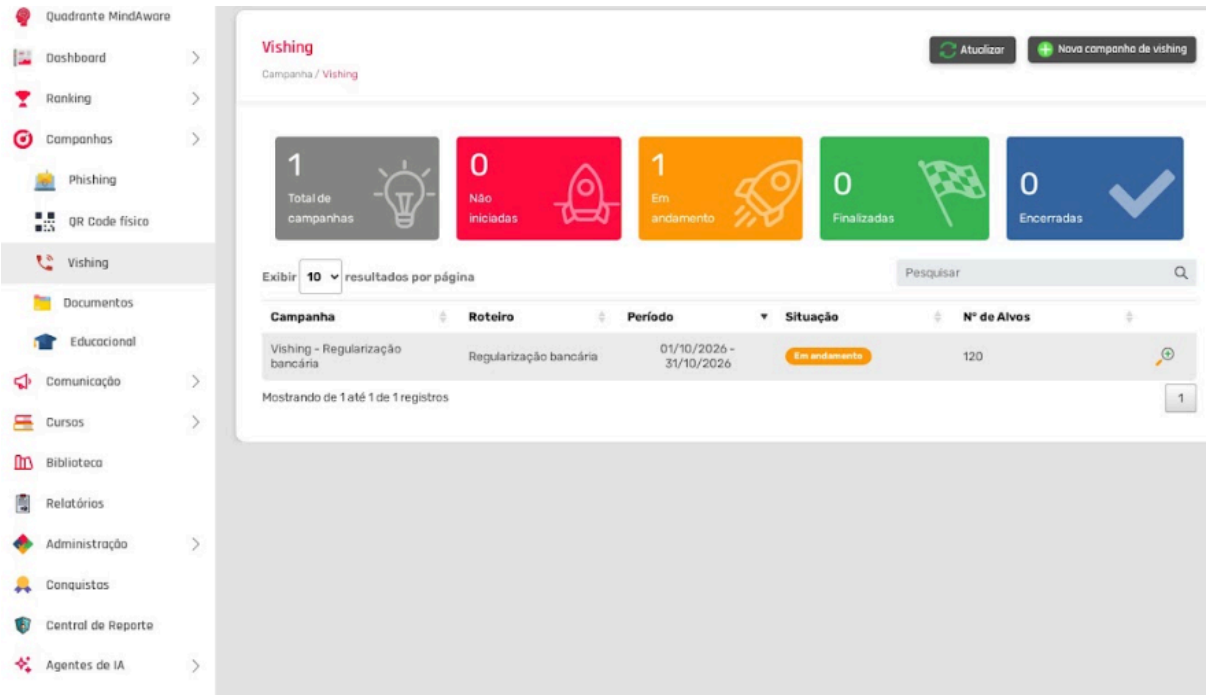
Essa funcionalidade possibilita avaliar o comportamento dos usuários diante de contatos telefônicos suspeitos, identificando situações em que o participante realiza uma ligação, informa um código de identificação ou fornece os dados solicitados durante a simulação.

As campanhas de Vishing utilizam roteiros que reúnem modelos de e-mail, mensagens de atendimento telefônico e orientações educativas, permitindo que o administrador configure diferentes cenários de conscientização.

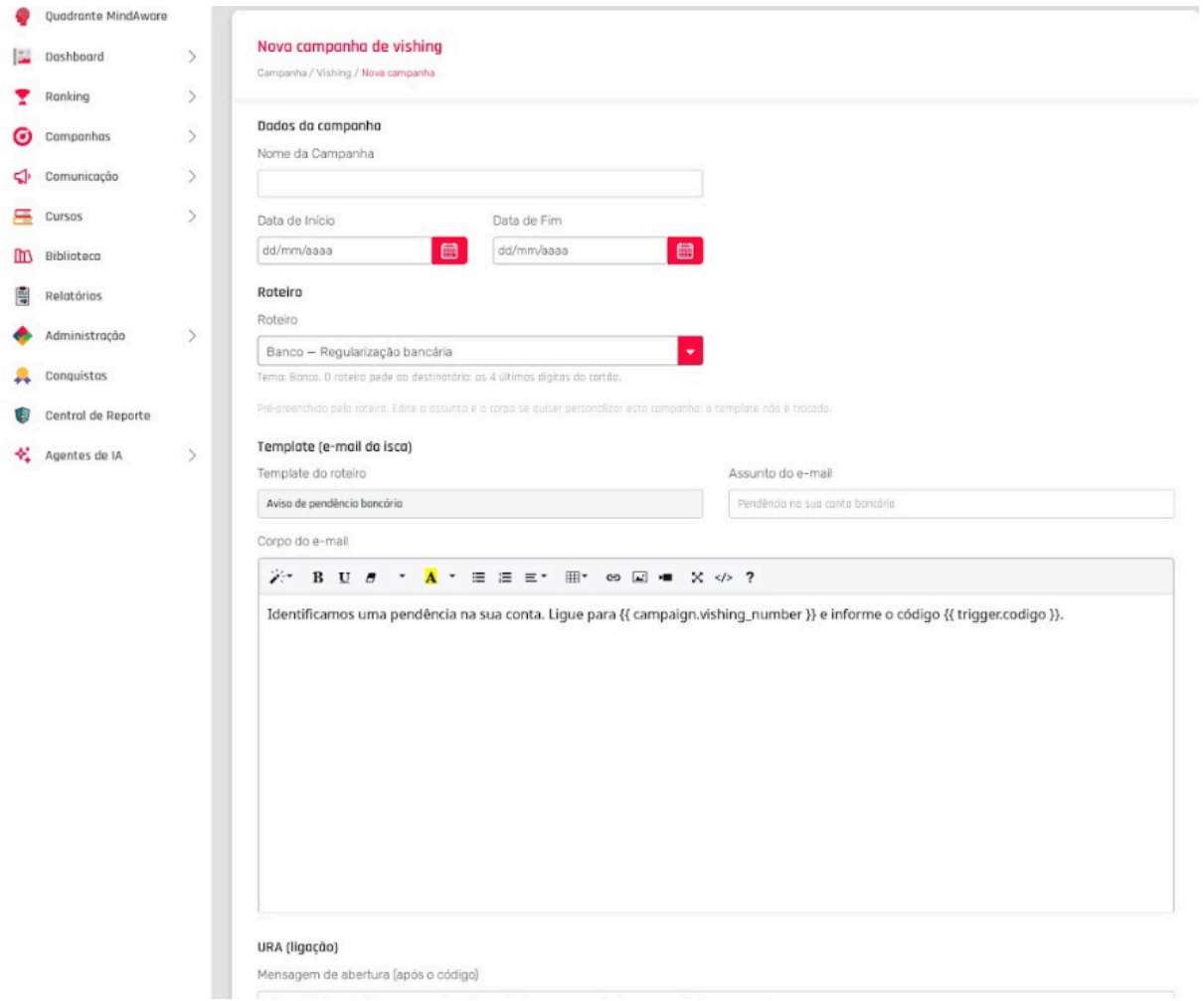
Além da criação e gerenciamento das campanhas, a plataforma disponibiliza indicadores, relatórios e dashboards para acompanhar os resultados e analisar o comportamento dos participantes.

Criação de Campanhas de Vishing

Para criar uma campanha de Vishing clique no botão **Nova campanha de vishing** e será aberto um formulário para preenchimento das informações e configurações da campanha.



E então abrirá uma tela onde o administrador deverá preencher as seguintes informações:



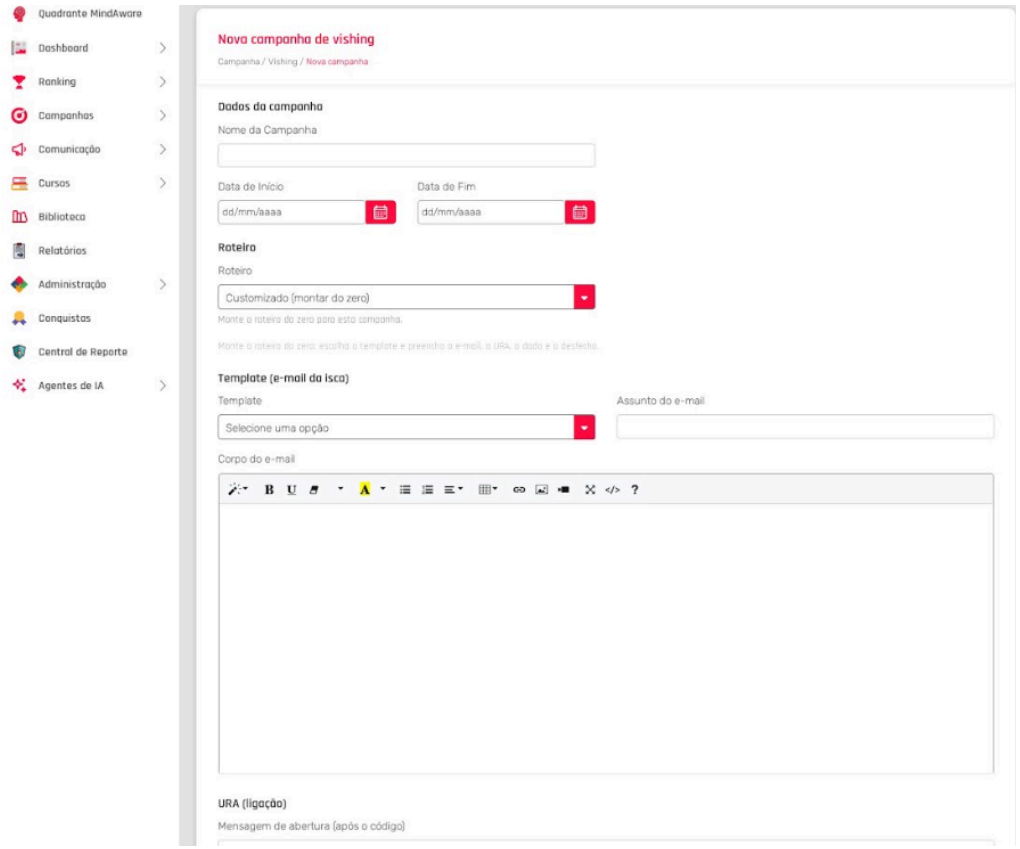
- **Nome da Campanha:** Identificação da campanha que será realizada.
- **Data de Início:** Define a data prevista para o início da campanha.
- **Data de Fim:** Define a data prevista para o encerramento da campanha.
- **Roteiro:** Permite selecionar um roteiro de Vishing previamente cadastrado ou criar um roteiro customizado. O roteiro determina as informações e mensagens utilizadas durante a simulação, incluindo o conteúdo do e-mail e as etapas da ligação telefônica.

O administrador poderá utilizar um roteiro existente ou selecionar a opção **Customizado (montar do zero)** para configurar uma nova simulação.

Quando um roteiro existente é selecionado, a plataforma apresenta as informações associadas ao roteiro, permitindo que o administrador revise o conteúdo antes de continuar.

Campanha Customizada

Caso o administrador deseje configurar uma campanha personalizada, deverá selecionar a opção **Customizado (montar do zero)** no campo Roteiro.



Em seguida, será necessário configurar:

- **Template (e-mail da isca):** Modelo de e-mail utilizado para apresentar a simulação ao colaborador.
- **Assunto do e-mail:** Define o assunto da mensagem enviada.
- **Corpo do e-mail:** Permite editar o conteúdo da comunicação utilizando o editor disponibilizado pela plataforma.
- **URA (ligação):** Define as mensagens e instruções apresentadas durante o atendimento telefônico.
- **Pedido do dado:** Informação que será solicitada ao participante durante a simulação.
- **Desfecho:** Mensagem educativa apresentada ao final da interação.

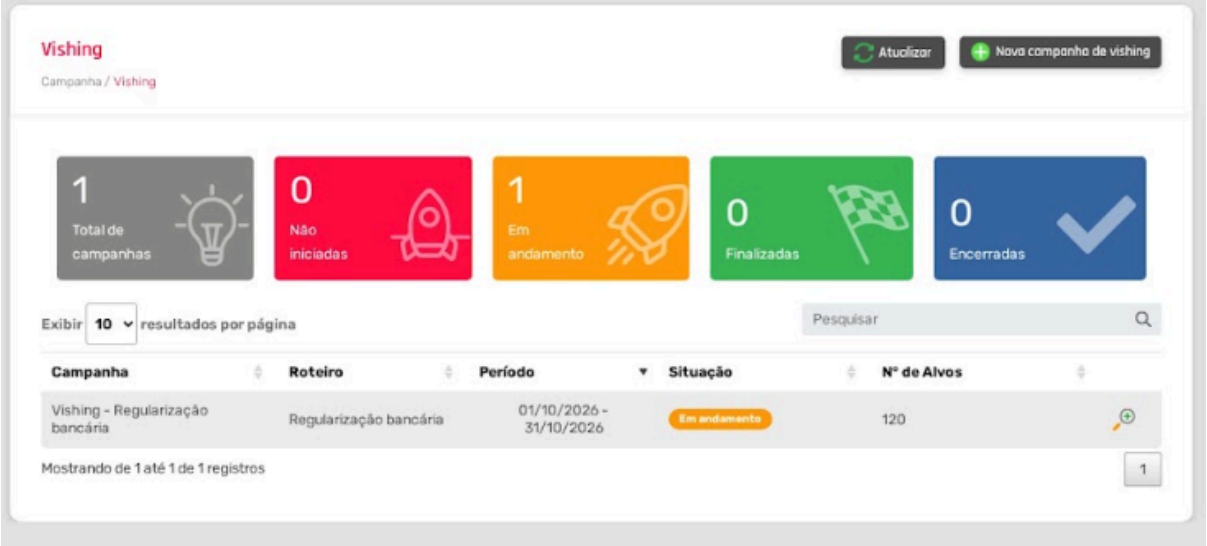
Após preencher as informações, o administrador deverá revisar as configurações da campanha e concluir as demais etapas do formulário.

Importante: Quando utilizadas no conteúdo do e-mail, as variáveis **{{ campaign.vishing_number }}** e **{{ trigger.codigo }}** devem ser preservadas, pois representam, respectivamente, o telefone da campanha e o código de identificação utilizado durante a ligação.

Gerenciamento das Campanhas de Vishing

O administrador poderá visualizar e acompanhar todas as campanhas cadastradas na plataforma.

Na parte superior da tela, são apresentados indicadores que permitem identificar a quantidade de campanhas conforme sua situação.



Logo abaixo, será exibida uma tabela contendo as informações das campanhas.

Nessa tabela, o administrador poderá consultar:

- **Campanha:** Nome da campanha cadastrada.
- **Roteiro:** Roteiro utilizado na simulação.
- **Período:** Data de início e término.
- **Situação:** Status atual da campanha.
- **Nº de Alvos:** Quantidade de usuários selecionados para participar.

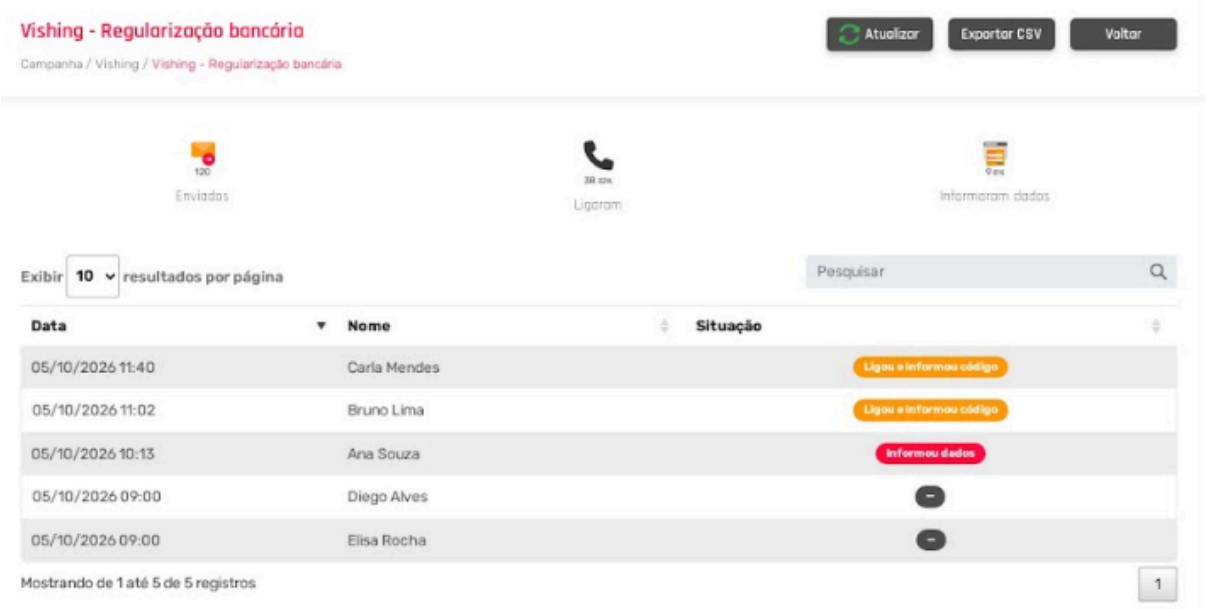
Para consultar os resultados de uma campanha, clique no **ícone de lupa** localizado ao lado do registro desejado.

Resultados das Campanhas de Vishing

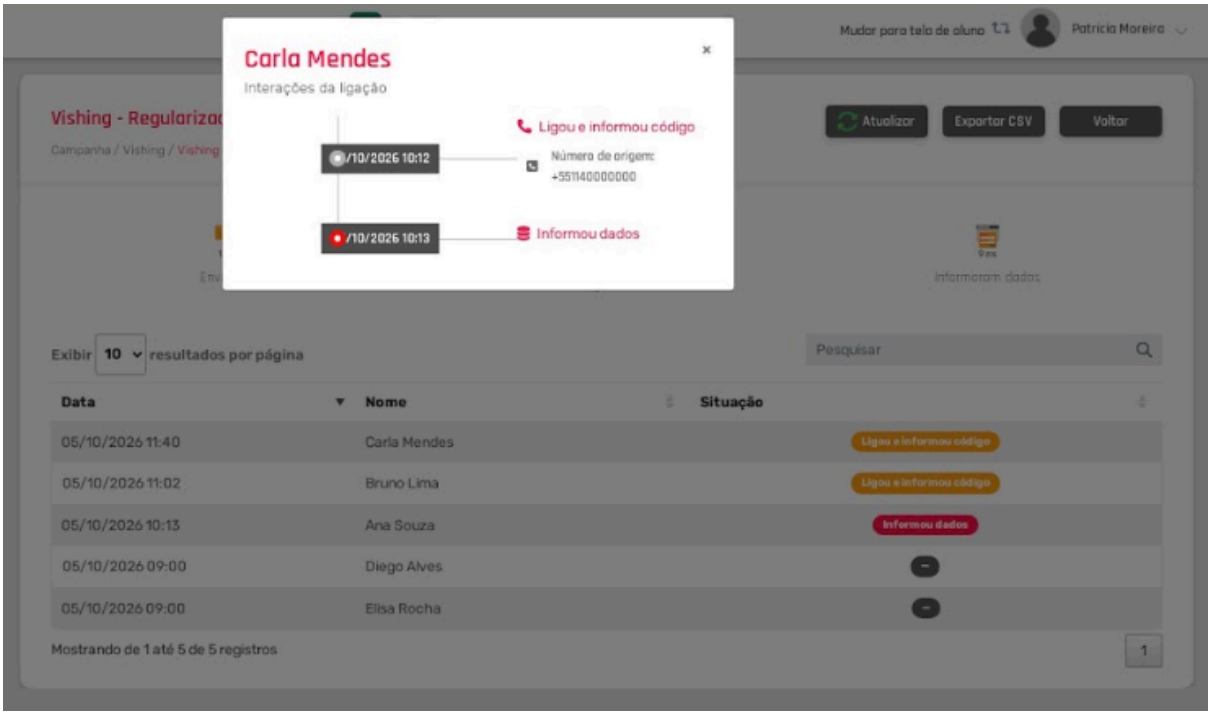
Ao selecionar uma campanha, será aberta uma tela contendo os resultados e as interações registradas durante a simulação.

Na parte superior, são apresentados os seguintes indicadores:

- **Enviados:** Quantidade de comunicações enviadas aos participantes.
- **Ligaram:** Quantidade de participantes que realizaram a ligação telefônica durante a campanha.
- **Informaram dados:** Quantidade de participantes que forneceram a informação solicitada durante a simulação.



Ao dar um duplo clique sobre o nome do usuário, será aberta uma janela com o histórico de interações da ligação, apresentando a data e o horário em que o participante realizou a chamada e, caso tenha fornecido os dados solicitados, a data e o horário em que essa ação foi registrada.

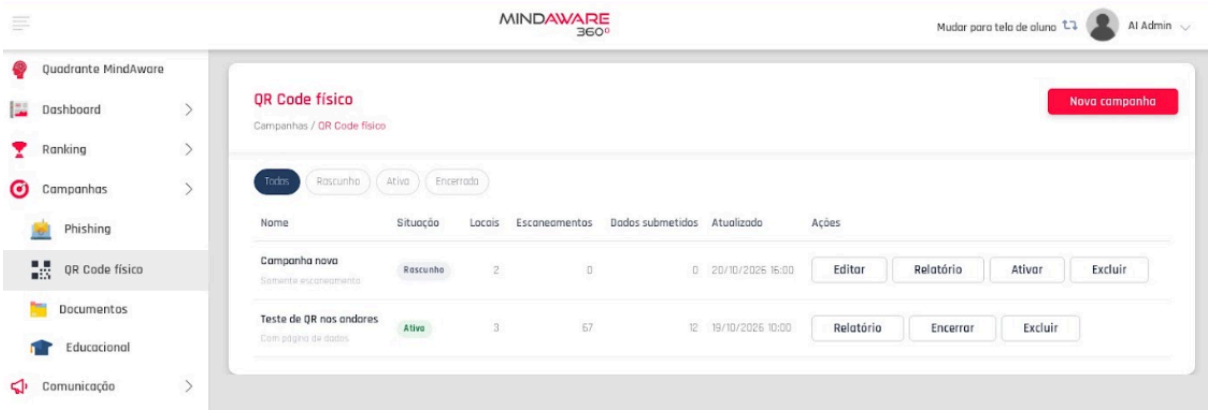


Esses indicadores permitem avaliar o comportamento dos colaboradores e identificar situações de maior exposição às técnicas de engenharia social por telefone.

Campanhas de QR Code Físico

O módulo **QR Code Físico** permite criar e gerenciar campanhas de conscientização em segurança da informação por meio de códigos QR disponibilizados em ambientes físicos da organização. A funcionalidade possibilita configurar páginas de destino, personalizar pôsteres e acompanhar as interações realizadas em cada local.

No menu lateral, acesse **Campanhas > QR Code físico**.



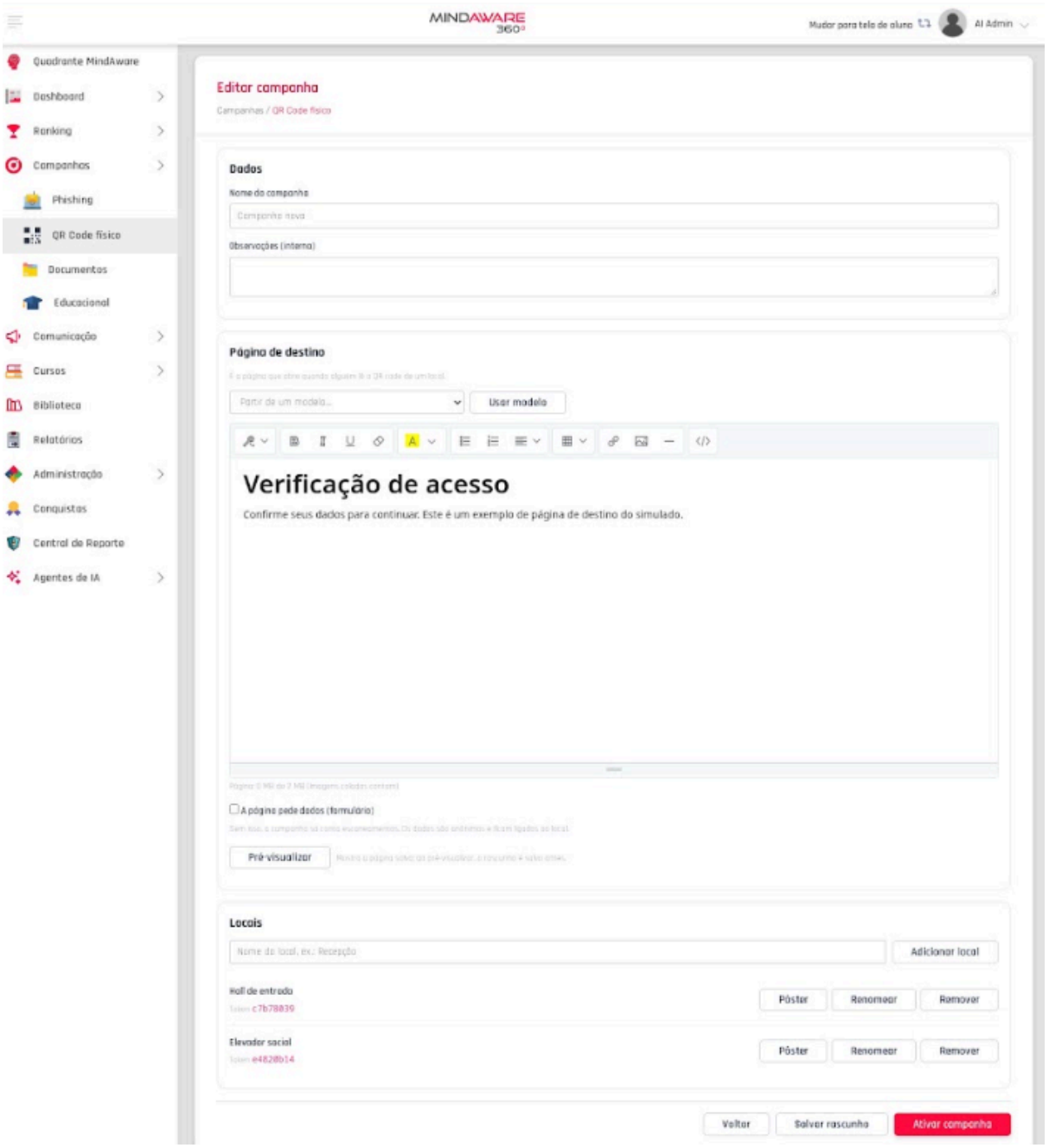
A plataforma apresentará a listagem das campanhas cadastradas.

Utilize os filtros **Todos, Rascunho, Ativo e Encerrado** para localizar as campanhas conforme sua situação.

A listagem apresenta o nome da campanha, situação, quantidade de locais, escaneamentos, dados submetidos e última atualização.

Configurar uma campanha

1. Clique em **Nova campanha**.
2. Na seção **Dados**, informe o nome da campanha e, se necessário, preencha o campo **Observações (interno)**.
3. Na seção **Página de destino**, selecione um modelo existente ou personalize o conteúdo utilizando o editor.
4. Habilite a opção **A página pede dados (formulário)** caso a simulação envolva o preenchimento de informações.
5. Clique em **Pré-visualizar** para conferir como a página será apresentada ao participante.



A página de destino corresponde ao conteúdo exibido após a leitura do QR Code. Quando a opção de formulário estiver desabilitada, a campanha contabilizará somente os escaneamentos.

Cadastrar os locais

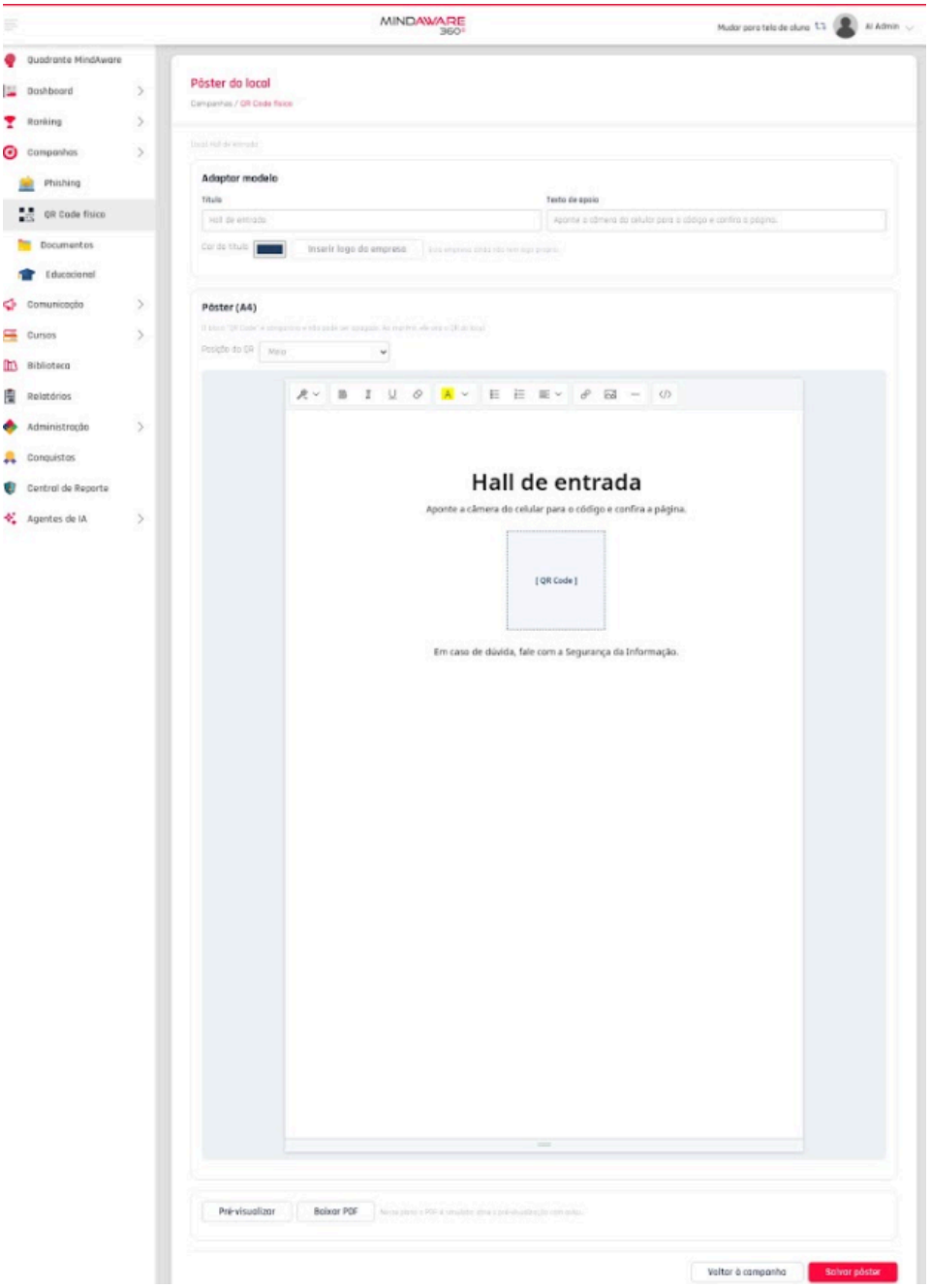
1. Na seção **Locais**, informe o nome do ambiente onde o QR Code será disponibilizado.
2. Clique em **Adicionar local**.

3. Repita o procedimento para cadastrar outros ambientes.
4. Utilize **Renomear** ou **Remover** para gerenciar os locais cadastrados.
5. Clique em **Pôster** para personalizar o material correspondente ao local.

Cada local possui um QR Code específico, permitindo acompanhar separadamente os resultados das interações.

Personalizar o pôster

1. Na seção **Adaptar modelo**, configure o título, o texto de apoio e a cor do título.



2. Insira o logotipo da empresa, caso esteja disponível.
3. Na seção **Pôster (A4)**, selecione a posição do QR Code.
4. Utilize o editor para personalizar o conteúdo do material.
5. Clique em **Pré-visualizar** para conferir o resultado.



6. Após a revisão, clique em **Salvar pôster**.

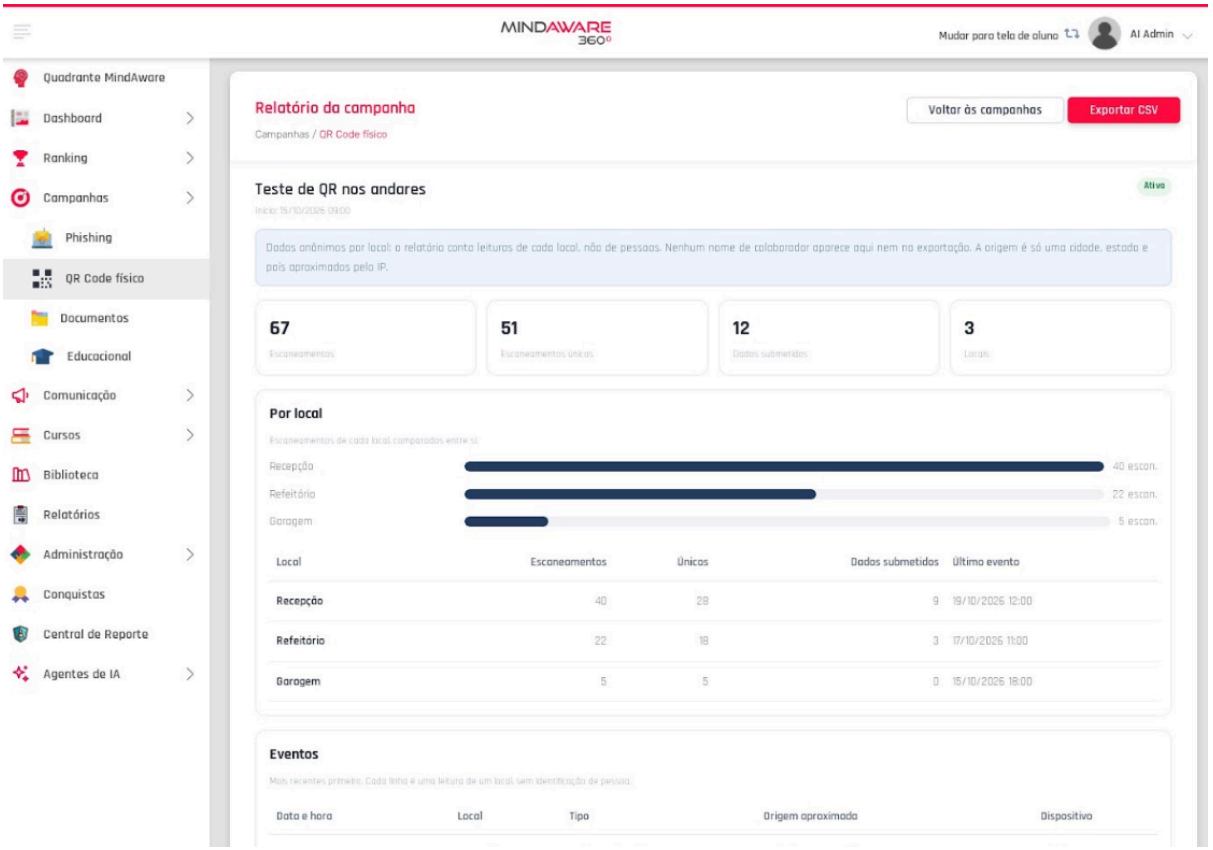
O bloco **[QR Code]** é obrigatório e será substituído pelo código correspondente ao local cadastrado.

Salvar e ativar a campanha

1. Revise as informações da campanha, a página de destino e os locais cadastrados.
2. Clique em **Salvar rascunho** para armazenar as configurações sem iniciar a campanha.
3. Quando estiver pronta, clique em **Ativar campanha**.
4. Para finalizar uma campanha ativa, utilize a opção **Encerrar** na listagem.

Consultar os resultados

Para consultar os resultados de uma campanha, acesse Campanhas > QR Code físico, localize a campanha desejada e clique em Relatório. A plataforma apresentará os indicadores gerais da campanha, incluindo o total de escaneamentos, escaneamentos únicos, dados submetidos e quantidade de locais cadastrados.



Na seção Por local, é possível visualizar um gráfico comparativo dos escaneamentos realizados em cada ambiente, além de uma tabela com a quantidade de escaneamentos, acessos únicos, dados submetidos e a data e o horário da última interação registrada.

Na seção Eventos, a plataforma apresenta o histórico das interações realizadas na campanha, organizadas da mais recente para a mais antiga. Cada registro contém a data e o horário da interação, o local associado ao QR Code, o tipo de evento (escaneamento ou submissão de dados), a origem geográfica aproximada e o dispositivo utilizado.

Os registros são anônimos e vinculados aos locais cadastrados, sem identificação nominal dos colaboradores. A localização geográfica é estimada com base no endereço IP.

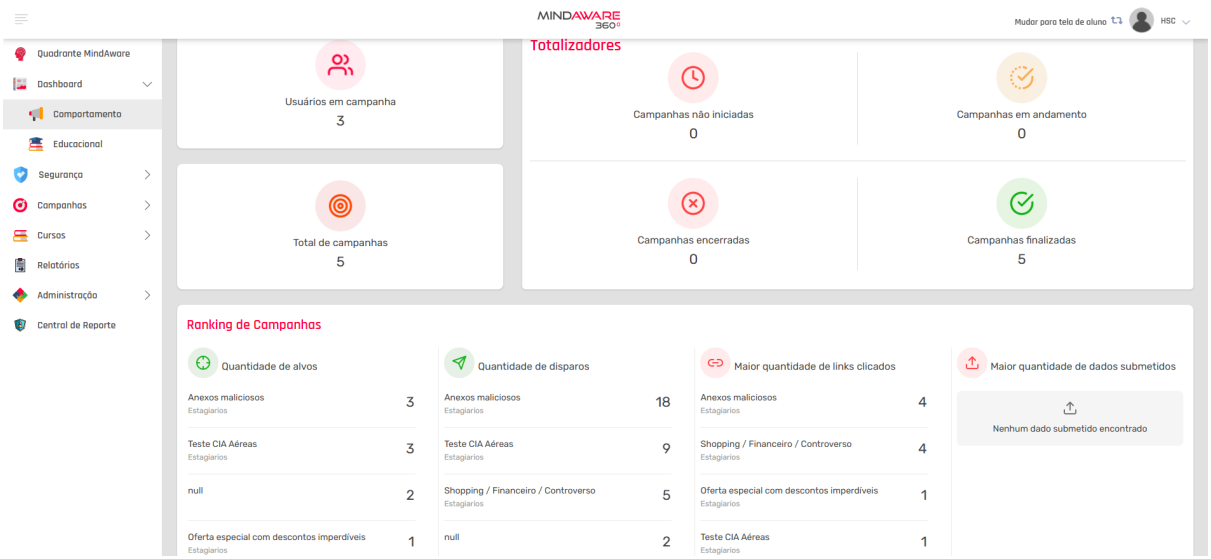
Para exportar os resultados, clique em Exportar CSV, localizado no canto superior direito da página.

Conteúdo educativo

A página de destino pode apresentar conteúdos de conscientização relacionados aos riscos de QR Codes maliciosos, orientando os participantes sobre a importância de verificar endereços, evitar o fornecimento de informações sensíveis e comunicar situações suspeitas à equipe de Segurança da Informação.

Dashboard

Essa seção mostra os dados e análises dos usuários em relação aos cursos e campanhas, dividindo-se em **Comportamento** e **Educacional**.



Comportamento

Nessa tela mostra as métricas das campanhas comportamentais, como **Usuários em campanha, Total de campanhas, Campanhas não iniciadas, Campanhas encerradas e Campanhas finalizadas.**



A plataforma mostra também alguns dados na forma de ranking, tais como:

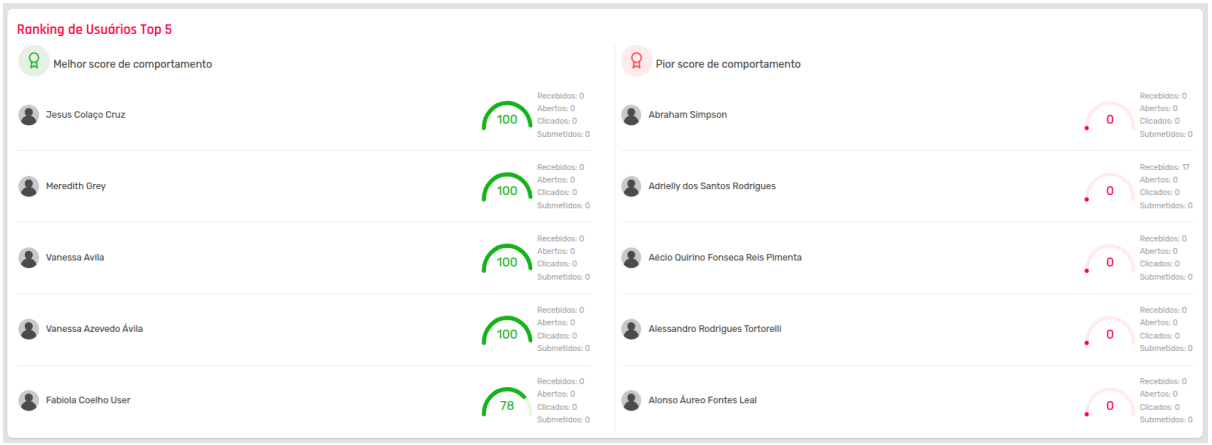
- Ranking de campanha: As campanhas que estão tendo maior quantidade de alvos, disparos, cliques e dados submetidos.



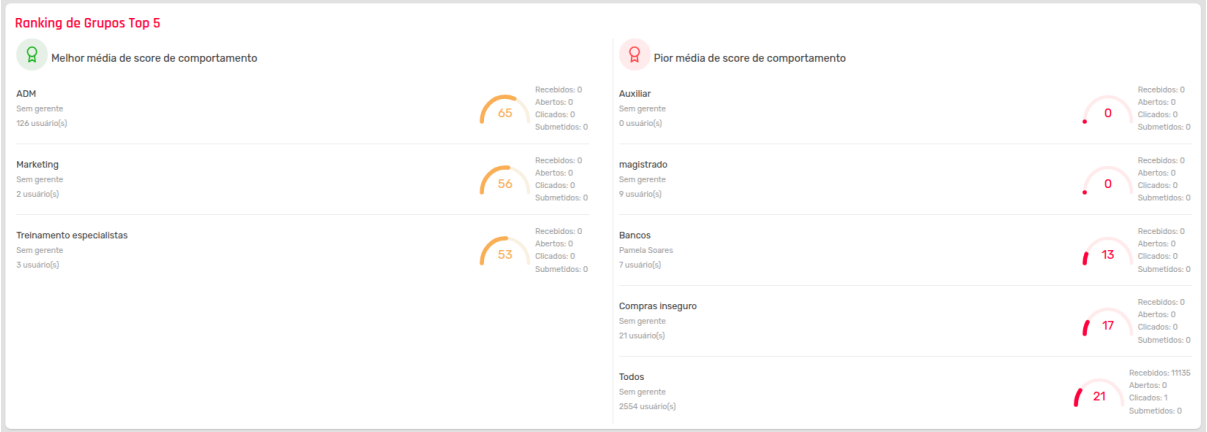
- Ranking da Categoria/Template: Mostra quais templates estão chamando mais atenção.



- Ranking de Usuários Top 5: Usuários que obtiveram o maior escore de melhor e de pior comportamento.

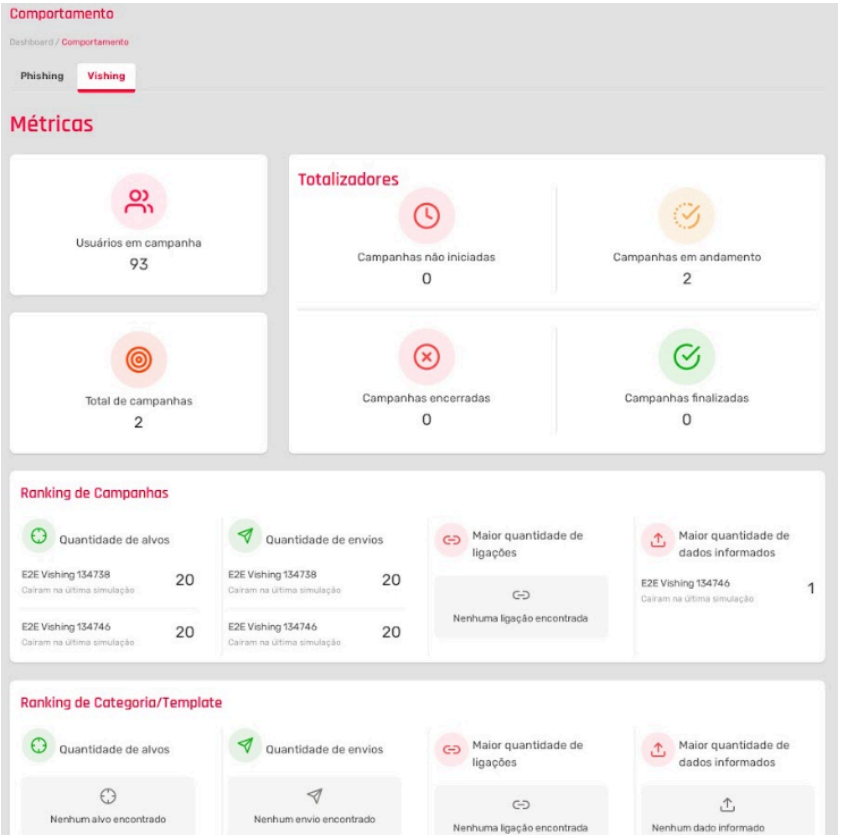


- Ranking de Grupos Top 5: Os grupos que obtiveram o maior escore de melhor e de pior comportamento.



Dashboard Comportamental — Vishing

Métricas das Campanhas



Na seção **Métricas**, o administrador poderá acompanhar os seguintes indicadores:

- **Usuários em Campanha:** Quantidade de usuários participantes das campanhas de Vishing.
- **Total de Campanhas:** Quantidade de campanhas cadastradas.

- **Campanhas Não Iniciadas:** Quantidade de campanhas que ainda não começaram.
- **Campanhas em Andamento:** Quantidade de campanhas em execução.
- **Campanhas Encerradas:** Quantidade de campanhas encerradas.
- **Campanhas Finalizadas:** Quantidade de campanhas concluídas.

Essas informações permitem acompanhar a execução das campanhas e visualizar o cenário geral das simulações realizadas pela organização.

Na seção **Ranking de Campanhas**, são apresentados os resultados das campanhas conforme os principais indicadores comportamentais.

O administrador poderá visualizar:

- **Quantidade de Alvos:** Campanhas com maior número de participantes.
- **Quantidade de Envios:** Campanhas com maior quantidade de comunicações enviadas.
- **Maior Quantidade de Ligações:** Campanhas que registraram mais ligações realizadas pelos participantes.
- **Maior Quantidade de Dados Informados:** Campanhas com maior número de participantes que forneceram as informações solicitadas.

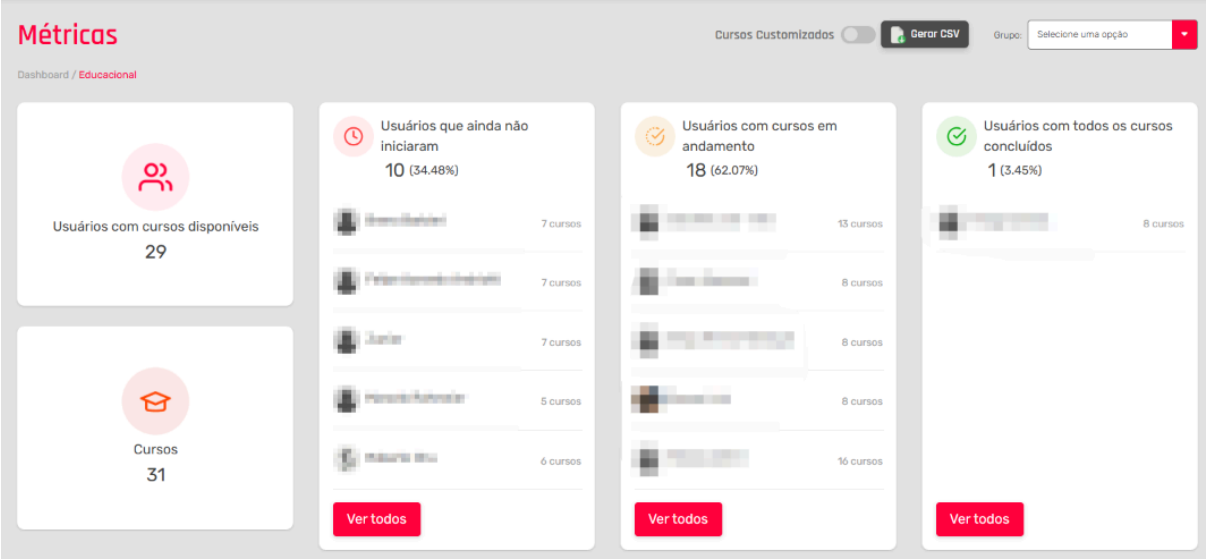
Esse ranking permite identificar quais campanhas apresentaram maior interação dos usuários e comparar os resultados das simulações.

A plataforma também disponibiliza o **Ranking de Categoria/Template**, que apresenta indicadores relacionados às categorias e aos modelos utilizados nas

Essas informações auxiliam na identificação dos modelos de engenharia social que geraram maior interação dos participantes.

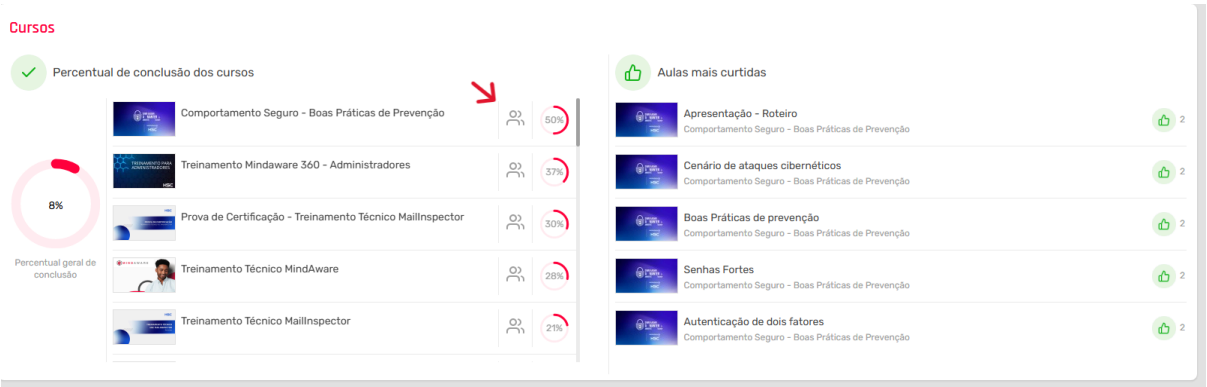
Educacional

Nesta seção, é possível realizar um acompanhamento geral do aproveitamento e rendimento dos colaboradores na realização dos treinamentos propostos. Abaixo veremos:

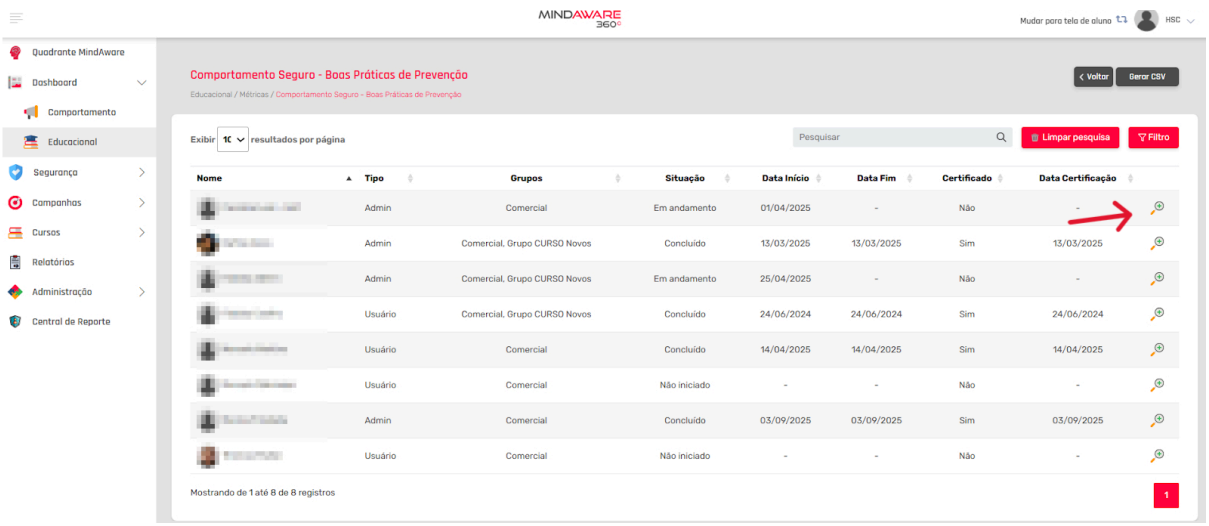


- **<u>Métricas de Cursos da Plataforma</u>**: Mostra a quantidade de usuários que possuem, a quantidade de cursos que a plataforma tem, os usuários que ainda não iniciaram os cursos, os que estão em treinamento e os que já terminaram todos os cursos disponíveis.

Abaixo também mostra o percentual de conclusão dos cursos e as aulas mais curtidas. Se quiser ver por curso o andamento dos usuários em relação a ele basta ir nesse ícone.

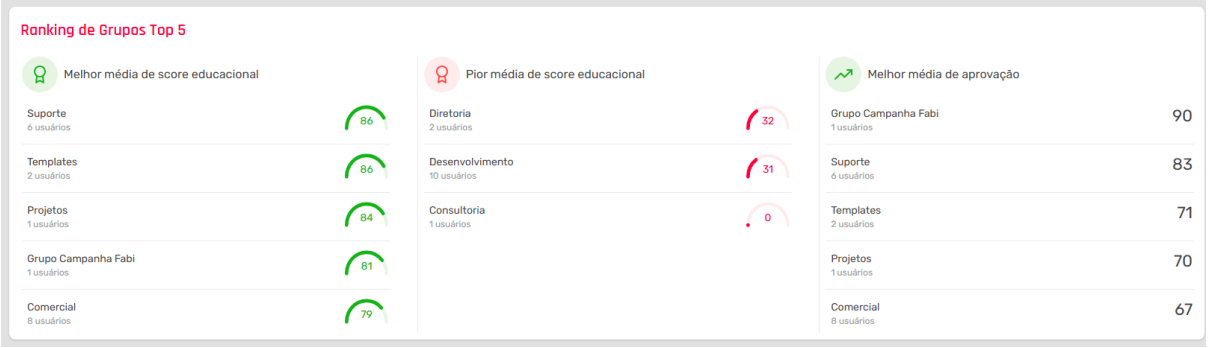


Nessa tela mostra as informações por usuário em relação ao curso escolhido.

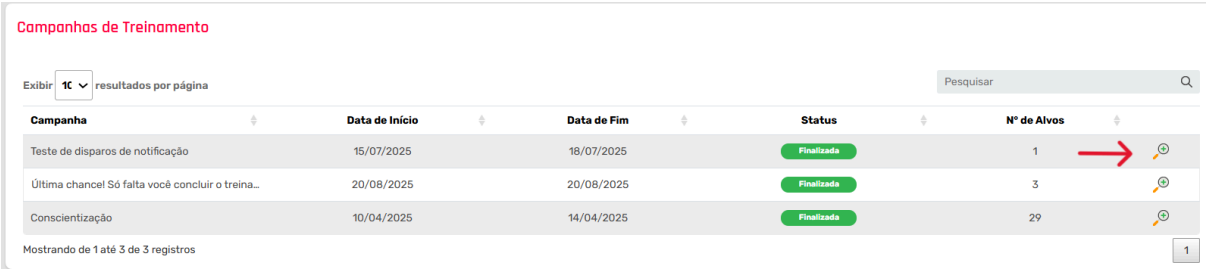


No ícone indicado é possível ver o dashboard por usuário que analisaremos em seguida.

Voltando para tela Dashboard educacional, temos os rankings dos grupos relacionados ao seu score e aprovação em cursos.

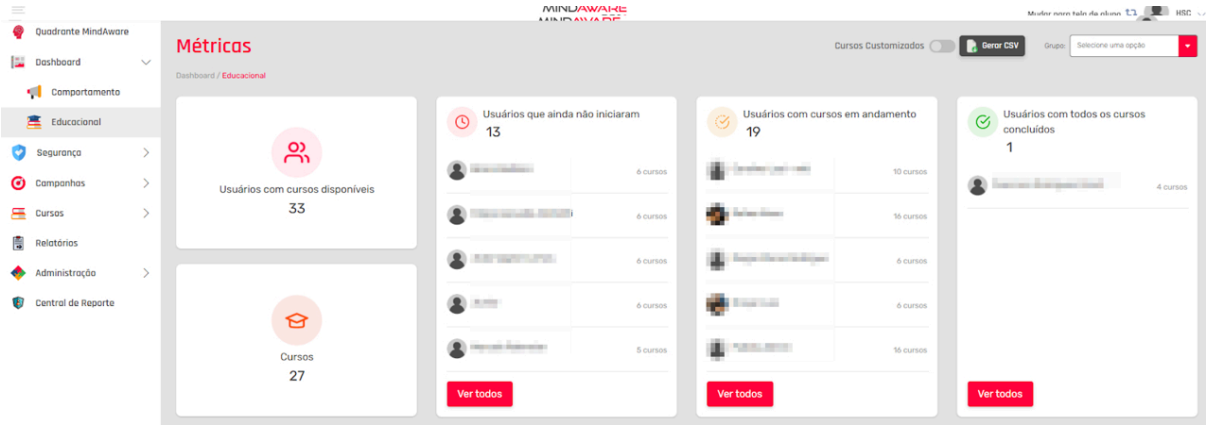


- **<u>Métricas de Campanhas Educacionais</u>**: Abaixo temos alguns dados das campanhas educacionais. Para acessar a análise dos resultados das campanhas clique no ícone.

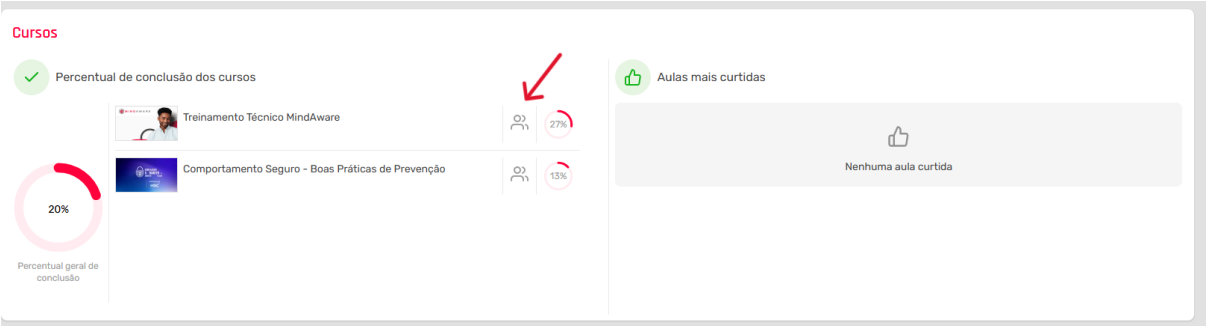


Ao selecionar uma campanha, será exibida uma tela com as métricas correspondentes. Nela, é possível visualizar a quantidade de usuários vinculados

à campanha que possuem cursos disponíveis, o total de cursos incluídos na campanha, o número de usuários que ainda não iniciaram nenhum curso, os usuários que possuem cursos em andamento e aqueles que já concluíram todos os cursos da campanha.



Abaixo mostra também o percentual de conclusão dos cursos, podendo assim como na tela anterior clicar no ícone e ver as métricas do curso escolhido por usuário.

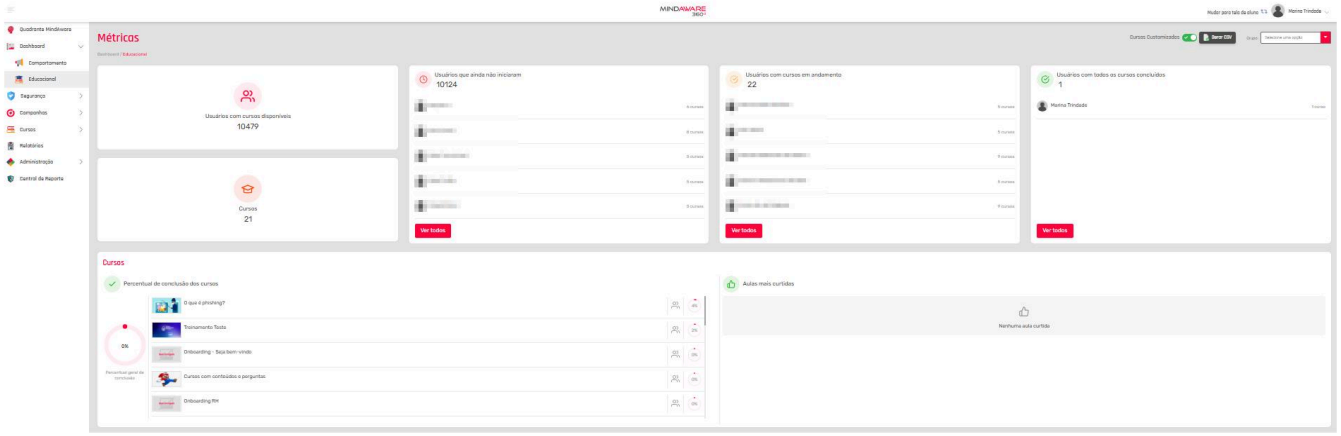


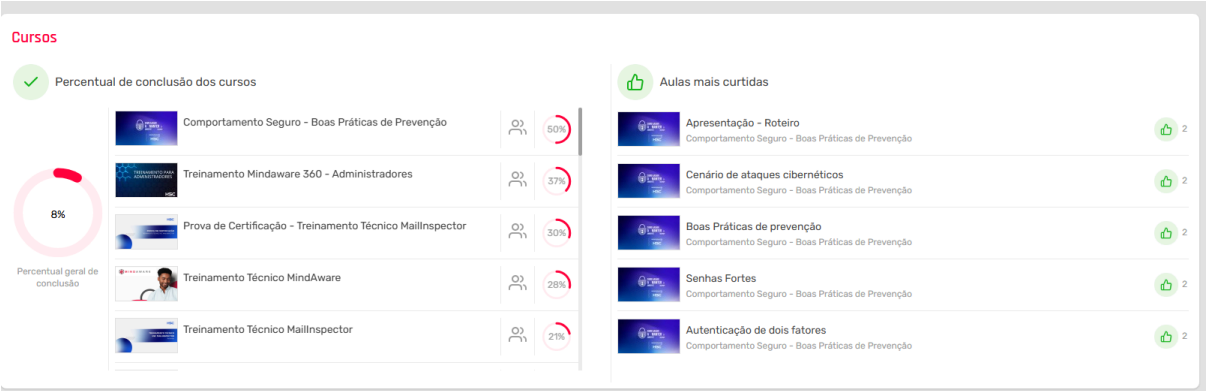
- **Métricas de Cursos Customizados**: Para visualizar as métricas dos cursos customizados, clique no botão indicado



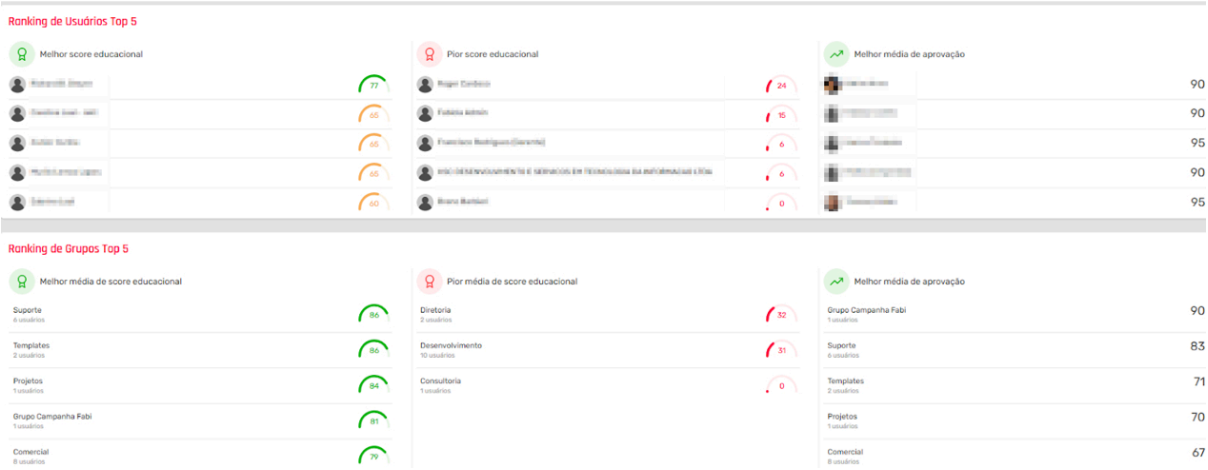
Assim aparecerá a tela de métricas de cursos customizados onde mostra:

- As análises dos usuários em relação aos cursos.

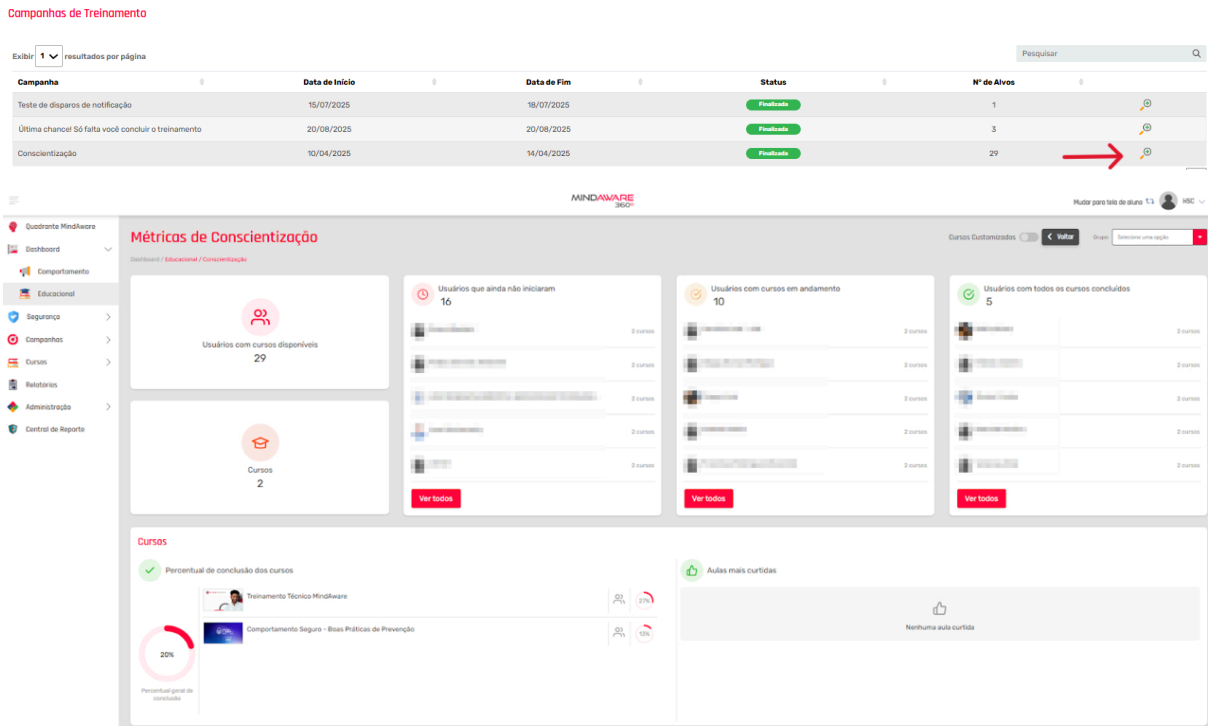




- Os rankings de score e aprovação por usuários e grupos.

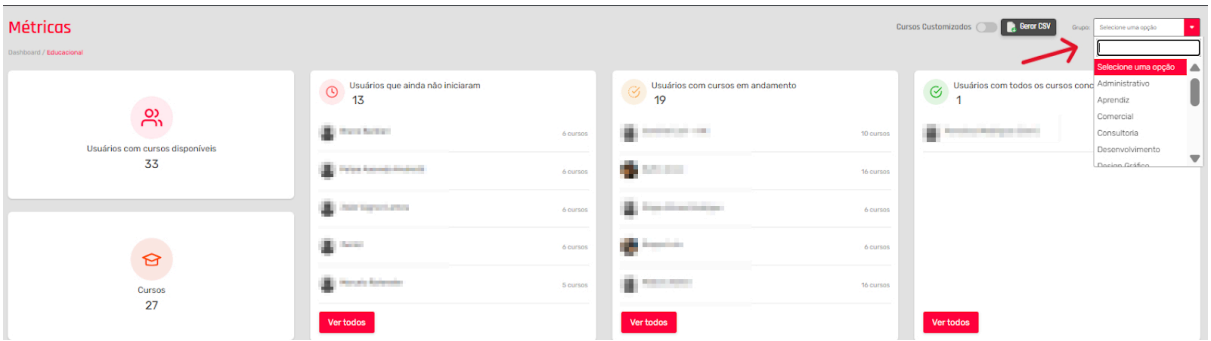


- E os detalhes das campanhas de treinamento, onde poderá acessar os detalhes de cada uma através do ícone indicado.



Dashboard por Grupo

Além das métricas totais ou por campanha, é possível visualizar os dados segmentados por grupo, selecionando a opção correspondente. Essa funcionalidade está disponível tanto para as métricas dos cursos da plataforma quanto para os cursos customizados. É possível também filtrar os usuários dos grupos por departamento, cargo, localidade e demais informações pelo filtro.

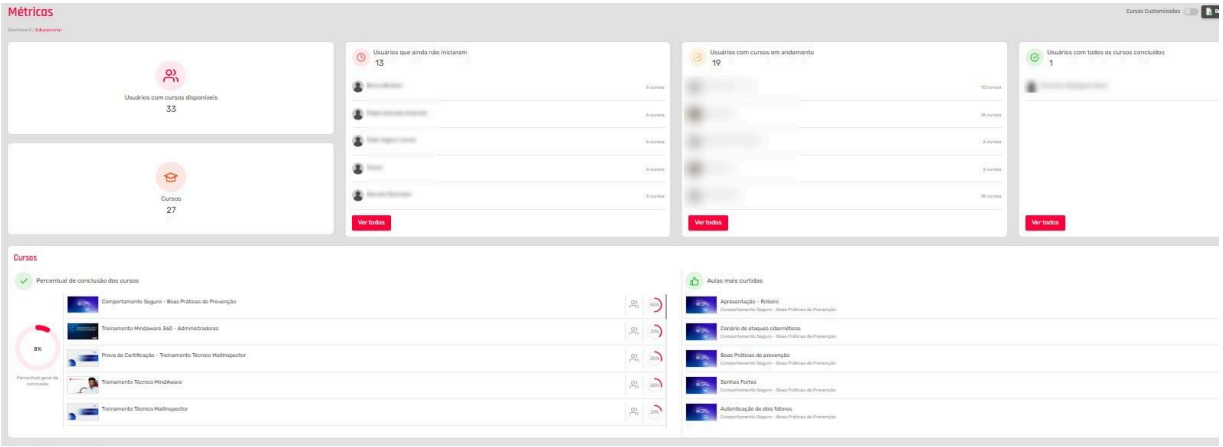


Dashboard por Usuário

Dentro do Dashboard Educacional, é possível visualizar o painel detalhado de um usuário específico.

Para isso, basta dar um **duplo clique** sobre o nome do usuário em qualquer seção onde ele apareça, como:

- Usuários que ainda não iniciaram o curso;
- Usuários com cursos em andamento;
- Usuários com todos os cursos concluídos;
- Métricas de um curso específico, como mostrado anteriormente;

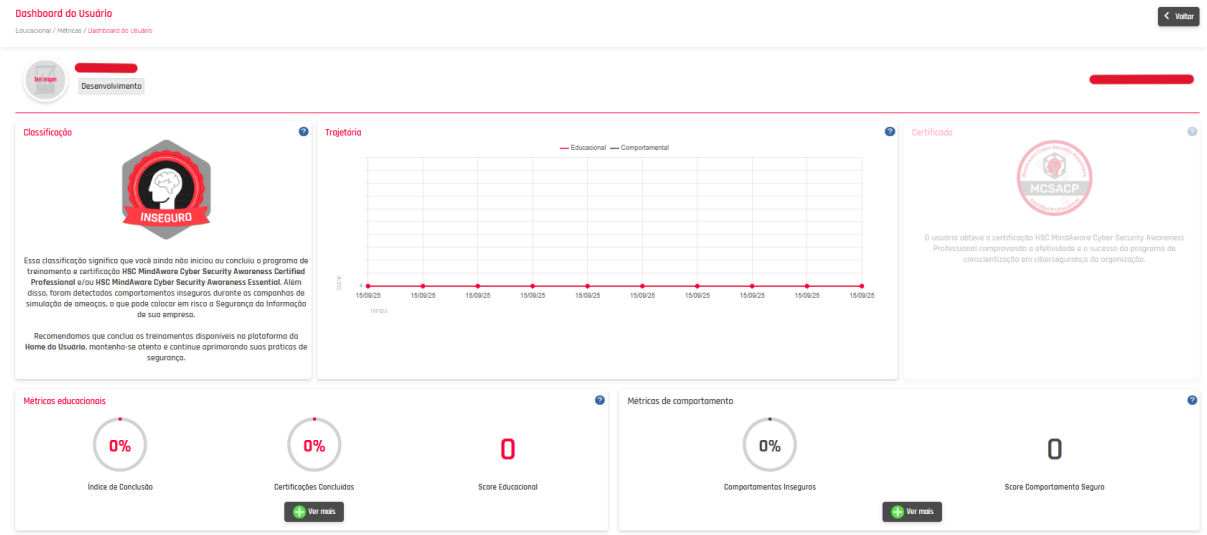


Ao acessar o perfil de um usuário, será exibida uma tela com diversas informações detalhadas, incluindo:

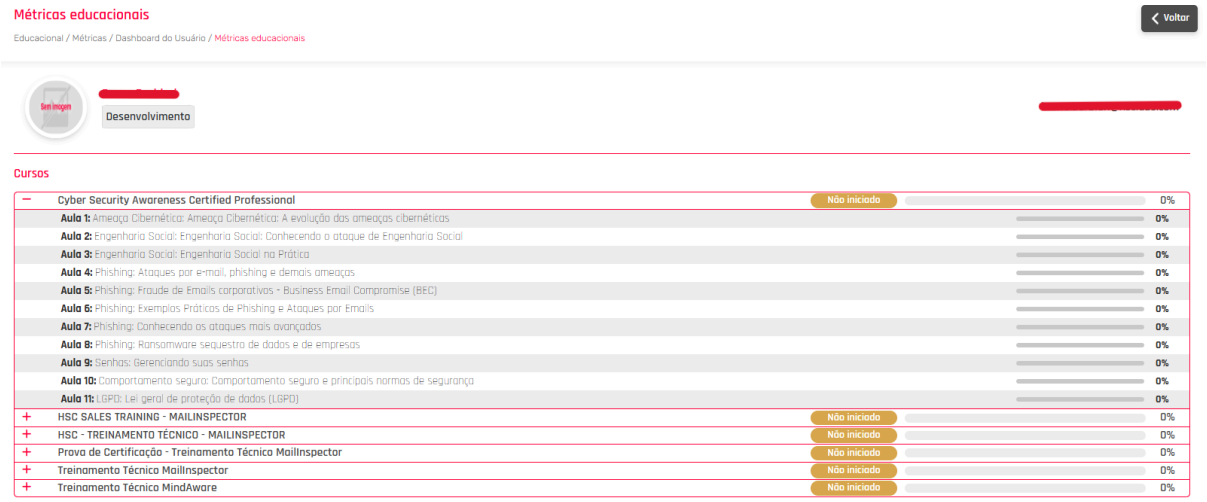
- Dados do usuário, como nome e grupos aos quais pertence;
- Classificação no quadrante MindAware;
- Trajetória dentro da plataforma;
- Métricas educacionais e comportamentais.

Dentro dessas métricas, é possível visualizar:

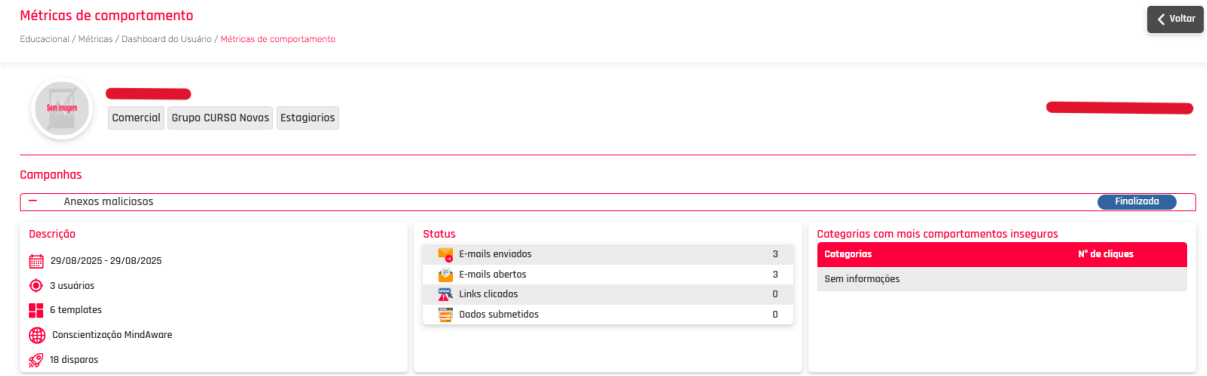
- Índice de conclusão de cursos;
- Certificações concluídas;
- Score educacional;
- Número de comportamentos inseguros identificados;
- Score de comportamento seguro (porcentagem que estima as chances do usuário de cair em um phishing real) .



Ao clicar em **"Ver Mais"** na seção de **Métricas Educacionais**, você poderá visualizar o desempenho do usuário em cada curso.
Clicando no ícone **"+"** ao lado de um curso, é possível ver o progresso detalhado por aula.



Já ao clicar em **"Ver Mais"** na seção de **Métricas de Comportamento**, será exibida uma tela com os resultados do usuário em cada campanha de phishing.
Da mesma forma, ao clicar no **"+"** ao lado de uma campanha, você poderá visualizar dados mais detalhados por campanha.



Nessa aba mostra as informações da campanha e as ações do usuário.

Ranking

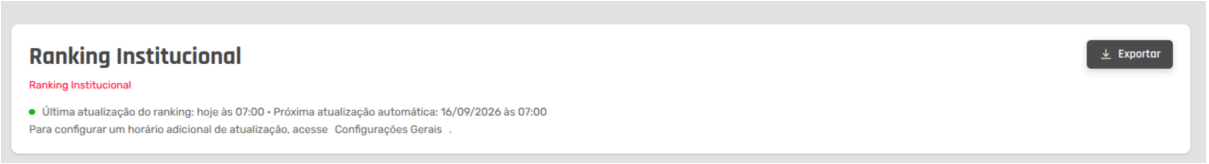
O menu Ranking permite acompanhar a evolução da organização, dos grupos e dos usuários com base nas pontuações obtidas nas atividades realizadas dentro da plataforma MindAware 360°.

O ranking consolida informações relacionadas ao comportamento, desenvolvimento educacional e evolução dos participantes, possibilitando uma visão geral da maturidade da organização e permitindo identificar os grupos e usuários com melhor desempenho.



Ranking Institucional

Na opção Ranking → Institucional, o administrador terá uma visão consolidada da pontuação da organização.



Na parte superior da tela são apresentadas informações relacionadas à atualização do ranking, como:

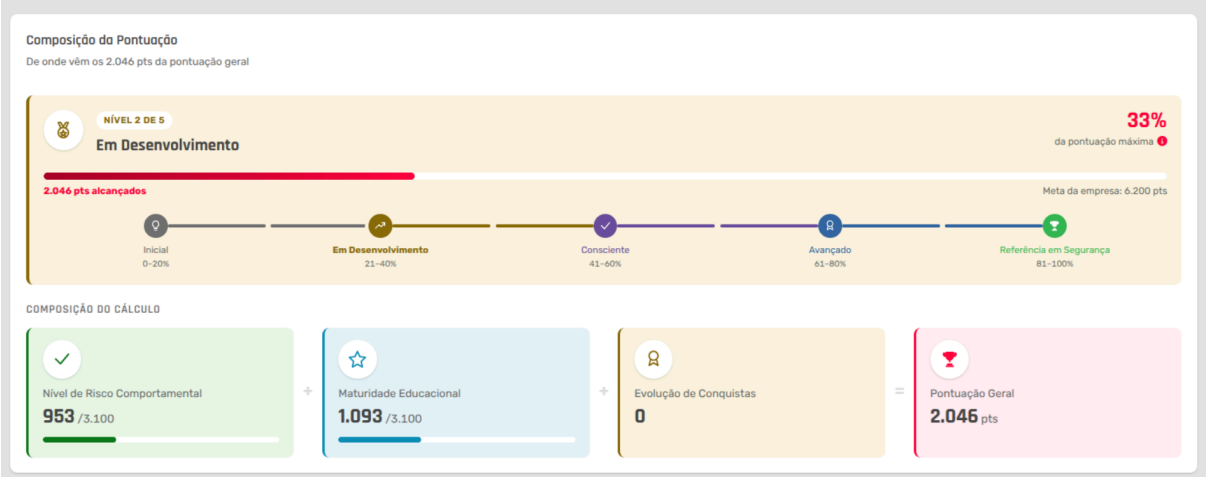
- data e horário da última atualização;
- data e horário da próxima atualização automática.

Caso seja necessário configurar um horário adicional para atualização, essa configuração poderá ser realizada através do menu Configurações Gerais.

Também é possível utilizar a opção Exportar para extrair as informações apresentadas no ranking.

Composição da Pontuação

O Ranking Institucional apresenta a Pontuação Geral alcançada pela organização e sua evolução em relação à pontuação máxima definida.



A pontuação é composta pelos seguintes indicadores:

- Nível de Risco Comportamental: considera os resultados comportamentais apresentados pelos usuários nas atividades e campanhas realizadas;
- Maturidade Educacional: considera a evolução dos usuários nos treinamentos e atividades educacionais;
- Evolução de Conquistas: considera as conquistas obtidas pelos usuários dentro da plataforma;
- Pontuação Geral: representa o resultado consolidado dos indicadores apresentados.

A plataforma apresenta também uma barra de evolução, permitindo visualizar o percentual alcançado pela organização em relação à meta definida.

Os níveis apresentados são:

Inicial: 0% a 20%;

Em Desenvolvimento: 21% a 40%;
Consciente: 41% a 60%;
Avançado: 61% a 80%;
Referência em Segurança: 81% a 100%.

Dessa forma, o administrador pode acompanhar de forma objetiva o nível de evolução institucional dentro do programa de conscientização.

Painel de Destaques

O Painel de Destaques apresenta informações relacionadas às alterações ocorridas desde a última atualização do ranking.



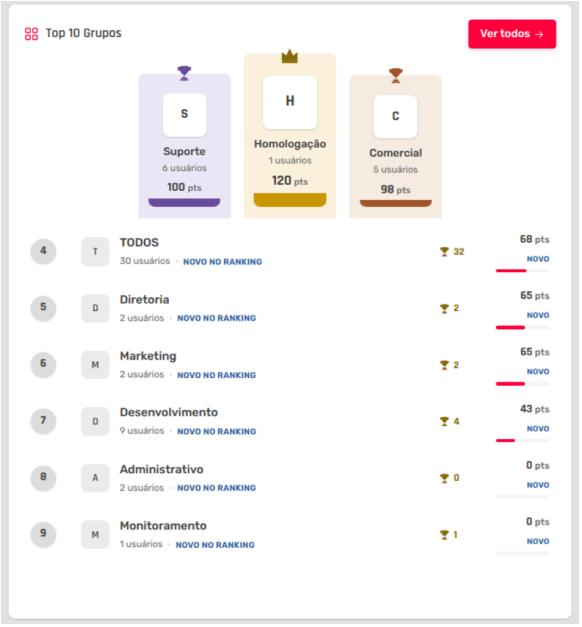
Entre as informações exibidas estão:

- 1º colocado do Ranking: usuário que ocupa a primeira posição;
- Perderam posições: quantidade de usuários que apresentaram redução de posição;
- Novos no Top 10: usuários que passaram a integrar as dez primeiras posições.

Esse painel permite identificar rapidamente mudanças relevantes ocorridas entre uma atualização e outra.

Top 10 Grupos

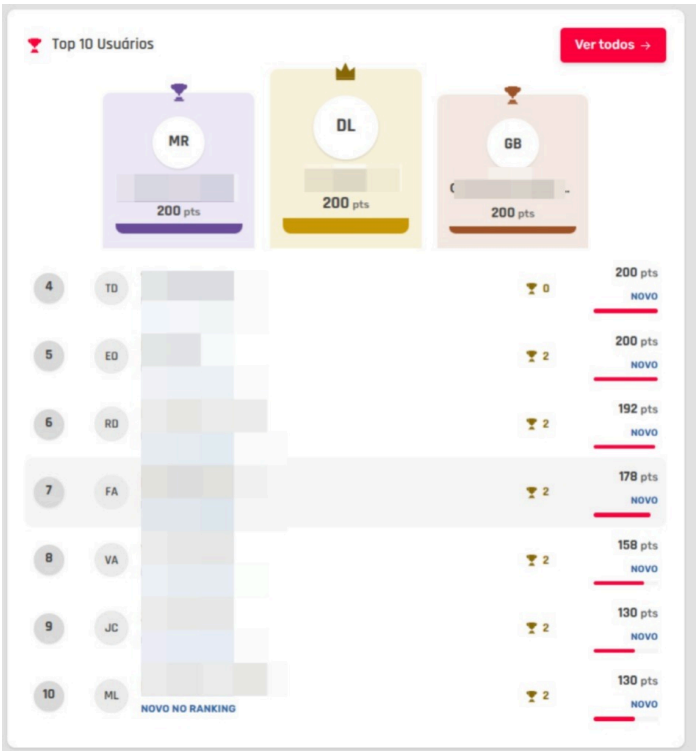
Na tela institucional também é apresentado o Top 10 Grupos, demonstrando os grupos com maior pontuação.



Os três primeiros colocados são destacados em formato de pódio.
Ao clicar em **Ver todos**, o administrador será direcionado para a tela completa do Ranking de Grupos.

Top 10 Usuários

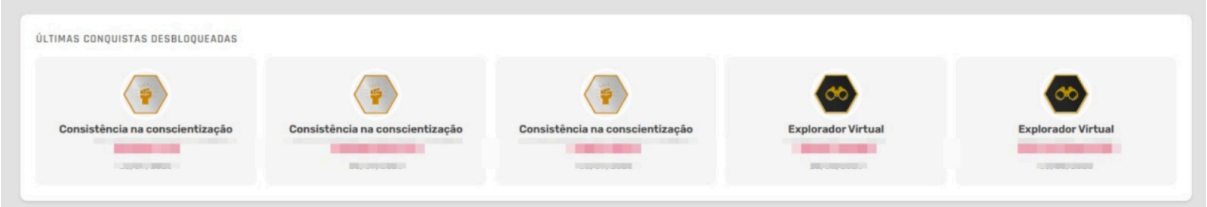
O Top 10 Usuários apresenta os usuários com maior pontuação dentro da organização.



Assim como no ranking de grupos, os três primeiros colocados são destacados no pódio.
Ao clicar em **Ver todos**, será aberta a tela completa do Ranking de Usuários.

Últimas Conquistas Desbloqueadas

Na área Últimas Conquistas Desbloqueadas, o administrador poderá visualizar as conquistas mais recentes obtidas pelos usuários.



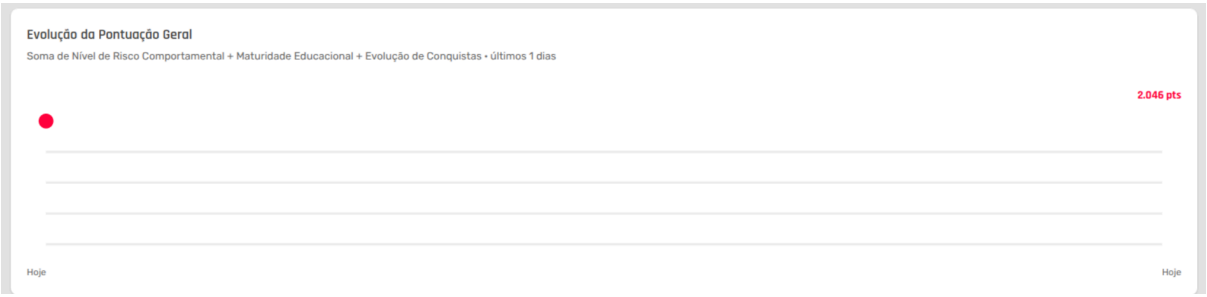
São exibidas informações como:

- identificação da conquista;
- usuário que alcançou a conquista;
- data em que ela foi obtida.

Essa informação complementa a visão do ranking e permite acompanhar eventos recentes relacionados à evolução dos participantes.

Evolução da Pontuação Geral

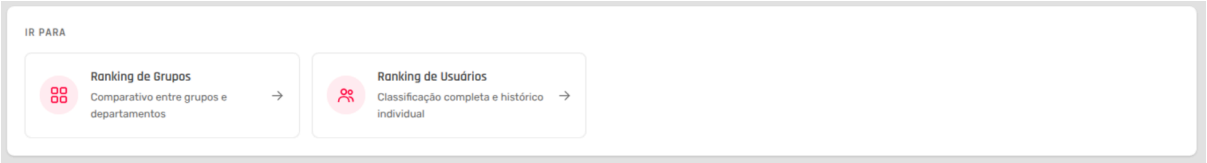
A seção Evolução da Pontuação Geral apresenta graficamente a variação da pontuação da organização ao longo do tempo.



O cálculo considera a soma dos indicadores utilizados na composição da pontuação geral, permitindo acompanhar a evolução institucional e identificar tendências de crescimento ou redução da maturidade.

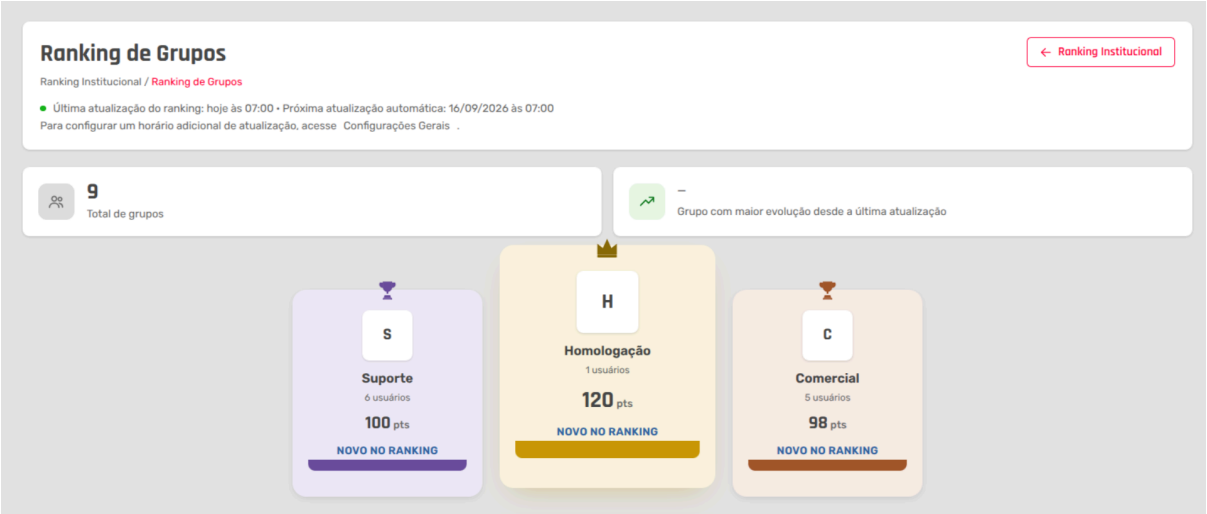
Na parte inferior da tela estão disponíveis atalhos para:

- Ranking de Grupos
- Ranking de Usuários



Ranking de Grupos

O administrador poderá analisar a classificação completa dos grupos cadastrados na plataforma.

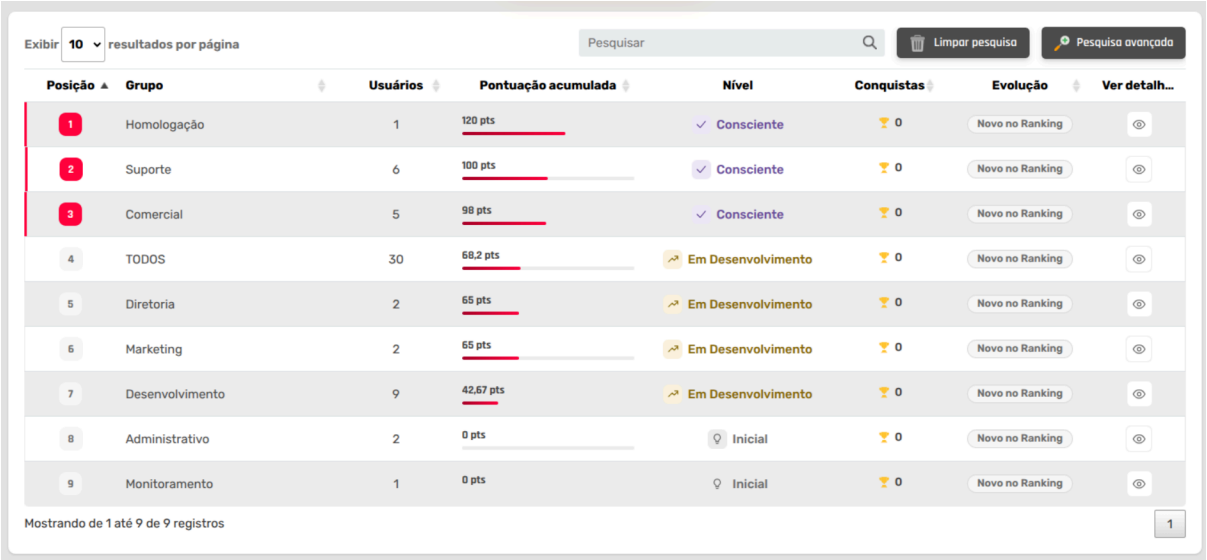


Na parte superior da tela são exibidas informações gerais, como:

- quantidade total de grupos;
- grupo que apresentou maior evolução desde a última atualização.

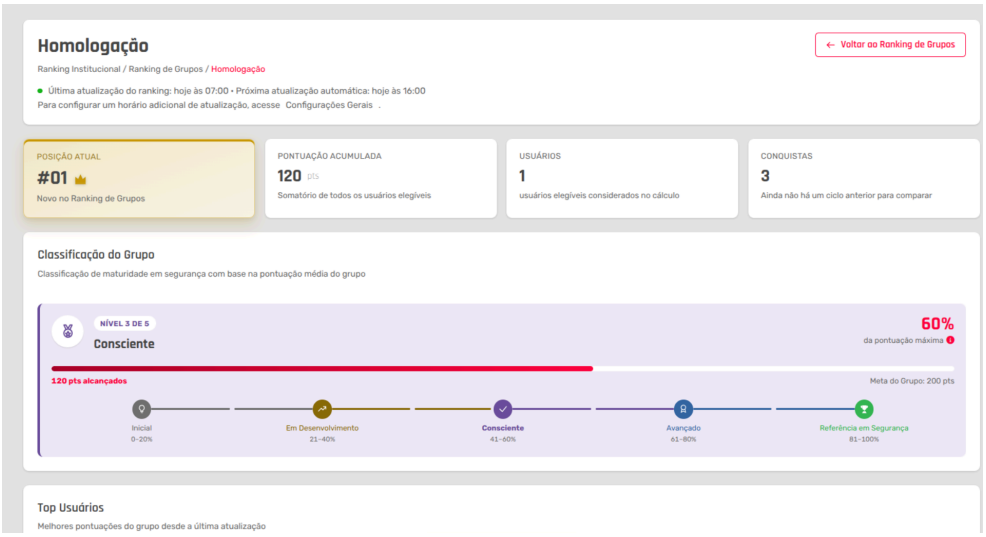
Os três grupos melhor classificados são destacados em formato de pódio.

Logo abaixo é apresentada a tabela completa do ranking.



As principais informações exibidas são:

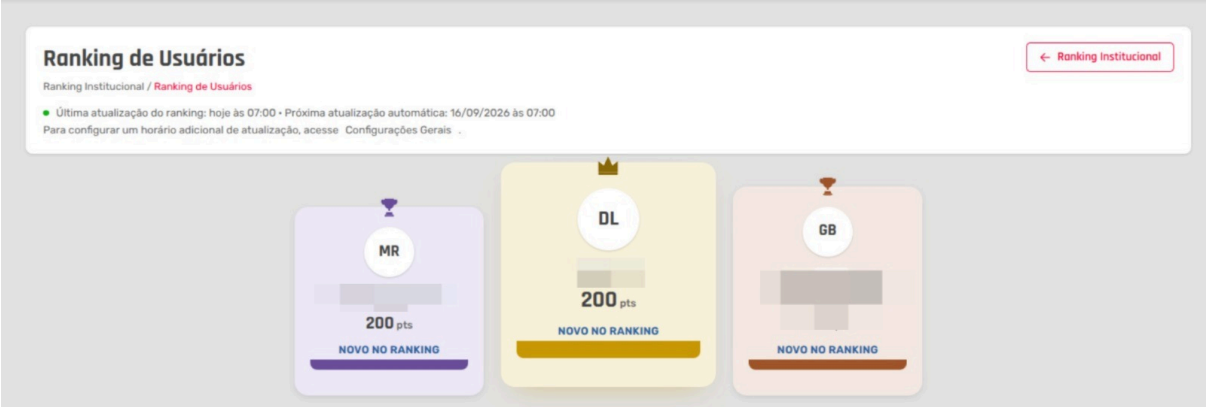
- Posição: classificação atual do grupo;
- Grupo: nome do grupo;
- Usuários: quantidade de usuários pertencentes ao grupo;
- Pontuação acumulada: total de pontos obtidos;
- Nível: classificação alcançada pelo grupo;
- Conquistas: quantidade de conquistas associadas;
- Evolução: situação do grupo em relação à atualização anterior;
- Ver detalhes: permite acessar informações adicionais do grupo.



A tela também disponibiliza recursos de pesquisa para facilitar a localização das informações.

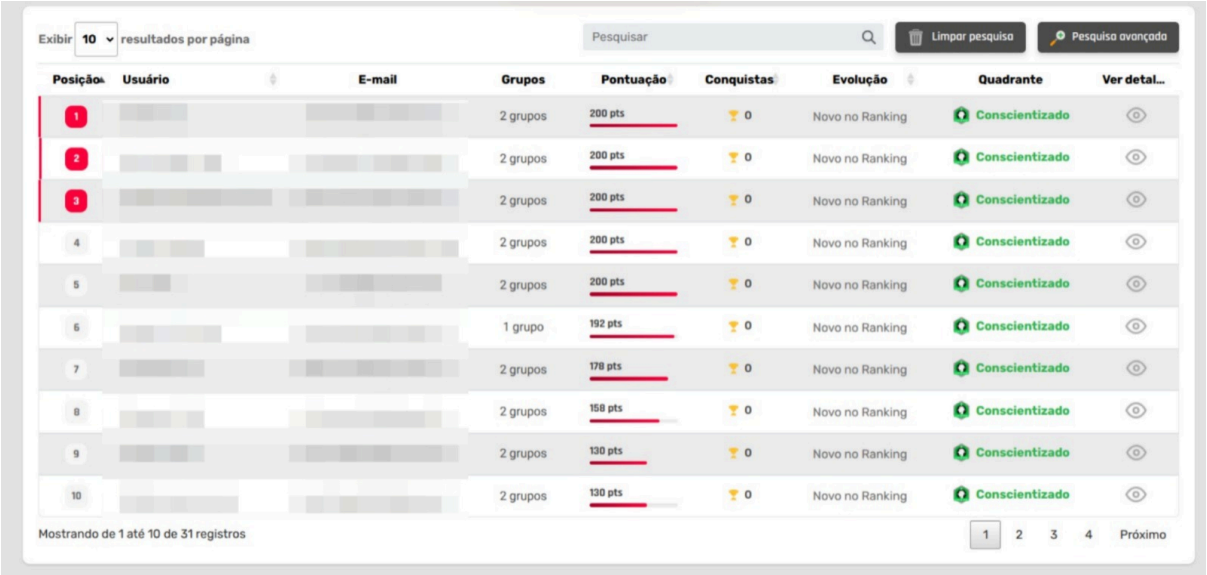
Ranking de Usuários

O Ranking de Usuários permite ao administrador identificar participantes com maior ou menor evolução e acompanhar a posição individual dos usuários dentro do programa de conscientização. Esses dados são utilizados também para retirar ou incluir automáticamente os usuários de campanhas educacionais ou comportamentais e atribuir cursos e conteúdos informativos.



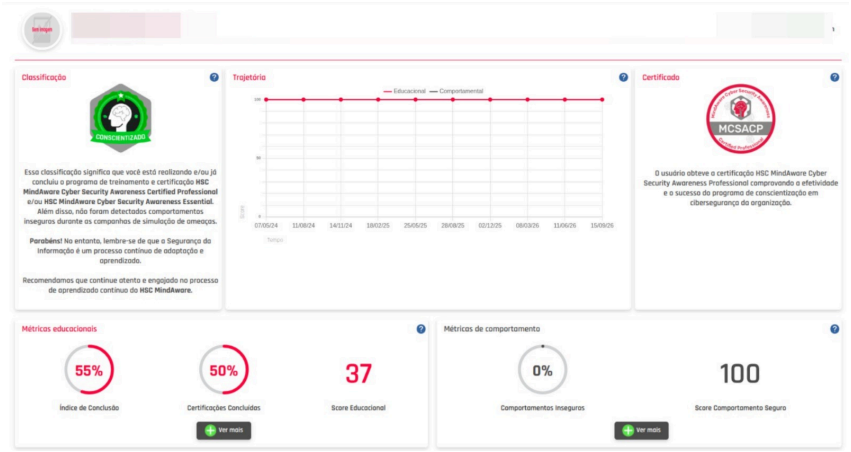
Os usuários que ocupam as três primeiras posições são apresentados em destaque no pódio.

Abaixo é exibida a tabela completa do ranking individual.

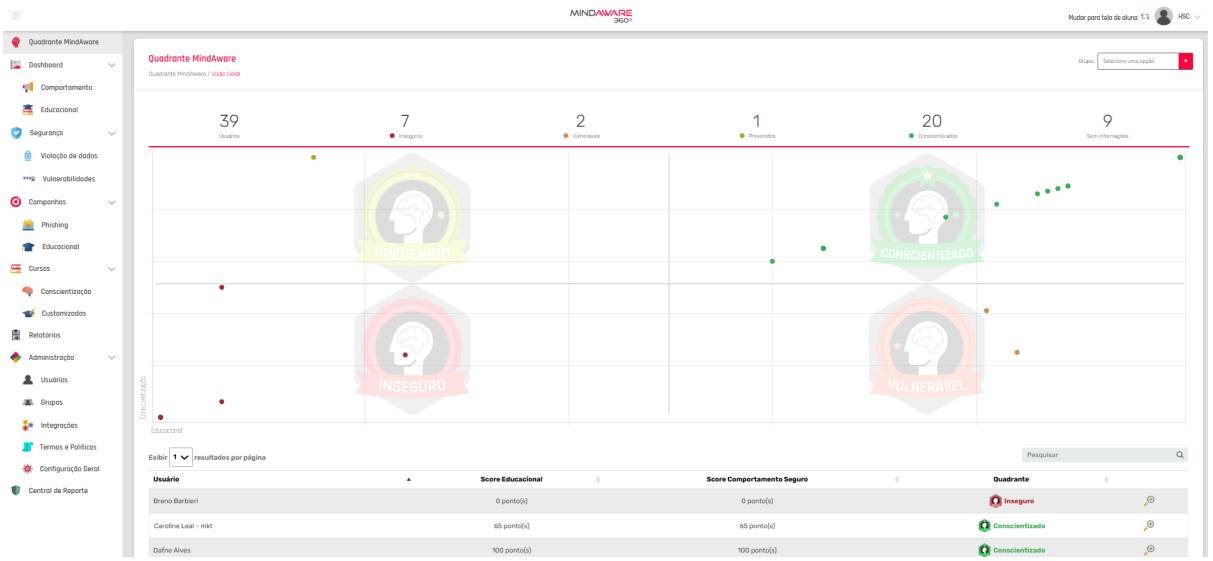


As principais informações disponíveis são:

- Posição: colocação atual do usuário;
- Usuário: nome do participante;

- E-mail: endereço de e-mail cadastrado;
- Grupos: quantidade de grupos dos quais o usuário participa;
- Pontuação: total de pontos obtidos;
- Conquistas: quantidade de conquistas obtidas;
- Evolução: variação de posição em relação à atualização anterior;
- Quadrante: classificação atual do usuário no Quadrante MindAware;
- Ver detalhes: permite acessar informações adicionais sobre o participante.
    - 

Quadrante MindAware



- **Visão Geral do Quadrante**: Explicação sobre o uso e aplicação do Quadrante MindAware na plataforma.
- **Dashboard por Status de Quadrante**: Como usar o dashboard para visualizar e analisar o status do quadrante.
- **Dashboard do Usuário**:
    - **Métricas Educacionais**: Análise dos resultados educacionais específicos para cada usuário.
    - **Métricas Comportamentais**: Análise dos padrões comportamentais e progresso individual dos usuários.

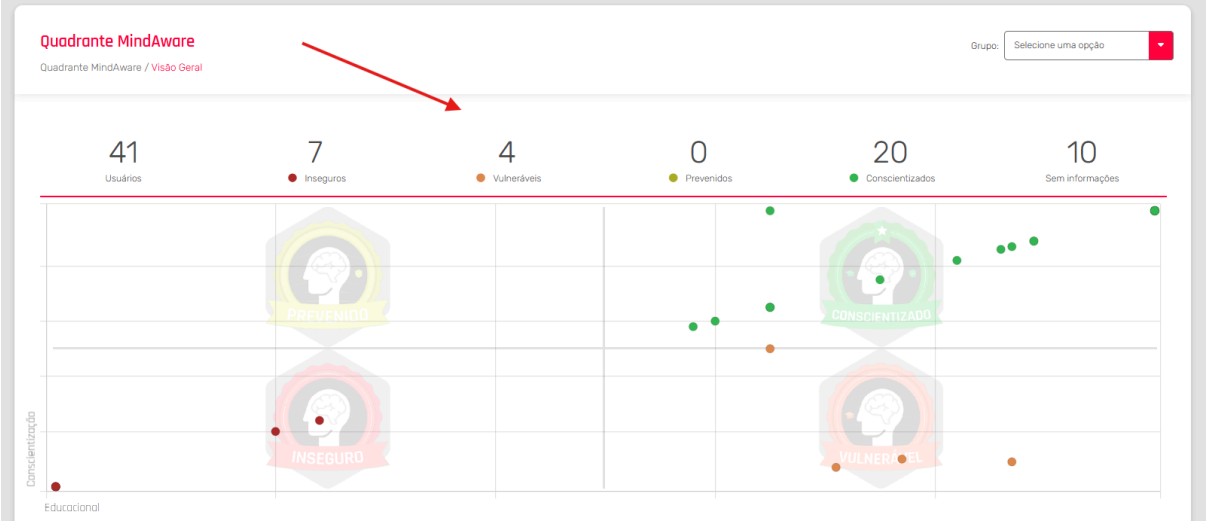
Ao acessar o Quadrante MindAware, teremos acesso ao grau de maturidade dos colaboradores diante os ataques de phishing. Nesta visão, podemos dividir em 04 grupos representando cada grau de maturidade.

- ***Inseguros:*** Nesta classificação, caracterizam-se os colaboradores que ainda não iniciaram o programa de treinamentos e certificação da HSC.
- ***Vulnerável:*** Nesta classificação, encontram-se os colaboradores que estão realizando ou já concluíram o programa de treinamento e certificação, mas, ainda apresentam comportamentos inseguros durante a realização de campanhas de simulação de ameaças que podem levar riscos à empresa.
- ***Prevenidos:*** Nesta classificação, encontram-se os colaboradores que ainda não iniciaram o programa de treinamentos e certificações, porém, não

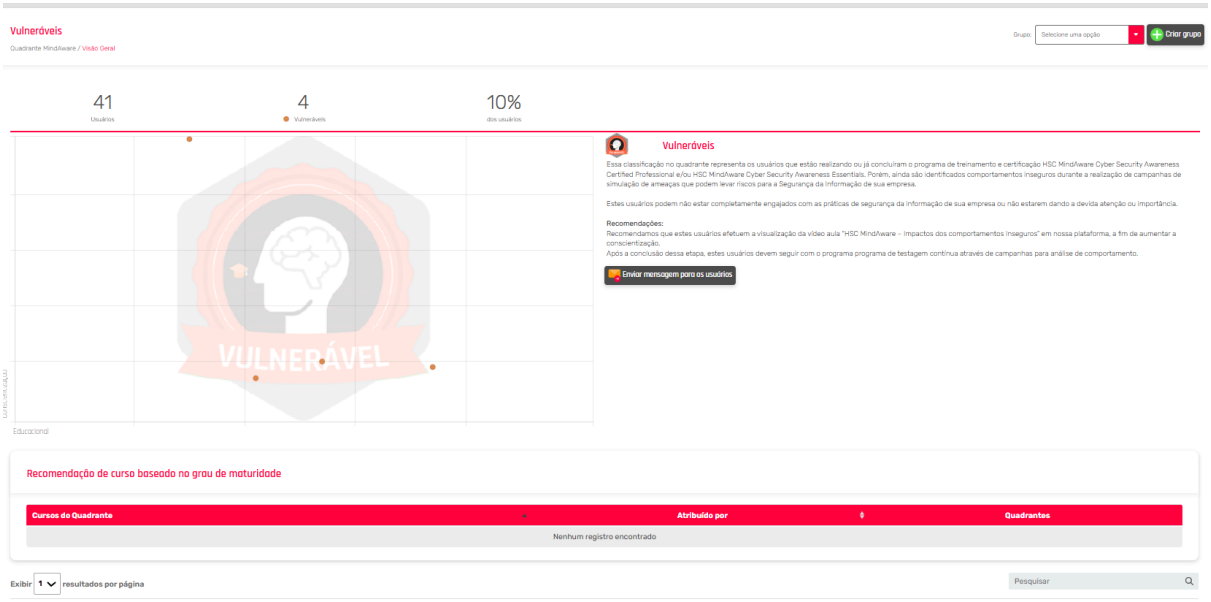
apresentam comportamentos inseguros durante a realização de campanhas de simulação de ameaças que poderiam levar riscos à empresa.

- ***Conscientizados:*** Este é o estágio ideal para garantir o processo de conscientização na empresa, pois representa os colaboradores que completaram o programa de treinamento e certificação da HSC e que não apresentam comportamentos inseguros.

Ao clicar no **número de um quadrante específico**, você será direcionado para uma nova tela que apresenta informações detalhadas sobre aquele quadrante, incluindo:



- **Número total de usuários** pertencentes ao quadrante;
- **Porcentagem** que esse grupo representa em relação ao total da campanha;
- **Descrição explicativa** do quadrante e seu significado;
- **Lista de usuários** incluídos no quadrante, acompanhada de suas métricas individuais.



Nesta tela, é possível realizar duas ações, a primeira consiste em criar um grupo com base no quadrante selecionado.

Para isso, clique em **"Criar grupo"**. O sistema criará automaticamente o grupo e redirecionará você para a tela de edição de grupo, onde será possível ajustar o nome, configurações ou qualquer outra informação necessária.

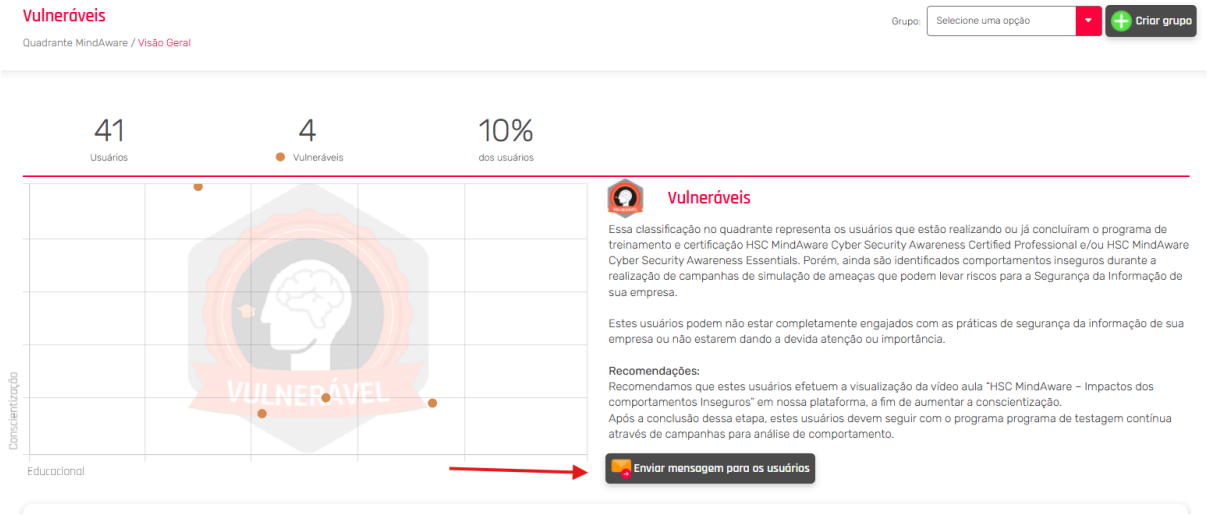


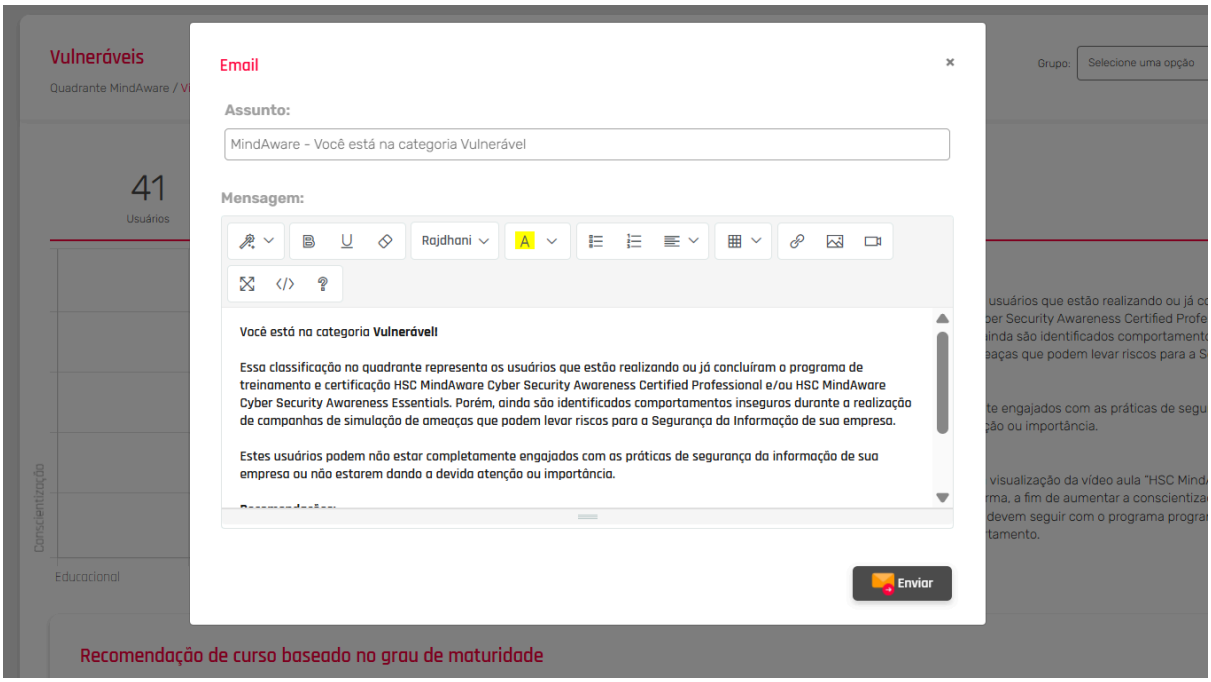


A segunda ação disponível é enviar um e-mail para todos os usuários do quadrante selecionado. A mensagem pode ser padrão ou personalizada, conforme a necessidade.

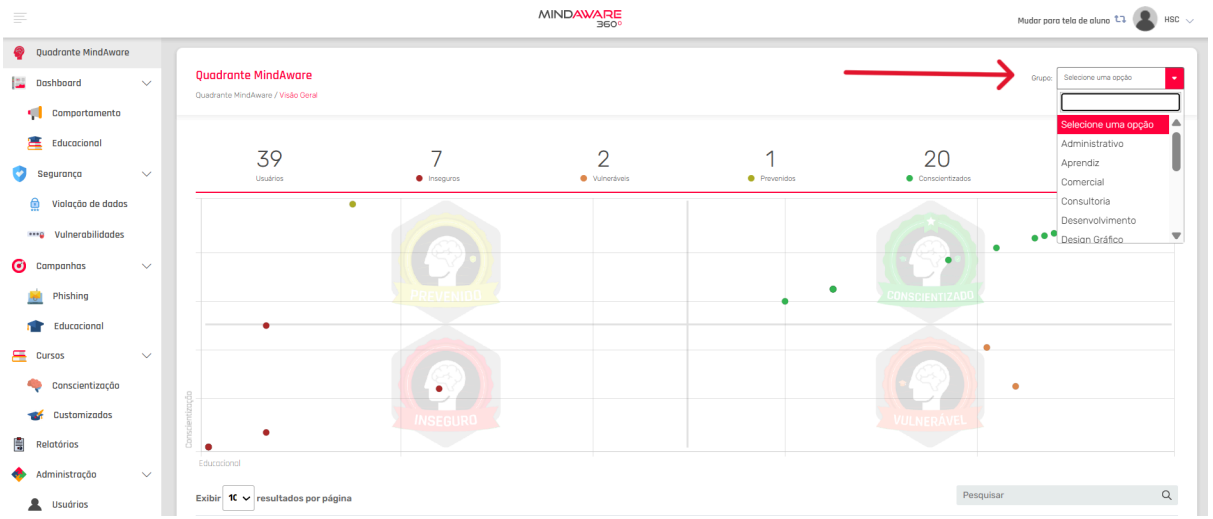
Para realizar o envio, clique em “Enviar mensagem para os usuários”, uma nova tela será exibida, onde você poderá revisar e, se desejar, editar o conteúdo da mensagem.

Após a conferência, clique em “Enviar” para finalizar o processo.





É possível utilizar o campo de seleção localizado na parte superior da tela para mostrar o quadrante por grupo.


MINDAWARE 360°
Mudar para tela de aluno
HSC
Quadrante MindAware
Dashboard
Comportamento
Educacional
Segurança
Violação de dados
Vulnerabilidades
Campanhas
Phishing
Educacional
Cursos
Conscientização
Customizados
Relatórios
Administração
Usuários
Quadrante MindAware
Quadrante MindAware / Visão Geral
Grupo:
Selecione uma opção
Selecione uma opção
Administrativo
Aprendiz
Comercial
Consultoria
Desenvolvimento
Design Gráfico
39
Usuários
7
Inseguros
2
Vulneráveis
1
Prevenidos
20
Conscientizados
PREVENIDO
CONSCIENTIZADO
INSEGURO
VULNERÁVEL
Conscientização
Educacional
Exibir
resultados por página
Pesquisar

Relatórios

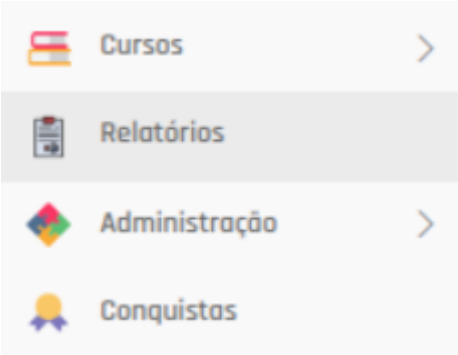
O menu **Relatórios** permite ao administrador criar, consultar e gerenciar relatórios com informações consolidadas ou individuais das principais atividades realizadas na plataforma MindAware 360°.

Os relatórios podem ser utilizados para acompanhamento de campanhas, cursos, grupos, usuários e licenças, permitindo que o administrador selecione o tipo de informação que deseja analisar e aplique filtros conforme a necessidade.

Além disso, é possível criar modelos de relatórios personalizados e programar o envio automático para endereços de e-mail previamente definidos. A cada envio, o sistema utiliza o mesmo modelo de relatório, atualizando automaticamente apenas os dados e indicadores conforme o período ou as informações mais recentes disponíveis.

Para acessar, utilize:

Menu Principal → Relatórios

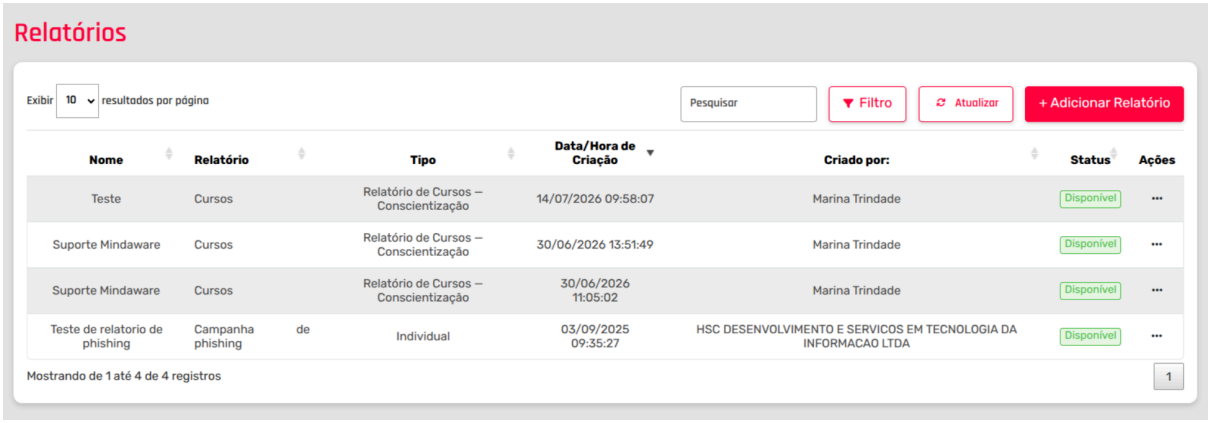


Na tela inicial, serão exibidos os relatórios já criados na plataforma.

As seguintes informações são apresentadas:

- **Nome:** identificação definida no momento da criação do relatório;
- **Relatório:** módulo ou origem das informações;
- **Tipo:** formato de análise selecionado, como grupo ou individual;
- **Data/Hora de Criação:** momento em que o relatório foi gerado;
- **Criado por:** usuário responsável pela criação;
- **Status:** situação atual do relatório;
- **Ações:** opções disponíveis para gerenciamento do relatório.

Também estão disponíveis as funções **Pesquisar**, **Filtro**, **Atualizar** e **Adicionar Relatório**.



Criar um Relatório

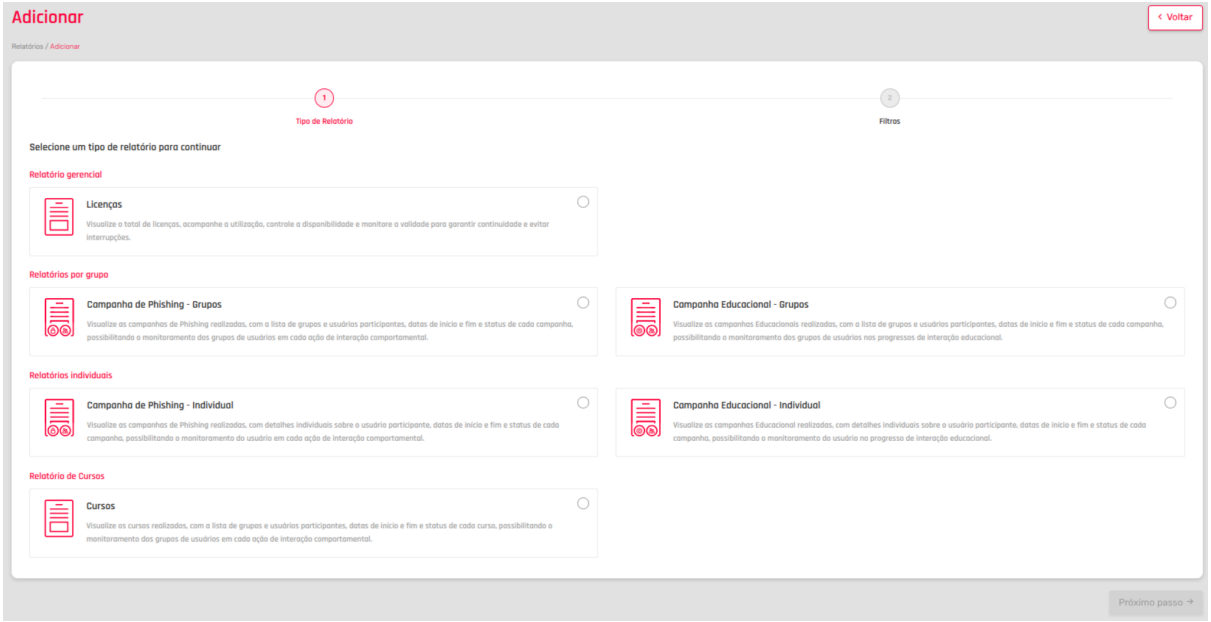
Para criar um novo relatório, clique no botão:

+ Adicionar Relatório

A criação é realizada em duas etapas:

1. **Tipo de Relatório**
2. **Filtros**

Na primeira etapa, deverá ser selecionado o tipo de relatório que será gerado.



A plataforma disponibiliza diferentes modelos de relatórios conforme a informação que se deseja acompanhar. Nos relatórios é possível filtrar os usuários por departamento, função, cargo, localidade e demais informações.

Licenças

Permite visualizar informações relacionadas às licenças da plataforma, possibilitando acompanhar sua utilização, disponibilidade e validade.

Campanha de Phishing — Grupos

Permite consultar as campanhas de phishing realizadas considerando os grupos participantes.

O relatório possibilita acompanhar informações relacionadas às campanhas, seus períodos e o comportamento dos grupos e usuários envolvidos nas simulações.

Campanha Educacional — Grupos

Permite consultar as campanhas educacionais realizadas considerando os grupos participantes.

Esse relatório auxilia o administrador no acompanhamento do progresso educacional dos grupos e usuários vinculados às campanhas.

Campanha de Phishing — Individual

Permite acompanhar individualmente a participação do usuário nas campanhas de phishing realizadas.

Esse tipo de relatório possibilita analisar as informações associadas ao usuário participante e seu comportamento nas ações de simulação.

Campanha Educacional — Individual

Permite acompanhar individualmente a participação e o progresso do usuário nas campanhas educacionais.

Por meio desse relatório, o administrador poderá analisar o andamento do usuário nas ações de conscientização atribuídas.

Cursos

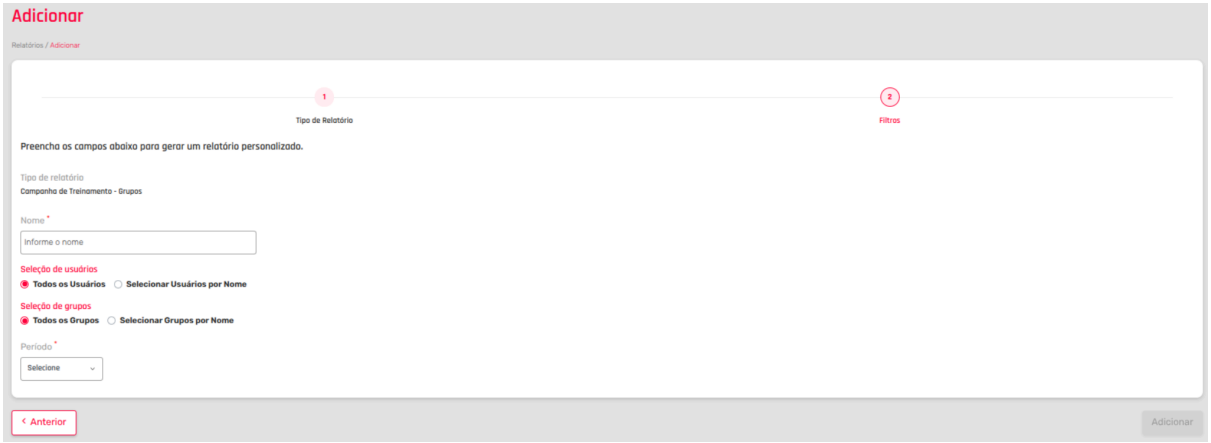
Permite acompanhar os cursos realizados e as informações associadas aos grupos e usuários participantes.

Esse relatório auxilia na análise do andamento das atividades educacionais disponibilizadas pela plataforma.

Após selecionar o tipo de relatório desejado, clique em: **Próximo passo.**

Na segunda etapa, serão definidos os critérios que determinarão quais informações farão parte do relatório.

A tela apresenta o **Tipo de Relatório** selecionado anteriormente e os campos disponíveis para configuração.



Informe um nome para identificar o relatório.

O administrador poderá definir quais usuários serão considerados no relatório.

Também é possível definir os grupos considerados no relatório.

No campo **Período**, deverá ser selecionado o intervalo de informações que será considerado na geração do relatório. O período permite restringir a análise aos dados correspondentes ao intervalo desejado.

Após preencher os campos obrigatórios e definir os filtros, clique no botão: **Adicionar.**

O relatório será processado e ficará disponível na tela principal do menu Relatórios.

Consultar Relatórios Criados

Após a criação, o relatório será apresentado na listagem principal.

Quando o processamento estiver concluído, o campo **Status** será apresentado como:

Disponível

A listagem permite acompanhar facilmente quem criou o relatório, sua data e hora de criação, tipo e respectivo módulo.

Ações do Relatório

Na coluna **Ações**, clique no ícone de três pontos correspondente ao relatório desejado.

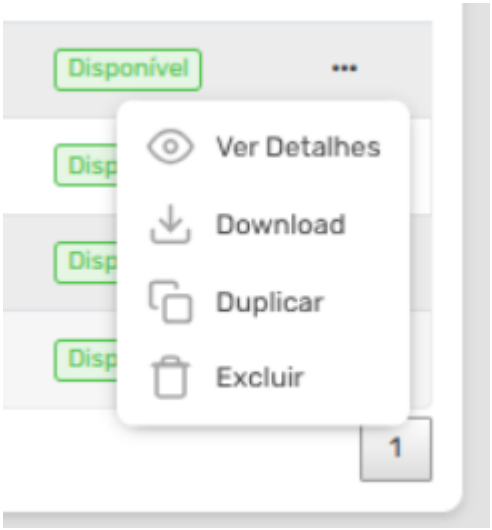
Serão apresentadas as seguintes opções:

Ver Detalhes - Permite acessar as informações detalhadas do relatório selecionado.

Download - Permite baixar o relatório gerado para utilização ou análise externa.

Duplicar - Permite criar uma nova versão utilizando como base as configurações do relatório existente.

Excluir - Permite remover da listagem o relatório selecionado.


Disponível
Ver Detalhes
Download
Duplicar
Excluir
1

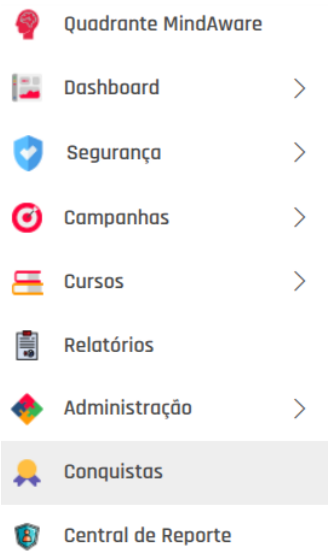
Insígnias e Conquistas

A funcionalidade de **Insígnias** faz parte dos recursos de gamificação do MindAware 360° e tem como objetivo reconhecer a evolução e a participação dos usuários nas atividades realizadas dentro da plataforma.

As insígnias estão associadas a diferentes **atividades, objetivos e marcos de evolução**, sendo concedidas conforme o usuário atende aos critérios definidos para cada conquista. Esse recurso complementa os mecanismos de pontuação e ranking utilizados pela plataforma para acompanhar a evolução dos participantes.

Visualização das Insígnias

Para acessar a funcionalidade, utilize o menu correspondente a **Conquistas** na área administrativa da plataforma.



Nesta tela, o administrador poderá visualizar as insígnias disponibilizadas pelo MindAware 360° e as informações relacionadas a cada conquista.

Cada insígnia representa um determinado marco dentro da jornada de conscientização e possui um **critério específico para sua obtenção**.



As insígnias permitem ao administrador identificar, de maneira visual, diferentes conquistas alcançadas.

Entre as informações associadas às conquistas estão:

- identificação da insígnia;
- descrição da conquista;
- critério necessário para obtenção;
- data em que a conquista foi obtida, quando aplicável.

A plataforma mantém o registro da obtenção das conquistas, permitindo relacioná-las à evolução dos participantes no programa de conscientização.

Além da visão administrativa apresentada, a plataforma também disponibiliza uma **visualização de Insígnias/Conquistas na tela do próprio usuário**, permitindo que cada participante acompanhe as conquistas obtidas ao longo de sua jornada na plataforma.

Essa visualização tem como objetivo proporcionar ao usuário uma percepção clara de sua evolução e dos marcos já alcançados.

Agentes de IA

O módulo **Agentes de IA** permite automatizar a identificação de públicos, sugerir campanhas de treinamento e simulação e organizar grupos dinâmicos conforme o comportamento dos colaboradores na plataforma. As sugestões geradas pelos agentes ficam disponíveis para análise e aprovação do administrador.

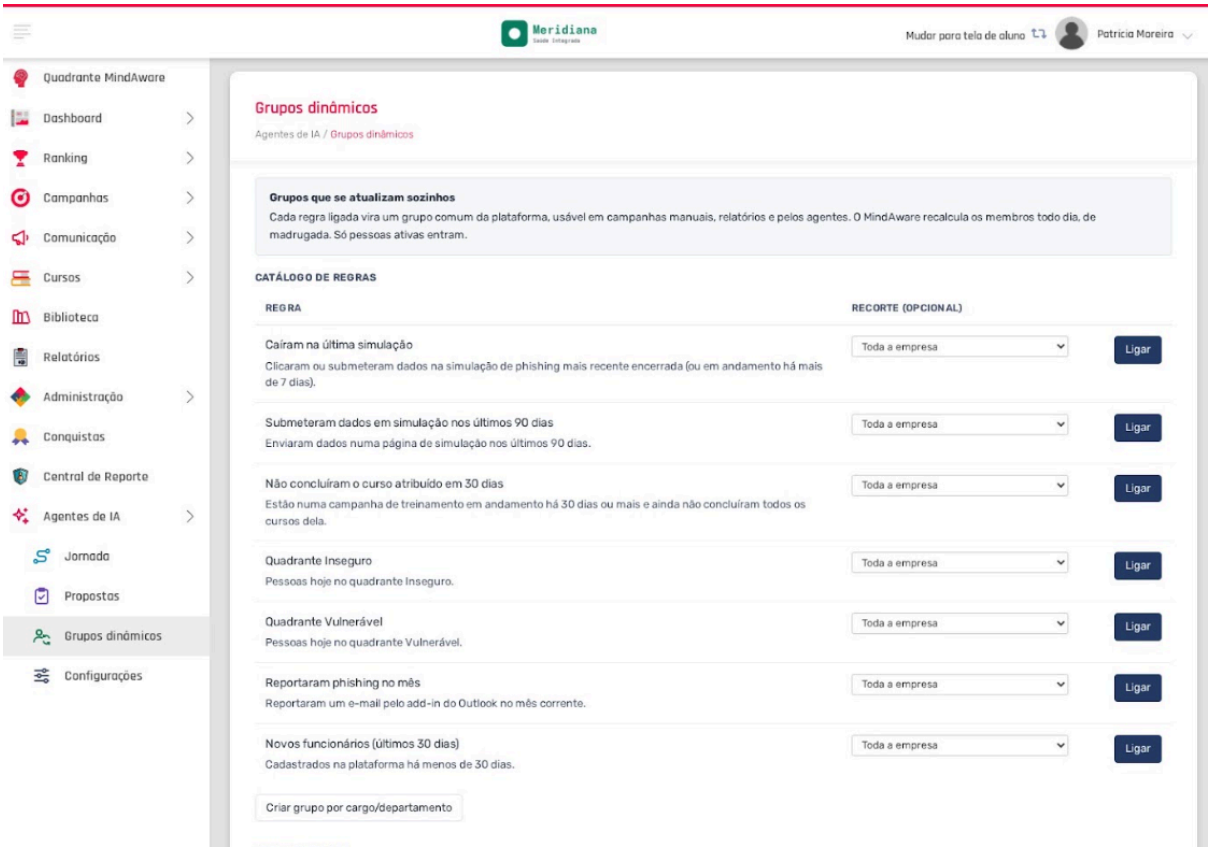
Acessar os Agentes de IA

1. No menu lateral, acesse **Agentes de IA**.
2. Selecione a funcionalidade desejada entre **Jornada, Propostas, Grupos dinâmicos e Configurações**.
3. Utilize **Propostas** para consultar e revisar as sugestões geradas pelos agentes.
4. Acesse **Grupos dinâmicos** para configurar grupos com atualização automática.
5. Utilize **Configurações** para definir as regras e os parâmetros das sugestões de campanhas.

Os agentes atuam conforme as regras configuradas e os dados disponíveis na plataforma, auxiliando na identificação de oportunidades de conscientização e treinamento.

Configurar grupos dinâmicos

1. Acesse **Agentes de IA > Grupos dinâmicos**.
2. Na seção **Catálogo de regras**, localize o critério desejado.
3. No campo **Recorte (opcional)**, selecione **Toda a empresa** ou um recorte disponível.
4. Clique em **Ligar** para ativar a regra.
5. Consulte a seção **Grupos ligados** para verificar o grupo criado.



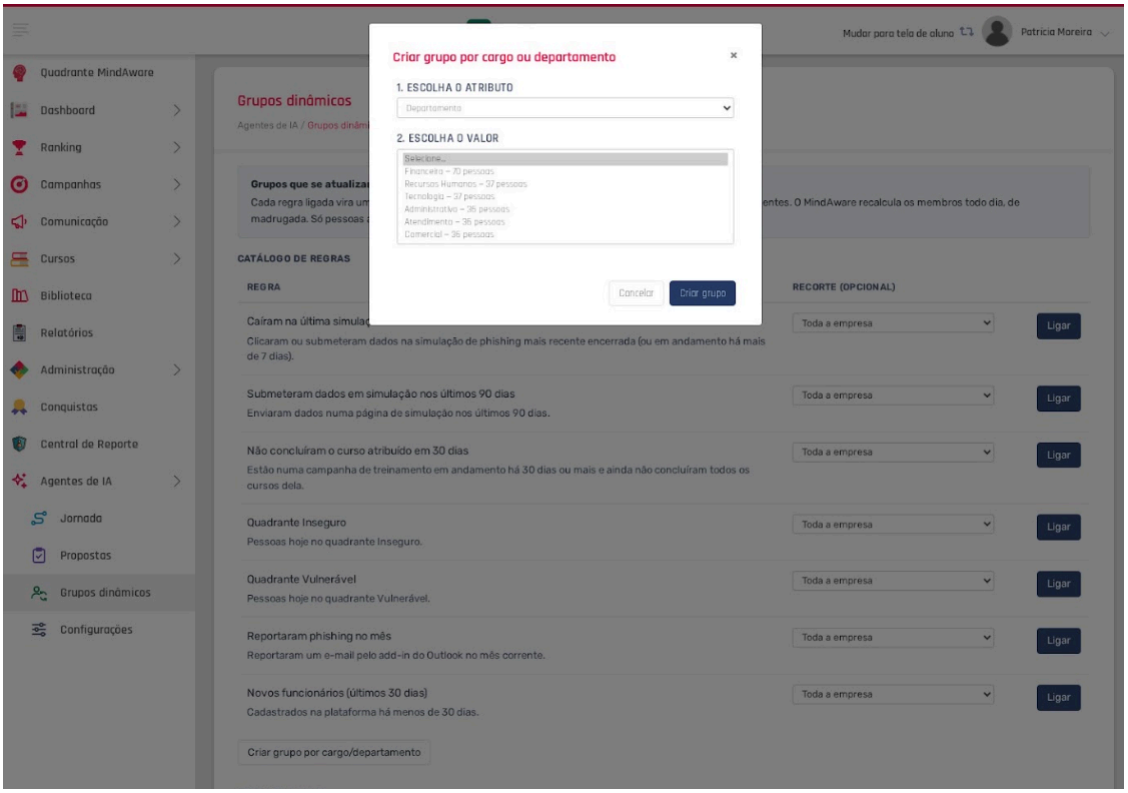
Os grupos dinâmicos são formados automaticamente a partir de critérios relacionados ao comportamento e às características dos colaboradores. A plataforma recalcula diariamente os integrantes de cada grupo, considerando somente usuários ativos.

As regras disponíveis permitem identificar colaboradores que clicaram ou submeteram dados na última simulação, enviaram informações em simulações nos últimos 90 dias, não concluíram treinamentos atribuídos há 30 dias ou mais, pertencem aos quadrantes Inseguro ou Vulnerável, reportaram phishing no mês corrente ou foram cadastrados na plataforma nos últimos 30 dias.

Os grupos criados podem ser utilizados em campanhas manuais, relatórios e nas sugestões dos agentes de IA.

Criar grupos por cargo ou departamento

1. Acesse **Agentes de IA > Grupos dinâmicos**.
2. Clique em **Criar grupo por cargo/departamento**.

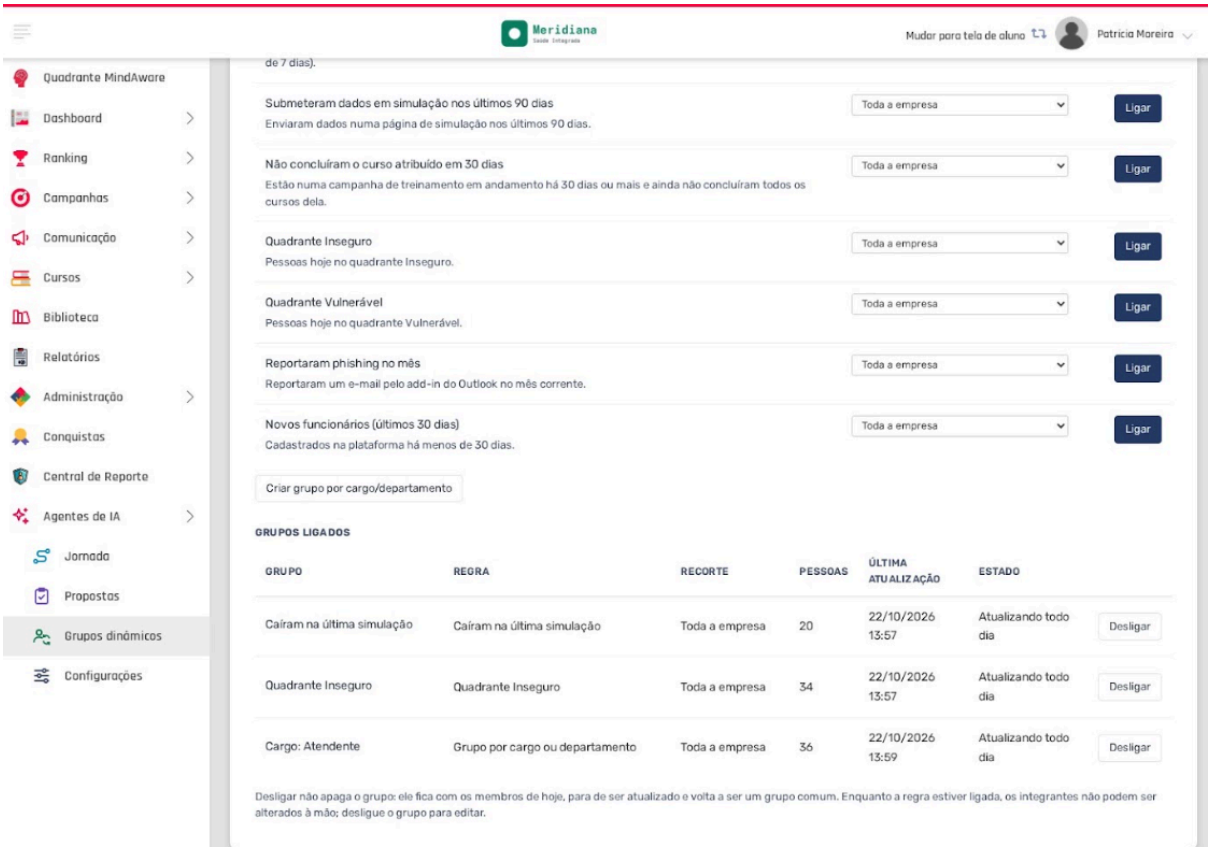


3. No campo **Escolha o atributo**, selecione **Cargo** ou **Departamento**.
4. Em **Escolha o valor**, selecione o cargo ou departamento desejado.
5. Confira a quantidade de colaboradores apresentada para a opção selecionada.
6. Clique em **Criar grupo** para concluir.

A funcionalidade permite organizar automaticamente os colaboradores conforme as informações cadastrais existentes na plataforma. Cada grupo criado utiliza o atributo selecionado como critério de composição, permitindo direcionar campanhas e treinamentos para públicos específicos.

Consultar e gerenciar grupos dinâmicos

1. Acesse **Agentes de IA > Grupos dinâmicos**.
2. Localize a seção **Grupos ligados**.
3. Consulte as informações de cada grupo, incluindo nome, regra, recorte, quantidade de pessoas, última atualização e estado.
4. Para interromper a atualização automática, clique em **Desligar** na linha correspondente.



A seção **Grupos ligados** apresenta os grupos que possuem regras ativas e estão sendo atualizados automaticamente pela plataforma.

Ao desligar uma regra, o grupo não é excluído. Ele mantém os integrantes existentes no momento da desativação, deixa de receber atualizações automáticas e passa a funcionar como um grupo comum.

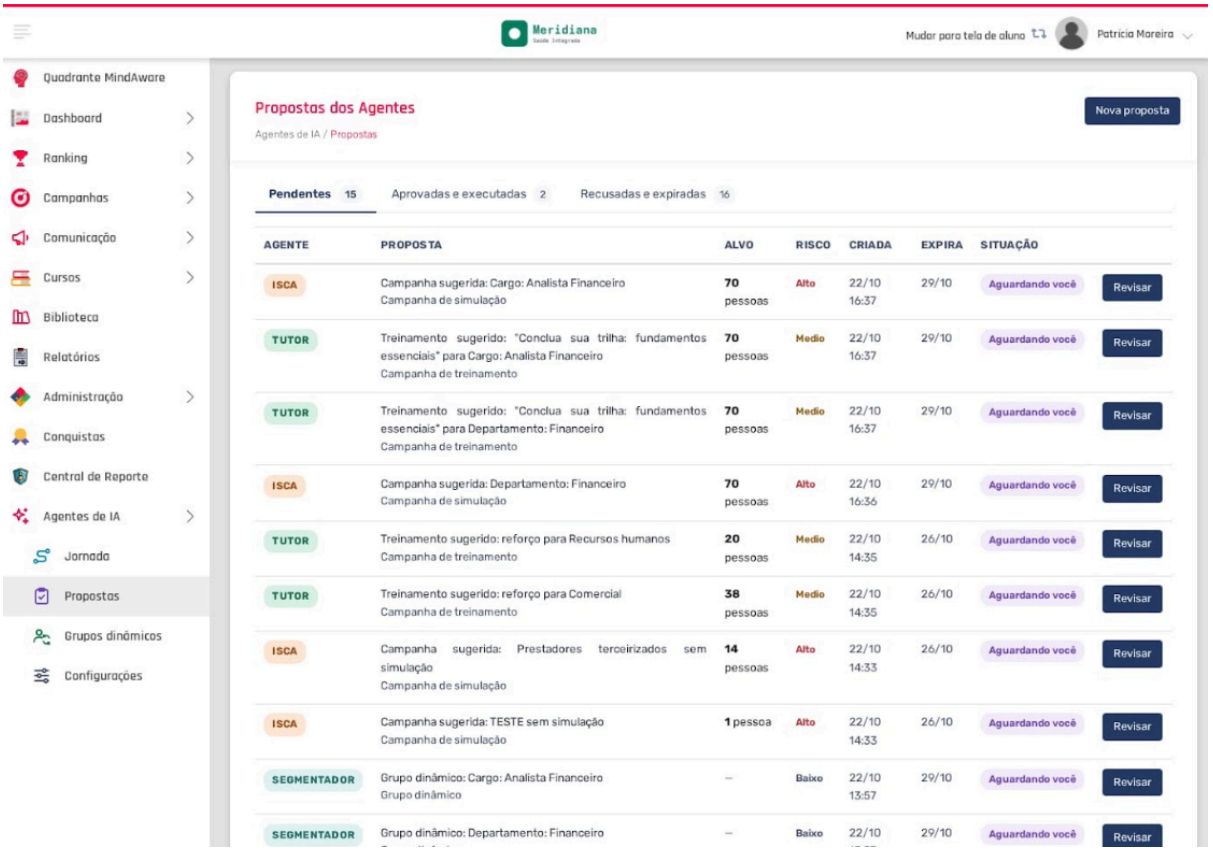
Enquanto a regra estiver ativa, os integrantes não poderão ser alterados manualmente. Para realizar alterações na composição, é necessário desligar a atualização automática.

Consultar propostas dos agentes

1. Acesse **Agentes de IA > Propostas**.
2. A plataforma apresentará a listagem das propostas geradas pelos agentes.
3. Utilize os filtros **Pendentes, Aprovadas e executadas** ou **Recusadas e expiradas** para localizar as propostas conforme sua situação.
4. Consulte as informações de agente, proposta, público-alvo, risco, data de criação, expiração e situação.

5. Clique em **Revisar** para visualizar os detalhes de uma proposta.

A plataforma apresenta propostas geradas por diferentes agentes, identificados conforme sua finalidade.



ISCA: Responsável por sugerir campanhas de simulação de phishing conforme os riscos identificados.

TUTOR: Responsável por sugerir campanhas de treinamento direcionadas aos colaboradores.

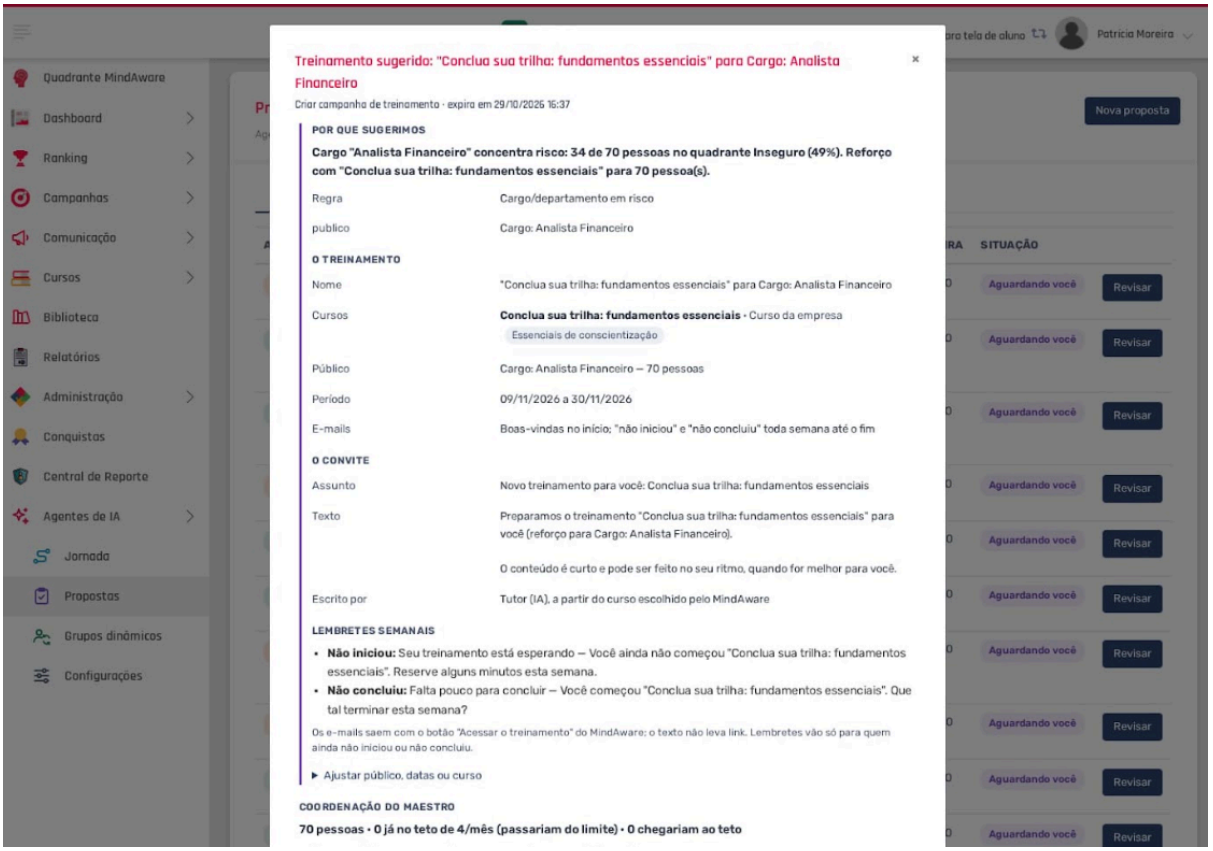
SEGMENTADOR: Responsável por propor grupos dinâmicos com base em características e comportamentos dos usuários.

INSTRUTOR: Responsável por propostas relacionadas à elaboração de questões e conteúdos de avaliação, como quizzes de políticas.

As propostas identificadas com a situação **Aguardando você** estão pendentes de análise administrativa. O administrador pode consultar a justificativa e os detalhes antes de decidir sobre a execução.

Revisar propostas de treinamento

1. Acesse **Agentes de IA > Propostas**.
2. Localize uma proposta gerada pelo agente **TUTOR**.
3. Clique em **Revisar** para abrir os detalhes.
4. Na seção **Por que sugerimos**, consulte a justificativa, a regra utilizada e o público identificado.
5. Em **O treinamento**, verifique o nome da campanha, os cursos selecionados, o público, o período e a programação de e-mails.
6. Na seção **O convite**, consulte o assunto e o conteúdo da mensagem que será enviada aos colaboradores.
7. Verifique os lembretes semanais destinados aos usuários que ainda não iniciaram ou concluíram o treinamento.
8. Utilize **Ajustar público, datas ou curso** caso seja necessário revisar as configurações propostas.
9. Consulte **Coordenação do Maestro** para verificar os indicadores relacionados aos limites de campanhas por colaborador.



A proposta apresenta as informações necessárias para avaliar a recomendação do agente, incluindo os motivos que levaram à seleção do público e do treinamento.

O conteúdo dos convites é elaborado pela IA a partir do curso selecionado pela plataforma. Os e-mails podem incluir mensagens de boas-vindas e lembretes periódicos para colaboradores que ainda não iniciaram ou concluíram suas atividades.

A seção **Coordenação do Maestro** apresenta informações relacionadas ao limite de campanhas por colaborador, auxiliando na avaliação da quantidade de ações direcionadas ao mesmo público.

As campanhas sugeridas dependem da aprovação de um administrador antes de sua execução.

Configurar sugestões de treinamento

1. Acesse **Agentes de IA > Configurações**.
2. Localize a seção **Campanhas de treinamento sugeridas**.
3. Utilize **Ligado** ou **Desligado** para habilitar ou desabilitar as sugestões automáticas.
4. Marque as regras que deverão ser consideradas pelo agente **TUTOR**.
5. Configure os parâmetros de dias, percentuais, intervalos e quantidade de sugestões simultâneas.

As regras disponíveis permitem gerar sugestões de treinamento conforme diferentes situações identificadas na plataforma.

Pós-simulação: Sugere treinamentos para colaboradores que clicaram ou submeteram dados em campanhas de simulação encerradas, utilizando cursos relacionados ao tema da simulação.

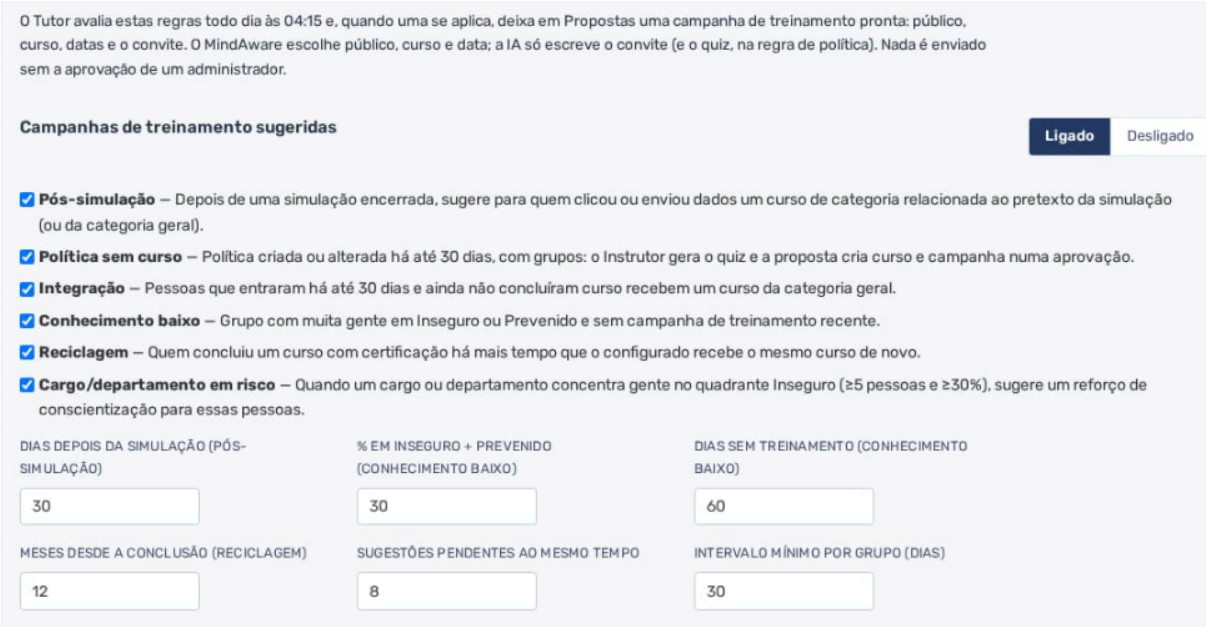
Política sem curso: Identifica políticas criadas ou alteradas recentemente e sugere a elaboração de um quiz e de uma campanha de treinamento.

Integração: Sugere treinamentos para colaboradores cadastrados recentemente que ainda não concluíram cursos.

Conhecimento baixo: Identifica grupos com concentração de colaboradores nos quadrantes Inseguro ou Prevenido e sem treinamento recente.

Reciclagem: Sugere a realização de um curso novamente após o intervalo definido desde sua conclusão.

Cargo/departamento em risco: Identifica cargos ou departamentos com concentração de colaboradores no quadrante Inseguro e sugere treinamentos direcionados.



Os parâmetros permitem definir o intervalo após uma simulação, o percentual de colaboradores em situação de risco, o período sem treinamento, o prazo para reciclagem, a quantidade máxima de sugestões pendentes e o intervalo mínimo entre sugestões para o mesmo grupo.

O agente **TUTOR** avalia diariamente as regras configuradas, às **04h15**, e disponibiliza as sugestões aplicáveis na área de **Propostas**. A plataforma seleciona o público, o curso e as datas, enquanto a IA elabora o conteúdo do convite e, quando aplicável, o quiz.

Nenhuma campanha é enviada sem aprovação administrativa.

Configurar sugestões de simulação

1. Acesse **Agentes de IA > Configurações**.

2. Localize a seção **Campanhas sugeridas**.
3. Utilize **Ligado** ou **Desligado** para habilitar ou desabilitar as sugestões.
4. Selecione as regras que deverão ser consideradas na geração de campanhas de simulação.
5. Configure os campos **Dias sem simulação**, **Dias depois do curso**, **Sugestões pendentes ao mesmo tempo** e **Intervalo mínimo por grupo (dias)**.
6. Acesse **Agentes de IA > Propostas** para acompanhar as sugestões geradas.

As regras disponíveis permitem identificar situações em que uma nova simulação pode contribuir para avaliar o comportamento dos colaboradores.

Grupo sem simulação: Sugere campanhas para grupos que permaneceram sem receber simulações durante o período configurado.

Reteste depois do curso: Sugere novas simulações para colaboradores que concluíram um treinamento e ainda não foram testados após sua conclusão.

Categoria nunca testada: Identifica temas do catálogo que não foram utilizados em simulações pela organização há mais de 180 dias.

Golpe real reportado: Sugere campanhas baseadas em ameaças reais classificadas como maliciosas ou suspeitas pelo Sentinela, utilizando um novo conteúdo com o mesmo pretexto.

Cargo/departamento em risco: Sugere campanhas direcionadas a cargos ou departamentos com pelo menos cinco colaboradores e concentração mínima de 30% no quadrante Inseguro.



Os parâmetros configuráveis permitem controlar a frequência das simulações e a quantidade de propostas pendentes, evitando sugestões repetidas para o mesmo público em intervalos reduzidos.

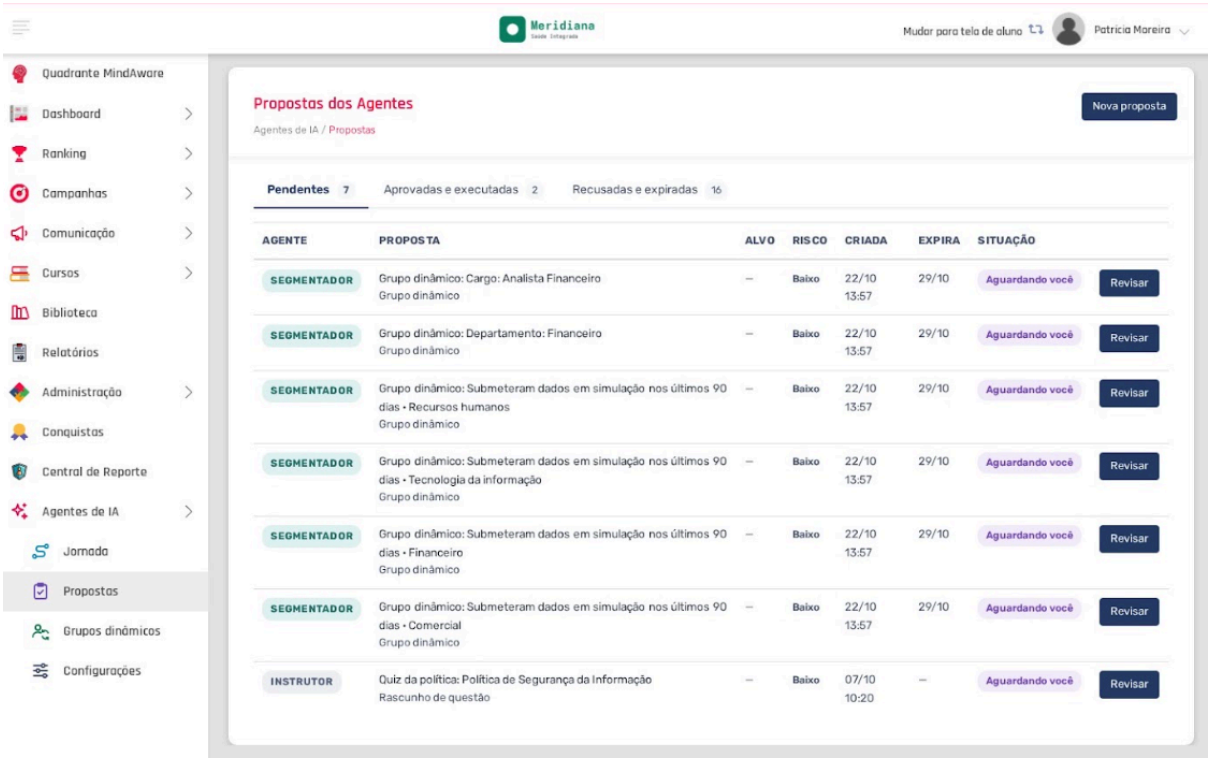
As sugestões geradas ficam disponíveis na seção **Propostas**, onde o administrador poderá consultar os detalhes e avaliar sua execução.

Acompanhar as propostas geradas

Para acompanhar as recomendações dos agentes, acesse **Agentes de IA > Propostas** e consulte as propostas disponíveis nas abas **Pendentes**, **Aprovadas e executadas** e **Recusadas e expiradas**.

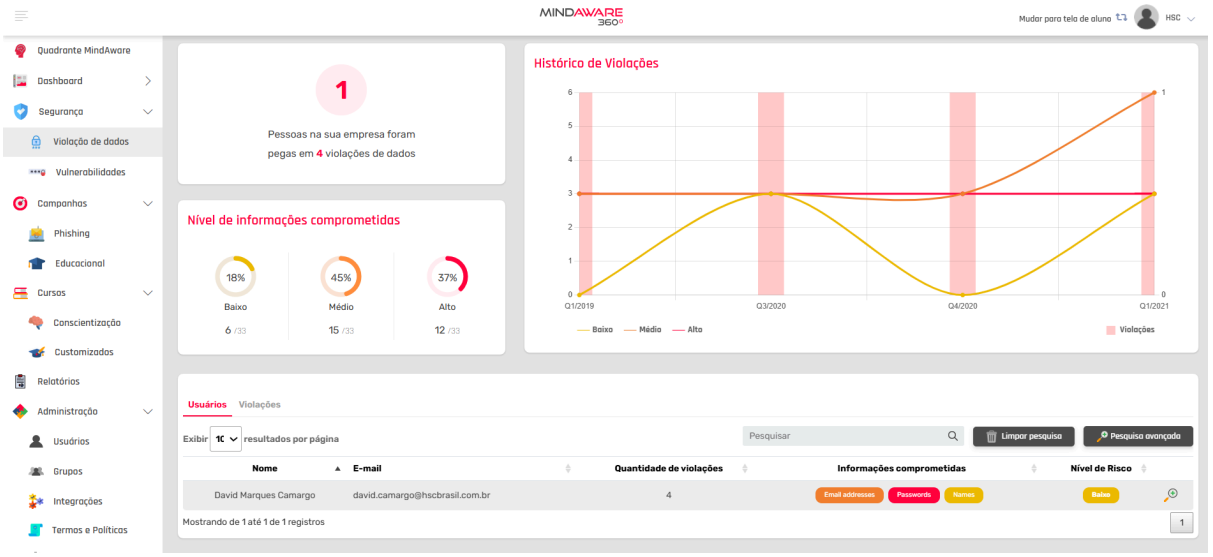
A listagem apresenta o agente responsável, a descrição da proposta, o público-alvo, o nível de risco, a data de criação, o prazo de expiração e a situação atual.

As propostas pendentes devem ser revisadas pelo administrador antes de sua execução. Esse processo permite avaliar a adequação do público, o conteúdo recomendado e a programação das campanhas, mantendo o controle administrativo sobre as ações sugeridas pelos agentes de IA.


Meridiana
Mudar para tela de aluno
Patricia Moreira
Quadrante MindAware
Dashboard
Ranking
Campanhas
Comunicação
Cursos
Biblioteca
Relatórios
Administração
Conquistas
Central de Reporte
Agentes de IA
Jornada
Propostas
Grupos dinâmicos
Configurações
Propostas dos Agentes
Agentes de IA / Propostas
Nova proposta
Pendentes 7
Aprovadas e executadas 2
Recusadas e expiradas 16
AGENTE
PROPOSTA
ALVO
RISCO
CRIADA
EXPIRA
SITUAÇÃO
SEGMENTADOR
Grupo dinâmico: Cargo: Analista Financeiro
Grupo dinâmico
Baixo
22/10 13:57
29/10
Aguardando você
Revisar
SEGMENTADOR
Grupo dinâmico: Departamento: Financeiro
Grupo dinâmico
Baixo
22/10 13:57
29/10
Aguardando você
Revisar
SEGMENTADOR
Grupo dinâmico: Submeteram dados em simulação nos últimos 90 dias • Recursos humanos
Grupo dinâmico
Baixo
22/10 13:57
29/10
Aguardando você
Revisar
SEGMENTADOR
Grupo dinâmico: Submeteram dados em simulação nos últimos 90 dias • Tecnologia da informação
Grupo dinâmico
Baixo
22/10 13:57
29/10
Aguardando você
Revisar
SEGMENTADOR
Grupo dinâmico: Submeteram dados em simulação nos últimos 90 dias • Financeiro
Grupo dinâmico
Baixo
22/10 13:57
29/10
Aguardando você
Revisar
SEGMENTADOR
Grupo dinâmico: Submeteram dados em simulação nos últimos 90 dias • Comercial
Grupo dinâmico
Baixo
22/10 13:57
29/10
Aguardando você
Revisar
INSTRUTOR
Quiz da política: Política de Segurança da Informação
Rascunho de questão
Baixo
07/10 10:20
Aguardando você
Revisar

Segurança

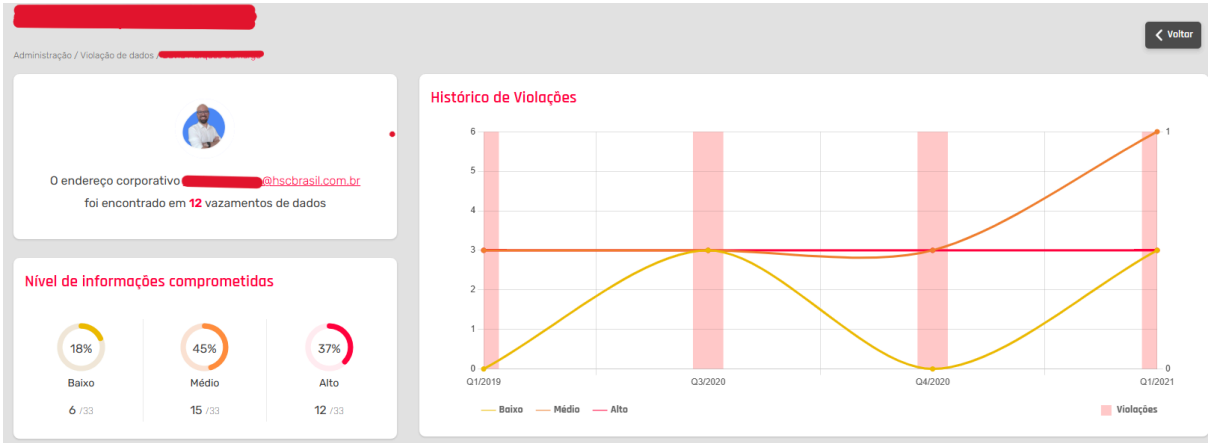
Violação de dados



É possível ver os usuários que violam dados e todas as ações que eles tomaram.



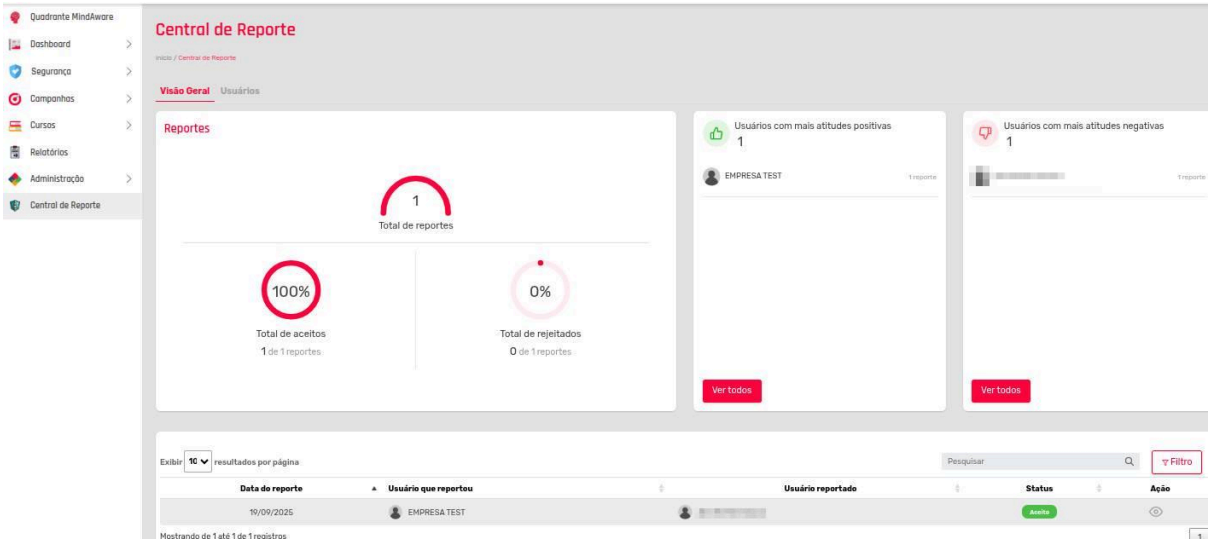
E ao clicar no ícone indicado você abre uma tela com análises detalhadas sobre os vazamentos de dados desse usuário.



Central de Reportes

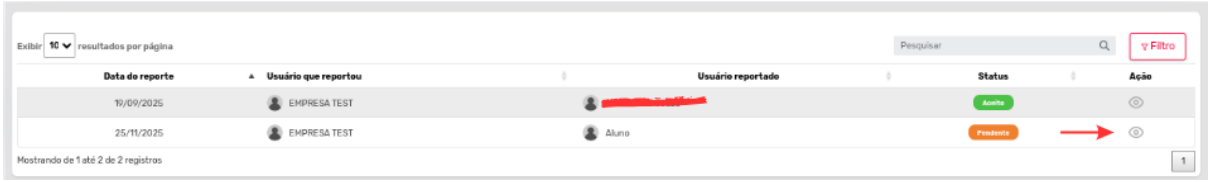
A Central de Reportes é um recurso que permite ver reportes que colaboradores fizeram para comunicar incidentes de segurança, comportamentos suspeitos ou ações consideradas inseguras diretamente aos administradores da plataforma.

Essas informações auxiliam a organização a identificar pontos de vulnerabilidade, direcionar ações corretivas e aplicar treinamentos adicionais aos usuários que demonstram maior necessidade de orientação.

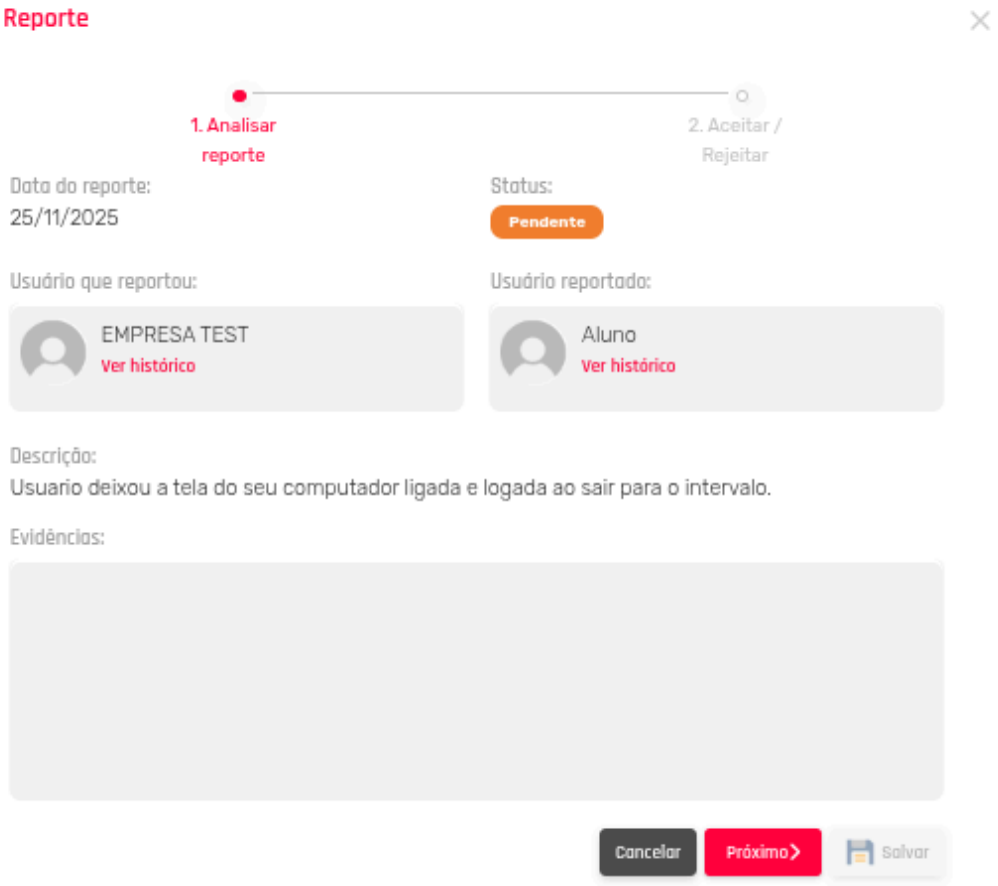


Nessa tela é possível ver a quantidade total de reportes e porcentagem de reportes aceitos e recusados. Também são exibidos os **usuários com atitudes positivas**, que podem receber pontos quando realizam um reporte coerente, e os **usuários com atitudes negativas**, que podem perder pontos caso tenham sido reportados por comportamentos inseguros.

Clicando no ícone indicado, é possível abrir as informações do reporte.;



Abrirá uma janela mostrando a data que foi feito o reporte, quem fez, o usuário reportado a descrição e algum anexo se tiver.



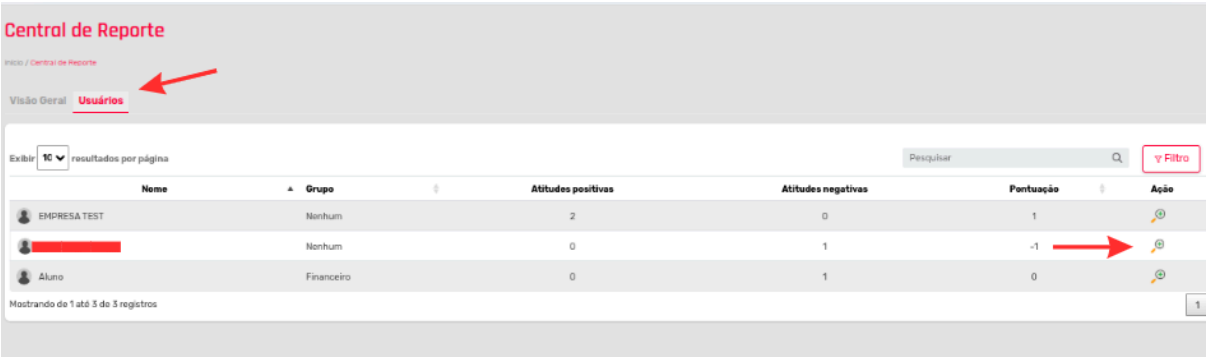
Ao clicar em **Próximo**, o administrador é direcionado para a etapa de análise do reporte, onde poderá **aceitar** ou **recusar** a sinalização enviada pelo usuário.

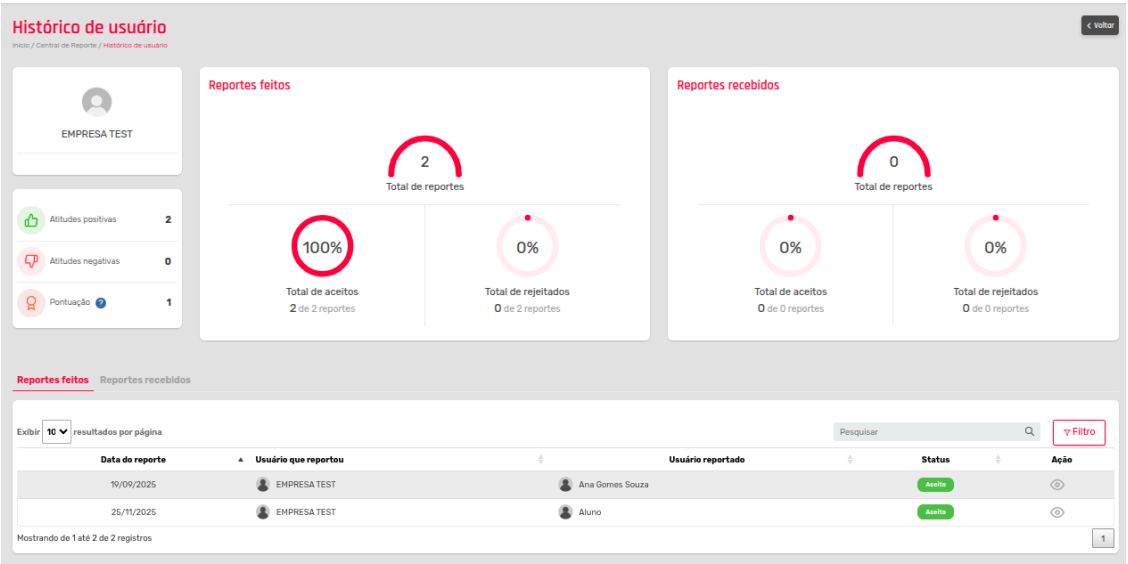
- **Se o reporte for aceito:** O administrador pode atribuir **pontuação positiva** ao usuário que realizou o reporte e, se desejar, **reduzir pontos** do usuário que foi reportado, reforçando comportamentos seguros ou sinalizando condutas inadequadas.
- **Se o reporte for recusado:** É necessário registrar uma **justificativa** informando o motivo da recusa.

Após definir a ação desejada, em ambos os casos, basta clicar em **Salvar** para concluir o processo.



Na tela central de reportes, é possível ir na parte **Usuários** para ver todos os usuários que tiveram atividades na central de reportes. Clicando no icone indicado irá para uma tela onde teŕa o histórico do usuário.





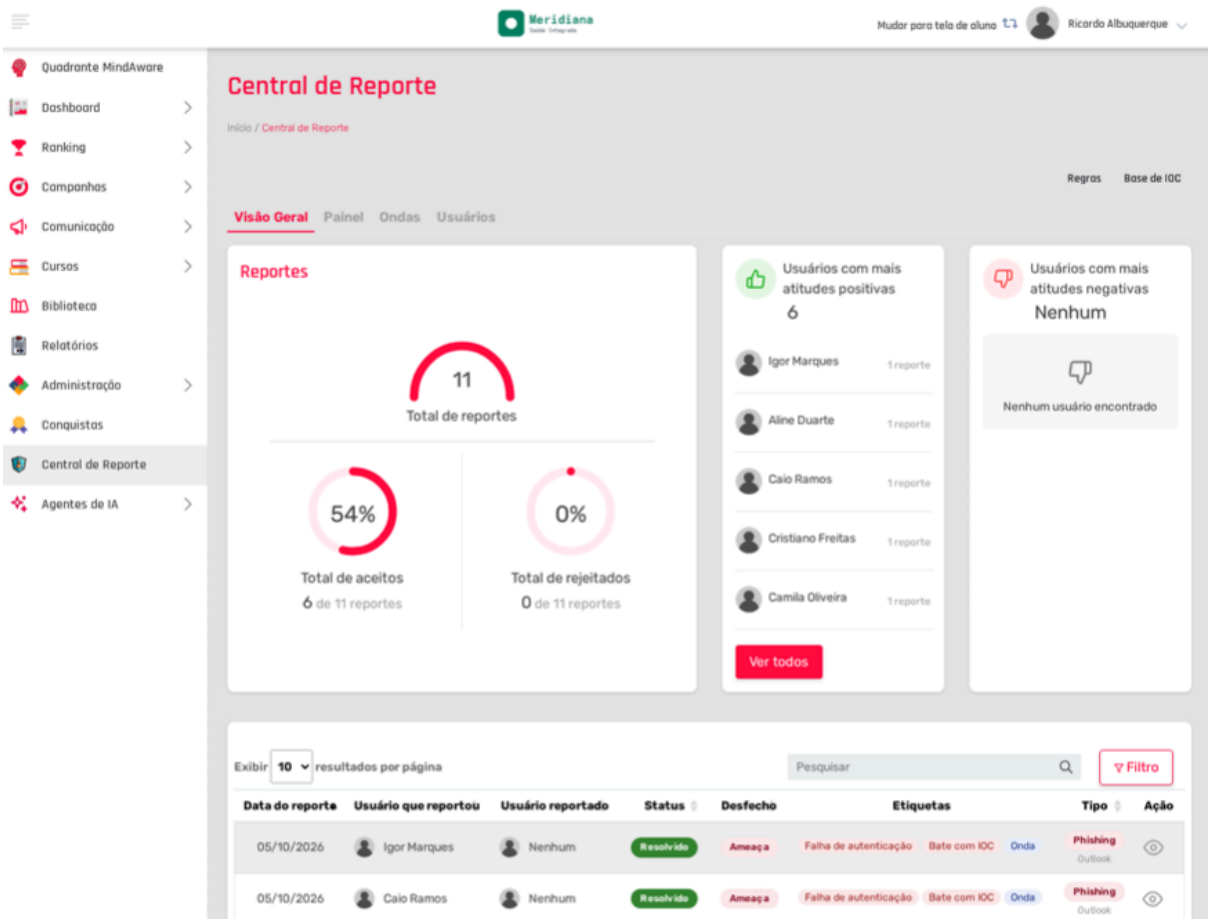
Essa tela mostra informações sobre os reportes feitos e recebidos.

Orquestração de Resposta a Phishing

A plataforma MindAware 360º permite ao administrador gerenciar os e-mails suspeitos reportados pelos colaboradores, analisar possíveis ameaças e executar ações de resposta a incidentes de phishing.

Por meio dessa funcionalidade, é possível acompanhar os casos reportados, consultar análises realizadas por Inteligência Artificial, identificar campanhas de phishing, configurar regras de tratamento e realizar ações de remediação nas caixas de e-mail dos colaboradores.

A plataforma também disponibiliza uma base de indicadores de comprometimento (IOC), recursos de automação e um painel operacional para acompanhamento dos resultados.



Gerenciamento dos Casos Reportados

Na área de casos, o administrador poderá consultar os e-mails suspeitos reportados pelos colaboradores e acompanhar o andamento de cada ocorrência.

A listagem apresenta os casos registrados, permitindo identificar sua situação, prioridade, responsável, classificação e possíveis indicadores de ameaça.

Os casos seguem as seguintes situações:

- Novo: Caso recebido que ainda não teve sua análise iniciada.
- Em análise: Caso que está sendo avaliado por um responsável.
- Escalonado: Caso encaminhado para tratamento adicional.
- Resolvido: Caso cuja análise foi concluída e recebeu uma classificação final.

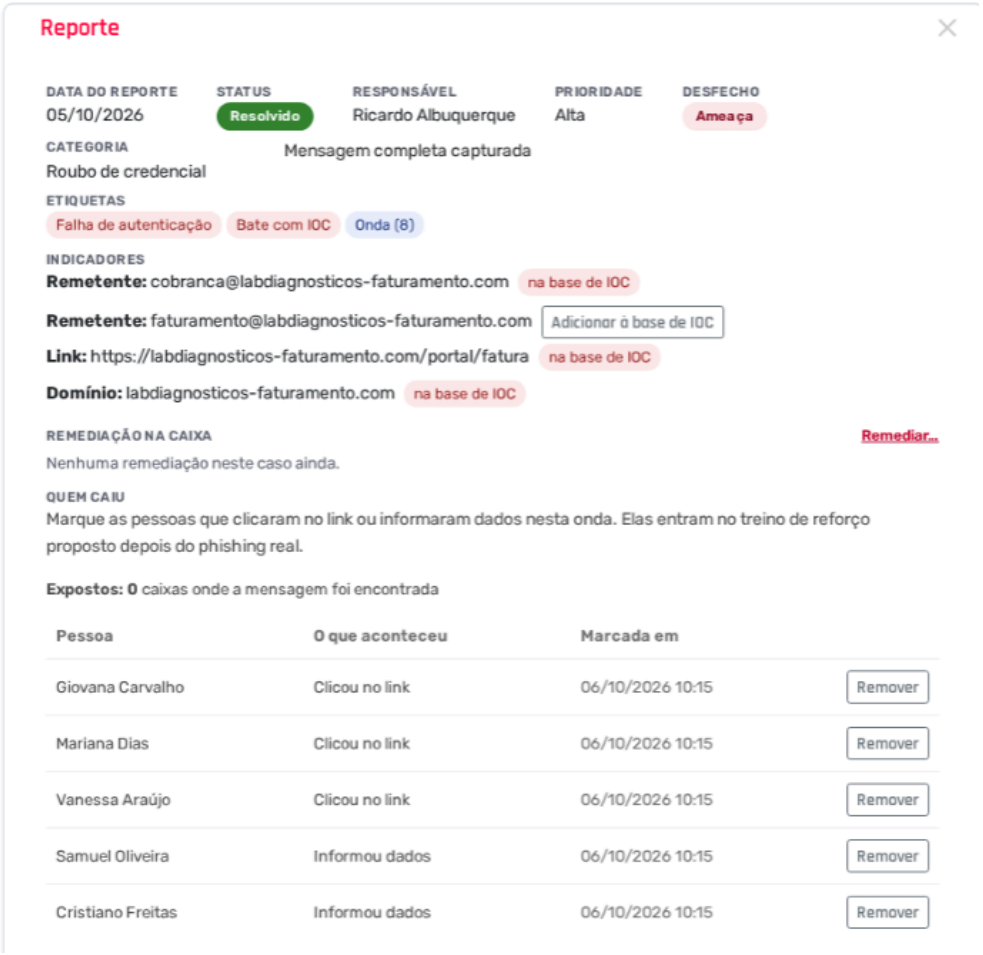
Ao concluir a análise, o caso poderá receber um dos seguintes desfechos: Ameaça, Spam ou Limpo.

A plataforma também apresenta etiquetas que identificam sinais relevantes, como falhas de autenticação, correspondência com indicadores de comprometimento e associação a ondas de e-mails semelhantes.

Análise de um Caso

Para consultar os detalhes de uma ocorrência, localize o caso desejado na listagem e clique sobre ele.

Será apresentada uma tela contendo as informações relacionadas ao reporte, incluindo situação, responsável, prioridade, desfecho, categoria e indicadores identificados.



Nesta tela, o administrador poderá utilizar a opção Assumir caso para iniciar o tratamento da ocorrência.

Após assumir o caso, sua situação será alterada para Em análise.

Durante a avaliação, estarão disponíveis informações como:

- E-mail reportado: Apresenta assunto, remetente, data, trecho da mensagem, cabeçalhos e detalhes da detecção.
- Indicadores: Apresenta remetentes, domínios, links e outros elementos identificados, permitindo verificar sua presença na base de IOC.
- Etiquetas: Identificam características relevantes relacionadas à ameaça.
- Remediação na caixa: Permite consultar e executar ações sobre mensagens presentes nas caixas de e-mail, conforme as permissões disponíveis.
- Quem caiu: Permite identificar os colaboradores que clicaram em links ou forneceram informações durante a interação com a mensagem.

Resolução do Caso

Após concluir a análise, o administrador poderá utilizar as opções Aceitar ou Rejeitar para registrar sua decisão.

Ao aceitar o reporte, o caso poderá ser classificado como Ameaça ou Spam. Ao rejeitá-lo, será classificado como Limpo.

A plataforma também permite atribuir uma nota ao colaborador que realizou o reporte.

Todas as alterações de situação e decisões realizadas ficam registradas no histórico do caso e na auditoria da plataforma.

Importante: Após a resolução, o caso recebe um desfecho definitivo, encerrando seu fluxo de tratamento.

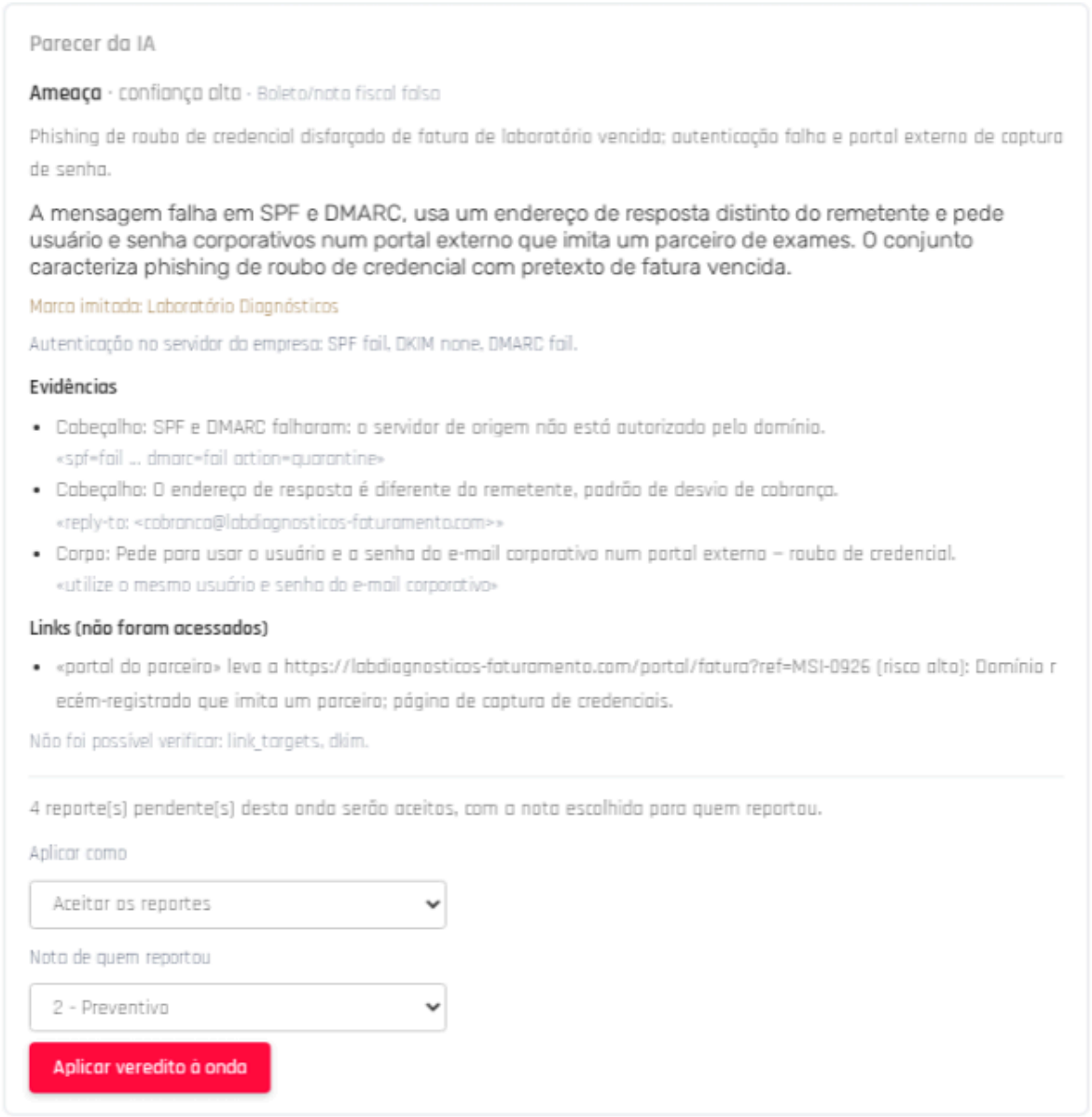
Análise por Inteligência Artificial

A plataforma permite utilizar Inteligência Artificial para auxiliar na identificação e classificação de mensagens suspeitas.

Quando a análise automática estiver habilitada e a mensagem completa tiver sido capturada, a IA poderá apresentar um parecer contendo:

- Classificação: Identifica se a mensagem representa uma ameaça, spam ou conteúdo legítimo.
- Categoria: Apresenta o tipo de ameaça ou conteúdo identificado.
- Confiança: Indica o nível de confiança da análise.
- Evidências: Apresenta os elementos que fundamentaram a classificação.
- Marca imitada: Identifica possíveis tentativas de utilização indevida da identidade de empresas ou serviços.
- Autenticação: Apresenta informações relacionadas à validação da origem da mensagem.

O parecer também poderá apresentar um resumo da análise e os motivos que levaram à classificação sugerida.



Aplicação do Parecer

Após consultar as informações, o administrador poderá utilizar a opção Aplicar veredito à onda para realizar o tratamento dos reportes relacionados.

A Inteligência Artificial atua como apoio à decisão, não substituindo a validação administrativa.

Quando a IA classificar uma mensagem como legítima, mas identificar sinais de risco, como falhas de autenticação ou domínios semelhantes aos de empresas conhecidas, a plataforma exigirá uma avaliação do administrador antes da aplicação do desfecho.

Nos casos em que uma ameaça for identificada com alta confiança, também poderá ser apresentada uma proposta de alerta aos colaboradores, sujeita à aprovação administrativa.

Gerenciamento de Ondas de Phishing

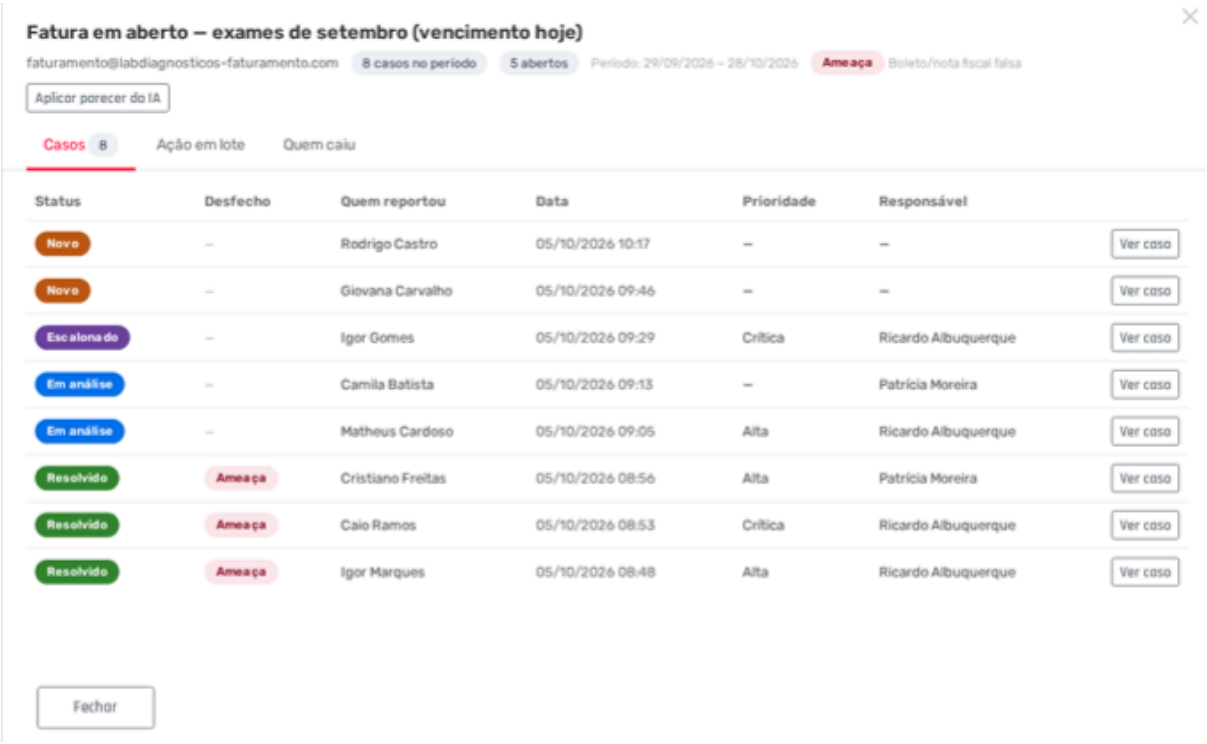
A funcionalidade de ondas permite agrupar diferentes reportes relacionados a uma mesma mensagem, facilitando a identificação de campanhas de phishing direcionadas à organização.

Na aba Ondas, o administrador poderá consultar os agrupamentos identificados no período selecionado.



A listagem apresenta informações como quantidade de casos, ocorrências abertas e resolvidas, sinais identificados e parecer da Inteligência Artificial.

Ao selecionar uma onda, será apresentada uma janela contendo as abas Casos, Ação em lote e Quem caiu.



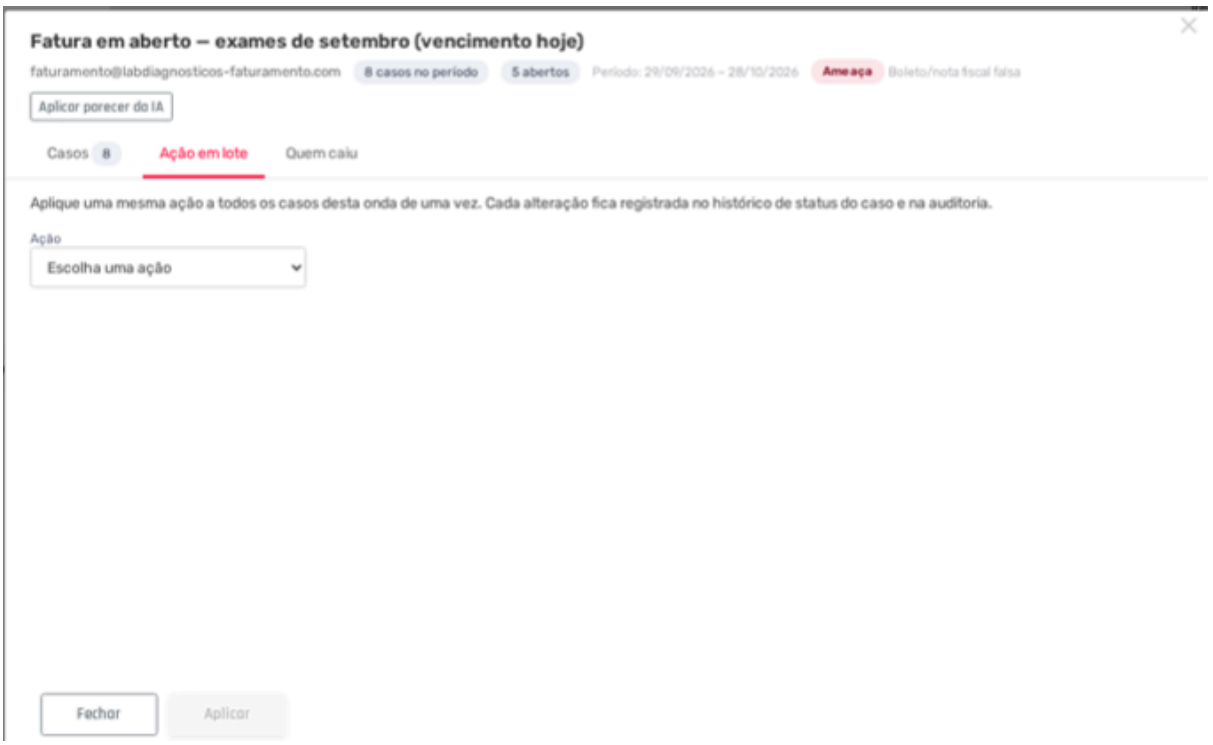
Ações em Lote

A opção Ação em lote permite executar uma mesma ação sobre todos os casos abertos de determinada onda, reduzindo a necessidade de tratamento individual.

Entre as ações disponíveis estão:

- Definir o desfecho dos casos.
- Alterar a situação e a prioridade.
- Definir categoria e responsável.
- Adicionar etiquetas.
- Incluir indicadores na base de IOC.
- Aplicar regras de tratamento.
- Executar ações de remediação nas caixas de e-mail.

Para realizar uma ação em lote, selecione a onda desejada, acesse a aba Ação em lote, escolha a operação e confirme sua execução.



As ações disponíveis dependem das permissões do usuário e ficam registradas no histórico e na auditoria da plataforma.

Remediação nas Caixas de E-mail

A plataforma permite realizar ações de remediação diretamente nas caixas de e-mail dos colaboradores, por meio da integração com o Microsoft 365.

Essa funcionalidade possibilita remover, isolar ou neutralizar mensagens suspeitas, reduzindo o risco de interação dos usuários com conteúdos maliciosos.

As ações podem ser executadas a partir de um caso individual, de uma onda de phishing ou de uma regra automatizada.

Entre as opções disponíveis estão:

- Mover para a Quarentena MindAware: Retira a mensagem da caixa de entrada e a transfere para uma pasta oculta.
- Mover para Lixo Eletrônico: Transfere a mensagem para a pasta de lixo eletrônico.
- Apagar (Itens Excluídos): Move a mensagem para a pasta de itens excluídos.

- Apagar definitivamente: Remove a mensagem de forma permanente, mediante confirmação.
- Remover anexos, desarmar links ou bloquear conteúdo: Preserva a mensagem original na quarentena e disponibiliza uma cópia modificada, sem os elementos identificados como perigosos.
- Marcar como phishing: Aplica uma categoria de aviso à mensagem no Outlook.

Execução da Remediação

Ao realizar uma ação de remediação, o administrador poderá definir seu alcance, selecionando apenas a caixa do colaborador que realizou o reporte ou todas as caixas relacionadas à onda.

A opção de remediação em todas as caixas da onda é exclusiva de administradores autorizados.

O andamento das ações poderá ser acompanhado no próprio caso, com informações sobre a execução em cada caixa de e-mail.

As ações de remediação ficam registradas na auditoria da plataforma e, quando reversíveis, poderão ser desfeitas por meio da opção Liberar.

Importante: Para utilizar essa funcionalidade, é necessário configurar a integração com Microsoft 365 e conceder a permissão Mail.ReadWrite. Caso necessário, o administrador poderá utilizar a opção Reconsentir na área de Integrações.

A exclusão definitiva não poderá ser revertida. A remediação também não realiza o bloqueio de remetentes ou domínios diretamente no Exchange.

A funcionalidade de remediação ainda depende de validação em um ambiente Microsoft 365 real, conforme a documentação fornecida.

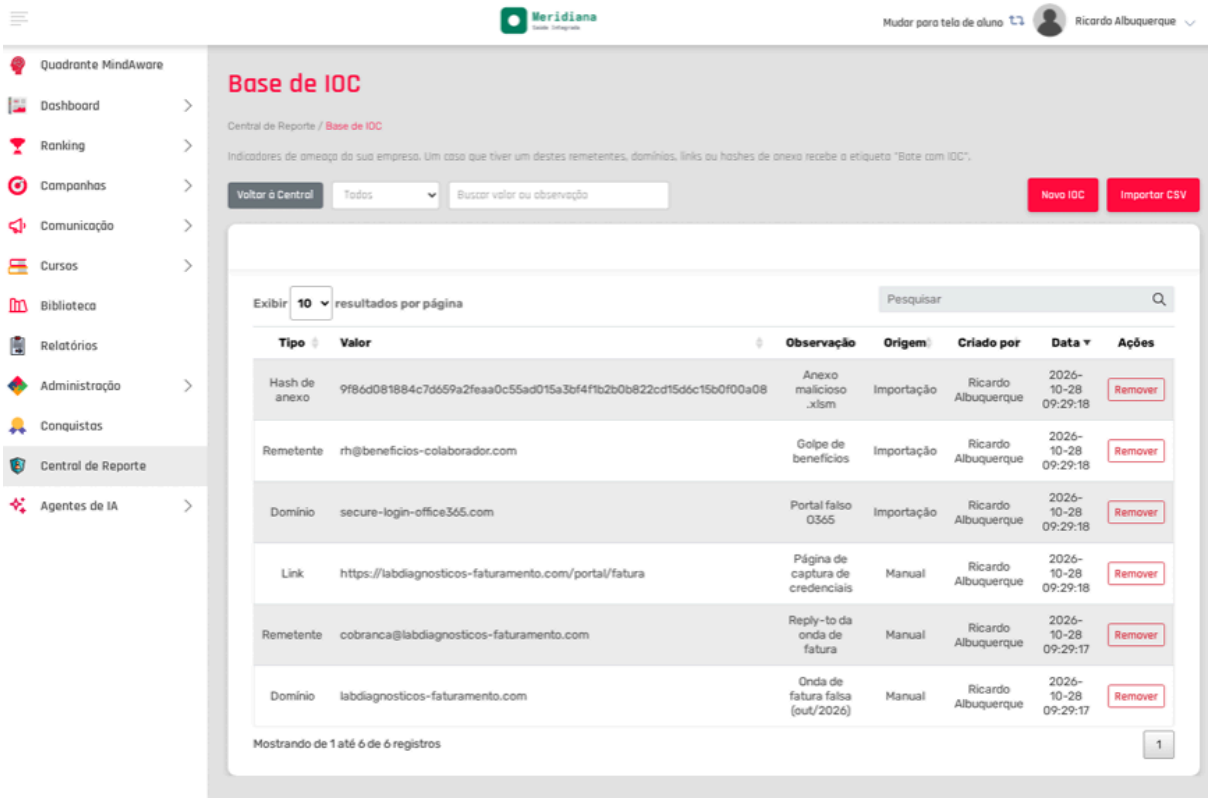
Base de Indicadores de Comprometimento (IOC)

A Base de IOC permite cadastrar e gerenciar indicadores associados a possíveis ameaças, auxiliando na identificação de mensagens suspeitas reportadas pelos colaboradores.

Os indicadores são exclusivos da organização e podem incluir:

- Remetente: Endereços de e-mail associados a ameaças.
- Domínio: Domínios identificados como suspeitos ou maliciosos.
- Link: Endereços eletrônicos relacionados a tentativas de phishing.
- Hash de anexo: Identificadores de arquivos associados a conteúdos maliciosos.

Quando um caso apresentar correspondência com algum indicador cadastrado, a plataforma adicionará automaticamente a etiqueta Bate com IOC.



Cadastro de Indicadores

Na tela Base de IOC, o administrador poderá consultar os indicadores cadastrados, seus tipos, observações e origem.

Para adicionar novos indicadores, estarão disponíveis as opções:

- Novo IOC: Permite cadastrar manualmente um indicador.
- Importar CSV: Permite importar indicadores por meio de um arquivo CSV contendo as colunas tipo, valor e observação, com limite de 1.000 linhas.

Também será possível cadastrar indicadores diretamente durante a análise de um caso, utilizando a opção Adicionar à base de IOC.

Sempre que um indicador for adicionado ou removido, a plataforma atualizará automaticamente as etiquetas dos casos que apresentarem correspondência.

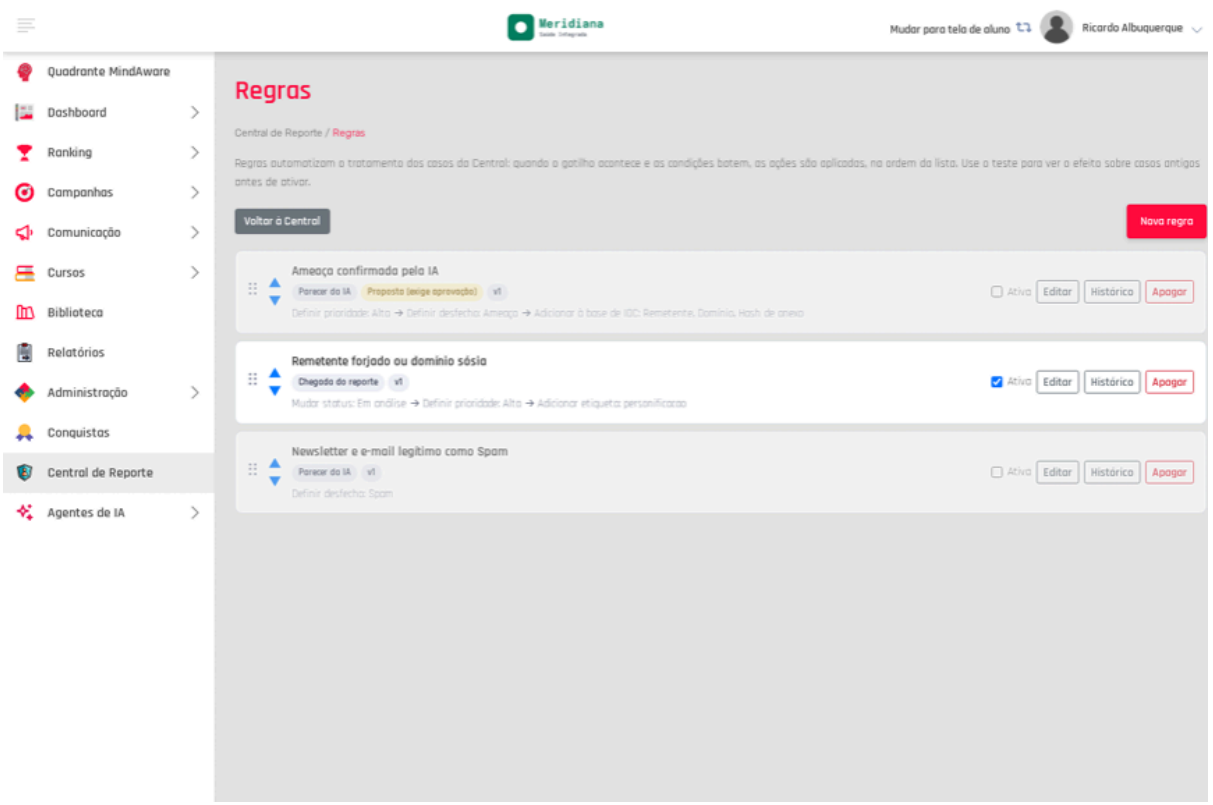
Configuração de Regras Automatizadas

O motor de regras permite automatizar o tratamento de casos de phishing, definindo condições e ações que serão executadas quando determinados eventos ocorrerem.

As regras podem funcionar de duas maneiras:

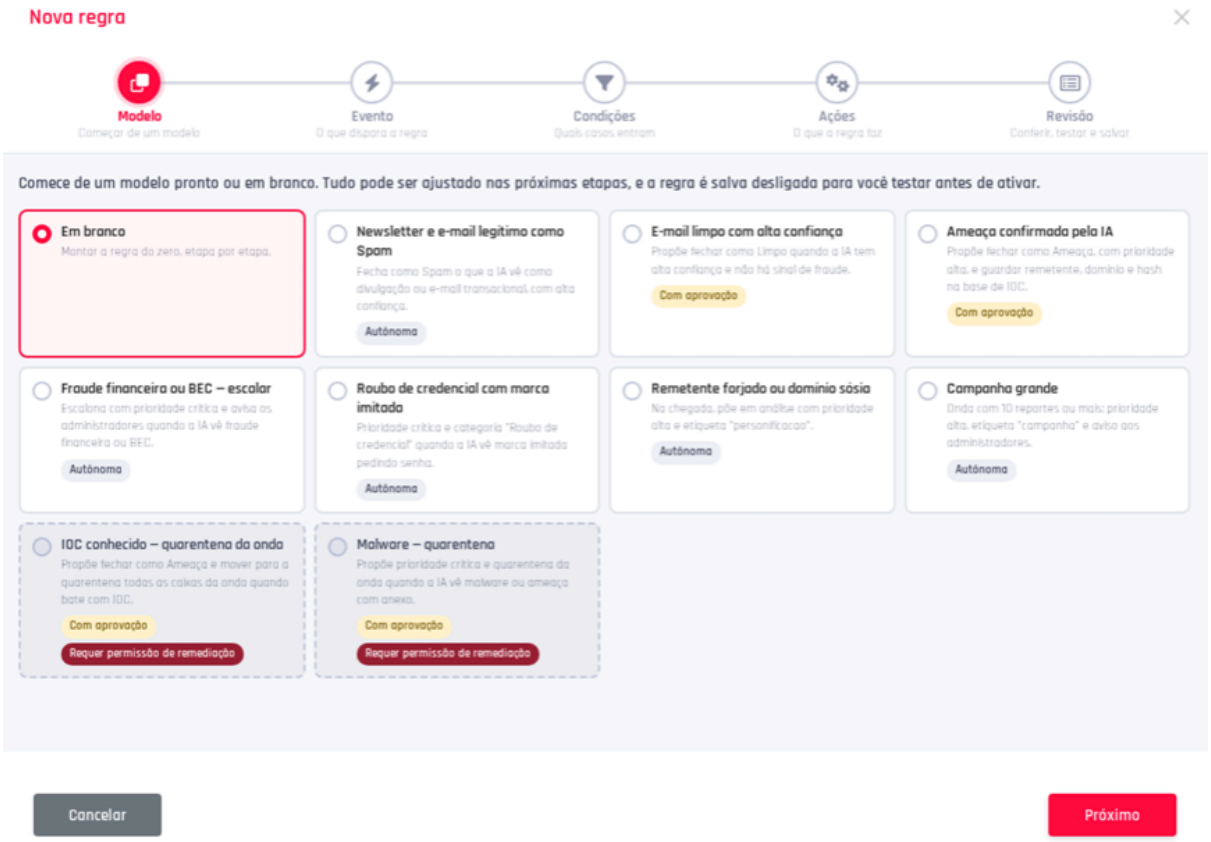
- Automática: Executa as ações configuradas quando as condições forem atendidas.
- Exige aprovação: Gera uma proposta para avaliação do administrador, que deverá aprová-la antes da execução.

Na tela de regras, o administrador poderá consultar as configurações existentes, seus gatilhos, modos de execução, versões e ações.



Criação de Regras

Para configurar uma nova regra, utilize o assistente de criação, composto por cinco etapas:



1. Modelo

Selecione um dos nove modelos disponibilizados pela plataforma ou inicie a configuração de uma regra em branco.

Os modelos apresentam condições e ações previamente configuradas, que poderão ser ajustadas conforme a necessidade da organização.

2. Evento

Defina os eventos que deverão iniciar a avaliação da regra.

Entre os gatilhos disponíveis estão:

- Chegada do reporte: Quando um colaborador reporta uma mensagem suspeita.

- Parecer da IA: Quando a Inteligência Artificial conclui a análise da onda.
- Mudança de status: Quando a situação de um caso é alterada.
- Entrada em onda: Quando um caso passa a integrar um agrupamento de reportes semelhantes.

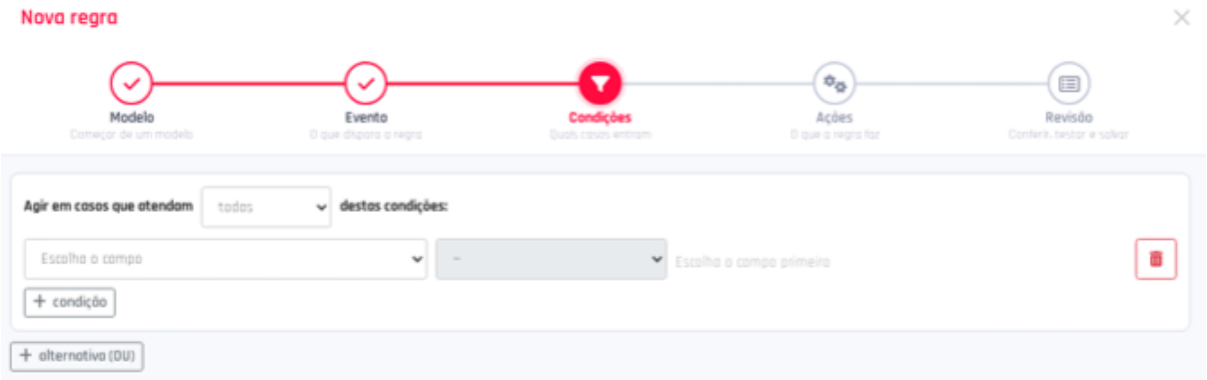
3. Condições

Configure os critérios que deverão ser atendidos para que a regra seja aplicada.

O administrador poderá combinar condições utilizando os operadores E e OU, definindo se todas ou apenas algumas condições deverão ser atendidas.

A plataforma permite configurar até dez blocos, com até vinte condições em cada um.

Os critérios poderão considerar informações como remetente, domínio, assunto, anexos, parecer da IA, confiança da análise, etiquetas, prioridade e situação do caso.



4. Ações

Defina as operações que deverão ser realizadas quando a regra atender às condições configuradas.

Entre as ações disponíveis estão:

- Definir desfecho.
- Alterar situação ou prioridade.
- Definir categoria e responsável.
- Adicionar etiquetas.
- Notificar administradores.

- Adicionar indicadores à base de IOC.
- Executar ações de remediação nas caixas de e-mail.

É possível configurar até dez ações por regra, executadas na ordem definida.

5. Revisão e Teste

Após concluir as configurações, revise os eventos, condições e ações selecionados.

Nesta etapa, será possível definir se a regra funcionará automaticamente ou exigirá aprovação administrativa.

Também estará disponível a opção Testar nos últimos 30 dias, que permite verificar quantos casos anteriores atenderiam às condições configuradas, sem executar nenhuma ação.

As regras são criadas inicialmente desativadas, permitindo realizar testes antes de sua ativação.

Modelos de Regras Disponíveis

A plataforma disponibiliza nove modelos para facilitar a configuração de automações:

- Newsletter e e-mail legítimo como Spam: Classifica automaticamente como Spam mensagens identificadas pela IA com alta confiança em categorias de divulgação ou transacionais.
- E-mail limpo com alta confiança: Propõe a classificação de mensagens legítimas como Limpo, mediante aprovação.
- Ameaça confirmada pela IA: Propõe classificar a mensagem como Ameaça, elevar a prioridade e adicionar indicadores à base de IOC.
- Fraude financeira ou BEC: Escalona casos relacionados a fraudes financeiras, atribui prioridade crítica e notifica administradores.
- Roubo de credencial com marca imitada: Identifica tentativas de roubo de credenciais associadas à imitação de marcas.
- Remetente forjado ou domínio sósia: Identifica possíveis tentativas de personificação e eleva a prioridade do caso.
- Campanha grande: Identifica ondas com dez ou mais reportes e notifica os administradores.

- IOC conhecido — quarentena da onda: Propõe o tratamento de mensagens que correspondam a indicadores cadastrados na base de IOC.
- Malware — quarentena: Propõe ações de remediação quando a IA identifica ameaças envolvendo malware ou anexos suspeitos.

Os modelos que executam ações de quarentena exigem as permissões necessárias para remediação nas caixas de e-mail.

Importante: As regras possuem controle de versões e histórico de alterações. Cada versão poderá atuar apenas uma vez sobre o mesmo caso. A edição ou desativação de uma regra poderá cancelar propostas pendentes relacionadas a ela.

Painel Operacional

O Painel Operacional permite acompanhar os indicadores relacionados aos reportes de phishing e às ações de resposta realizadas pela organização.

Nesta tela, o administrador poderá selecionar o período de análise, utilizando os filtros de 7, 30 ou 90 dias, ou definir um intervalo personalizado.

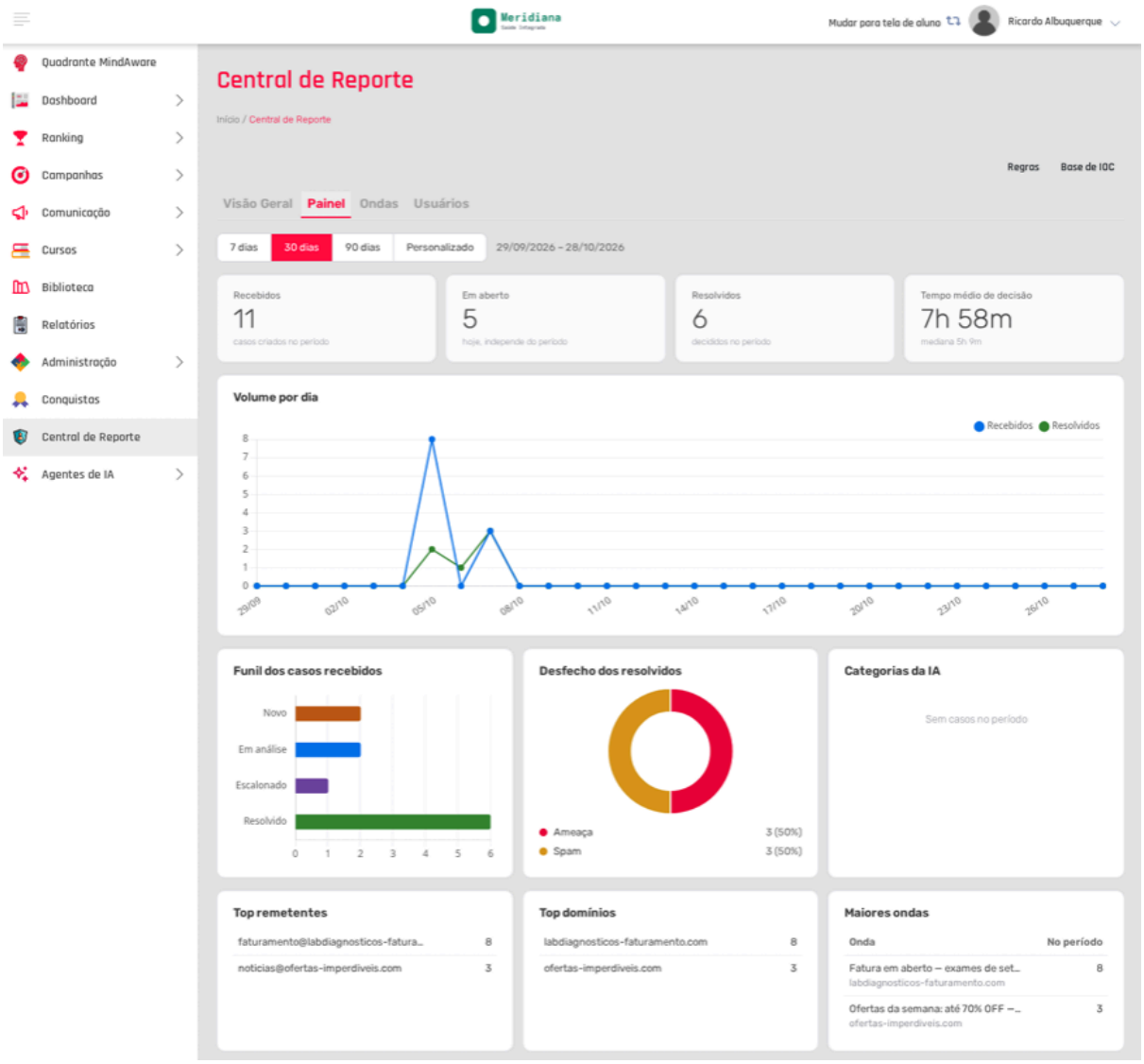
O painel apresenta informações como quantidade de casos recebidos, casos em aberto, casos resolvidos e tempo médio de decisão (MTTR), além de gráficos que demonstram a evolução dos reportes, a distribuição dos desfechos e as categorias identificadas pela Inteligência Artificial.

Também estarão disponíveis informações sobre os principais remetentes e domínios envolvidos, as maiores ondas identificadas e o desempenho dos responsáveis pelo tratamento dos casos.

O indicador Tempo médio de decisão (MTTR) considera o intervalo entre a criação e a resolução dos casos no período selecionado, permitindo avaliar o tempo necessário para concluir as análises.

A tabela de desempenho por responsável apresenta a quantidade de casos abertos, resolvidos e o tempo médio de tratamento de cada pessoa.

Essas informações auxiliam o administrador na identificação de tendências, no acompanhamento das ocorrências e na avaliação da eficiência das ações de resposta a phishing.



Captura da Mensagem Completa

É possível configurar a captura da mensagem completa reportada pelos colaboradores, possibilitando análises mais detalhadas pela Inteligência Artificial.

Essa funcionalidade é opcional e poderá ser configurada por domínio na área de Integrações, na aba correspondente ao add-in.

Para habilitá-la, utilize a opção **Enviar** a mensagem completa para análise.

Quando ativada, a plataforma poderá capturar a mensagem e seus anexos, armazenando as informações de forma criptografada.

O conteúdo completo não será disponibilizado para visualização ou download. No detalhe do caso, será apresentada apenas a identificação Mensagem completa capturada.

As mensagens capturadas serão mantidas por até 90 dias, sendo excluídas automaticamente após esse período.

O conteúdo somente será encaminhado ao serviço de Inteligência Artificial quando a análise automática estiver habilitada.

Importante: Sem a captura da mensagem completa, a Inteligência Artificial não realizará a análise dos reportes daquele domínio.

Ações Após a Resolução de Casos

Após a confirmação de uma ameaça de phishing, a plataforma poderá gerar propostas de ações educativas e de reconhecimento aos colaboradores.

Essas ações são integradas aos Agentes de IA e dependem de aprovação administrativa.

Entre as possibilidades estão:

- Conquista Guardião: Reconhece colaboradores que reportaram corretamente ameaças confirmadas, com níveis associados a 1, 5 e 20 reportes.
- Agradecimento: Permite gerar uma proposta de mensagem de agradecimento ao colaborador que realizou o reporte, sem divulgar informações do e-mail malicioso.
- Treinamento pós-phishing: Permite propor treinamentos de reforço aos colaboradores expostos à ameaça, com conteúdos diferenciados para aqueles que interagiram com a mensagem.

Para os colaboradores que clicaram ou forneceram dados, poderá ser proposta uma trilha completa e uma simulação de reforço, realizada pelo menos sete dias após o treinamento.

As propostas geradas poderão ser consultadas em Agentes de IA → Propostas, onde deverão ser avaliadas pelo administrador antes da execução.

As configurações relacionadas a essas ações estarão disponíveis na área de Configurações de IA.

Privacidade e Segurança das Informações

A plataforma utiliza mecanismos de proteção para preservar as informações relacionadas aos e-mails reportados e às análises realizadas.

As mensagens completas capturadas são armazenadas de forma criptografada e excluídas automaticamente após o período de retenção de 90 dias.

O conteúdo original não é disponibilizado para visualização ou download, nem incluído nos registros de auditoria, logs ou na Jornada da IA.

Os identificadores dos anexos são calculados pela própria plataforma e não são encaminhados ao serviço de Inteligência Artificial.

Esses controles contribuem para a proteção das informações da organização durante os processos de análise, classificação e resposta a incidentes de phishing.

Liberação de Filtragem de Campanhas de Phishing em Sistemas de Proteção de Email

O módulo de simulação de Campanhas de Phishing utiliza as mesmas técnicas que ataques reais. Para seu correto funcionamento é necessário criar exceções nas ferramentas de proteção. Caso sua empresa possua ferramentas de proteção como Firewall, Proxy, Anti-Spam e análise de conteúdo e outras, faça a inclusão dos seguintes IPś e domínios para que não sejam bloqueados ou alterados por este tipo de filtragem.

Sendo assim, para garantir a qualidade da entrega dos e-mails de simulação de Phishing enviados pela plataforma Mindaware, é necessário permitir os seguintes endereços IP, domínios e Headers em seu ambiente:

IP's: 187.108.197.245 187.45.189.90	**Domínios** mindaware.com.br app.mindaware.com.br
Remetentes app@mindaware.com.br noreply@mindaware.com.br	**Host's** mx01.mindaware.com.br mx02.mindaware.com.br
Header's X-Mindaware	**URL's:** https://app.mindaware.com.br/next/*

Os IP's e domínios mencionados, são de propriedade da HSC Mindaware e são de uso restrito e exclusivo para campanhas de conscientização.

A plataforma HSC MindAware não coleta ou armazena as informações inseridas pelos usuários na página de simulação de coleta de credenciais. Todas as informações inseridas na página são descartadas. Somente a ação 'clique' é gravada a fim de registrar o evento de comprometimento de credenciais.

Liberação em Sistemas Microsoft Office 365

Premissas

É necessário que o administrador tenha acesso e privilégios no Office 365 da Microsoft.
Vamos fazer a configuração de Office365, para uso com o MindAware em três etapas:

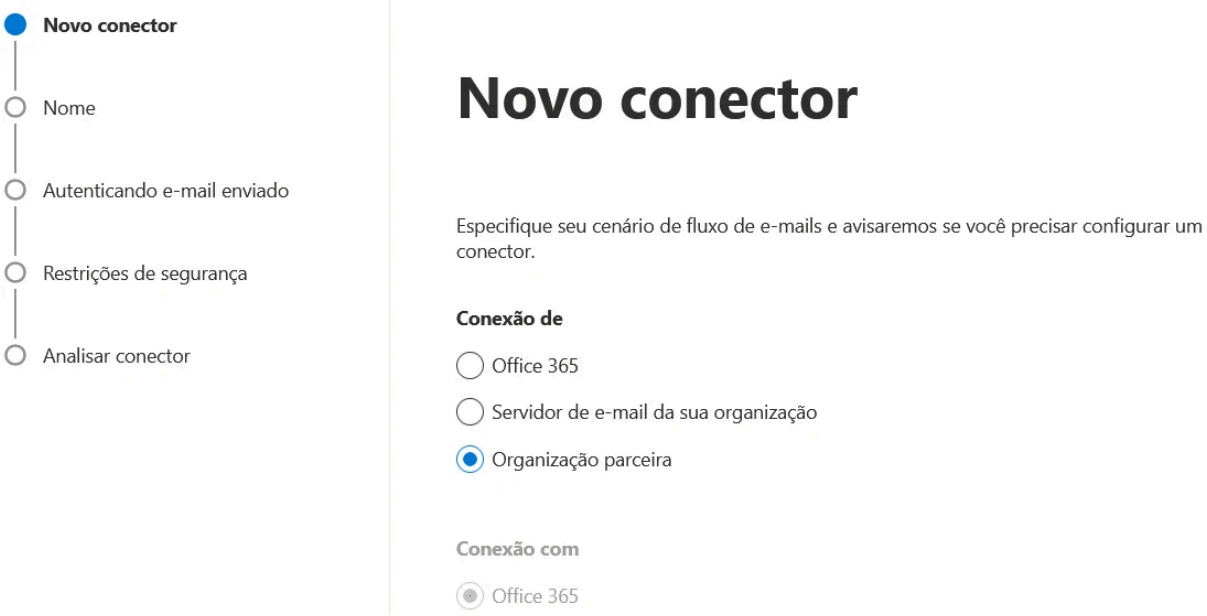
1. Criação de Conector de Entrada;
2. Criação de Regra para não spam e safelinks;
3. Caso tenha Microsoft Defender, criação de regra de permissão de simulação de ataque de phishing pelo MindAware;

Procedimento

Primeira Etapa: Criação de Conector de Entrada

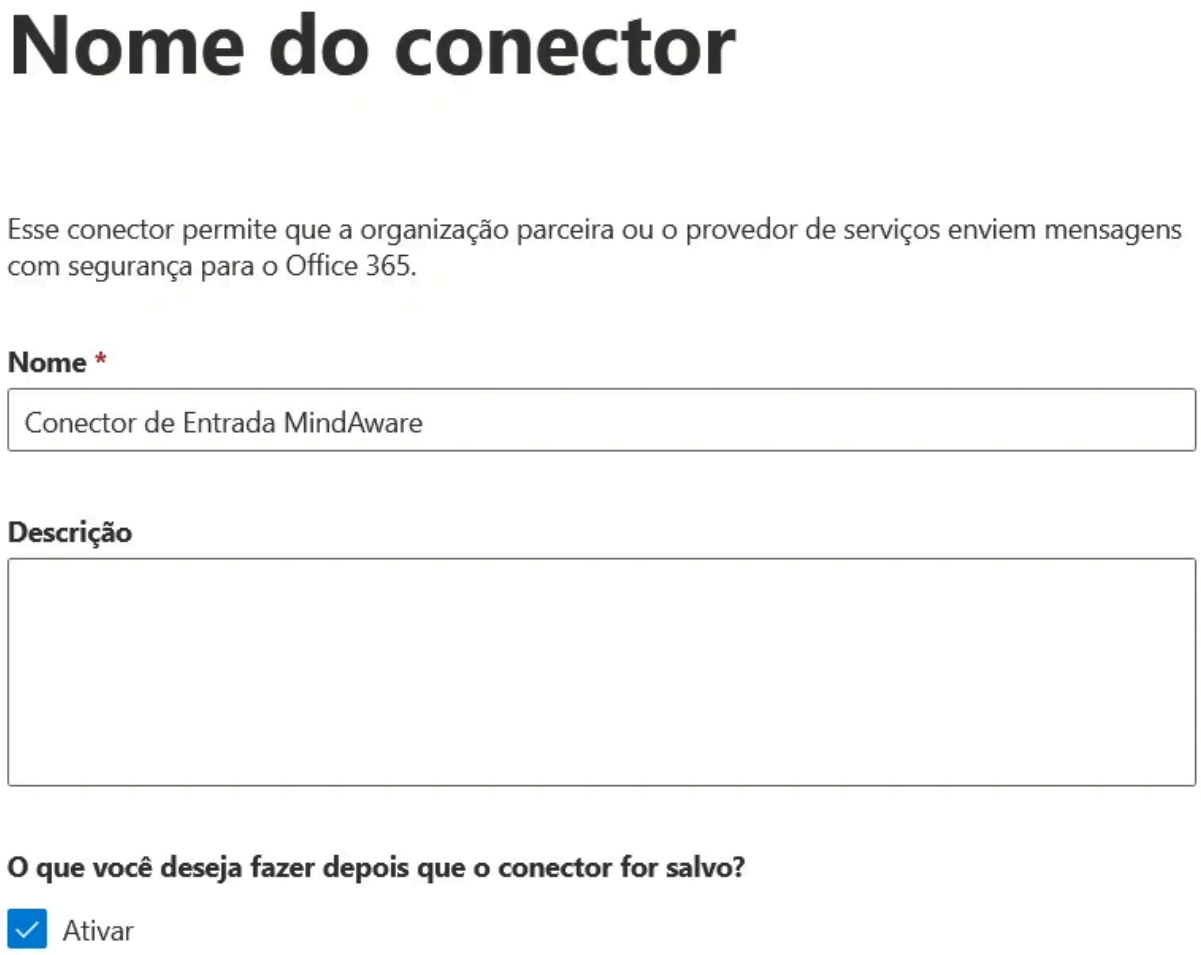
Essa primeira etapa é para que o Office 365 não bloqueie emails dos IP's do MindAware, por excesso de emails enviados de um unico IP.

1. Entre no Office 365 Exchange Admin Center (EAC)
2. Clique em Fluxo de Email (Mail Flow) > Conectores (Connectors)
3. Clique no ícone com sinal de mais (+), para criar novo conector.
   DE: Partner Connection (Organização Parceira)
   PARA: Office 365



4. Clique em Next / Próxima

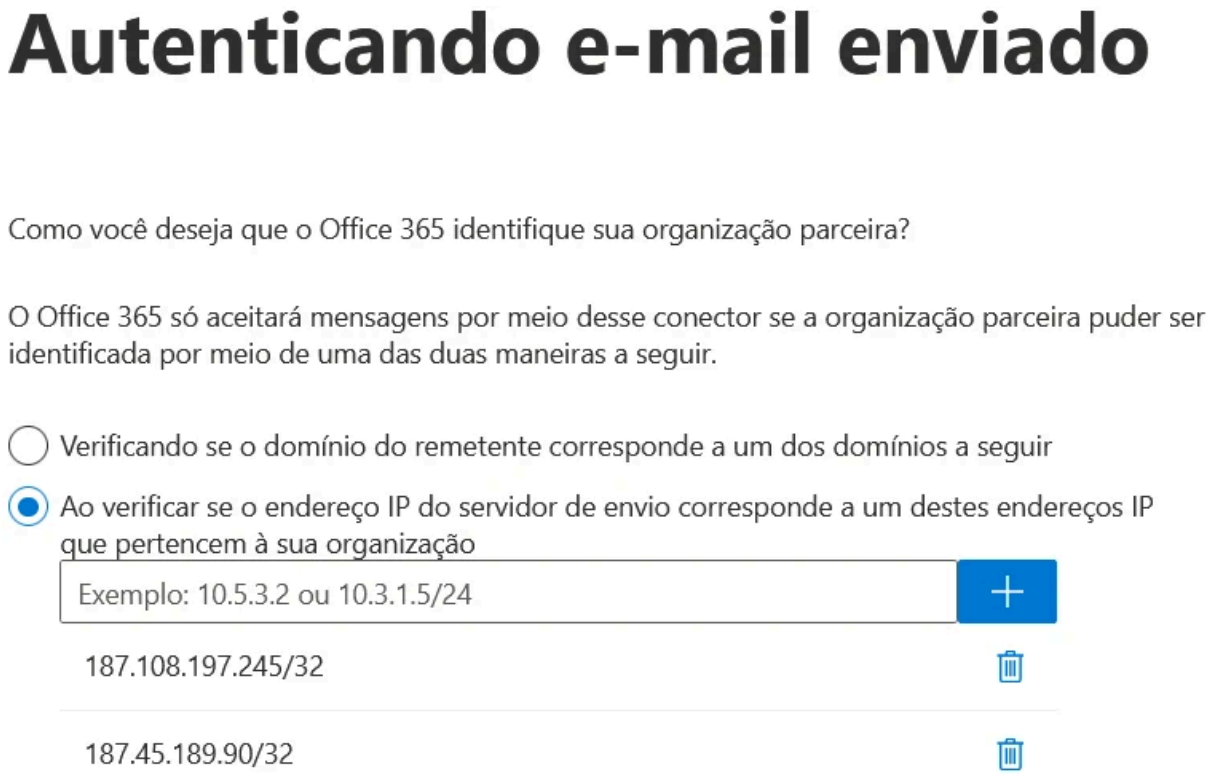
5. No campo Nome, insira um nome para a regra. No exemplo vamos colocar o nome: **Conector de Entrada MindAware**



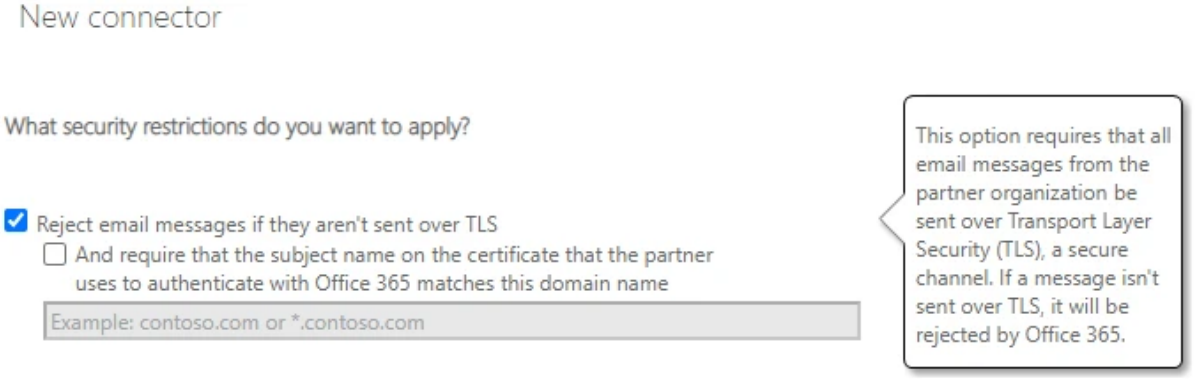
6. Clique em Next
7. Selecione a opção:
   Ao verificar se o endereço IP do servidor de envio corresponde a um desses endereços IP que pertencem à sua organização
   Insira os IPs dos Servidores MindAware, conforme a seguir:
   a. 187.108.197.245/32
   b. 187.45.189.90/32
   c. 131.100.228.128/25
   d. 177.136.253.0/26

   Obs: Se você estiver usando qualquer sistema de Email Gateway, será necessário incluir os IPs dos agentes de filtragem do Email Gateway nessa relação.

Deve ficar algo parecido com:



8. Após inserido todos os IP's, clique em Next/Próxima
9. Mantenha as configurações indicadas (de TLS)

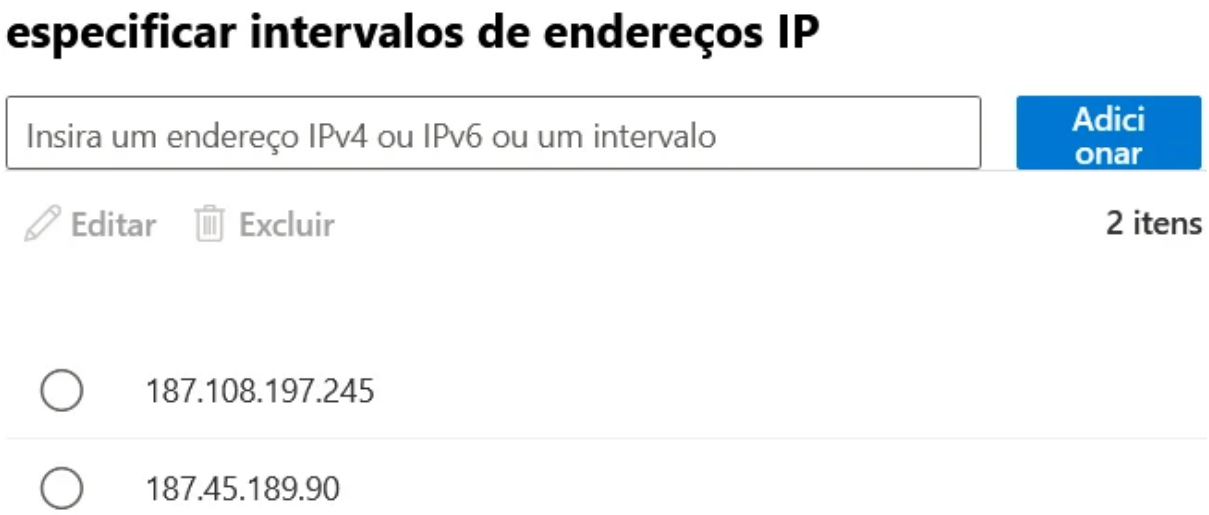


10. Clique em Next
11. Irá aparecer uma tela de resumo das informações. Clique em Criar conector.

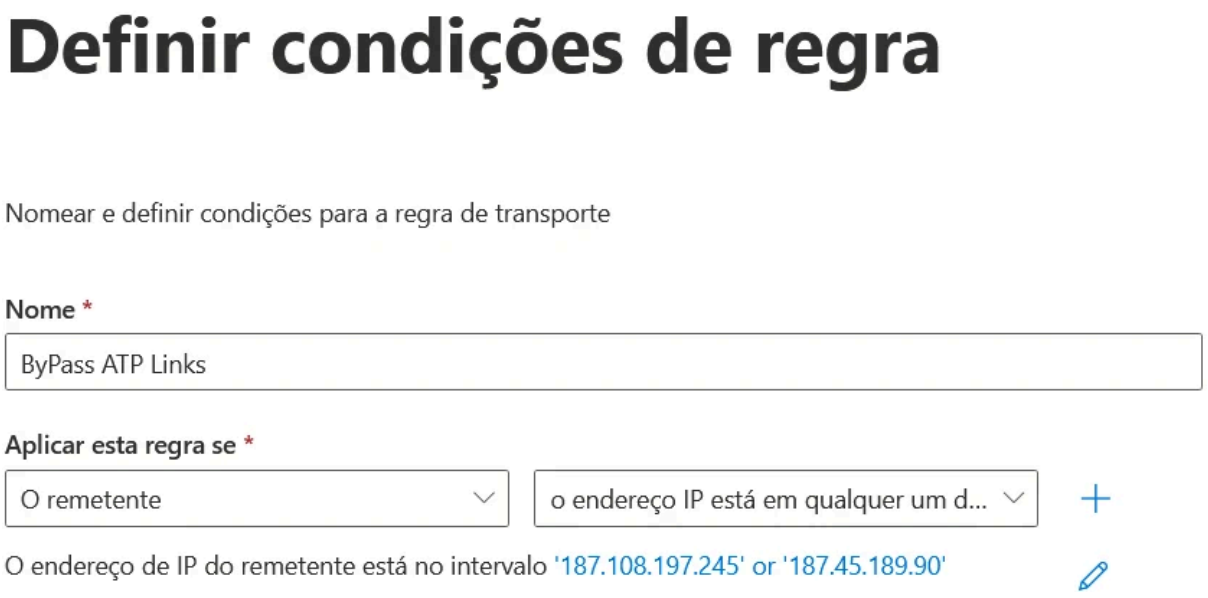
Segunda Etapa: Criando regra para não bloquear o email como spam e SafeLink Exception

Regra de Exceção a links (Safe Link ByPass)

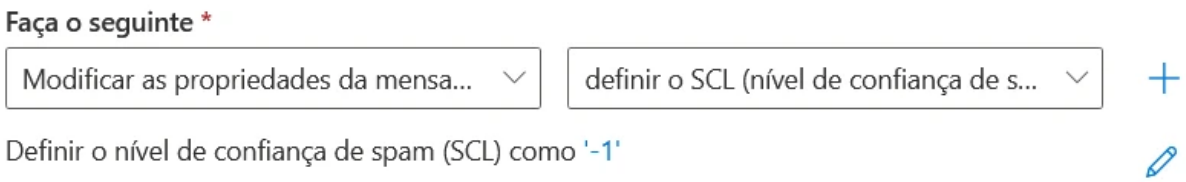
1. Crie uma Regra de Entrada de Email. Coloque o nome ByPass ATP Links
2. Selecione a opção:
   Aplicar esta regra se: O remetente
   O endereço de IP do remetente está no intervalo
   187.108.197.245 **ou** 187.45.189.90 **ou** 1131.100.228.128/25 **ou** 77.136.253.0/26
   Obs: Se você estiver usando qualquer sistema de Email Gateway, será necessário incluir os IPs dos agentes de filtragem do Email Gateway nessa relação.



A regra ficará assim:

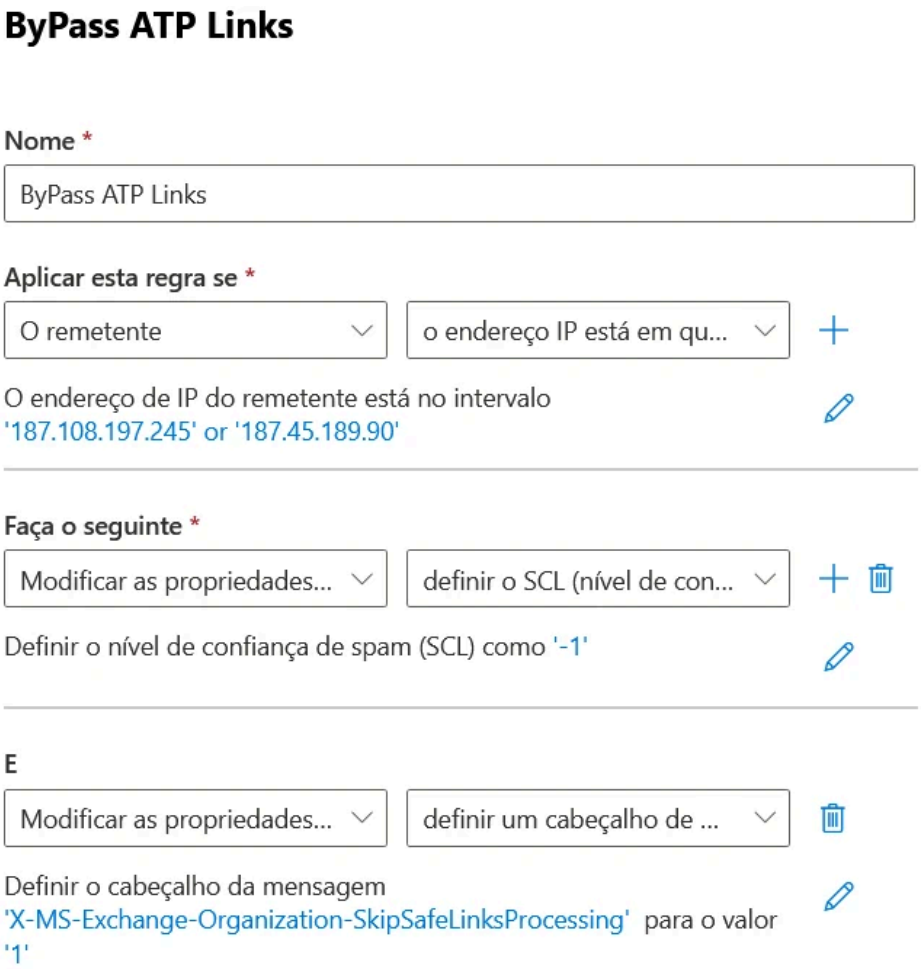


3. Em Faça o Seguinte:
   Selecione a opção: Modificar as propriedades da mensagem e
   Definir o SCL (nível de confiança de SPAM) em Bypass (-1)
   Vai ficar assim:



4. Clique no sinal de + para adicionar mais uma ação.
5. Adicione a ção de Modificar as propriedades da mensagem e definir um cabeçalho de mensagem
   No texto do cabeçalho coloque:
   X-MS-Exchange-Organization-SkipSafeLinksProcessing
   No valor coloque: **1**

   Deve ficar algo parecido com:



6. Em configurações, selecione a opção de Parar de Processar mais regras



Verifique que a regra seja somente executada nela, ou seja, não tenha continuidade de execução (tem que marcar uma opção que tem no Office365 indicando para não dar continuidade na execução da regra)

Clique em Avançar

7. Clique em Salvar

Terceira Etapa: Criando Regra para Microsoft Defender não pegar como Phishing

Essa etapa é necessária para caso você tenha pacote Microsoft Defender, mas em todo caso, recomendamos tentar configurar, pois em muitas empresas, mesm o que não tenha o pacote com o Microsoft Defender ativo, a Microsoft acaba liberando para o cliente e com isso, pode ocorrer o bloqueio indevido das simulações.
Por padrão os planos que possuem o Defender ativo são:

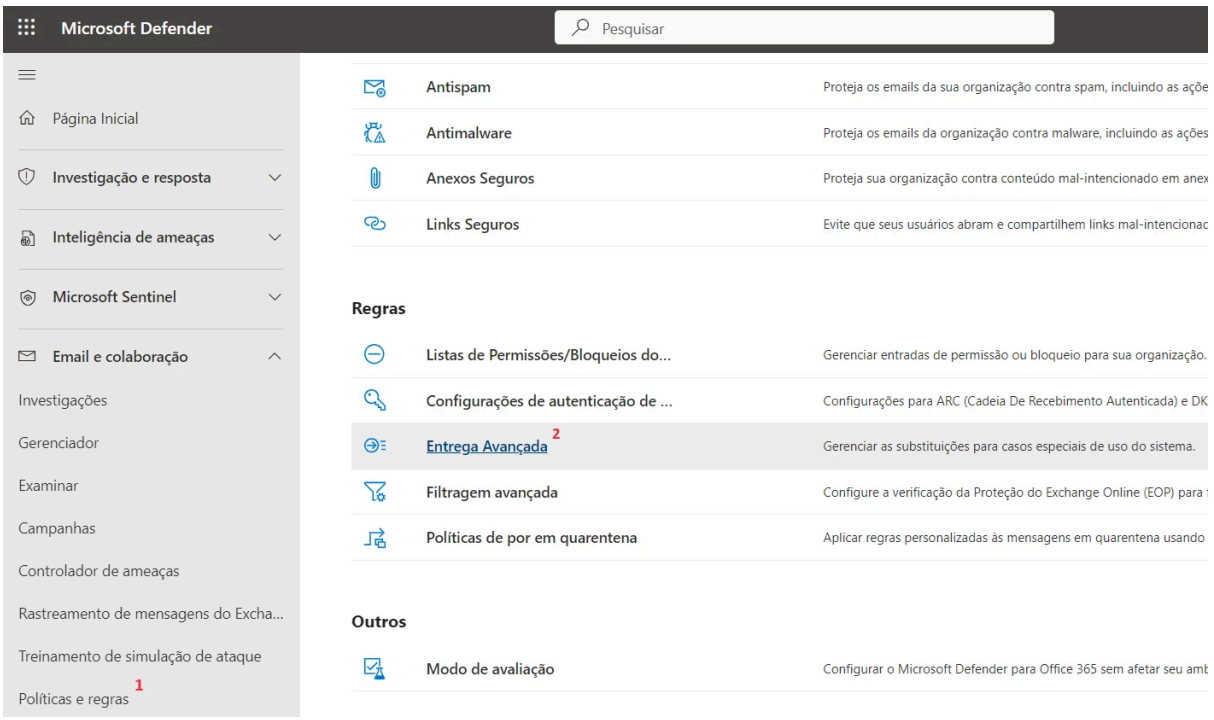
- Office 365 ATP Plan 1 (E1)
- Office 365 ATP Plan 2 (E2)
- Microsoft 365 Business Premium (antes chamado de Microsoft 365 Business)
- Office 365 E5
- Microsoft 365 E5

Procedimento para desativar o Defender
(específico para simulação de phishing vindos do MindAware)

1. Vá em: https://security.microsoft.com/advanceddelivery?viewid=PhishingSimulation

   Caso você queira ir pelo menu da esquerda em vez de usar o link, o caminho é:

   Email e Colaboração > Política e Regras > Política de Ameaças > Regras > Entrega Avançada > Aba de Simulação de Phishing



2. Clique no botão Edição
3. Inclua:
    - Os domínios que podem mandar simulação de phishing para a sua empresa:
    - app.mindaware.com.br

mindaware.com.br
drivedocs.com.br,
facebk.com.br,
gougle.com.br,
happ.net.br,
seraaza.com.br,
tiktoook.com.br,
whatsp.com.br

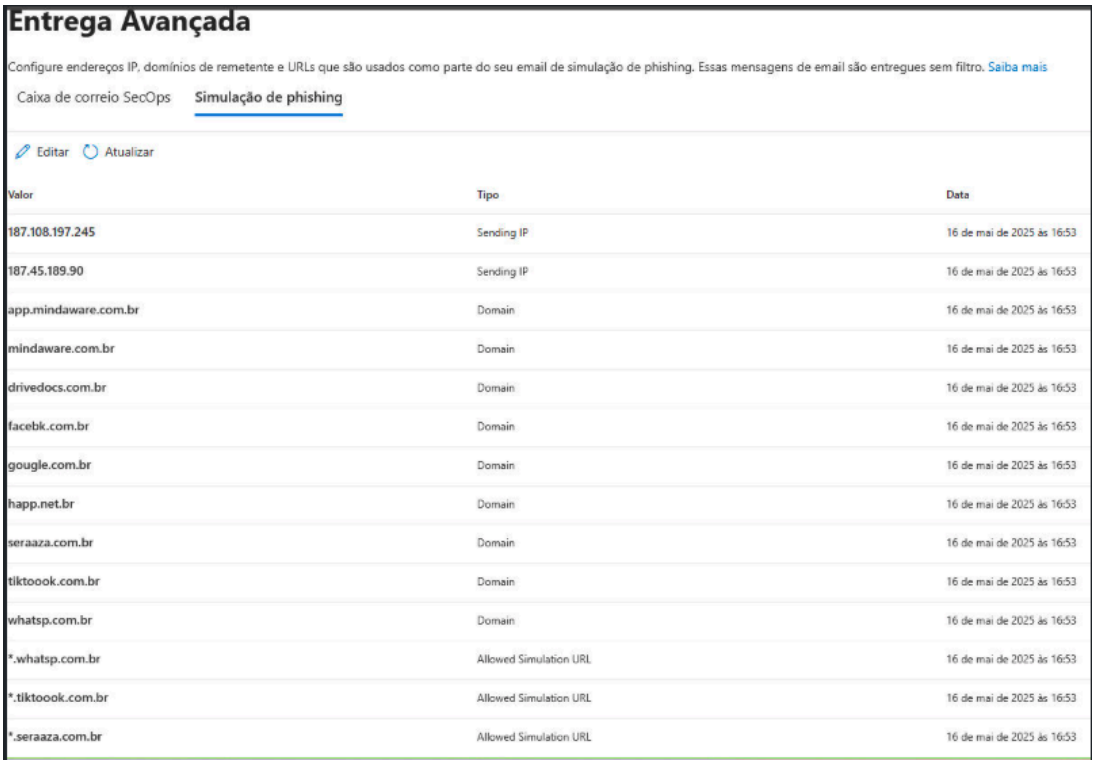
- Os IP que podem mandar simulação de phishing

187.108.197.245
187.45.189.90
131.100.228.128/25
177.136.253.0/26

Obs: Se você estiver usando qualquer sistema de Email Gateway, será necessário incluir os IPs dos agentes de filtragem do Email Gateway nessa relação.

- As URLs que são usados para simulação de phishing
  .mindaware.com.br/next/
  *.mindaware.com.br
  *.drivedocs.com.br
  *.facebk.com.br
  *.gougle.com.br
  *.happ.net.br
  *.seraaza.com.br
  *.tiktoook.com.br
  *.whatsp.com.br
  *govbrasil-seguro.com.br
  *bancoonline-combr.com.br
  *cartaoalerta-com.com.br
  *ofertahojeonline.net.br
  *rastreioentregas.com.br
  *trabalheagora.net.br
  *assinadigitaldoc.com.br
  *streamvionline.com.br
  *pet-amorstore.com.br
  *securemailpro.com.br

4. Clique em Salvar
   Deve ficar com a tela similar a:



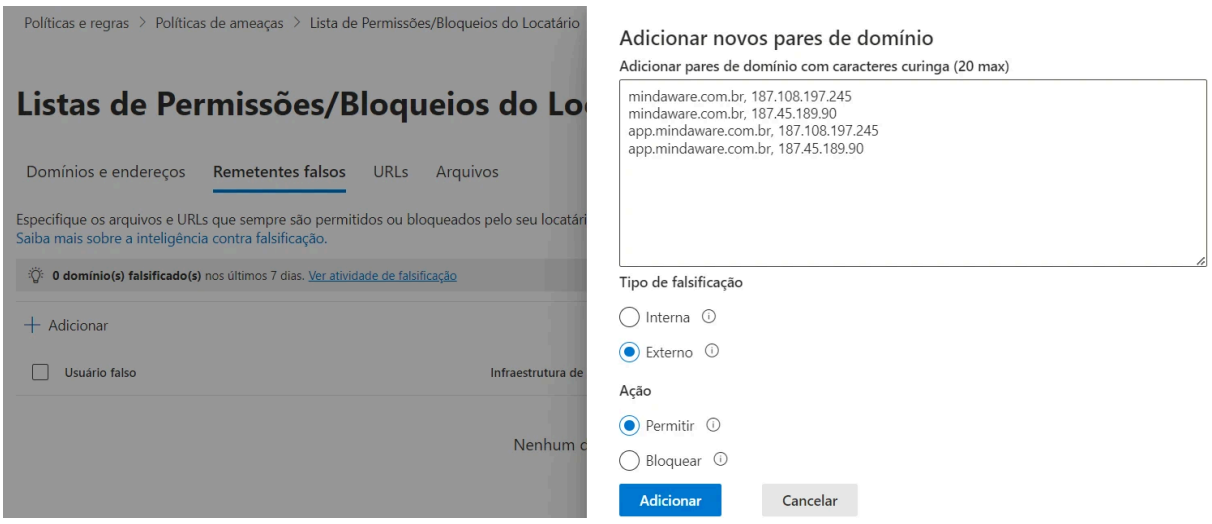
Opcionalmente

Caso ainda esteja sendo bloqueado como phishing, mesmo com as três etapas configuradas no Office 365.
Crie uma regra de Exceção para domínios forjados, uma vez que o MindAware irá forjar os remetentes da Campanha de Phishing.

1. Vá para o seguinte endereço: https://security.microsoft.com/tenantAllowBlockList
2. Vá na opção Remetentes falsos



3. Clique em Adicionar e preencha as informações conforme indicado na imagem a seguir:



Domínios, conforme imagem acima:
mindaware.com.br, 187.108.197.245
mindaware.com.br, 187.45.189.90
app.mindaware.com.br, 187.108.197.245
app.mindaware.com.br, 187.45.189.90

Obs: Se você estiver usando qualquer sistema de Email Gateway, será

necessário incluir os IPs dos agentes de filtragem do Email Gateway nessa relação (atribuindo tanto ao mindaware.com.br, como para o app.mindaware.com.br).

Ação: **Permitir**

4. Ficará similar a:



Liberação em Sistemas G-Suite

Caso esteja utilizando o Google Workspace, o método de liberação de aceite para os emaisl do Mindware fica em: https://knowledge.workspace.google.com/kb/how-to-bypass-the-spam-filter-for-incoming-emails-000006661?hl=pt-br

Durante a execução das campanhas de simulação de phishing, a solução registra os cliques realizados nas URLs contidas nos e-mails simulados, a fim de medir a suscetibilidade dos usuários a ataques de engenharia social. No entanto, é importante ressaltar que não é possível garantir com total precisão que todos os cliques registrados foram, de fato, realizados conscientemente pelos usuários finais.

Motivos Técnicos para Falsos Positivos:

- Varredura Automática por Sistemas de Segurança: Soluções de segurança de e-mail (como filtros antiphishing, sandboxes e scanners de URL) muitas vezes acessam automaticamente os links presentes nos e-mails para análise de segurança. Essas varreduras automatizadas podem gerar registros de clique mesmo sem ação do usuário.

- Reescrita e Monitoramento de Links por Gateways de Segurança: Ferramentas como Microsoft Defender for Office 365,entre outras, costumam reescrever os links para monitoramento e podem simular acessos durante a análise.

- Ferramentas Antivírus e Antimalware: Soluções instaladas nos endpoints podem acessar URLs de forma automatizada como parte de sua análise de comportamento ou reputação.

- Pré Visualização por Clientes de E-mail: Alguns clientes de e-mail realizam a pré-carga de links (por exemplo, ao gerar visualizações rápidas), o que também pode ser interpretado como um clique.

- Plugins e Extensões de Navegadores: Plugins de segurança e extensões de navegador podem verificar URLs automaticamente durante a navegação, resultando em registros de cliques sem envolvimento do usuário.

Recomendações:

Para garantir maior confiabilidade nos dados das simulações e minimizar a ocorrência de falsos positivos, recomenda-se:

1. Criar Exceções nas Ferramentas de Segurança:

Adicionar os domínios utilizados pela solução de simulação (ex: *.mindaware.com.br) à lista de exclusão (allowlist/whitelist) dos seguintes sistemas:

- Gateways de e-mail (ex: Microsoft Defender, HSC MailInspector, etc.)
- Ferramentas de sandboxing
- Firewalls de perímetro
- Antivírus e EDRs instalados nas estações
- Plugins/extensões de navegadores com funções de análise de segurança

Importante: As URLs de simulação não contêm conteúdo malicioso e são utilizadas exclusivamente para fins de conscientização e testes internos.

2. Evitar a Reescrita de Links em Campanhas:

Sempre que possível, configure a política do seu gateway para não reescrever ou inspecionar os links utilizados nas campanhas simuladas.

Se a reescrita for obrigatória, configure exceções por domínio ou caminho das URLs.

4. Testar antes da Campanha Real:

Realize campanhas-piloto com um grupo reduzido de usuários ou contas de teste para verificar se há registros indevidos de cliques.

Use logs e relatórios da solução para identificar padrões de acessos automatizados.

5. Adicionar Etapa de Simulação de Envio de Dados:

A plataforma permite configurar a campanha com um passo adicional após o clique, simulando o envio de dados sensíveis (como um login e senha fictícios) por meio de um formulário.

Esse comportamento só pode ser executado por um usuário real, o que torna o registro de interação muito mais confiável e reduz significativamente os falsos positivos, pois ferramentas automáticas não costumam preencher nem submeter formulários.

Conclusão:

Apesar das medidas de mitigação, é importante compreender que nenhuma solução é imune a 100% de falsos positivos, devido ao comportamento automatizado de muitas ferramentas de segurança atuais.

Para apoiar o processo de validação e análise, a plataforma HSC Mindaware oferece dados detalhados sobre os eventos de clique, como:

- Endereço IP
- Data e hora do acesso
- Geolocalização estimada
- Sistema operacional e navegador utilizados
- Informações do dispositivo

Esses dados permitem ao administrador de segurança avaliar com mais precisão a origem dos acessos e identificar com maior confiança se houve interação real por parte do usuário ou se trata-se de um acesso automatizado.

Além disso, o uso do formulário de simulação de envio de dados como etapa complementar nas campanhas reforça significativamente a confiabilidade dos resultados, ao exigir uma ação consciente por parte do usuário.

Material exclusivo da HSC, referente ao MindAware 360°.

Copyright © 2025 HSC.
Não copie sem permissão.



hsclabs.com

+55 51 3500 8255