RL higiene O VALOR DA LIMPEZA	**Tipo de documento:** **Política de Tecnologia da Informação**	**Assunto:** **Cargos e Salários**
Versão: 1	Última Revisão: 13/11/23	Publicada em: 20/11/23

1. ESCOPO E ABRANGÊNCIA

Esta política aplica-se a todos os usuários dos recursos de informática - equipamentos, sistemas aplicativos, softwares etc., já adquiridos ou que venham a ser adquiridos pela empresa, para o desempenho de suas funções, sejam estes funcionários, prestadores de serviço ou terceirizados.

2. OBJETIVO

Estabelecer o conjunto de controles e responsabilidades que resultem em maior segurança na disponibilização e utilização de recursos de informática da Rede RL (equipamentos, sistemas aplicativos, softwares, e-mail, redes de computadores e acessos à internet) a serem praticados pelos usuários e pela organização, garantindo a manutenção e continuidade do negócio.

3. DEFINIÇÕES E ABREVIATURAS

i. TI: abreviatura de Tecnologia de Informação;
ii. Hardware: todo equipamento que, direta ou indiretamente, esteja envolvido, ou seja, disponibilizado ou utilizado pelos usuários no desempenho de suas atividades.
iii. Software: toda parte lógica desenvolvida ou disponibilizada para controlar e operar o negócio da RL Sistemas de Higiene.
iv. Usuários: empregados, estagiários, prestadores de serviço e consultores que tenham autorização de acesso e utilização dos softwares e/ou equipamentos instalados na rede de dados da RL Sistemas de Higiene.
v. Criptografia: técnica pela qual a informação pode ser transformada da sua forma original para outra ilegível, de maneira que possa ser conhecida apenas por seu destinatário.
vi. Sistemas aplicativos: conjunto de programas, telas e funcionalidades desenvolvidos internamente ou externamente por outras empresas ou adquiridos em forma de pacotes, que venham a ser utilizados na operacionalização do negócio da RL Sistemas de Higiene.
vii. Senha: Cadeia de caracteres que autoriza o acesso a um conjunto de operações em um sistema de computadores ou equipamentos.

4. PRINCÍPIOS BÁSICOS

Os aspectos referentes aos controles internos tratados nesta Política poderão ser objeto de auditoria quanto à sua efetiva aplicação e eficácia.

A violação da Política de TI pode levar a suspensão temporária e até definitiva do acesso do usuário aos recursos de TI a ele disponibilizados e a sanções em conformidade com a legislação trabalhista e normas internas da RL Sistemas de Higiene.

Esta Política, assim como todas as outras citadas neste texto, se encontra disponível no acervo de Políticas da RL.

5. DIRETRIZES CORPORATIVAS

i. Todos os colaboradores contratados (sejam eles efetivos, estagiários ou jovens aprendizes), devem assinar o **Termo de Conduta do Usuário**, mostrando ciência e concordância com as diretrizes, normas e regras da **Política de Segurança da Informação**;
ii. Os prestadores de serviço (funcionários terceirizados) devem ter ciência e concordar com a

Política de TI;

iii. A Política de TI deve ser divulgada para todos os colaboradores e permanecer acessível a qualquer momento.
iv. Todo acesso físico as dependências e lógico a sistemas da empresa deve ser autorizado.
v. Toda e qualquer senha disponibilizada ao colaborador é de uso pessoal e intransferível.
vi. Periodicamente será solicitada a alteração de senhas.
vii. Os recursos tecnológicos assim como as informações confidenciais, devem ser protegidos da divulgação indevida a terceiros.
viii. Os recursos tecnológicos devem ser utilizados única e exclusivamente para fins profissionais no exercício da função na empresa RL Sistemas de Higiene.
ix. As informações contidas nos sistemas internos e arquivos nos recursos de TI são confidenciais.
x. A empresa RL Sistemas de Higiene está obrigada a proteger e a manter a confidencialidade dos dados de seus clientes em conformidade com as melhores práticas e a Lei Geral de Proteção de Dados (LGPD).
xi. Não devem ser conectados nas estações de trabalho da empresa RL Sistemas de Higiene dispositivos móveis, tais como: tablet, telefone celular, pen-drive, hd externo, cd/dvd-rom, etc.
xii. Os notebooks, telefones celulares e modems de acesso à internet são recursos tecnológicos disponibilizados pela empresa e devem ser tratadas como tal.
xiii. Todas as solicitações de suporte técnico devem ser realizadas no Sistema de Chamados (Alert).

5.1 AQUISIÇÃO E MANUTENÇÃO DE EQUIPAMENTOS E SISTEMAS

Todas as solicitações de manutenção, nos sistemas aplicativos existentes, desenvolvimento de novos sistemas e funcionalidades, aquisição ou manutenção dos recursos tecnológicos devem ser registrados via chamado para o Departamento de TI.

i. Os equipamentos a serem adquiridos devem ser homologados e estar de acordo com os parâmetros operacionais exigidos para instalação na rede da RL Sistemas de Higiene.

5.2 COMPUTADORES, TRABLETS E CELULARES

i. Não é permitido efetuar alterações nas configurações de softwares e sistema operacional dos computadores. Quaisquer alterações necessárias deverão ser solicitadas via chamado (Suporte de TI);
ii. Todo usuário é responsável pela correta utilização do computador e periféricos (impressora, mouse, teclado e monitor);
iii. Os usuários que utilizam tais equipamentos deverão informar as razões de eventuais danos causados a estes para que eles sejam reparados e/ou substituídos;

5.3 ANTIVÍRUS

Todas as estações de trabalho têm instalado um antivírus autorizado, licenciado e homologado, de acordo com a Política de Segurança da Informação vigente na empresa RL Sistemas de Higiene

i. Caso haja alguma mensagem ou alerta do software de antivírus, o usuário deve comunicar imediatamente a área de TI através do Sistema de Chamados (Mencionar o documento ou Processo);
ii. Os usuários não têm autorização para desabilitar ou realizar qualquer alteração nas configurações do antivírus.

5.4 REDE CORPORATIVA

i. A rede de computadores só poderá ser utilizada por usuários autorizados, através da inserção de seu login e senha, não é permitida a utilização de computadores, notebooks e dispositivos móveis que não façam parte dos recursos tecnológicos da RL Sistemas de Higiene, sem a devida autorização;
ii. Diariamente, ao encerrar suas atividades no computador, o usuário deverá efetuar a finalização do seu acesso. Caso a saída do sistema não seja efetuada, qualquer acesso realizado por

terceiros ou danos causados pelo desligamento incorreto do equipamento serão de responsabilidade do usuário;

iii. Caso o usuário deseje se ausentar temporariamente de sua posição de trabalho, o sistema de seu computador deverá ser bloqueado (Ctrl + Alt + Del ou pressionando a Tecla do Windows + L), evitando que terceiros façam uso dessa sessão em andamento.

iv. Indivíduos que utilizarem os computadores (ou outros recursos computacionais) sem permissão ou que tentarem burlar a Política de Tecnologia da Informação ou outra política interna estarão sujeitos às sanções administrativas ou judiciais cabíveis.

5.5 ACESSO À INTERNET

Por ser uma ferramenta de trabalho, o acesso à Internet tem como objetivo prover informações e recursos que auxiliem na realização de tarefas e atividades relacionadas às funções de cada usuário.

i. Todo e qualquer site/conteúdo acessado no ambiente de trabalho da empresa RL Sistemas de Higiene é de responsabilidade do usuário que mantém o poder do recurso tecnológico disponibilizado a ele, podendo o usuário ser chamado para prestar esclarecimentos caso haja alguma necessidade e/ou dúvidas sobre os acessos;

ii. O acesso a sites é controlado e não são permitidos acessos dos usuários a sites que não dizem respeito às atividades profissionais.

iii. A liberação de sites bloqueados será realizada mediante registro de chamado e após aprovação do gestor da área solicitante.

iv. Todos os sites visitados pelos usuários são registrados, inclusive tentativas de acesso a sites não autorizados e tentativas de burlar o sistema de segurança.

v. Os registros de acesso são armazenados e eventualmente poderão ser solicitados pelo RH, caso haja alguma inconformidade serão tomadas eventuais ações cabíveis, havendo necessidade.

vi. Para qualquer forma de tentativa de burlar o sistema de bloqueio de sites, a conduta do usuário estará passível de penalidades;

5.6 CORREIO ELETRÔNICO (E-MAIL)

i. Identificado como um dos recursos tecnológicos mantidos pela empresa e de uso dos funcionários, o correio eletrônico (e-mail) deve ser usado especificamente para o exercício da função na empresa.

ii. Todas as mensagens eletrônicas enviadas ou recebidas e/ou armazenadas nos computadores são de propriedade da empresa RL Sistemas de Higiene, porém são de responsabilidade do usuário que as manipula;

iii. Não é permitido aos colaboradores o uso do correio eletrônico da RL Sistemas de Higiene para:

- Enviar mensagem pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou outro endereço que não seja autorizado a utilizar;

- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou da RL Sistemas de Higiene vulneráveis a ações civis ou criminais;

- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- Apagar mensagens pertinentes de correio eletrônico quando a RL Sistemas de Higiene estiver sujeita a algum tipo de investigação.

- Produzir, transmitir ou divulgar mensagem que:

    1. Vise vigiar secretamente ou assediar outro usuário;
    2. Vise acessar informações confidenciais sem explícita autorização do proprietário;
    3. Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

4. Inclua imagens criptografadas ou de qualquer forma mascaradas;
5. Tenha conteúdo considerado impróprio, obsceno ou ilegal.

5.7 ARQUIVOS (DISPOSITIVOS E REDE)

i. Todos os arquivos críticos ou vitais para o negócio devem estar armazenados nos servidores de arquivos designados, dessa forma estão protegidos pelo backup;
ii. É terminantemente proibido o armazenamento destes arquivos (arquivos críticos como o CUBO e/ou vitais para o negócio), nos computadores locais;
iii. Promover o uso consciente de arquivos na rede, armazenando arquivos que sejam importantes para a empresa e para o desenvolvimento do trabalho;
iv. É terminantemente proibida e cabível de punição definida pela área de Recursos Humanos a utilização das pastas em rede para armazenamento de arquivos pessoais e não relativos ao negócio da empresa (músicas, vídeos, fotos particulares, etc.);
v. Atividades como o transporte de arquivos através de mídia removível colocam em risco informações internas e valiosas para a RL Sistemas de Higiene e dessa forma só poderão ser realizadas com a prévia autorização do gestor da área e abertura de chamado.

5.8 SOFTWARES

i. Nenhum tipo de jogo ou software recreativo pode ser armazenado ou utilizado nos computadores;
ii. Só podem ser instalados nos computadores softwares homologados pela área de Tecnologia da Informação / Comitê Gestor de TI;
iii. Nenhum tipo de software não legalizado ou não licenciado pode ser instalado nos servidores ou estações de trabalho;
iv. Todo software instalado e/ou executado sem uma prévia autorização, será de responsabilidade do usuário da estação de trabalho.

5.9 TELEFONA (FIXA E MÓVEL)

i. Assim como a Internet e o correio eletrônico, a telefonia (seja ela móvel ou fixa) deve ser utilizada apenas e exclusivamente para fins corporativos, pois é uma ferramenta de trabalho disponibilizada pela empresa;
ii. Senhas e/ou dados confidenciais nunca devem ser passados por telefone, seja essa informação do cliente ou da RL Sistemas de Higiene.
iii. Todos os ramais da empresa estão sujeitos a monitoração e gravação das chamadas para uso interno com efeitos de auditoria e melhoria.

6. RESTRIÇÕES À DIVULGAÇÃO DE INFORMAÇÕES

Todos os documentos e informações produzidos pela empresa e colaboradores devem receber critérios de criticidade para orientar a divulgação e uso dos mesmos:

i. **Confidenciais:** são informações e documentos registrados e transacionados no ERP. Este tipo de informação é proibido de ser transacionado por e-mail, pen-drive, CD/DVD, etc. bem como não devem ser divulgadas no portal do colaborador.

   Ex: relatórios de faturamento por cliente, nome, dados, preços e informações dos clientes.

   Considerando que algumas dessas informações sejam absolutamente necessárias para o bom andamento das atividades, o usuário deve adotar um comportamento seguro: utilizar exclusivamente o e-mail corporativo, nunca utilizar o e-mail pessoal, utilizar locais seguros para acesso dessas informações (unicamente em dispositivos exclusivamente da RL), nunca utilizar lan houses, computadores e outros aplicativos pessoais.

ii. **Restritos:** são informações e documentos internos que devem manter-se restritos a um determinado time de trabalho. Da mesma forma que as informações confidenciais, o usuário

deve adotar um comportamento seguro, caso exista a necessidade de trocar essas informações, devem: utilizar exclusivamente o e-mail corporativo, nunca utilizar o e-mail pessoal, utilizar locais seguros para acesso dessas informações (unicamente em dispositivos exclusivamente da RL), nunca utilizar lan houses, computadores e outros aplicativos pessoais.

iii. **Públicos:** são as informações que estão disponíveis no portal do colaborador, no site da RL, bem como fichas técnicas e manuais. Eles podem ser transacionados sem prejuízos.
    a. Fotos de eventos internos e externos, os participantes devem ser avisados desse registro, já que elas podem ser publicadas no portal do colaborador.
    b. Informações da empresa consideradas confidenciais devem ser protegidas da divulgação indevida a terceiros, sua divulgação apenas será permitida com prévia autorização dos Gestores responsáveis pela área;
    c. Nunca divulgar senhas de acesso, sejam elas para acesso interno e/ou externo, a fim de garantir a confidencialidade, integridade e disponibilidade dos arquivos da empresa RL Sistemas de Higiene.

7. PADRÕES DE TECNOLOGIA

7.1 INFRAESTRUTURA E DISPOSITIVOS

Unidades físicas (matriz e filiais) – as unidades da empresa seguirão com arquitetura de firewall (conectividade e segurança) e equipamentos de rede para conexão dos pontos e Access Point para distribuição de rede WiFi.

Estações de trabalho – equipamentos utilizados pelos usuários internos e externos serão do tipo notebook, preferencialmente das marcas DELL, HP e Lenovo.

Telefonia móvel - Inserir a definição de modelos ou tipo de telefones móveis disponibilizados.

7.2 PLANEJAMENTO E ACEITAÇÃO DE SISTEMAS

Os critérios de aceitação de novos sistemas, englobando atualizações ou novas versões, deverão ser definidos de acordo com um processo formal de certificação e reconhecimento, para garantir que os requisitos de usabilidade e segurança tenham sido devidamente implantados, incluindo:

i. Requisitos de desempenho e de demanda de capacidade computacional.
ii. Recuperação de erros, procedimentos de reinicialização e planos de contingência.
iii. Elaboração e teste de procedimentos operacionais de rotina para o estabelecimento de padrões.
iv. Concordância sobre o conjunto de controles de segurança utilizados.
v. Manuais operacionais eficazes.
vi. Requisitos de continuidade do negócio.
vii. Evidência de que a instalação do novo sistema não afetará de forma adversa os sistemas já existentes, particularmente nos períodos de pico de processamento, como, por exemplo, em final de mês.
viii. Evidência de que tenha sido considerado o impacto do novo sistema na segurança da organização como um todo.
ix. Treinamento na operação ou uso dos novos sistemas.
x. Facilidade de uso, a fim de evitar perda de desempenho pelo usuário ou falhas humanas.

8. INCIDENTES OU FALHAS DE SEGURANÇA

Caso algum usuário tome conhecimento de falhas de segurança ou permissões indevidas nos recursos e/ou sistemas, deve-se comunicar estas informações direta e imediatamente à área de Tecnologia da Informação (Suporte Técnico), através da abertura de um chamado (conforme procedimento).

9. SUPORTE TÉCNICO

O Suporte técnico ao usuário será realizado por fornecedor externo (Alert), onde o colaborador deverá abrir chamado para atendimento, conforme anexo II.

10. KEY USER

O Key User deverá ter o conhecimento pleno e domínio do processo. Não só de suas atividades, mas de todo o processo e ligado a estratégia da empresa.
Ele terá as seguintes responsabilidades:

a. Documentar os processos de negócio impactados pela mudança que se pretende fazer, indicando como são hoje e como devem ser no futuro.
b. Contribuir para a definição do escopo da mudança e identificar seus impactos.
c. Atuar junto aos gestores (os "donos do processo") facilitando o trabalho dos consultores e áreas usuárias;
d. Planejar e conduzir testes e validação de nova solução;
e. Atuar na resolução de questões pendentes junto as áreas de negócio;
f. Disseminar o conhecimento relativo às mudanças que estão por vir;
g. Elaborar e aplicar treinamentos para as equipes de colaboradores;
h. Dar suporte às ações finais para a implantação das mudanças;
i. Dar apoio após a implantação.

COMITÊ TI

Os objetivos do Comitê de TI são:

i. Orientar a Rede RL para a melhor aproveitamento dos recursos tecnológicos;
ii. Manutenção do parque tecnológico
iii. Promover análise crítica sobre o desempenho do P10 - Gestão de TI;
iv. Promover o alinhamento das unidades em relação as diretrizes da Rede RL;
v. Contemplar as diferentes necessidades das unidades;
vi. Disseminar as melhores práticas;
vii. Promover inovação em processos, tecnologias, ferramentas, abordagens;
viii. Promover integração com os demais Comitês;
ix. Promover alinhamentos com o comitê de TI da Allia.

O escopo que serão abordados nas reuniões que terão frequência bimestral é:

- P10 - Gestão de TI;
- Tecnologia e automação;
- Segurança da Informação;
- Inovação;
- Sustentabilidade
- Benchmarking;

Faz parte do comitê o Jarbas, que é o líder e terá o mandato de Janeiro de 2023 a Dezembro de 2025, Adriana, Ricardo e Rodrigo (Externo).

11. GOVERNANÇA NAS REDES SOCIAIS

Para adequar as páginas às pessoas de todas as idades que têm acesso às redes sociais, as mensagens e os comentários de usuários estarão sujeitos a moderação e filtragem. Conforme definido pelo Marketing estas são regras de uso e convivência para que a relação seja respeitosa e atinja seu objetivo principal:
São vedadas mensagens e/ou comentários/fotos/vídeos desrespeitosos, abusivos, ilegais, caluniosos, ameaçadores, jocosos, profanos, difamatórios, discriminatórios, ofensivos, obscenos, preconceituosos, racistas, homofóbicos, de caráter publicitário (spam) ou comercial, fraudulentos, danosos, fora de contexto, que contenham links suspeitos, que divulguem informações pessoais, sejam escritos em caixa alta (letras maiúsculas).
Não serão aceitas mensagens que usem a imagem de terceiros, entidades ou marcas comerciais sem autorização.

Caso sejam identificadas manifestações com qualquer um desses temas ou teor, a mensagem será removida e o usuário poderá ser bloqueado imediatamente, independentemente de justificativa, consulta ou alerta prévio.
A gestão dos conteúdos serão validados pela gestão do Marketing e publicados pela agência ou pelo Marketing interno da RL.

12. NORMAS E PROCEDIMENTOS

i. **Procedimento de abertura e acompanhamento de chamados**

ii. **Política da Privacidade e Proteção de Dados**

iii. **Procedimento gestão dados dos titulares**

iv. **Aviso de privacidade do Site**

v. **Governança Redes Sociais**

vi. **Key Users**

Anexo I

Procedimento de abertura e acompanhamento de chamados

Sumário

1. APRESENTAÇÃO 9
2. COMO ACESSAR O SISTEMA 10
3. COMO CRIAR UM CHAMADO 11
a. Portal CAC 11
b. E-mail (cac@alerti.com.br) 13
c. WhatsApp 14
d. Telefone 14
4. ACOMPANHAMENTO DE UM “CHAMADO” 14

1. APRESENTAÇÃO

O Manual de procedimentos de abertura e acompanhamento de chamadas no Portal CAC – Centro de Atendimento ao Cliente visa estabelecer os procedimentos para a utilização do sistema de gerenciamentos dos chamados de Suporte Técnico, bem como oferecer acesso às informações dos usuários e equipamentos envolvidos no ambiente atendido e no processo de abertura/solução de chamados.

O Portal CAC tem por objetivo ainda auxiliar os responsáveis/gestores no acompanhamento das demandas registradas e no cumprimento pleno das métricas e acordos de nível de Serviço estabelecidos.

Abaixo segue o fluxograma do ciclo de vida dos chamados registrados desde a sua abertura, passando pela execução do atendimento até a conclusão. O fluxograma apresentado tem finalidade pedagógica para auxiliar a compreensão de todo o processo pelos usuários do sistema.

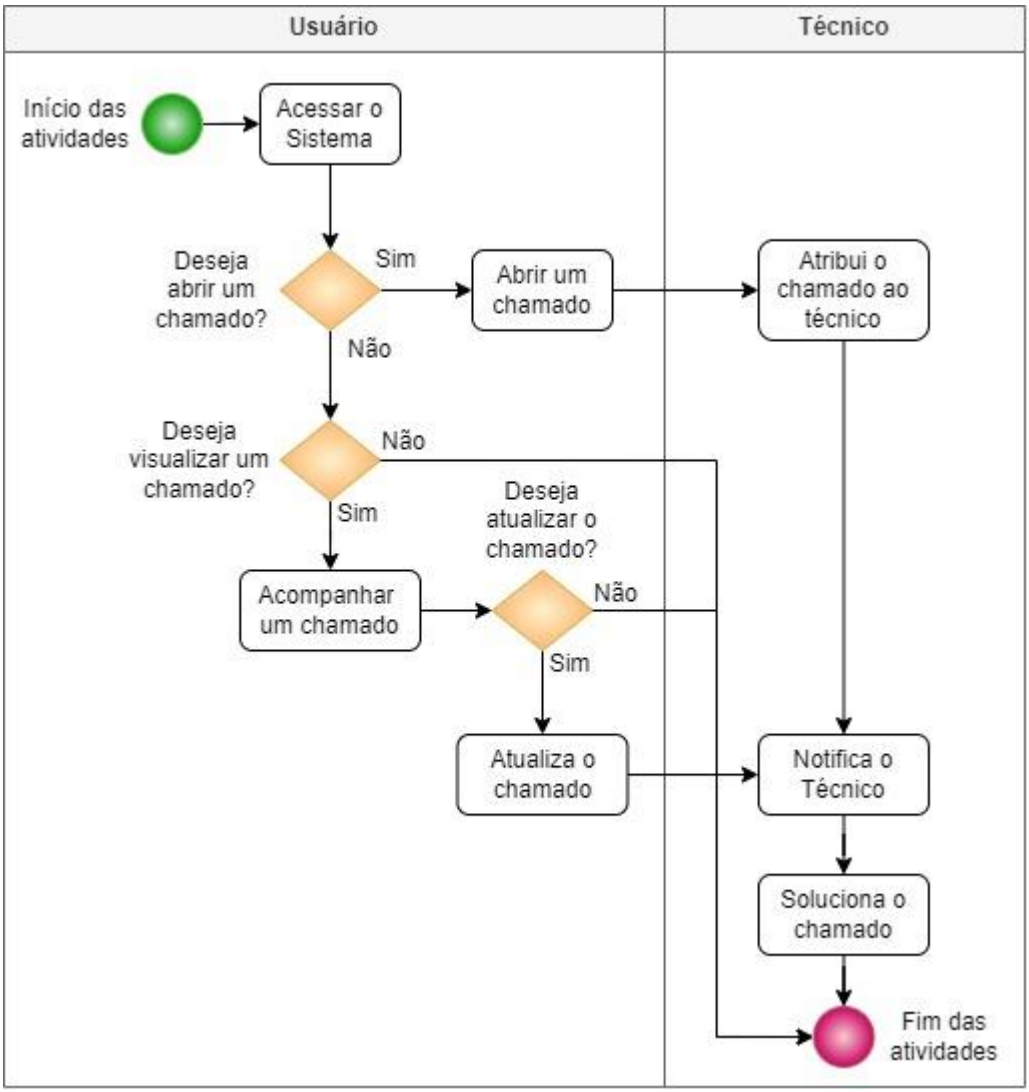


Figura 1 - Fluxograma do processo de abertura de chamados.

2. COMO ACESSAR O SISTEMA

Primeiramente, é necessário abrir um navegador Internet. A seguir, é necessário acessar o seguinte site web https://portal.alerti.com.br.

A tela de identificação se abrirá:

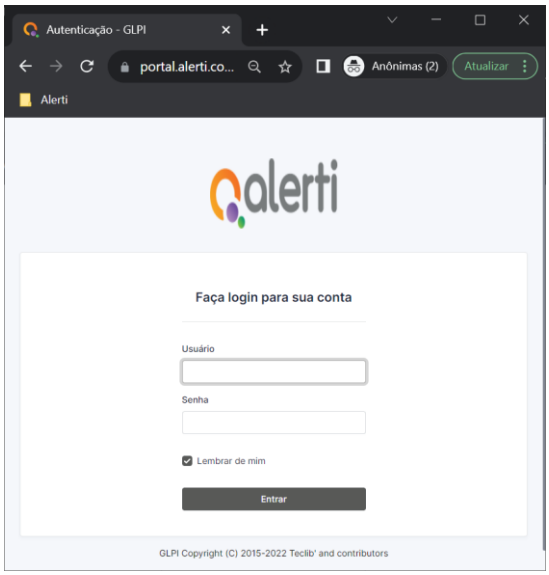


Figura 1 - Tela de identificação

Para acessar o Portal CAC basta inserir a credencial (usuário e senha). Cada usuário possui seu própria login e senha.

Para obter esta credencial, caso não tenha, é necessário entrar em contato através dos canais de atendimento E-mail, WhatsApp ou Telefone para validação das informações e envio através de mensagem.

As funcionalidades do portal são acessadas a partir da tela principal, composta pelo menu: Home, Criar um chamado, Chamados, FAQ (Perguntas mais frequentes).

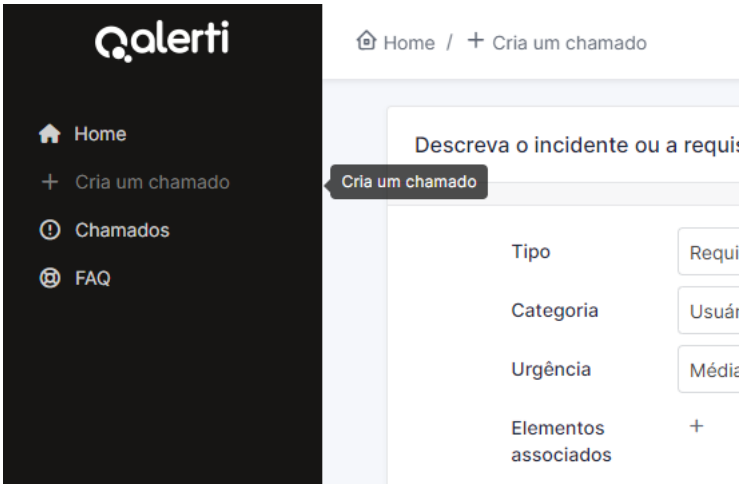


Figura 2 - Tela inicial do Portal

Na tela “Chamados” é possível visualizar um resumo dos chamados feitos pelo usuário e os respectivos status de atendimento:

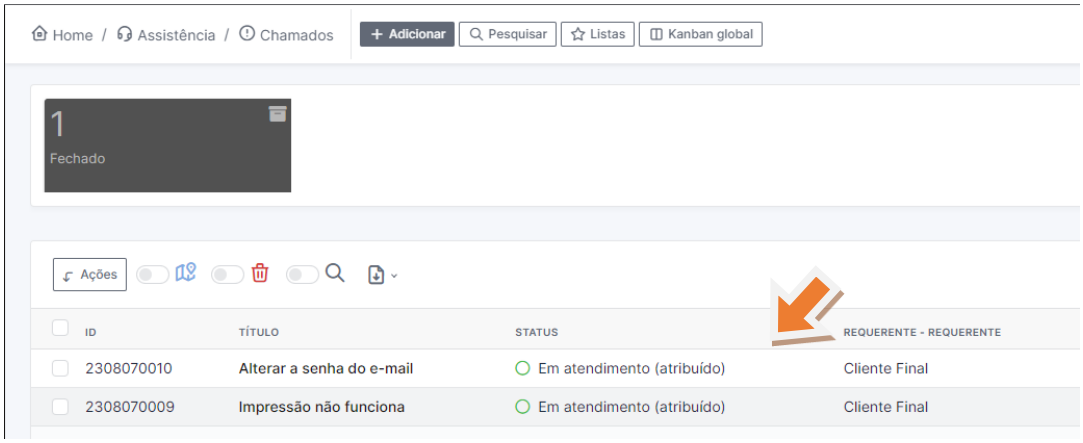


Figura 3 - Tela de chamados

- **Novo** - São aqueles abertos recentemente, que o atendimento inda não foi iniciado pelo time de Atendimento;
- **Processando (atribuído)** - São aqueles onde há um ou mais responsáveis pelo chamado e a tratativa já foi iniciada;
- **Processando (planejado)** - Casos em que há a programação das ações a serem tomadas e definidas as datas para realização do atendimento;
- **Pendente** – Chamados aguardando interação de terceiros ou retorno do usuário para prosseguir com atendimento;
- **Solucionado** – O time de Atendimento realizou a tratativa do chamado e sinaliza como atendido/solucionado.
- **Fechado** – Após o prazo de 3 (três) dias como Solucionado o chamado é automaticamente alterado para Fechado, não podendo mais ser reaberto. Em caso de reincidência será necessária a abertura de um novo chamado.

3. COMO CRIAR UM CHAMADO

Os chamados podem ser abertos através de quatro canais de atendimento diferentes:

- Portal CAC
- E-mail
- WhatsApp
- Telefone

a. Portal CAC

Este canal de contato requer cadastro prévio da credencial de acesso (usuário e senha)

No menu lateral, clique na opção “+ Criar um chamado” para abrir um novo chamado através do preenchimento do formulário.

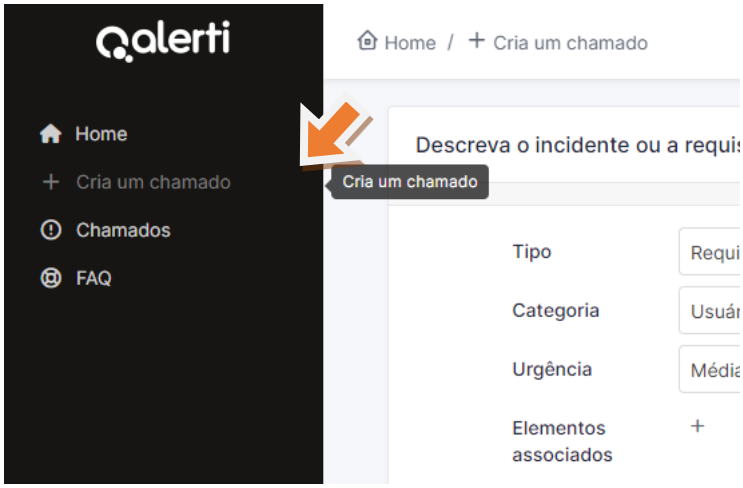


Figura 4 - Menu de abertura de chamados

É necessário observar que os campos “Título” e “Descrição” são de preenchimento obrigatório. Ao clicar no botão “+ Enviar mensagem” o chamado será registrado e direcionado para o time de Atendimento.

A seguir uma breve descrição de cada campo exibido no formulário:

Tipo – são exibidas duas opções. A primeira é “Requisição”, esses são serviços rotineiros que podem ser urgentes, mas não com prioridade menor que os tipos “Incidentes". O tipo “Incidente” são casos de urgência, com impacto na execução de rotinas ou atividades como por exemplo: queima de equipamento, indisponibilidade de acesso à Sistemas ou recursos, etc.

Categoria – Definição da categoria desse chamado. Já vem preenchida e será revisada pelo responsável do atendimento caso não seja alterado pelo usuário;

Urgência - as opções “Muita baixa”, “Baixa”, “Média”, “Alta”, “Muito Alta” são pré-selecionados e podem ser alteradas de acordo com o tipo do chamado, pois casos específicos e de maior urgência são classificados com valores diferentes;

Elementos associados – para usuários com diferentes equipamentos associados é possível especificar para qual deseja atendimento;

Observadores – campo para adicionar outros usuários para acompanharem o chamado. Quando atualizado, os observadores também recebem as notificações;

Localização - Lista as opções de lugares ou unidades da empresa, se aplicável;

Título - Informar o resumo da demanda, uma referência para o caso a ser registrado;

Descrição – Descrever as informações detalhadas relativas à demanda. Se um problema ou erro, especificar mensagens, códigos de erro ou imagens da tela.

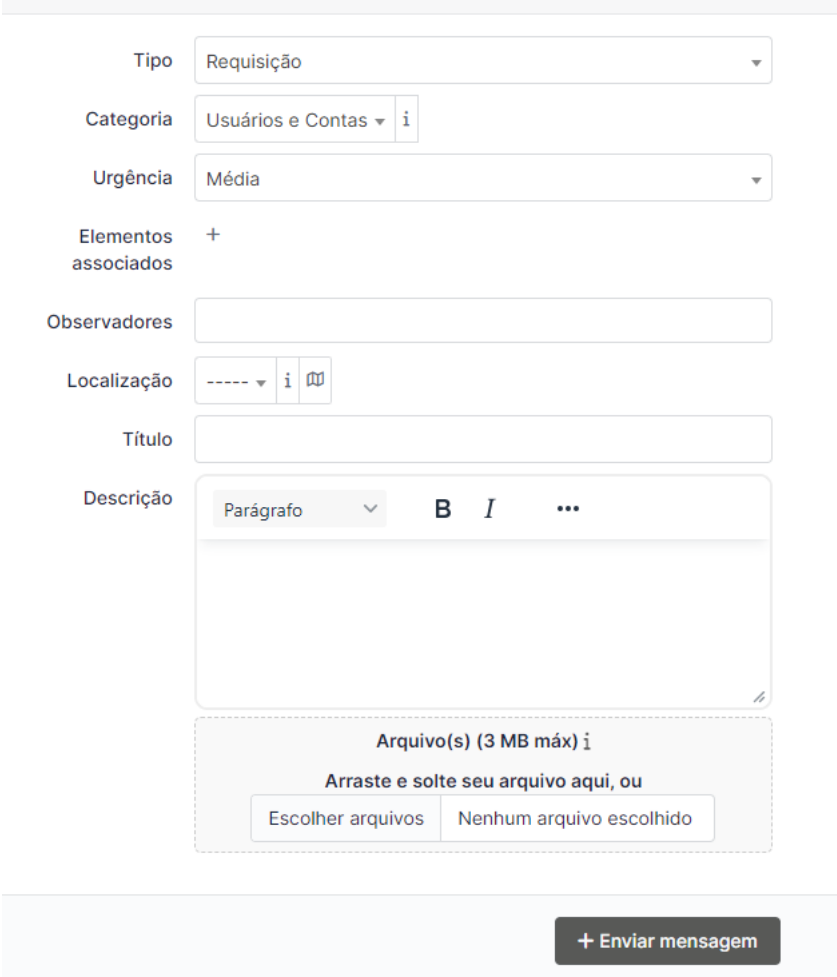


Figura 5 - Menu de abertura de chamados

b. E-mail (cac@alerti.com.br)

*Este canal de contato **NÃO** requer cadastro prévio*

Ao enviar mensagem de e-mail para o endereço:

cac@alerti.com.br

O chamado será automaticamente aberto com a associação dos campos abaixo:

Remetente – O endereço de e-mail de origem será consultado na base de dados e se existente, o caso será associado ao usuário como Requerente;

Assunto – O assunto do e-mail será salvo como o Título do chamado (breve descrição)

Mensagem (Corpo do E-mail) – Todo o conteúdo da mensagem será adicionado na Descrição do chamado, incluído anexos, texto, imagens, etc.

Importante – Endereços que estejam em cópia no e-mail enviado serão adicionados como Observadores no chamado e também receberão as interações do time de Atendimento.

c. WhatsApp

Este canal de contato requer cadastro prévio da credencial de acesso e número de celular

Ao enviar mensagem para o número de contato:

(11) 5199-6199

Será respondida com uma mensagem de saudação e solicitadas interações com opções de meu e respostas para a abertura do chamado.

Assim que concluído o registro do caso no sistema de chamados, o usuário receberá uma nova notificação de Abertura de Novo Chamado com o número do Protocolo.

Importante – Caso o processo de abertura do chamado não seja concluído com sucesso, o sistema informará imediatamente via mensagem e solicitará o contato através de outro canal de atendimento.

d. Telefone

Este canal de contato requer cadastro prévio da credencial de acesso

Ao entrar em contato via telefone com o número de contato:

(11) 5199-0811

O usuário deve digitar a opção 3 (três) para falar com o Suporte Técnico.

O técnico solicitará algumas informações cadastrais para localização do cadastro e acessos. Em seguida serão registradas as informações do motivo do contato para iniciar a tratativa.

4. ACOMPANHAMENTO DE UM “CHAMADO”

Os chamados abertos pelo usuário podem ser visualizados com uma descrição analítica de cada um. Eles podem ser acessados através do botão “Chamados” no menu lateral da tela.

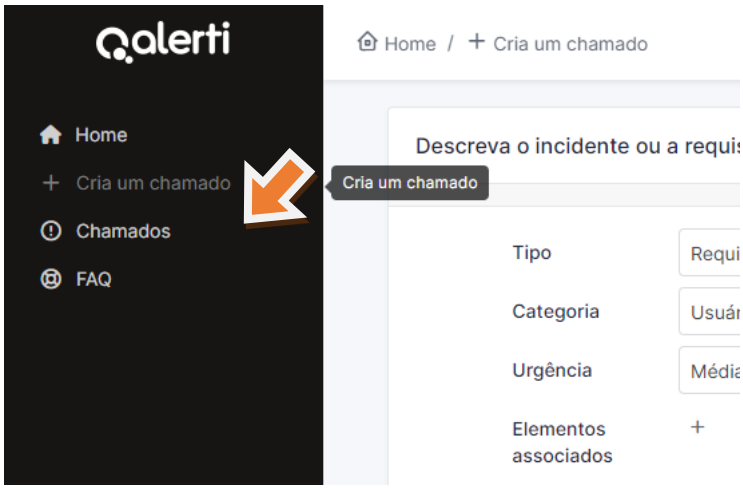


Figura 6 - Botão "Chamados"

A visualização de chamados pode ser feita com filtros, ao escolher as opções desejadas.

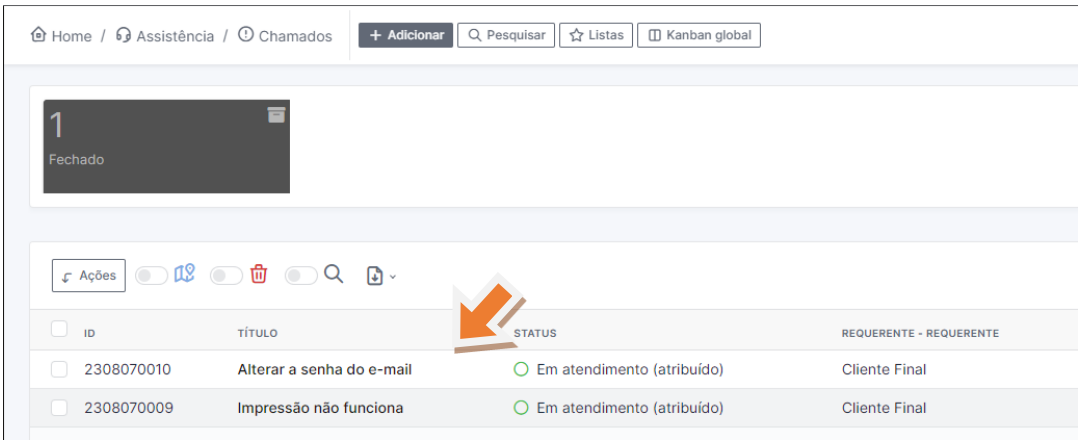


Figura 7 - Menu de acompanhamento de chamados.

É possível verificar detalhes de um chamado clicando diretamente no nome do mesmo.