ANEXO I

REQUISITOS TÉCNICOS

ÍNDICE

1. REQUISITOS FUNCIONAIS GERAIS DA SOLUÇÃO

A automação de processos e fluxos de trabalho da solução deve ser interativa, prática e de fácil implementação. O desenvolvimento de soluções ágeis e dentro da velocidade que o negócio da CONTRATANTE exige, deve ser suportado pela solução, para tanto, a solução deve suportar a criação de soluções, automações de fluxos de trabalho, processos de TI e de negócio e suportar a implementação de rotinas e processamento de funcionalidades com uma programação mínima e básica (Low-Code), usando componentes integrados e nativos da própria plataforma.

- A solução deverá ser ofertada na modalidade Software como Serviço - SaaS, em nuvem com Data Centers localizados exclusivamente em território nacional, sem qualquer replicação de dados no exterior.
- Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados em decorrência da prestação de serviços, bem como suas cópias de segurança, residam em território brasileiro, para tanto, a CONTRATADA deve garantir a territorialidade única na prestação do serviço, em vez de um ambiente tecnológico multinacional, não sendo admitida nenhum tipo de replicação para fora do país, tão pouco o fornecimento de informações.
- A solução ofertada deverá ser implementada em plataforma única, na mesma base de dados e com integração nativa entre todos os seus fluxos e módulos, contemplando a totalidade dos requisitos técnicos solicitados com tecnologia do mesmo fabricante. Essa demanda visa não somente a garantir a simplificação e redução de custos com integrações e desenvolvimento, mas reduzir gastos com customizações, evitar o uso de componentes externos, simplificar o acesso dos usuários aos serviços e garantir as atualizações de forma automática de toda a plataforma, reduzindo riscos operacionais e de segurança e problemas de compatibilidade.

- Deverão ser garantidos a disponibilidade, a integridade, a confidencialidade, o não-repúdio e a autenticidade dos conhecimentos, informações e dados hospedados em ambiente tecnológico sob custódia da CONTRATADA.
- A CONTRATADA deverá garantir a atualização tecnológica da solução durante o período de vigência do contrato. As atualizações deverão ser transparentes aos usuários, sem perda de dados e de forma que todas as parametrizações e personalizações sejam integralmente mantidas.
- Garantia de foro brasileiro;
    - Garantia de aplicabilidade da legislação brasileira;
    - Garantia de que o acesso aos dados, metadados, informações e conhecimentos utilizados e/ou armazenados na solução, ferramentas, softwares, infraestrutura ou em qualquer outro recurso que a CONTRATADA utilize para a prestação de serviços somente serão acessados pela CONTRATANTE e serão protegidos de acessos de outros clientes e de colaboradores da CONTRATADA;
    - Garantia que, em qualquer hipótese, a CONTRATANTE tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços;
    - Vedado o uso não corporativo dos conhecimentos, informações e dados pelo prestador de serviço, bem como a replicação não autorizada;
- A CONTRATADA deve executar os serviços em conformidade com a legislação brasileira aplicável, em especial as certificações sobre segurança da informação solicitadas para Qualificação Técnico-Operacional, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.
- A CONTRATADA deve disponibilizar canais de atendimento para o registro e abertura de chamados, com no mínimo um canal de atendimento via WEB e um canal telefônico, do tipo 0800 junto ao fabricante da solução.

2. DISPONIBILIDADE E ACORDO DE NÍVEL DE SERVIÇO

- A solução deve estar disponível em regime 24x7 (24 horas por dia, 7 dias por semana) com disponibilidade mínima de 99.8%.
    - "Disponível" significa que a instância de produção do SaaS pode ser acessada por usuários autorizados durante um mês do calendário, excluindo o tempo de inatividade justificado.
    - “Tempo de Inatividade Justificado” significa: (a) Tempo de Manutenção de até duas horas por mês; e (b) sempre que o Serviço de Assinatura não estiver Disponível devido a circunstâncias fora do controle do serviços SaaS, um Evento de Força Maior, interrupções gerais da Internet, falha de infraestrutura ou conectividade do cliente (incluindo conectividade direta e conectividade de rede privada (“VPN”) ao Serviço de Assinatura), falhas de computador e telecomunicações e atrasos e intrusões de rede ou negação de serviço ou outros ataques criminosos.
    - “Modificação de Infraestrutura” significa reparos, manutenção, melhorias ou alterações na infraestrutura de nuvem usada pela fornecedora da solução SaaS para operar e entregar o Serviço de Assinatura. A empresa notificará o CONTRATANTE com 10 dias de antecedência sobre uma Modificação de Infraestrutura se a empresa, em seu julgamento razoável, acreditar que a Modificação de Infraestrutura afetará o uso pelo Cliente de suas instâncias de produção do Serviço de Assinatura, a menos que, no

julgamento razoável, a Modificação de Infraestrutura é necessária para: (a) manter a disponibilidade, segurança ou desempenho do Serviço de Assinatura; (b) cumprir a Lei; ou (c) evitar a violação ou apropriação indevida de DPI de terceiros.

- "Tempo de Manutenção" significa o tempo em que o Serviço de Assinatura não está Disponível devido a uma Modificação, Upgrade ou Atualização de Infraestrutura.

- Quando houver a custódia de conhecimentos, informações e dados pelo prestador de serviços, a CONTRATADA deverá cumprir as seguintes diretivas:
    - A solução deve fazer uso de criptografia nas camadas e protocolos de redes de ativos computacionais para os dados em trânsito e/ou armazenados;
- A solução deve disponibilizar mecanismos para auditoria, como log de atividades dos usuários, ferramenta integrada a estes logs e painéis para os gestores. A solução deve permitir diversos tipos de consulta aos logs, gerando relatórios customizados. Deve ser possível, ainda, a triagem de eventos relacionados à segurança que garantam um gerenciamento de incidentes completo e ágil;
- Possuir procedimentos para triagem de eventos e incidentes de segurança da informação e garantir um tratamento de incidentes de segurança de forma completa e ágil;
- Eventos e incidentes de segurança de informação devem ser comunicados através de canais predefinidos de comunicação, disponibilizados pela CONTRATADA, de maneira rápida e eficiente e de acordo com os requisitos legais, regulatórios e contratuais;
- Logs de auditoria do provedor que registram atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema e eventos de segurança da informação devem ser mantidos em conformidade com as políticas e regulamentos aplicáveis e serem comunicados para a CONTRATANTE;
- O acesso e uso de ferramentas de auditoria que interajam com os sistemas de informação da CONTRATANTE deverão estar devidamente segmentados e restritos para evitar comprometimentos e uso indevido de dados de log;
- Disponibilizar meios de replicação de logs de auditoria para que a CONTRATANTE possa armazenar cópias de segurança destas informações para futuras consultas e auditorias;

3. SEGURANÇA

- Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas pela CONTRATANTE, incluindo as Políticas e Diretrizes de Governo, normativos associados ou específicos de Tecnologia da Informação, Política de Segurança da Informação e Comunicações – POSIC e Normas Complementares – NC do Gabinete de Segurança Institucional – GSI da Presidência da República – PR.
- Prover a criptografia de arquivos em repouso utilizando chave simétrica usando, no mínimo, algoritmo AES com 128 bits ou 3DES com 168 bits;
- Possuir nas instâncias da plataforma proteção antivírus para proteger contra upload ou download de conteúdo malicioso. Os anexos de arquivos devem ser verificados por servidores dedicados em cada data center regional para proteção.
- Manter uma política de backup dos dados, de pelo menos 20 (vinte) dias, dos metadados, dados, informações e conhecimento, produzidos ou custodiados pela CONTRATANTE e hospedados em ambiente de nuvem da CONTRATADA, a fim de garantir tempo de replicação pela CONTRATANTE.

- Estar em conformidade com a ISO/IEC 27001- padrão para sistema de gestão da segurança da informação (ISMS – Information Security Management System). Esta norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Uma solução em nuvem tem que adotar um SGSI e ser certificado nessa norma. A especificação e implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, exigências de segurança, os processos empregados e o tamanho e estrutura da organização.
- Estar em conformidade com a ISO/IEC 27017:2015 que fornece orientações quanto aos aspectos de segurança de informações de computação em nuvem, recomendando a implementação de controles de segurança de informações específicas da nuvem que complementam a orientação das normas ISO/IEC 27001. Esse código de práticas disponibiliza instruções de implementação de controles adicionais de segurança da informação específicos para provedores de serviços de nuvem.
- Estar em conformidade com a ISO/IEC 27018:2014 que é um código de práticas concentrado na proteção de dados pessoais na nuvem. Ela é baseada no padrão de segurança da informação e fornece orientação sobre a implementação dos controles aplicáveis às Informações de Identificação Pessoal (PII) de nuvens públicas. Esta Norma estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteger as Informações de Identificação Pessoal (PII) de acordo com os princípios de privacidade.
- Estar em conformidade com a SSAE 18 (SOC 1 – TYPE 2 E SOC 2 – TYPE2) - Statement on Standards for Attestation Engagements - A SSAE18 norma padrão de auditoria que obriga as empresas prestadoras de serviços possuírem mais controle e propriedade sobre a identificação e classificação de riscos, e gerenciamento adequado de suas subcontratadas. A grande vantagem dessa norma é o controle e a confiança nos negócios firmados. SOC 1 – TYPE 2 – Relatório que trata de controles internos relevantes para uma auditoria das demonstrações financeira de uma subcontratada, por um período e o SOC 2 – TYPE 2, relatório que detalha os controles de uma organização de serviços que são relevantes para suas operações e conformidade, conforme descrito pelos Critérios de serviços de confiança (Segurança, disponibilidade, Integridade no processamento, confidencialidade e privacidade) TSC da AICPA.

- Possuir e disponibilizar em ambiente de nuvem no mínimo um ambiente não-produtivo, por exemplo, ambientes de Desenvolvimento - DEV, Quality Assurance – QA e um ambiente Produção – PROD e, possuir funcionalidades de desenvolvimento em ambiente de DEV e publicação em outros ambientes, com controle de versionamento e publicação;
- Permitir a criação de campos compartilhados nos formulários da aplicação e que possam ser utilizados em quaisquer outras entidades, sem a necessidade de programação ou alteração do código-fonte;
- Consolidar vários recursos de automação em um único ambiente para que os proprietários e desenvolvedores de processos possam construir e visualizar processos de negócios a partir de uma única interface;
- Incluir fluxos e ações acionadas por eventos, como por exemplo itens do catálogo de serviço;
- Consolidar as informações de configuração e tempo de execução em uma única interface para que os proprietários e desenvolvedores de processos possam criar, operar e solucionar problemas de fluxos a partir desta interface;

- Permitir que sejam criados processos automatizados em um único ambiente utilizando linguagem natural para automatizar ações, tarefas, notificações e operações de registro sem codificação;
- Fornecer descrições em linguagem natural da lógica de fluxo para ajudar usuários não técnicos a entender gatilhos, ações, entradas e saídas;
- Promover a automação de processos, permitindo que especialistas no assunto desenvolvam e compartilhem ações reutilizáveis com designers de fluxo;
- Fornecer uma biblioteca de ações reutilizáveis, reduzindo os custos de desenvolvimento de novos fluxos para o CONTRATANTE.

4. PORTAL WEB

- Disponibilizar um portal web de serviços onde os usuários finais possam encontrar soluções para seus problemas e registrar solicitações de serviço através de um catálogo de serviços, conforme permissões pré-estabelecidas, este portal deve ser parametrizável em recursos gráficos de forma que permita acesso a todas as funcionalidades e recursos de gerenciamento e utilização disponíveis para o usuário final;
- Fornecer capacidade de autoatendimento ao cliente, no qual um cliente pode acessar artigos da base de conhecimento e perguntas frequentes, enviar e atualizar solicitações e monitorar o status de suas solicitações;
- Fornecer funcionalidade para pesquisa de soluções na base de conhecimento por meio de palavras-chave, operadores booleanos e pesquisa de texto completo;
- Associar usuários finais a grupos específicos, linhas de negócios etc., e adaptar o conteúdo apresentado, informações e opções de autoatendimento de acordo com assinaturas baseadas em regras para funções ou grupos;
- O portal de serviços deve ser personalizável para atender as necessidades da CONTRATANTE permitindo que áreas de inserção de conteúdos sejam criadas e organizadas de acordo com a necessidade da CONTRATANTE;
- A partir da página inicial do portal de serviços deve ser possível a pesquisa de itens de catálogo de serviço, artigos de conhecimento e artigos de autosserviço;
- Deve disponibilizar recursos que possibilitem a criação de múltiplas visibilidades do portal de autoatendimento, para segmentar diferentes perfis de usuário ou diferentes serviços, de diferentes departamentos;
- O portal de serviços deve permitir aos usuários dos serviços a visualização completa da situação atual dos serviços, indicando se existem degradações, indisponibilidades, problemas e manutenções programadas nos serviços;
- A solução deve prover, automaticamente, que os itens cadastrados no catálogo de serviço web estejam também disponíveis no mesmo Catálogo de Serviços acessado por meio de aplicativo móvel;
- Deve fornecer ao atendente informações sobre os registros pendentes (ex. requisição de serviço, resolução de incidente, problema, liberação e mudança, etc) facilitando as ações de atendimento.

- Permitir o detalhamento de diversas informações, tais como: serviço solicitado, solicitante, data de criação e de modificação, prioridades, descrição, status e notas nas solicitações.
- Permitir que os atendentes e analistas da contratante ou de empresas terceirizadas registrem as ações tomadas durante o atendimento dos Incidentes, Problemas, Requisições de Serviço, Requisições de Mudança e Tarefas, mantendo um histórico completo das ações tomadas, a data e o profissional que realizou a ação.
- Permitir que os atendentes e analistas da contratante ou de empresas terceirizadas possam registrar o tempo gasto e os custos associados com cada ação tomada durante o atendimento dos Incidentes, Problemas, Requisições de Serviço, Requisições de Mudança.
- Permitir a atribuição automática de requisições para profissionais ou equipes de atendimento em específico, com o uso de regras e parâmetros definidos pelo administrador. Estas regras e parâmetros poderão se utilizar, no mínimo, das seguintes informações: especialidade da equipe de serviço; item de configuração afetado; criticidade ou impacto do incidente; e carga de trabalho, agenda e habilidades de cada profissional.
- Deve possuir recursos para a condução de enquetes ou pesquisas de satisfação.
- Permitir que clientes e usuários finais respondam a pesquisas de satisfação - associadas ou não a uma solicitação específica - que auxiliem a área de tecnologia da contratante a conhecer a percepção de seus clientes e permitam melhorar continuamente seus serviços.
- Permitir pesquisas elaboradas conforme a metodologia NPS (Net Promoter Score), questionários elaborados conforme escalas de Likert, entre outros métodos de avaliação de satisfação consagradas no mercado.
- Permitir a realização das perguntas das enquetes ou pesquisas no formato sim/não ou verdadeiro/falso por meio de “check box", de forma que os pesquisados respondam, no formato lista de alternativas por meio de “option button", todas as respostas que se aplicam, garantindo assim uma única resposta válida.
- Deve armazenar em banco de dados as respostas dos usuários às enquetes ou pesquisas a fim de que seja possível a confecção de relatórios estatísticos.
- Permitir que as enquetes ou pesquisas também sejam enviadas de forma periódica, bem como, também permitir que sejam enviadas toda vez que ocorra uma atividade associada.
- Deve possuir recurso que garanta uma única resposta por usuário de determinada pesquisa ou enquete, prevenindo que usuários enviem repetidamente a mesma resposta.
- Deve possibilitar o envio de enquetes ou pesquisas para um determinado grupo de usuários, para que respondam quando puderem, dentro de um determinado período de tempo.
- Deve oferecer funcionalidade que facilite a disseminação de informação para a comunidade de usuários através do uso de recursos, tais como: envio automático de mensagens de correio eletrônico e quadro de avisos.
- Permitir a busca nos registros de chamados (requisições de serviço, incidentes, problemas e requisições de mudança) com critérios de data, tipo de atividade, descrição e nome da pessoa que abriu o chamado.
- Deve possuir um mecanismo automático para as escaladas funcionais e hierárquicas, ou seja, deve ser capaz de direcionar um atendimento para outra equipe e enviar alertas para os

gerentes da organização em seus diversos níveis hierárquicos, com base na categoria, na prioridade e no tempo transcorrido do atendimento.

- Permitir o envio de alertas por e-mail, SMS, Microsoft Teams e WhatsApp.
- Permitir ao administrador configurar as regras de notificação e escalação.
- Permitir rastreabilidade completa do fluxo do chamado que está sendo tratado por diversas equipes de serviço.
- Deve ter incorporada ferramentas de comunicação e colaboração dos atendedores com os usuários e clientes, tais como, bate-papo (chat), as quais deverão estar disponíveis em todas as plataformas de execução da aplicação.
- O sistema deve permitir um recurso de rastreamento de solicitação visual (por exemplo, breadcrumbs, linha do tempo, Chevron process flow, etc.).
- Deve ser possível aos atendentes transferir solicitações para outras equipes / times de serviço.
- O aplicativo móvel deve ser disponível, de forma gratuita, para as plataformas iOS e Android.

5. PAINÉIS, GRÁFICOS, RELATÓRIOS E DASHBOARDS

- Deve oferecer formulários, painéis e relatórios inerentes aos processos de gerenciamento de serviços disponíveis na solução que sejam usuais de mercado (conforme biblioteca ITIL v4 e outras referências) e Out-of-the-Box (OOTB), ou seja, prontos para uso imediatamente a instalação sem qualquer configuração, customização ou modificação especial.
- Permitir a criação de painéis e *dashboards* com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código fonte;
- Permitir a criação de painéis e *dashboards* com gráficos do tipo pizza, linha, colunas, barras, mapa de calor e tabelas dinâmicas, sem a necessidade de programação e alteração do código-fonte;
- Permitir alterações de atributos de forma dinâmica em gráficos de gestão, contidos em painéis e *dashboards* da solução, possibilitando a alteração de eixos, título do gráfico, legenda, escala, rótulos de dados, tamanho do gráfico, de forma gráfica na solução e sem a necessidade de alterações do código fonte;
- Permitir aos atendentes e solucionadores de chamados criarem seus próprios painéis e gráficos dentro da solução e compartilharem com grupos de usuários ou usuários específicos da solução, permitindo gerenciar as permissões de compartilhamento de acordo com os perfis de usuários da solução;
- Suportar a definição de indicadores de desempenho (KPIs);
- Prover visão da central de serviços em tempo real;
- Permitir exportar ou agendar a exportação dos *dashboards* em formato PDF;
- Permitir o detalhamento de informações contidas em gráficos de *dashboards* em gráficos detalhados;
- Permitir ao usuário organizar os gráficos e informações, em seus painéis e *dashboards* de gestão, ajustando o layout e conteúdo do painel de acordo com suas necessidades;

- Permitir aos usuários a configuração de painéis e *dashboards* agrupados por assunto e independentes entre si;
- Permitir o gerenciamento de permissões por usuários e grupos para acesso aos painéis e *dashboards* da solução;
- Permitir ao usuário organizar seus painéis e *dashboard*s com listas de registros de seu interesse, possibilitando a escolha de colunas, realização de filtros e ordenação da lista;
- Permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.
- Permitir a cópia e a personalização dos objetos mencionados no item anterior de forma não programática (“codeless” ou “lowcode”).
- Deve prover um mecanismo de desenvolvimento de formulários, painéis e relatórios básicos ou avançados, de forma gráfica, por meio de recursos de arrastar e soltar (drag and drop), para a inclusão dos campos escolhidos e separadores.
- Permitir o desenvolvimento de painéis de controle (dashboards) capazes de apresentar relatórios e gráficos operacionais e gerenciais em tempo real, e de acordo com o papel do usuário.
- Devem os painéis de controle ter capacidade de navegação (drill down) até o nível do registro de atendimento.
- Deve prover recursos para explorar tendências, padrões, anomalias e correlações em dados, permitindo, ao usuário, realizar análises complexas (slice and disse), reorganizar dinamicamente (pivot), filtrar, fazer análises detalhadas (drill-down) e representar graficamente os dados, em tempo real.
- Devem prover recursos que permitam o cálculo e exibição do tempo de resolução de diferentes alvos SLA - tempo de resposta e tempo de solução - e exibição de informações resumidas sobre a quebra do SLA em incidentes, problemas, mudanças e serviços.
- Permitir a geração de relatórios com base em qualquer combinação dos atributos (campos) contidos no âmbito da infraestrutura de dados.
- Permitir a produção de relatórios customizados avançados, integradamente a outros processos ITSM.
- Permitir a geração de relatórios, no mínimo, nos seguintes formatos: Adobe Reader® (PDF), Comma-separated values (CSV), Microsoft Office e HTML.
- Permitir a integração com, no mínimo, as seguintes fontes de dados: XML, CSV, Web Services SOAP, Web Services Rest e Bancos de Dados relacionais através de ODBC e JDBC.
- Deve ser possível criar relatórios gerenciais específicos para uma ou mais unidades de negócios ou grupos de usuários.
- Permitir a distribuição automatizada de relatórios diretamente por e-mail para destinatários únicos ou listas de distribuição.
- Deve prover a emissão de relatórios comparativos entre os níveis de serviço acordados e os níveis de serviço efetivamente realizados.
- Deve prover a emissão de gráficos gerenciais consolidados por período, contendo os KPIs.

- Deve prover recursos para o Gerenciamento dos SLAs, contemplando um Dashboard para aferição dos objetivos de níveis de serviço.
- Permitir a geração, no mínimo, de relatórios tais como os listados a seguir: Relatório de serviços registrados no Catálogo de Serviços, com indicadores de número de serviços em transição, em produção e total.

6. CATÁLOGO DE SERVIÇOS

- O catálogo de serviços deve ser acessível via web, mostrar os serviços conforme a permissão de acesso dos usuários;
- Permitir a personalização da apresentação do catálogo nos canais de Autoatendimento.
- Permitir a criação de múltiplos catálogos de serviços.
- Deve possuir uma interface gráfica para o desenho da estrutura do Catálogo de Serviços em níveis e subníveis, sem a necessidade de usar qualquer tipo de linguagem de programação ("codeless" ou “lowcode”), de forma que não seja necessária a intervenção de um programador para manter o Catálogo de Serviços atualizado.
- Permitir a organização do Catálogo de Serviços em uma visão de clientes, usuários ou tipos ou categorias de usuários dos serviços de TI. Os itens do catálogo de serviços deverão ser distintos das categorias de serviços de TI, contudo, deverá ser garantido o relacionamento entre eles.
- Permitir o cadastro e manutenção de Serviços de Negócio e Serviços de TI.
- Permitir relacionar cada Serviço de TI aos itens de configuração que o compõem, às suas janelas de manutenção e seus períodos de congelamento.
- Permitir a definição de quais Grupos de Usuários podem acessar cada serviço e item do catálogo, de forma que seja possível manter um único Catálogo de Serviços, sem duplicação de informações.
- Permitir a definição de quais Grupos de Usuários podem acessar cada serviço e item do catálogo, de forma que seja possível manter um único Catálogo de Serviços, sem duplicação de informações.
- Permitir o registro da descrição detalhada do item e da categoria de serviço, bem como, associar esses registros à artigos da base de conhecimento.
- Deve exibir os itens de configuração componentes técnicos utilizados para entregar cada serviço em específico.
- Permitir a vinculação de cada oferta de serviço com a respectiva instância de processo, seja o processo de incidentes, requisições de serviços ou qualquer outro.
- Permitir a visualização do catálogo nos canais de autoatendimento e console de servicedesk para os usuários de acordo com as políticas de acesso pré-estabelecidas.
- Permitir o cadastro de documentação detalhada aos usuários associada a cada oferta de serviço.
- Deve oferecer suporte ao gerenciamento do ciclo de vida do catálogo de serviços, incluindo as seguintes funcionalidades:
    - Criar, modificar e excluir categorias / modelos de serviços.
    - Criar, modificar e excluir serviços.

    - Criar, modificar e excluir componentes de serviço.
    - Rastrear o status de implementação dos serviços.
    - Definir métricas, KPIs e SLAs / OLAs para modelos de serviço, serviços e componentes de serviço.
- Permitir a definição do catálogo de serviços e o cadastro e manutenção de descrição de serviços, assim como de seus atributos;
- Permitir a customização da estrutura do catálogo de serviços, devendo esta parametrização ser realizada através da própria interface da ferramenta pelos administradores da ferramenta;
- Permitir que, para cada serviço e/ou item de configuração, seja possível informar o seu grau de prioridade (importância) para o negócio de forma a estabelecer a priorização no atendimento;
- Permitir a criação e configuração de catálogos de serviços negociais e catálogos de serviços técnicos;
- Permitir a criação de ilimitadas categorias de navegação nos catálogos de serviços, permi ndo a organização do catálogo em quantos níveis forem necessários;
- O Catálogo de Serviços deve permitir o agrupamento de serviços conforme a necessidade da Contratante, a qual definirá seus próprios grupos e ofertas;
- Permitir a criação de múltiplos catálogos de serviços ou perfis de visibilidade para oferta de serviços dos departamentos do CONTRATANTE como uma central de serviços compartilhados;
- Todos os catálogos, níveis e agrupamentos criados para a interface web deve estar, da mesma maneira, disponíveis e agrupados no aplicativo móvel disponibilizado;
- A solução deve implementar e seguir corretamente o fluxo de Gerenciamento de Catálogo de Serviços;
- Para a automação dos serviços, o Gerenciamento do Catálogo de Serviços deve permitir associar à oferta de serviço os formulários personalizados para entrada de dados pelo usuário final e fluxos de trabalho automatizados e estruturados para o cumprimento das requisições;
- Deve ser possível criar serviços técnicos e serviços de negócio de forma gráfica e sem a necessidade de programação ou alterações do código-fonte;
- Deve ser possível associar *Service Level Agreement* – SLA aos serviços;
- Deve ser permitido copiar as ofertas de serviço para rapidamente publicar novas ofertas semelhantes, herdando as informações de configuração, parâmetros, SLA, custos, demanda e visibilidade; e
- Deve ser possível carregar valores automáticos com base em respostas anteriores do formulário de serviços e com isso o item de catálogo pode seguir fluxos de trabalho específicos.

7. GERENCIAMENTO DE NÍVEL DE SERVIÇO

- Permitir a definição de parâmetros que são utilizados para definir o Service Level Agreement - SLA, tais como: por cliente, por serviço, dentro de um calendário a que se aplica o SLA, meta de nível de serviço relacionados ao SLA, escalações automatizadas relacionadas ao SLA;
- Permitir a definição de critérios que possibilitem a associação de SLA a registros de atendimentos, incidentes, problemas, solicitações de mudanças e fluxos de trabalho do CONTRATANTE, automatizados na solução;

- Permitir a definição de alertas com regras que viabilizem a emissão de avisos de registros incidentes, problemas, mudanças, solicitações de serviço, tarefas e atividades de fluxos de trabalho que estejam próximos de limites de SLA estabelecidos;
- Manter um histórico dos níveis mínimos de serviço para acompanhamento de desempenho dos serviços;
- Permitir a definição do tempo de duração para os níveis mínimos de serviço ou percentual de disponibilidade de um item de configuração;
- Indicar quando o nível de serviço não foi cumprido ou está próximo do não cumprimento;
- Permitir definição de múltiplos SLA;
- Permitir a criação de modelos de SLA para reutilização e facilidade de configuração de novos serviços;
- Possuir um repositório único com todos os registros de SLA, consolidando os Acordos de Nível de Serviço e Acordos de Nível Operacional;
- Permitir o acesso seguro e controlado às informações do processo de gerenciamento de níveis de serviço e de SLA;
- Permitir gerenciar o ciclo de vida de SLA;
- Permitir anexar SLA a qualquer processo ou fluxo de trabalho do CONTRATANTE, automatizado na plataforma;
- Permitir monitorar automaticamente os tempos de resposta, resolução e escalação relacionados com SLA;
- Permitir a configuração de contabilização de SLA apenas em horários definidos pelo CONTRATANTE, a exemplo da necessidade de contabilização de
- SLA apenas em horas úteis;
- A solução deve garantir o monitoramento dos prazos não apenas do SLA, firmado entre TI e usuários finais, mas também entre equipes (OLA) e prestadores de serviço externos (UC);
- A medição de prazos deve ser insumo para a composição de indicadores gráficos de performance, exibidos em painéis do tipo dashboards;
- A solução deve permitir que eventos sejam disparados através da integração com ferramentas de monitoramento e gerenciamento de eventos e a contagem de seus prazos iniciados, para acompanhamento do atingimento dos limites definidos;
- A solução deve permitir emitir relatórios das métricas de SLA;
- A solução deve permtir a automação da escalação e notificação, baseado nos tempos de resposta e resolução;
- A solução deve garantir a integração nativa entre o Gerenciamento de Níveis de Serviço com o Gerenciamento de Incidentes, Problemas e Mudanças, garantindo que a execução de ações siga tempos pré-definidos; e
- Permitir alertar ao time e à gestão, caso um evento exceda um número específico de atribuições e escalações.
- Permitir a criação de SLAs, OLAs e KPIs definidos pelo administrador de uma forma não programática (“codeless” ou “lowcode”).
- Permitir a definição, gerenciamento, revisão, monitoramento e divulgação dos Acordos de Nível de Serviço (SLAs), Acordos de Níveis Operacionais (OLAs) e Contratos de Apoio (UCs).

- Deve prover calendário com datas, feriados e horários de trabalho, parametrizáveis por Acordo em seus diversos escopos (SLA, OLA, UC), permitindo a aferição dos níveis de serviço oferecidos pelas áreas ou equipes de atendimento da Sefa-PR.
- Permitir a definição de níveis de serviço para os processos de Gerenciamento de Incidentes, Gerenciamento de Problemas, Gerenciamento de Mudanças e Cumprimento de Requisições de Serviços.
- Permitir a definição e ser capaz de medir e monitorar prazos de resposta e prazos de resolução tanto para o atendimento como um todo ("nível de serviço") quanto para as atividades que compõem o atendimento ("nível operacional") de forma que seja possível avaliar o desempenho de cada equipe envolvida no atendimento, em comparação com o seu nível de serviço acordado.
- Permitir, no mínimo, a definição dos níveis de serviço para:
    - Tempo de início do atendimento.
    - Tempo de solução do atendimento.
    - Tempo de resposta do chamado.
    - Disponibilidade do serviço.
- Permitir a diferenciação dos níveis de serviço estabelecidos para um chamado, associando automaticamente o acordo apropriado, de acordo com o usuário, item de configuração, setor (ex.: seção, departamento ou divisão.) ou serviço. Se nenhum destes tiver um SLA associado, o SLA padrão deve ser utilizado.
- Permitir a definição de paradas programadas e janelas de manutenção para os serviços de TIC, de modo que interrupções durante esses intervalos não influenciem o cálculo dos níveis de serviço correspondentes.
- Deve auxiliar na monitoração de OLAs, UCs, do mesmo modo que trata um SLA.
- Permitir a programação de revisão SLAs, OLAs e UCs.
- Permitir a configuração e a emissão de alertas automáticos, por exemplo, via correio eletrônico ou SMS, quando um nível de serviço estiver próximo de seu limite acordado.
- Permitir a integração do processo de Gerenciamento de Níveis de Serviço com os processos de Gerenciamento de Incidentes, Gerenciamento de Problemas e Cumprimento de Requisições de Serviço.
- Deve prover, ao processo de Gerenciamento de Mudanças, o acesso a informações de SLAs, para tratar requerimentos de disponibilidade, janelas para implementações, detalhes acordados e assuntos correlatos.
- Deve prover mecanismos de relacionamento entre SLAs, OLAs e UCs.
- Permitir a associação de incidentes a serviços e SLAs, possibilitando a visualização dos incidentes que impactaram serviços e SLAs.
- Permitir a associação de problemas a serviços e SLAs, possibilitando a visualização dos problemas que impactaram cada serviço.

- Permitir a associação de mudanças a serviços e SLAs, possibilitando a visualização das mudanças que impactaram cada serviço.
- Permitir a associação de SLAs a serviços.
- Permitir a definição de penalidades nos seguintes acordos: SLA, OLA e UC.
- Deve implementar aferição e monitoração de níveis de serviço para cada IC.
- Deve prover a correlação entre os parâmetros dos SLAs com os UCs.
- Permitir o desenvolvimento e monitoração de UCs com fornecedores externos, da mesma forma como são desenvolvidos e monitorados os OLAs.
- Deve possibilitar a monitoração automática dos limites de níveis de serviço, entregues com base nos SLAs.
- Permitir o cadastramento de detalhes do fornecedor, incluindo dados do contato: nome, e-mail, telefone, data de assinatura, datas de efetivação, renegociação e encerramento do contrato, objeto do contrato, periodicidade (mensal, trimestral, anual), etc.
- Permitir o rastreamento e alteração de detalhes de manutenção por fornecedor e por ICs.

8. BASE DE CONHECIMENTO

- Possuir uma base de dados para armazenamento de artigos de conhecimento da organização;
- Permitir configurar e gerenciar o ciclo de vida de registros de artigos de conhecimento;
- Possuir recurso para busca indexada, apresentando soluções para os atendentes;
- Permitir classificar e atribuir categorias para os artigos de conhecimento;
- Permitir a pesquisa de artigos de conhecimento nas telas de atendimento de registros dos processos de gerenciamento de incidente, mudança, problema, requisições;
- Possuir campos de pesquisa de conhecimento, integrados com a base de conhecimento da solução, nas interfaces de solicitação e operação de aplicações, processos e fluxos de trabalho do CONTRATANTE;
- Permitir gerenciar documentos de conhecimento estabelecendo prazos de validade e de revisão;
- Permitir o gerenciamento de acesso de usuários aos artigos de conhecimento;
- Permitir inserir ou anexar imagens, vídeos e textos artigos de conhecimento;
- Permitir pesquisar através de palavras-chave ou frases inteiras;
- Permitir controlar o processo de aprovação de um documento, antes do mesmo ser publicado na base de conhecimento;
- Permitir o ranking de uso das informações de conhecimento e identificar as necessidades não atendidas por conhecimento, de forma que o próprio usuário final possa classificar a utilidade (ou não) do artigo de conhecimento;
- Deve permitir o cadastro, alteração, revisão, desativação, publicação de procedimentos para a base de conhecimento (perguntas frequentes, erros conhecidos, soluções de contorno, entre outros.) e o público para o qual deve ser disponibilizado (equipes de TI, usuários finais, etc.),

de forma que incidentes e problemas já diagnosticados ou resolvidos possam ser registrados e pesquisados para facilitar e aumentar a velocidade de solução de futuras ocorrências.

- Deve integrar nativamente o processo de Gerenciamento de Conhecimento aos processos de Gerenciamento de Incidentes, Gerenciamento de Problemas e Gerenciamento de Configurações.
- Permitir o recebimento de propostas de ativos de conhecimento, sua posterior análise e sua aceitação ou rejeição. Esse recebimento de propostas deve ter origem no Gerenciamento de Incidentes, no Gerenciamento de Problemas, no Gerenciamento de Configuração ou em uma solicitação direta de um usuário.
- Deve permitir revisões para cada ativo de conhecimento.
- Deve implementar recursos comuns de gerenciamento de documentos, incluindo: captura, classificação, marcação e indexação, pesquisa e recuperação, controle de versão, segurança e gerenciamento de acesso.
- Deve permitir a estruturação do conteúdo da KB (Knowledge Base) na forma "Wiki", sem depender de codificação.
- Deve fornecer uma plataforma de gerenciamento de KB (Knowledge Base) exclusiva para todos os usuários de diferentes equipes e departamentos.
- Deve controlar as permissões de acesso à plataforma KB (Knowledge Base) com base em papeis, equipe do usuário ou com base em grupos.
- Deve obter automaticamente itens relevantes da base de conhecimento com base nas pesquisas dos usuários ou contextualmente, para resolução de incidentes de autoatendimento
- Deve oferecer funcionalidade semelhante blogs para permitir a pesquisa, postagem e acompanhamento de tópicos de resolução de problemas.
- Permitir uma variedade de mídias, incluindo arquivos de áudio e vídeo internos ou externos (por exemplo, vídeos do YouTube), links, arquivos, etc.
- Deve fornecer recursos de colaboração social, incluindo: perfis e funções dos usuários, postagens dos usuários, curtidas e comentários, bate-papos e mensagens (internos à solução).
- Possuir uma interface fácil e iterativa para a consulta a base de conhecimento, tanto para o analista quanto para o usuário final;
- Possuir a integração nativa do Gerenciamento do Conhecimento com os demais processos (nativos da solução ou implementados para atendimento de processos de trabalho), permitindo, por exemplo, mas não limitado a tal, a associação de documentos e artigos de conhecimento a eventos, incidentes, problemas, mudanças e registros de fluxos de trabalho automatizados na solução;
- Possuir recursos de pesquisa de soluções aos usuários enquanto registram as solicitações;
- Rastrear, automaticamente, quantas vezes um artigo ou informação de conhecimento foi utilizado.
- Deve possuir uma base de conhecimento onde serão registradas soluções para os problemas e erros conhecidos, possibilitando relacionar os problemas e suas respectivas soluções a mudanças e a incidentes específicos.
- Permitir consulta rápida, por palavras-chave, das informações que se encontram na base de conhecimento e possibilitar a navegação na hierarquia de tópicos ou assuntos.

Deve possibilitar, aos usuários administrativos, ou outros usuários, com nível de autorização suficiente, o gerenciamento (inclusão, alteração, consulta e exclusão) das informações armazenadas na base de conhecimento.

9. REGISTRO DE COMUNICAÇÃO

- Possuir funcionalidade de chat;
- Permitir a interação em tempo real entre o atendente do chamado e o cliente solicitando, mantendo o registro da solicitação atualizado e visível para ambas as partes;
- Permitir a utilização dos seguintes meios para abertura e resolução de chamados:
    - telefone;
    - e-mail;
    - whatsapp;
    - chatbot;
    - ferramentas de gestão de infraestrutura (monitoração);
    - portal web;
    - Permitir que o atendente faça anotações nos registros de trabalho podendo escolher entre a mensagem estar visível para o cliente solicitante ou somente para o time de atendimento.
- Permitir que solicitantes abram requisições consultem bases de conhecimento utilizando agentes ativos (funcionários), agentes virtuais (chatbots) ou ambos usando as interfaces de conversação
- Permitir explorar, implementar e manter as interfaces de conversação com mais rapidez e facilidade com uma experiência guiada no Portal, Intranet e/ou pagina dos católogos disponibilizados na plataforma.
- Todas as parametrizações, fluxos, treinamentos e configurações que seja preciso para configurar e iniciar as interfaces, como Agente Virtual e Chat devem ser realizadas na mesma interface da plataforma.
- A interface de criação das conversas do agente virtual deve permitir desenvolver, testar e implantar conversas automatizadas que auxiliam usuários com problemas comuns ou tarefas de autoatendimento;
- Possuir nativamente o entendimento para linguagem natural (NLU - Natural Language Understand);
- A interface de conversação do chatbot deve oferecer aos seus usuários várias opções para gerenciar a conversa;
- Deverá permitir interação com o Assistente Virtual Inteligente utilizando “linguagem natural ou coloquial”, em língua Portuguesa Brasileira, como se estivesse falando com um humano, tornando mais fácil e produtiva sua interação, devendo tratar neologismos, gírias e regionalismos, de forma a entender a real intenção dos usuários ao efetuarem uma pergunta ou busca por conteúdo;
- Deverá oferecer um Modelo de Linguagem Natural parametrizável que contemple vocabulário, conceitos e termos específicos para emular (intent) a atividade humana de atendimento ao usuário e permita a customização de vocabulário específico;

- A interface de criação deve ser uma ferramenta gráfica para construir os fluxos de diálogo das conversas (tópicos)., devendo cada fluxo ou tópico capaz de definir o diálogo trocado entre um agente virtual e um usuário para atingir um objetivo específico ou resolver um problema.
- Permitir desviar os problemas mais comuns e fáceis de resolver do usuário para um bot de agente virtual disponível 24 horas por dia, 7 dias por semana.
- Permitir configurar, gerenciar e monitorar os agentes virtuais e ao vivo na página inicial em uma interface integrada e graficamente intuitiva.
- Permitir criar tópicos de Agente Virtual para desviar solicitações comuns de usuários.
- Permitir chat assíncrono, ou seja, os agentes e usuários finais podem participar de conversas de longa duração sem estarem online simultaneamente, podendo o agente entrar em contato proativamente com os usuários sempre que houver informações úteis para compartilhar, como alertas ou atualizações importantes.
- Para o chat assíncrono, a interface de conversação deve ser a mesma que no chat online, devendo essas conversas sejam executadas em canais de mensagens que permitem que seus usuários e agentes se comuniquem em momentos diferentes e retomem as conversas de onde pararam.
- O chat assíncrono deve permitir indicadores de mensagens que informam os usuários sobre mensagens novas e não lidas recebidas quando estão fora da janela de bate-papo ou offline.
- O chat assíncrono deve permitir mensagens do sistema, exibidas para usuários e agentes, que são personalizadas para canais de mensagens ou bate-papo.
- Deve ser possível configurar para o chat assíncrono com um período de tempo limite de conversa ociosa, onde administradores possam ajustar o valor para canais de mensagens, conforme necessário.
- Deve possuir recurso proativo de mensagens que permite que os agentes iniciem a comunicação com os usuários
- O sistema deve possuir configuração como expressões regulares para cada tipo de dados confidenciais (por exemplo CPF, cartão de credito, OAB etc), onde manipulador de dados confidenciais detecta e mascara os dados confidenciais para que não sejam visualizados pelo agente ou solicitante.
- Deve ser possível configurar o mascaramento de dados no chat do agente de modo que a manipulação de dados confidenciais funcione apenas para mensagens de entrada (do solicitante), mensagens de saída (do agente ativo) ou ambas.
- O sistema deve validar os dados sensíveis e caso o solicitante envie uma mensagem contendo dados confidenciais para um agente, uma mensagem do sistema será enviada ao solicitante e ao agente notificando que a mensagem continha dados confidenciais. Os dados confidenciais devem ser mascarados na transcrição e marcados como confidenciais na transcrição interna.
- Deverá ser possível a criação de fluxos de atendimento, por meio de programação de árvores de decisões e perguntas de esclarecimento e de direcionamento dos usuários;
- Permitir que os usuários recebam alertas de áudio e visuais automaticamente quando recebem uma mensagem de um agente ao vivo ou bot virtual;
- Permitir que usuários autenticados possam ativar ou desativar alertas audíveis e de notificações de bate-papos por meio do botão de alternância no menu de bate-papo ou em configuração própria;
- Possuir mecanismo que disponibilize para o desenvolvedor facilidade na criação de fluxos de conversação;

- Permitir dentro da plataforma inserir em qualquer portal a função chat virtual robotizado, com atendimento virtual por meio de chatbot;
- Possuir mecanismos diversos para automação como: árvore de decisões gráficas, looping, conteúdos e serviços de localização;
- A interface de conversação deve oferecer aos seus usuários várias opções para gerenciar a conversa, podendo os usuários interromperem a conversa atual e iniciar uma nova ou entrar em contato com o suporte para acessar um agente ao vivo e obter assistência imediata;
- Quando os usuários são transferidos para um agente ativo, analista da CONTRATANTE, o cabeçalho da janela de bate-papo deve mudar para indicar que agora eles estão interagindo com um agente ativo;
- Deve ser possível na janela de bate-papo efetuar o upload de uma imagem, texto ou arquivo PDF e enviá-lo ao agente; de forma nativa na solução, sem a necessidade de integração com ferramentas de terceiros.
- Possuir, na mesma interface/sistema, a possibilidade de construir fluxos de conversação de forma gráfica (inicio-> iterações-> fim) com o virtual agente (chatbot), utilizando recursos como: entradas do usuário, respostas de bot e utilitários (ler um registro da base, executar uma ação de script, decisão de fluxo etc) para definir o fluxo;
- Possuir a capacidade sobre as construções dos fluxos de conversação para inserir utilitário de Decisão em um tópico do Agente Virtual para adicionar duas ou mais ramificações que representam caminhos diferentes em uma conversa. Por exemplo: um controle de escolha estático solicita que o usuário selecione entre três cores disponíveis e a seleção é armazenada em uma variável. O controle do utilitário de decisão é configurado com uma ramificação para cada seleção possível. Cada ramificação contém um script na propriedade/condição que identifica quando uma cor específica é selecionada.
- O sistema deve validar caso um agente tente enviar uma mensagem contendo dados confidenciais a um solicitante, a mensagem não deverá ser enviada ao solicitante. Em vez disso, um erro deve ser exibido para o agente e a mensagem deve ser marcada como confidencial na transcrição interna.
- Deve permitir configurar o agente virtual em interface do Portal de Serviços e em aplicativos disponibilizados nas plataformas Apple iOS e Google Android.
- Deve permitir, de forma nativa, integrações com aplicativos de mensagens corporativas de terceiros, no mínimo: Slack , Microsoft Teams, Workplace do Facebook e facebook Messenger para usuário externo.
- Permitir criar integrações de bate-papo personalizado de conversação com outros provedores de bate-papo, como Whatsapp por exemplo;
- Deve possuir capacidade de criar conversas baseadas em palavras-chave que os usuários inserem ou aplicar modelos de compreensão de linguagem natural (NLU), que permitam que o agente virtual entenda, processe e responda ao que os usuários estão dizendo durante uma conversa.
- Permitir que quando os usuários iniciem uma conversa com o bot, eles possam inserir uma solicitação ou ver uma lista de tudo o que o bot pode ajudar. Caso eles optem por ver tudo, a janela de bate-papo exibirá todos os tópicos disponíveis para o usuário.
- Deverá utilizar NLU para processar a linguagem humana com base no contexto e nos dados da organização.

- Deverá o NLU possuir a capacidade de aprender a sintaxe, a semântica e o vocabulário de organização usando um construtor de modelo NLU e o serviço de inferência NLU para permitir que o sistema aprenda e responda à intenção do usuário.
- Na parametrização de intenções (Intent) NLU deve permitir criar palavras-chave de backup caso uma intent não seja correspondida. Se houver várias correspondências, o agente virtual retornará no mínimo três intents por padrão. O administrador deve poder alterar o número de tópicos retornados usando a propriedade do sistema.
- Permitir que o sistema identifique e gere automaticamente variável de contexto identificando se o usuário está em uma conversa web ou usando um dispositivo móvel, para fornecer experiências de conversação personalizadas e relevantes com base no dispositivo que está sendo usado
- Permitir que administradores criem scripts para personalizar o comportamento dos tópicos do Agente Virtual e fornecer contexto para tópicos, como reter informações sobre um usuário ou a entrada de um usuário permitindo usar essas informações para personalizar uma conversa, como para apresentar uma saudação ou confirmação com script. Os scripts também podem especificar determinadas ações a serem executadas em informações obtidas durante uma conversa.
- Caso o agente virtual não encontre nenhuma correspondência/intenção/intent correspondente no NLU, ele deve usar a pesquisa de IA (Inteligência Artificial) para gerar resultados de pesquisa que exibam links relevantes para artigos de conhecimento de perguntas e respostas, itens do catálogo de serviços ou registros de pessoa (usuário).
- As pesquisas de IA devem ser controladas pelo tópico de configuração de pesquisa AI exclusivo e parametrizável,
- Possuir solução de análise e relatório de agente virtual contendo painel de análise de conversação pré-configurado para ajudar a melhorar as interações do agente virtual.
- Para compor os gráficos e painéis o Agente Virtual deverá manter registros das interações com os usuários. O painel deve conter informações sobre essas interações para que possa visualizar como o Virtual Agent entendeu e resolveu os problemas do usuário, com métricas como: Qual porcentagem de usuários transfere do Agente Virtual para um agente ativo, Tópicos mais e menos usados, detalhes da conversa (interface web, mobile, id do usuários, inicio e fim da conversa, duração), mostrar o número de vezes que o modelo de previsão NLU entendeu com precisão a intenção da conversa do usuário ou selecionou um tópico automaticamente, exibir informações sobre o número de problemas do usuário interceptados pelo serviço de resolução automática e resolvidos pelo Agente Virtual
- Possuir API de integração API Rest ou Soap para o chatbot/virtual agent.

10. NOTIFICAÇÕES

- Poder inserir notificações automatizadas em qualquer momento de fluxo de trabalho e processos automatizados na solução;
- Permitir configurar notificações automáticas de alertas, para reiteração de chamados técnicos abertos;
- Enviar notificações com informações contendo dados de qualquer parte do registro de um fluxo de trabalho ou processo implementado na solução;
- Enviar notificações baseadas em condições e eventos da solução incrementados ou alternados.

11. INTERFACE MOBILE

- Ser responsiva para dispositivos móveis podendo ser operada por meio de aplica vos mobile nos sistemas operacionais Android e IOS;
- Possuir funcionalidades, para usuários e operadores solucionadores, que permitam interações com aplicações, processos e fluxos de trabalho automatizados, como por exemplo:
    - Visualizar o catálogo de serviços e disparar solicitações e registrar incidentes;
    - Visualizar seus chamados e ações tomadas sobre eles;
    - Interação com o registro de trabalho, podendo inserir anotações de trabalho, realizar atendimentos, encerrar atendimentos;
    - Aprovar e atualizar tarefas.
- Tomar decisões e realizar ações que possam afetar o fluxo de um workflow;
- Notificações do tipo push;
- Possuir aplicativo mobile próprio da solução para IOS e Android.

12. USABILIDADE

- Possuir uma mesma interface (Ex.: estilos de menus, listas e telas de registros, gráficos, dashboards, relacionamento de registros, etc.) de navegação e uso em todos os fluxos de trabalho, processos e aplicações que sejam automatizadas dentro da solução;
- Permitir inserir quantidade ilimitada de anexos em registros de trabalho, fluxos de trabalho e processos automatizados na solução;
- Possuir interface de acesso totalmente WEB para todas as funcionalidades (administração e uso);
- Possuir interface de acesso e todas suas telas de administração e uso em idioma português padrão Brasil;
- Possuir interface amigável e intuitiva para os usuários e administradores;
- Permitir acesso controlado à solução por meio de usuário e senha e com autenticação utilizando serviços de Diretórios LDAP e Microsoft Active Directory – AD;
- Permitir a adequação de menus da interface de atendimento para cada operador, permitindo que o operador organize seus menus com os principais links que utiliza dentro da solução;
- Permitir a criação de menus específicos paras as aplicações e automatizações de fluxos de trabalho e processo do CONTRATANTE, desenvolvidos na solução;
- Permitir o desenvolvimento de formulários, sem a necessidade de programação e diagramação, para a inclusão, exclusão e alteração de campos escolhidos.

13. RELACIONAMENTO DE REGISTROS

- Possuir interface de lista de registros de qualquer processo ou fluxo de trabalho da solução, seja nativo ou criado para o CONTRATANTE, totalmente customizável, permitindo adicionar, remover ou alterar a ordem das colunas no grid de visualização de registros;
- Permitir filtros e consultas a partir de qualquer coluna listada no grid de registros;
- Permitir que usuários refinem a pesquisa com consultas avançadas, podendo inserir vários critérios de consulta e filtros no grid de registros;
- Permitir que consultas personalizadas possam ser gravadas e compartilhadas com outros usuários da solução;
- Permitir aos usuários inserir e remover quantas colunas forem necessárias em sua lista e grids, desde que estas estejam na tabela de banco de dados ao qual estão sendo listados os registros;
- Permitir a alteração da ordem de apresentação das colunas no grid de registros;
- Permitir ordenar a lista de registros por qualquer das colunas do grid de visualização, de A a Z e de maior para menor, ou vice-versa;
- Permitir atualizar manualmente as consultas exibidas nas listas e grids (refresh) sem fechar ou atualizar toda a janela atual do navegador;
- Permitir que usuários salvem seus filtros / pesquisas;
- Permitir que usuários compartilhem os filtros entre usuários e grupos;
- Permitir que usuários realizem pesquisas e filtros avançados;
- Permitir que os usuários exportem para arquivos formato Excel, CSV e XML;
- Permitir que usuários importem dados para criação e alteração de registros com base em modelo no formato Excel, CSV e XML;
- A personalização de listas e grids não devem depender de um usuário administrador, sendo facultado a qualquer outro operador a criação de suas próprias listas e grids, não estando restrito às listas e grids originalmente disponíveis na aplicação ou disponibilizadas pelos administradores;
- Permitir a alteração de registros, inclusive alterações em lote (vários registros), na própria tela de visualização de registros e grid da solução;
- A solução deve possuir recurso que permita aos operadores fazer a listagem de todos os registros em sua fila ou fila de grupos de solução a que pertence, combinando registros de incidentes, requisições, mudanças e tarefas de processos e fluxos de trabalho;
- Permitir a criação de novos registros ou exclusão de registros, a par r da lista de registros;
- Prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte; e
- Permitir o relacionamento de tabelas de bancos de dados criadas para automação de aplicações, processos e fluxos de trabalho do CONTRATANTE, com tabelas e bancos de dados nativos da solução, sem a necessidade de programação ou alterações do código-fonte.

14. FUNCIONALIDADES DE APROVAÇÕES EM FLUXOS DE TRABALHO

- Prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte;
- Permitir configurar aprovação em fluxos trabalho no mínimo com as seguintes regras para andamento do fluxo, sem necessidade de programação ou alterações do código-fonte:
    - Aprovação por um usuário específico;
    - Aprovação por conjuntos de usuários e regras específicas para sequência de aprovação;
    - Aprovação pelo gerente de um grupo solucionador;
    - Aprovação pelo gerente do solicitante;
    - Aprovação de acordo com o cargo e a estrutura de cargos da organização de forma recursiva (independentemente da quantidade de níveis ascendentes) e dinâmica (não atrelado à usuário específico);
    - Aprovação por quantidade definida de pessoas em um grupo de solução;
    - Aprovação por vários grupos de solução;
    - Aprovação por grupos de solução juntamente com usuário específico.

15. RELACIONAMENTO DE REGISTROS

- Prover recursos que possibilitem a parametrização de regras para aprovações de fluxos de trabalho, processos, requisições e outros registros da solução, com base nas regras de negócio do CONTRATANTE, sem a necessidade de alteração do código-fonte;
- Permitir o relacionamento de tabelas de bancos de dados criadas para automação de aplicações, processos e fluxos de trabalho do CONTRATANTE, com tabelas e bancos de dados nativos da solução, sem a necessidade de programação ou alterações do código-fonte.

16. GERENCIAMENTO DE USUÁRIOS E PERMISSÕES DE ACESSO

- Permitir atribuir a um usuário ou grupo de usuários específico, o acesso à abertura, modificação e fechamento de registros;
- Permitir a delegação de responsabilidades, papéis e funções dentro da solução, para fins de substituição temporária do usuário principal;
- Permitir configurar a aprovação em fluxos de trabalho no mínimo com as seguintes regras para andamento do fluxo, sem necessidade de programação ou alterações do código-fonte:
    - Permitir aprovação por um usuário específico;
    - Permitir aprovação por conjuntos de usuários e regras específicas para sequência de aprovação;

- Permitir aprovação pelo gerente de um grupo solucionador;
- Permitir aprovação pelo gerente do solicitante;
- Permitir aprovação de acordo com o cargo e a estrutura de cargos da organização de forma recursiva (independentemente da quantidade de níveis ascendentes) e dinâmica (não atrelado à usuário específico);
- Permitir aprovação por quantidade definida de pessoas em um grupo de solução;
- Permitir aprovação por vários grupos de solução;
- Permitir aprovação por grupos de solução juntamente com usuário específico.

- Permitir a configuração, sem alteração de código-fonte, para aprovações que não se enquadram no subitem anterior;
- Permitir atribuir a um usuário ou grupo de usuários específico, o acesso à abertura, modificação e fechamento de registros;
- Permitir a delegação de responsabilidades, papéis e funções dentro da solução, para fins de substituição temporária do usuário principal.

17. GESTÃO DE SERVIÇOS DE TI (ITSM)

a. GERENCIAMENTO DE MUDANÇA:

- Permitir o registro, a modificação, tratamento e o encerramento de mudanças;
- Permitir configurar e gerenciar o ciclo de vida de registros de mudanças de acordo com o processo do CONTRATANTE;
- Permitir a configuração de “n” aprovações em fluxos de registros de mudança e atender aos requisitos de aprovações em fluxos de trabalho descritos no processo do CONTRATANTE;
- Permitir o relacionamento de registros de mudanças com registros de incidente, problemas, riscos e outros registros da solução;
- Permitir o relacionamento de registros de mudança com serviços de negócio e outros itens de configuração, inclusive com “n” itens de configuração;
- Permitir identificar visualmente o conflito de calendário (data/hora) com outros registros de mudança programados ou em andamento;
- Permitir a criação de modelos de mudança para utilizar e facilitar o preenchimento de outros registros de mudança;
- Permitir o encerramento de erros conhecidos, de problemas e de incidentes quando uma mudança relacionada a estes é implementada com sucesso;
- Dever ser possível alterar os valores da requisição de mudança durante o seu ciclo de vida, tais como, mas não limitado a prioridade, categoria, ICs e SLA, baseado em permissões;
- A solução deve facilitar a produção do calendário de mudanças em suas diversas fases, tais como estágios de construção, implementação, testes e implantação;
- Deve ser possível disparar consultas à base de conhecimento a partir do Gerenciamento de Mudanças;

- Possuir funcionalidade de realização de reuniões de Comitês Consultivos de Mudanças em sala virtual online, possibilitando a reunião remota e a votação por integrantes do Comitê em tempo real, inclusive via aplicativo mobile;
- Disponibilizar recursos para criar, avaliar, aprovar e executar mudanças e ainda gerar procedimentos de reversão de mudança;
- Permitir a configuração de várias etapas de aprovação em fluxos de registros de mudança, conforme critérios de aprovação pré-definidos, comunicando as informações de Mudanças e PM (Programação de Mudanças) que possam ser distribuídas para a Central de Serviços e grupos de usuários;
- Permitir a criação, de forma gráfica, de fluxos de trabalho associados a tipos específico de mudança, conforme a necessidade do CONTRATANTE, sem necessidade de alteração do código-fonte;
- Exibir alertas quando no preenchimento de solicitações de mudanças baseados no calendário de mudanças programadas para serviços que podem causar impacto em um mesmo IC (Ex.: conflitos de janelas das mudanças que envolvem um mesmo IC);
- Criar relacionamentos entre problemas, mudanças, incidentes, riscos e outros registros de solução;
- Suportar a tarefa de atualização de informações de IC no CMDB quando ocorrer uma mudança bem-sucedida no mesmo.
- Permitir o gerenciamento de todo o processo de mudanças, controlando o planejamento, as requisições, os registros, o andamento, as aprovações, a autorização da implementação, a implementação, a avaliação e o monitoramento do trâmite da Requisição de Mudança.
- Permitir a definição de relacionamentos do tipo "resolvido por" entre incidentes e mudanças, e entre problemas e mudanças.
- Permitir a inserção de dados em texto livre e em arquivos, assim como o uso de códigos, para a classificação de requisições de mudança (categoria e prioridade).
- Deve permitir que mudanças não autorizadas sejam devidamente justificadas e notificadas para a Central de Serviços e para os usuários.
- Deve permitir o registro de um ou mais itens de configuração associados à mudança.
- Permitir o cadastramento, dentro do registro de mudança, de informações sobre a avaliação de impacto, para subsidiar o processo de autorização de mudanças (ex: relatórios técnicos anexos).
- Permitir a elaboração de programação de mudanças, assim como a definição de janelas (dias e horários) para a execução de mudanças, em função dos itens de configuração envolvidos, do tipo e da criticidade da mudança.
- Permitir os seguintes tipos de mudanças definidos no ITIL V4:
    - Mudanças padrão (Standard Changes).
    - Mudanças normais (Normal Changes).
    - Mudanças emergenciais (Emergency Changes).

- Deve permitir o registro dos procedimentos para se desfazer uma mudança malsucedida (Planos de Retorno de Mudanças).
- Permitir a identificação dos erros conhecidos, problemas e incidentes associados a uma mudança implementada com sucesso, com o objetivo de permitir a sua revisão e o seu fechamento.
- Permitir a divulgação de comunicados para grupos de usuários sobre informações e programações de mudanças, via correio eletrônico e quadro de avisos.
- Permitir a tarefa de atualização automática de informações de itens de configuração no CMS, quando uma mudança for bem-sucedida.
- Permitir o acesso aos relacionamentos entre vários itens de configuração para analisar o impacto e respaldar a avaliação de uma autorização de mudança. Esses relacionamentos devem ser visualizados em gráfico construído automaticamente, com o objetivo de apoiar a tomada de decisões pelo gerente do processo.
- Permitir o gerenciamento de mudanças encadeadas, controlando o seu tempo de execução e o seu fluxo, incluindo mudanças predecessoras e sucessoras.
- Deve prover acesso às informações do processo Gerenciamento de Mudanças, como a programação e o histórico de mudanças, de acordo com o nível de autorização do perfil do usuário.
- Permitir a solicitação de autorização a grupos de usuários ou a usuários individuais, de acordo com o nível de autorização de seu perfil, com o impacto e criticidade da mudança.
- Deve permitir que os usuários envolvidos ou impactados pela mudança possam acompanhar a sua realização.
- Deve ser capaz de solicitar autorização, caso uma mudança necessite ser cancelada.
- Deve o processo de Gerenciamento de Mudanças ser nativamente integrado com os seguintes processos:
    - Gerenciamento de Configuração e de Ativo de Serviço, com a possibilidade de associação de itens de configuração e pessoas a mudanças, e de auditar alterações no CMS, para as quais não há mudança registrada.
    - Gerenciamento de Incidentes, com a possibilidade de associação de Incidentes a uma mudança, com relacionamentos tipo, "causado por" ou "resolvido por".
    - Cumprimento de Requisições de Serviço.
    - Gerenciamento de Liberações e Implantações.
    - Gerenciamento de Níveis de Serviço, com a possibilidade de associar a mudança sendo gerenciada ao serviço impactado por ela.
- Permitir o controle de acesso e as modificações realizadas nas Requisições de Mudanças, em diferentes estágios do processo, mantendo histórico sobre as alterações realizadas.
- Deve prover facilidades de notificação, através de e-mail, quadro de aviso ou SMS aos envolvidos com uma mudança, durante todo o ciclo de vida da Requisição de Mudança, com disparo manual ou automático por gatilhos de tempo ou eventos operacionais.

- Permitir a solução automática de incidentes e problemas, quando uma determinada Requisição de Mudança tiver sido fechada com sucesso.
- Permitir a comunicação das informações de mudanças e programação de mudança que possam ser distribuídas para a Central de Serviços e grupos de usuários, através de e-mail ou painéis dinâmicos de monitoramento.
- Permitir o cálculo de janelas de trabalho para a execução de atividades que indisponibilizem um item de configuração e que possam causar impacto ao serviço prestado, sugerindo períodos de menor impacto. Esses períodos devem ser calculados considerando:
    - Os horários permitidos constantes em SLA dos serviços que usam o IC a ser indisponibilizado.
    - Os horários dos "clientes" dos serviços.
    - Os horários que o Item de Configuração deve estar operacional para não causar impacto ao serviço.
- Deve o calendário de mudanças alertar para mudanças que estejam planejadas fora da janela de manutenção de um item, dentro de uma janela de congelamento, ou quando conflitarem sobre o mesmo item de configuração.
- Deve permitir a criação e armazenamento de pesquisas para Requisições de Mudança, facilitando o acesso às informações. Tais pesquisas devem definir tanto o critério de seleção dos registros (filtros) quanto o formato de apresentação (colunas que devem aparecer na lista de resultados da pesquisa).
- Deve permitir a configuração e armazenamento de filtros de pesquisa padrão para Requisições de Mudança, facilitando o acesso às informações.

b. GERENCIAMENTO DE LIBERAÇÃO E IMPLANTAÇÃO:

- Permitir o registro e o gerenciamento de liberações e implantação em serviços de TIC;
- Permitir configurar e gerenciar o ciclo de vida de registros de liberações e implantações de acordo com o processo do CONTRATANTE;
- Permitir o relacionamento de registros de liberações e implantações com registros de mudança, registros de projetos e outros registros de processos e fluxos de trabalho automatizados na solução;
- Permitir a automação da mudança de estado em registros de mudança, de acordo com a mudança de estado de registros de liberações e implantações;
- Permitir o agendamento das atividades de distribuição e entrega de liberações;
- Facilitar o processo de autorização e agendamento de liberação de pacotes de forma integrada ao processo de Gerenciamento de Mudanças;
- Garantir que uma Liberação passe por processos de agendamento da distribuição e todas as aprovações requeridas pelo processo de Gerenciamento de Mudanças.

- Deve ser possível executar funcionalidades comuns de gerenciamento de liberação, como documentar, planejar, aprovar e rastrear liberações em uma variedade de classes de ativos e ICs.
- Deve ser possível realizar o gerenciamento de bugs e integrar este processo com os de gerenciamento de incidentes e problemas.
- Deve ser possível realizar a rastreabilidade e gerenciamento de requisitos e integrá-los aos processos de gerenciamento de bugs, incidentes, problemas, solicitações, demandas, projetos e liberações.
- Permitir processo de gerenciamento de requisitos que permita estimar e planejar os custos e esforços de implementação.
- Deve ser capaz de auxiliar na geração de scripts de teste (semi-) automatizados e oferecer suporte a testes automatizados e funcionais.
- Deve ser capaz de produzir relatórios de testes incluindo informações agregadas e granulares (detalhamento).
- Permitir o acesso ao Banco de Dados de Gerenciamento de Configurações (CMDB), possibilitando a extração de informações sobre liberações, configurações, distribuições e implementações.
- Permitir a associação entre a entrega da liberação (release) com o processo de Gerenciamento de Mudanças, no que concerne o agendamento e autorização.
- Deve permitir a utilização de um fluxo de Gerenciamento de Mudanças para o planejamento e gerenciamento dos rollouts (disponibilização para uso) de software, o hardware associado e sua documentação.
- O fluxo deve incluir todas as fases de Gerenciamento de Liberação, e respectivas tarefas/alçadas de aprovação.
- Permitir a especificação de prazos, tanto para o projeto como um todo, quanto para cada fase e para cada tarefa.
- Permitir a liberação de componentes e produtos de software baseada no critério de tipo de versão (completa ou pacote).
- Deve permitir que planejamentos específicos de mudança sejam associados para garantir o sucesso da implementação.
- Permitir a integração nativa e na mesma plataforma entre a disciplina de Gerenciamento de Liberação e as de Gerenciamento de Configuração e de Ativo de Serviço e de Gerenciamento de Mudanças.
- Permitir a definição de linha de base (baseline) para a implantação (disponibilização para uso) bem-sucedida de software e ou hardware, através de uma metodologia sistêmica, segura e autorizada.
- Permitir a especificação de prazos para uma liberação, de forma integrada ao módulo de Gerenciamento de Mudanças, considerando cada fase e cada tarefa de uma liberação.

c. GERENCIAMENTO DE INCIDENTES:

- Permitir o registro, a modificação, tratamento e o encerramento de incidentes;
- Permitir consultar a Base de Conhecimento a partir da tela do registro do incidente;
- Sugerir resoluções e apresentar informações, para resolução de incidentes, na tela do registro de incidente, sem a necessidade de realizar pesquisa, oferecendo sugestões de resolução do incidente ao operador, apenas com a digitação ou preenchimento de campos básicos do registro de incidente;
- Integrar com o Banco de Dados de Gerenciamento de Configuração – BDGC (do inglês CMDB), para relacionamento de incidentes com serviços de negócio e outros itens de configuração;
- Deve oferecer todas as funcionalidades comuns de gerenciamento do ciclo de vida de incidentes, incluindo criação, priorização, atribuição, transferência, documentos e anexo de notas, fechamento e verificação.
- Permitir a inserção de dados em texto livre e a inclusão de arquivos anexados para a descrição de incidentes e atividades ligadas à sua resolução.
- Permitir, no registro de incidentes, o preenchimento automático de atributos (campos), tais como data, hora e identificador do incidente.
- Deve permitir o registro de um ou mais itens de configuração associados ao Incidente.
- Deve permitir a definição dos níveis de impacto e de urgência automaticamente, a partir do serviço impactado.
- Deve permitir o registro de um código de prioridade para os incidentes.
- Deve definir o código de prioridade dos incidentes a partir de cálculo que se baseie no código de impacto, no código de urgência do atendimento e no marcador de cliente ou usuário VIP.
- Deve possuir um mecanismo automático para as escaladas funcionais e hierárquicas, ou seja, deve ser capaz de direcionar um atendimento para outra equipe e enviar alertas para os gerentes da organização, com base na categoria, na prioridade, no tipo de usuário afetado, na importância dos ICs afetados e no tempo transcorrido do atendimento.
- Deve permitir que o incidente seja escalado manualmente, de forma funcional e hierárquica.
- Permitir o redirecionamento de incidentes, entre atendentes de um ou mais grupos de suporte (equipe de serviço) técnico.
- Deve ser possível a um determinado atendente ou grupo (equipe de serviço), repassar o incidente ou o problema para outro atendente ou outro grupo, sempre mantendo o histórico desses repasses.
- Permitir a notificação do(s) grupos(s) de atendentes de suporte técnico, quando houver chamados recém-abertos, atrasados, escalados ou concluídos, devendo esta notificação ser encaminhada, no mínimo, através de correio eletrônico.
- Permitir a associação de determinado incidente a um registro de problema.
- Permitir a associação de determinado incidente ao serviço impactado.

- Permitir, através de regras configuráveis, o envio de alertas de incidentes para grupos de usuários pré-definidos.
- Deve fornecer consultas ou relatórios que suportem a análise de incidentes com o objetivo de identificar padrões e tendências.
- Permitir a geração de relatórios de incidentes por estado, como por exemplo: resolvidos, não resolvidos ou cancelados.
- Deve permitir a criação e armazenamento de pesquisas para Incidentes, facilitando o acesso às informações. Tais pesquisas devem definir tanto o critério de seleção dos registros (filtros) quanto o formato de apresentação (colunas que devem aparecer na lista de resultados da pesquisa).
- Deve permitir a configuração e armazenamento de filtros de pesquisa padrão para Incidentes, facilitando o acesso às informações.
- Deve disponibilizar um registro histórico para auditoria de todos os incidentes registrados, bem como das atividades realizadas para resolução desses incidentes.
- Deve possuir um mecanismo que facilite a comparação de incidentes ("incident matching") inteligente, pesquisando automaticamente registros de atendimentos anteriores com características semelhantes ao incidente que está sendo reportado (mesmos sintomas, mesmo usuário, mesmo serviço, mesmo item de configuração, mesma localidade, entre outros) e listando os problemas possíveis que podem estar associados ao incidente.
- Deve permitir a configuração, pelo administrador, dos critérios de similaridade sem a necessidade de codificação (“codeless” ou “lowcode”).
- Deve prover acesso seguro e controlado ao CMS (Configuration Management System), permitindo a navegação, modificação e extração de informações relacionadas a incidentes, como por exemplo, indicadores de criticidade de um item de configuração.
- Permitir a associação de incidentes a mudanças, provendo acesso seguro e controlado às informações do processo de Gerenciamento de Mudanças, tais como a programação e histórico de mudanças.
- Permitir a associação de incidentes a problemas, provendo acesso seguro e controlado às informações do processo de Gerenciamento de Problemas.
- Permitir a busca de mudanças programadas, permitindo, ao gestor de incidentes e problemas, verificar se alguma delas proverá a solução para incidentes existentes.
- Permitir a especificação de determinado incidente como sendo uma pergunta frequente (FAQ) e assim, disponibilizá-lo facilmente, via os canais de autoatendimento e e-mail, para outros usuários.
- Permitir a definição de roteiros de apoio ao diagnóstico e resolução de incidentes, que deverão ser automaticamente apresentados ao analista durante o preenchimento do formulário de incidente no contato com o usuário, com base em, pelo menos, o item de configuração afetado e a categoria do incidente reportado.
- Deve fornecer as seguintes informações, em tempo real ou em intervalo de tempo ajustável, relativas ao processo de Gerenciamento de Incidentes:
    - Número total de incidentes.

    - Situação do incidente em cada fase da busca da solução.
    - Relação de incidentes pendentes.
    - Quantidade e percentual de incidentes classificados como graves.
    - Tempo médio para resolução de incidentes.
    - Percentual de incidentes que foram resolvidos no tempo acordado.

- Deve integrar o processo de Gerenciamento de Incidentes nativamente com os seguintes processos: Gerenciamento de Mudanças, Gerenciamento de Problemas, Gerenciamento de Conhecimento, Gerenciamento de Configuração e de Ativo de Serviço.
- Deve prover recurso de monitoramento e rastreamento dos registros de incidentes para que eles possam ser acompanhados pelos usuários responsáveis pelo registro/abertura e pela equipe responsável pela sua solução.
- Permitir, em cada fase do ciclo de vida do incidente, o registro, a categorização e priorização desse incidente, de acordo com os padrões de SLA e OLA previamente definidos.
- Deve permitir o registro de um código de fechamento distinto do código da categorização inicial do incidente, a fim de permitir-se a verificação da classificação original do chamado e a ocorrência de ajustes na classificação do chamado por parte do Service Desk.
- Deve permitir tomar ações em lote, como por exemplo, registrar uma ação ou resolver diversos registros de incidente ao mesmo tempo.
- Permitir pesquisas de satisfação online no seu encerramento, através da interface com o usuário.
- Permitir acessar mapas de serviço, para consulta ao relacionamento de itens de configuração, a partir da tela do registro do incidente;
- Permitir consultar, ou apresentar automaticamente, sem a necessidade de realizar pesquisa, outros registros de incidentes relacionados com o mesmo usuário solicitante;
- Permitir criar um registro de problema ou de mudança a partir da tela do registro de incidente;
- Permitir a associação e a manutenção de relacionamentos entre registros de incidentes e de problemas e outros tipos de registros da solução;
- Permitir a associação entre incidentes, com a possibilidade de gestão de comunicação entre incidente pai e filho;
- Permitir a gestão de comunicação para incidentes principais ou críticos, podendo definir tarefas pré-definidas de comunicação;
- Permitir a priorização, atribuição e escalação automática dos incidentes baseados na categorização do registro;
- Permitir a escalação automática dos incidentes baseados em usuários afetados e intervalos de tempo pré-determinados;
- Permitir a integração com ferramentas de monitoração viabilizando a abertura e fechamento de registros de incidentes de forma automática conforme estado de eventos em ferramentas de monitoração;

- Apresentar automaticamente, sem a necessidade de realizar pesquisa, outros registros de incidentes relacionados com o mesmo usuário solicitante.

d. AGENDAMENTO – ATENDIMENTO BALCÃO:

- Permitir criar e gerenciar um local de balcão de serviços de TI, onde as solicitações e os problemas deverão ser atendidos e resolvidos por agentes pessoalmente e/ou remotamente
- Permitir agendamento para atender a todos os usuários da CONTRATANTE
- Permitir que funcionários e convidados de negócios possam receber ajuda em tempo real, pessoalmente ou remotamente para seus problemas e solicitações de dispositivos.
- Permitir que cada funcionário ou convidado possa fazer check-in e obter suporte em um centro de balcão de serviços estabelecido.
- Permitir aos técnicos de suporte criar incidentes tradicionais quando os problemas não podem ser resolvidos no local de balcão de serviços diretamente no portal.
- Permitir minimamente:
    - Acesso On-line e via dispositivo móvel
        - Por computador, tablet ou telefone celular, permitir o check-in online rapidamente para o local de balcão de serviços mais próximo disponível
    - Acesso as horas de operação, o tempo de espera estimado e sua posição na fila no local de check-in por meio do widget Status do balcão de serviços no Portal.
    - Próximos dias disponíveis e a posição atual da fila do balcão de serviços por local. As visitas à Sala de Tecnologia deverão ser exibidas, se houver dados associados. Se não houver dados, a seção deverá ficar oculta.
    - Programar horários para receber suporte e lembretes de compromisso. Possibilidade de cancelar ou remarcar compromissos de links no lembrete ou na interface de check-in online.
    - Programar apenas um compromisso por fila de local de balcão de serviços de cada vez
    - Programar consultas em nome de outras pessoas que precisam de suporte de TI, como executivos ou subordinados
    - Receber notificações por e-mail ou dispositivo móvel quando:
        - a solicitação for atribuída a um executante de suporte de TI
        - a posição na fila estiver próxima do atendimento
        - a solicitação de balcão de serviços tiver sido encerrada ou abandonada ou o usuário decidir sair da fila.
    - Exibir todos os agendamentos e compromissos no calendário principal com a Microsoft Office 365 integração de calendário do Outlook.
    - Permitir atualização do calendário quando marca, modifica ou cancela um compromisso
- Para os agentes, permitir minimamente:

- Que os técnicos de TI gerenciem as operações diárias nas filas dos locais de balcão de serviços, resolvendo problemas relacionados a TI, oferecendo suporte a laptops e dispositivos móveis e atendendo a solicitações de produtos de software e hardware.
- Que os agentes possam aceitar e fechar interações do agendamento por meio da interface do portal do agente.
- O portal do agente deverá conter uma caixa de entrada pessoal em que as interações de balcão de serviços, deverão ser enviadas automaticamente para atribuição.
- Que os agentes possam gerenciar todos os aspectos de execução do agendamento, com base na capacidade deles e, se os registros estiverem em espera, eles poderão trabalhar em várias transações ao mesmo tempo e promover interações com incidentes ou solicitações, ou acessar produtos de depósitos parceiros.
- Que os técnicos possam ver e aceitar compromissos agendados na caixa de entrada pessoal. Os compromissos deverão ser encaminhados para a caixa de entrada de acordo com a disponibilidade do agente. Como alternativa, os agentes deverão poder selecionar e escolher compromissos manualmente.
- Se necessário, permitir que os técnicos possam trabalhar com qualquer pessoa na fila a qualquer momento. Os técnicos deverão poder atribuir a si próprios manualmente uma interação de balcão de serviços, aceitando a interação de uma lista de interações não atribuídas na fila
- Os agentes deverão poder usar o recurso Assistência do agente para agilizar a resolução do incidente.

- Para os gerentes, permitir minimamente:
  - Permitir aos gerentes de TI que supervisionem os técnicos de locais de balcão de serviços e supervisionem as operações diárias.
  - Permitir aos gerentes de suporte possam observar e capturar dados operacionais e de desempenho monitorando o painel do balcão de serviços.

e. GERENCIAMENTO DE PROBLEMA:

- Permitir o registro, a modificação, o tratamento e o encerramento de problemas;
- Permitir configurar e gerenciar o ciclo de vida de registros de problemas de acordo com o processo do CONTRATANTE;
- Permitir consultar a Base de Conhecimento a partir da tela do registro do problema;
- Permitir a integração com o Banco de Dados de Gerenciamento de Configuração – BDGC com o gerenciamento de problema;
- Permitir acessar mapas de serviço, para consulta ao relacionamento de itens de configuração, a partir da tela do registro de problema;
- Permitir o fechamento de todos os incidentes relacionados quando o problema associado ou o erro conhecido é resolvido;
- Permitir a associação e a manutenção de relacionamentos entre registros de problemas e de incidentes e outros tipos de registros da solução (Ex.: registros de projetos);

- Permitir procedimentos de escalamento do gerenciamento de incidente para o gerenciamento de problema.
- Deve oferecer todas as funcionalidades comuns de gerenciamento do ciclo de vida de problemas, incluindo a identificação, o registro, a classificação, a designação, a investigação, a identificação da causa raiz e a resolução de problemas.
- Deve ser possível realizar análise de causa raiz, integradamente a CMDB e ao Gerenciamento de Mudanças.
- Deve ser possível calcular ou prever impactos de problemas em termos de estimativas de número de incidentes para um problema especificado e usar essas informações para triagem dos problemas.
- Deve ser possível gerenciar a comunicação relacionada à identificação de problemas, a fim de evitar o acúmulo de solicitações (por exemplo: a partir da descrição da solicitação já correlacioná-la com problemas em aberto e informar algo ao usuário como "estamos trabalhando nisso, deseja prosseguir ao registro dessa solicitação").
- Permitir a apropriação de horas por serviço contratado objetivando gerar informações para o faturamento, através do registro das horas estimadas (planejadas) e as horas técnicas realmente utilizadas para a solução de problemas.
- Permitir a definição de associação (relacionamentos) do tipo "causado por" entre problemas e incidentes.
- Permitir o controle de erros conhecidos de acordo com as definições do ITIL V4, permitindo sua identificação, avaliação, registro e fechamento.
- Permitir a associação e manutenção do relacionamento entre incidentes, problemas e erros conhecidos. Esta associação deverá ser feita a partir do item de configuração afetado ou pela sua categoria, bem como por outros atributos que caracterizam os problemas e incidentes envolvidos.
- Deve permitir o registro de um ou mais itens de configuração associados ao Problema.
- Deve prover indicadores de prioridade, de impacto e de urgência para os problemas, através de regras configuráveis, podendo levar em consideração, entre outras variáveis, o impacto e a urgência do problema cadastrado.
- Deve disponibilizar um histórico de problemas e erros conhecidos para auxiliar na investigação e solução de um novo problema.
- Permitir a inserção de dados em texto livre ou provenientes de arquivos, para a descrição de problemas e atividades ligadas à sua resolução.
- Deve prover a integração com o processo de Gerenciamento de Mudanças, suportando, para isso, a abertura de uma requisição de mudanças a partir de um ou mais registros de problemas existentes.
- Deve prover facilidade de identificação dos erros conhecidos e associados a uma mudança implementada com sucesso, permitindo a revisão e o fechamento desses erros.
- Deve permitir que as alterações no estado de determinado problema sejam informadas à Central de Serviços, bem como os progressos alcançados e as soluções temporárias.

- Permitir o aumento automático do grau de severidade ou de impacto, em razão do número de incidentes associados, do número de usuários finais afetados ou de acordo com outras regras configuráveis.
- Deve disponibilizar, no mínimo, os indicadores chave de desempenho (KPIs) para o processo de gerenciamento de problemas.
- Permitir a associação do tipo "causado por" ou "resolvido por" de um problema a uma mudança anteriormente efetuada.
- Permitir a associação de requisições de serviço a problemas.
- Permitir a associação de determinado problema a um (ou mais) serviço impactado.
- Deve o processo de Gerenciamento de Problemas ser integrado, de forma nativa, com o processo de Gerenciamento de Conhecimento.
- Deve identificar e informar, aos usuários do grupo gestor do processo de Gerenciamento de Problemas, as tendências de ocorrência de problemas, provenientes de análise dos volumes e tendências dos registros de incidentes, viabilizando o Gerenciamento Proativo de Problemas.
- Permitir a associação entre um problema a outro, a mudanças, a incidentes, a requisições de serviços, sendo que os registros dependentes (“filhos”) serão encerrados automaticamente quando o registro “pai” for encerrado.
- Permitir a escalada funcional (direcionamento) de problemas entre grupos de atendentes (equipes de serviço), ou seja, deverá ser possível a um atendente ou a uma equipe repassar o problema para outra, sempre armazenando esse histórico.
- Deve permitir o registro de um código de fechamento distinto do código da categorização inicial do problema.

f. GERENCIAMENTO DE REQUISIÇÕES DE SERVIÇO:

- Permitir o registro de solicitações de serviços, por meio do portal de serviços ou de tela própria de requisições de serviço;
- Permitir gerenciar o ciclo de vida de requisições de serviço;
- Permitir vinculação de várias tarefas para o atendimento em um mesmo registro de solicitação, inclusive para grupos de atendimento diferentes;
- Permitir configurar fluxos de trabalho diferentes para cada solicitação, conforme necessidade da CONTRATANTE;
- Permitir aos atendentes a visualização do fluxo de trabalho, a partir da tela do registro da solicitação;
- Atender aos requisitos de aprovação de fluxos de trabalho descritos neste documento técnico;
- Permitir a realização de atendimento da solicitação por fases, permitindo ainda a visualização gráfica das fases de atendimento e situação atual;
- Permitir a criação de modelos de requisições de serviço permitindo a reutilização para configuração de outras requisições;

- A solução deve possuir uma visão baseada em permissões do requisitante dos serviços no catálogo que o usuário tem direito a requisitar;
- A solução deve automatizar o roteamento de requisições para a coleta das autorizações apropriadas;
- A solução deve permitir que o usuário submeta requisições de serviço, mantenha a visibilidade detalhada do cumprimento da requisição e acompanhe todo o ciclo de vida do cumprimento de sua requisição, sem a necessidade de entrar em contato com a central de serviços para acompanhamento;
- A solução deve permitir que indicadores de impacto, prioridade e urgência sejam atribuídos ao registro da Requisição de Serviço;
- A solução deve orquestrar os processos de trabalho de requisições complexas através de tarefas sequenciais e paralelas;
- A solução deve facilitar a geração de relatórios de requisições de serviço pelo próprio usuário sem a necessidade de intervenção de administradores;
- Integração com sistemas de e-mail padrão de mercado, para envio de e-mails (alertas, notificações) de forma automática, ou manual (pelo operador), bem como troca de mensagens entre os profissionais da TI ou outros usuários da solução;
- A solução deve permitir a criação de regras de negócio para requisições específicas ou grupos de requisições, para automatizar processos, tarefas e notificações;
- A solução deve suportar a criação de Requisições a partir de registros de incidentes;
- O Gerenciamento de Requisições de Serviço deve ser nativamente integrado ao CMDB, para permitir associar um IC à Requisição de Serviço.

18. GERENCIAMENTO DE ATENDIMENTO AO CLIENTE (CSM)

A solução deve possuir em sua plataforma uma aplicação de Gerenciamento de Serviços a Clientes internos e externos do CONTRATANTE, a qual possui como foco atender aos usuários de uma forma avançada e com qualidade. Neste ponto, a solução deve:

- Possuir funcionalidade que permita construir (customizar) de forma no code/low code portais de atendimento por tipo de cliente;
- Possuir um modelo de dados centralizado e integrado baseado em nuvem com CMDB nativo;
- Permitir suporte para desenvolvedores no-code, low-code e pro-code;
- Possuir ambiente único de trabalho, permitindo que o atendimento do telefone, portal, chat e a interação por e-mail sejam feitos pela mesma aplicação;
- Permitir automatizar tarefas redundantes para o cliente por meio do Chatbot;
- Possuir regras de roteamento sofisticado, utilizando regras baseado em perfil do agente e da solicitação, geografia do agente, compromisso contratual, disponibilidade do agente, carga de trabalho do agente e outras prioridades customizáveis;

- Possuir a funcionalidade de forçar perfis mandatórios para atendimento de casos que exigem esse tipo de perfil profissional;
- Possuir funcionalidade de Inteligência Artificial e Machine Learning para automaticamente assinalar quem irá atender, categorizar e priorizar automaticamente. Essa inteligência deve aprender com base nos dados históricos;
- Fornecer alertas aos agentes e fazer a linha de tempo de interação com o cliente/solicitante;
- Deve ter uma camada de colaboração avançada para suportar as comunicações da equipe;
- Deve fornecer notificações proativas de suporte via e-mail, SMS e portal para os clientes afetados;
- Deve ter um recurso de serviço de atendimento em campo totalmente integrado na mesma plataforma, por meio de aplicativo móvel, que deve funcionar on-line e off-line para atividades, permitindo a sincronização quando estiver conectado;
- Deve fornecer autoatendimento personalizado por meio de um portal de serviços configurável que incorpora uma base de conhecimento, catálogo de serviços e comunidades;
- Deve ser capaz de conectar outros departamentos aos processos de atendimento ao cliente em uma única plataforma com aderência interna aos níveis mínimos de serviços;
- Deve ser capaz de suportar diferentes SLA's para diferentes produtos pertencentes a um cliente;
- Permitir controlar SLA's para objetos diferentes do objeto "caso", como em tarefas, incidentes, problemas, alterações e solicitações associados a um caso;
- Deve fornecer gerenciamento de solicitações com várias camadas e permitir o relacionamento com registros de incidente, problemas e outras solicitações de serviço;
- Deve fornecer escalonamento automático sem intervenção manual;
- Deve fornecer chatbot ou agente virtual que permita o desenvolvimento de diálogos conversacionais;
- Deve fornecer um espaço de trabalho eficiente do agente que permita que os agentes executem várias tarefas no trabalho em vários canais, como telefone, bate-papo, e-mail e web;
- O espaço de trabalho deve exibir informações contextuais automaticamente para oferecer suporte à resolução rápida de casos. Isso inclui artigos de conhecimento contextualizado, publicações na comunidade e itens de catálogo de serviços. Os agentes devem poder anexar artigos aos casos;
- A solução deve permitir o feedback do cliente sobre o artigo da base de conhecimento por meio de um processo estruturado e automatizado de feedback;
- Permitir que os agentes sinalizem quando algo está faltando no artigo da base de conhecimento e isso deve alimentar o processo de feedback estruturado de ajuste da base de conhecimento;
- Na gestão do conhecimento, a solução deve permitir a definição de blocos de conteúdo reutilizáveis que possam ser incorporados em vários artigos de conhecimento, a fim de reduzir a redundância. Os blocos de conhecimento devem poder ser restringidos pelo papel do usuário.

- O sistema deve ser capaz de fazer leitura de documentos, incluindo PDF e documentos em papel digitalizados. usando reconhecimento óptico de caracteres (OCR), em combinação com recursos de IA para identificar, entender e extrair texto e dados desses documentos, inicialmente para um valor mínimo de 5.000 páginas/ano podendo ser contratado maior volume.
- Possuir capacidades de desenhos de fluxos aderentes aos processos de atendimento externo do CONTRATANTE, sempre de forma nativa e altamente personalizável (low-code/no-code), exemplo de fluxo: Solicitação de crédito.

a. PROCESSAMENTO DE DOCUMENTOS DIGITALIZADOS DURANTE O ATENDIMENTO

- Ser capaz de processar documentos digitalizados e através de algoritmos de Machine Learning (ML) extrair textos e dados identificando a estrutura desses documentos;
- Ser capaz de processar documentos que contenham uma ou várias páginas;
- Ser capaz de processar documentos digitalizados nos formatos JPEG, PNG ou PDF;
- Ser capaz de criar regras definindo como a extração dos dados contidos no documento, deve ocorrer;
- Ser capaz de associar a extração dos dados contidos no documento, como parte de um fluxo maior de automação;
- Ser capaz de agrupar os campos/chaves extraídas de um documento;
- Possuir algoritmo de Inteligência Artificial capaz de sugerir valores corretos para os campos/chaves capturados;
- Possuir a capacidade de aprendizado contínuo, através das aprovações e reprovações das sugestões dos valores para os campos/chaves;
- Permitir a configuração de modos de extração sem a necessidade de utilização de uma linguagem de programação (no-code), recomendando os campos baseados em inteligencia artificial para uma possível revisão enquanto o nível de aprendizagem for baixo e permitindo o auto-preenchimento ou processamento automático quando o nível de acertividade/acuracidade já for suficientemente elevado
- Possuir a capacidade de se criar regras de acesso, segregando os usuários pelo menos em grupos capazes de visualizar, criar tarefas de extração e administrar as tarefas já criadas.
- Possuir a capacidade de se criar domínios, segregando assim dados, processos e tarefas administrativas em grupos lógicos;
- Possuir algoritmo de Inteligência Artificial capaz de classificar a confiança na identificação dos campos/chaves do documento digitalizado;
- Possuir a capacidade de configuração de tresholds por tarefa;
- Fornecer uma visão gráfica do documento com a exibição dos campos identificados e a classificação desses campos, considerando o nível de assertividade do índice atribuído pela classificação do algoritmo de Inteligência Artificial;

- Fornecer visão unificada pré-configurada contendo indicadores referente aos documentos e tarefas executadas, como por exemplo: índice com a quantidade de páginas processadas nos últimos 365 dias, Índice com a quantidade de tarefas ativas no momento, Índice com a quantidade de campos/chaves identificadas nos últimos 365 dias e etc...
- Possuir a capacidade de integrar de forma nativa o processamento de documentos em quaisquer fluxos de automação, permitindo que um documento anexado a qualquer tarefa possa ser processado tendo os dados requeridos extraídos de forma automática;
- Permitir que as tarefas de processamento de documentos possam ser executados de forma assíncrona;

b. GESTÃO DE ATENDIMENTO EXTERNO

- A solução deve fornecer regras de roteamento sofisticadas com base nas qualificações do Gerente, localidade geográfica, compromissos contratuais, disponibilidade, afinidade, carga de trabalho e outras prioridades personalizadas.
- A solução deve oferecer suporte à otimização de rota automatizada, otimização de rota invocada pelo Gerente Executivo e otimização de rota invocada pelo Gerente atendimento em campo.
- A solução deve oferecer suporte a um gráfico de Gantt interativo baseado em arrastar e soltar para permitir que o Gerente de Atendimento em campo gerencie as atribuições de trabalho.
- A solução deve ter a capacidade de mostrar tarefas, Gerentes de atendimento em campo e locais (mapa) em uma única visualização.
- A solução deve oferecer suporte a recursos de calendário para permitir que os Gerentes de atendimento em campo documentem o horário em que não estão disponíveis para agendamento, incluindo folgas, reuniões, treinamento e etc.
- A solução deve suportar a geração de ordens de atendimento de várias fontes, incluindo atendimento ao cliente, gerenciamento de projetos ou cronogramas de atendimentos planejados.
- A solução deve oferecer, por meio de configuração (sem codificação), suporte à atribuição de habilidades necessárias para atendimentos específicos e também possuir pesquisa dinâmica dentro das regras de determinação de habilidades.
- A solução deve suportar a marcação de atendimento, permitindo que os clientes do Banco selecionem a hora e a data do atendimento a partir dos horários disponíveis.
- A solução deve ter um recurso de aprendizado de máquina que possa ser treinado para prever campos personalizados adicionais além de categorias, prioridades e grupos de atribuição.

- A solução deve ter uma rica camada de colaboração para dar suporte às comunicações da equipe.
- A solução deve suportar a capacidade de identificar rapidamente subconjuntos de clientes e enviar comunicações direcionadas para informá-los sobre alterações no produto, política ou serviço.
- A solução deve fornecer notificações proativas por e-mail, SMS e portal para os clientes.
- A solução deve oferecer recursos de chatbot para automatizar o trabalho do Gerente.
- A solução deve oferecer suporte a uma trilha de auditoria completa, incluindo autor, data, carimbo de data/hora, valor antigo e novo valor, permitindo que os usuários façam engenharia reversa de transações em nível de registro.
- A solução deve suportar o registro de tempo de viagem e tempo de trabalho.
- A solução deve ser habilitada para dispositivos móveis e deve suportar trabalho offline.
- A solução deve suportar dados de geolocalização para locais de atendimento externo.
- O sistema deve se integrar com sistemas de mapeamento de geolocalização.
- A solução deve suportar o rastreamento e visualização dos dados capturados de geolocalização ao longo do tempo.
- A solução móvel deve estar na mesma plataforma e suportar fácil configuração de aplicativos móveis, tanto para estender o aplicativo de serviço de campo, quanto para criar aplicativos personalizados.
- A solução móvel deve oferecer suporte a relatórios completos de campo, incluindo aceitação, início de viagem, início de trabalho, pesquisa de conhecimento, relatório de despesas, listas de verificação, anexos, registro de horas, captura de assinatura, relatório de resumo em PDF e encerramento.
- A solução móvel deve permitir que os Gerentes de Atendimento criem novos agendamentos.
- A solução deve fornecer autoatendimento personalizado por meio de um Portal de Serviços configurável que incorpore base de conhecimento, catálogo de serviços e comunidades.
- A solução deve ser capaz de conectar outros departamentos aos processos de atendimento ao cliente em uma única plataforma.
- A solução deve ser capaz de oferecer suporte a diferentes SLAs para diferentes produtos pertencentes a um cliente.
- A solução deve suportar a capacidade de anexar arquivos, imagens e vídeos e registros relacionados a uma tarefa de atendimento.
- A solução deve suportar a capacidade de capturar uma assinatura do cliente.

- A solução deve suportar a criação de mapas personalizados sem exigir código.
- A solução deve ser capaz de fornecer suporte específico ao idioma em todas as regiões.
- O provedor de soluções deve ser capaz de oferecer integração a um ecossistema de aplicativos para preencher quaisquer lacunas em uma única plataforma.
- A solução deve fornecer um meio de acompanhamento da melhoria contínua.
- A solução deve oferecer suporte ao agendamento da força de trabalho contratada de terceiros.
- A solução deve oferecer acesso externo para terceiros.
- A solução deve oferecer acesso móvel ao portal para terceiros contratados.
- A solução deve fornecer aos despachantes a capacidade de agendar o trabalho para trabalhadores internos e contratados a partir de uma tela configurável
- A solução deve permitir definir tarefas de qualquer duração com recursos aprimorados de calendário
- A solução deve atribuir automaticamente o trabalho de vários dias aos usuários.
- A solução deve fornecer notificações ao cliente via SMS.
- A solução deve suportar um mapa voltado para o cliente com localizações de Gerentes e a rota até ele.
- A solução deve oferecer suporte a definições de capacidade por número de tarefas, horas ou agendamento do agente.
- A solução deve suportar facilmente a criação, gerenciamento e agendamento de equipes.
- A solução deve atribuir tarefas automaticamente/manualmente às equipes.
- A solução deve fornecer dinamicamente as melhores tarefas disponíveis para preencher vagas na agenda de um Gerente.
- A solução deve responder rapidamente às mudanças na programação e reprogramar os trabalhos automaticamente
- A solução deve atribuir tarefas automaticamente a um Gerente com base nas habilidades, localização, disponibilidade e distância (Agendamento dinâmico).
- A solução deve permitir integração através de Web Services (REST/SOAP), email, arquivo (CSV, XLS, XML), LDAP, ODBC/JDBC, PowerShell, SSH e Java.

c. GESTÃO DE ATENDIMENTO FINANCEIRO E CICLO DE VIDA DO CLIENTE:

- Possuir capacidade criar e gerenciar casos e tarefas para solicitações de pagamento, incluindo consultas e investigações de pagamento.

- Possuir capacidade de solicitações de cartão de crédito, incluindo solicitações de novos cartões, aumento ou diminuição de limites de crédito e bloqueio ou desbloqueio de cartões de crédito.
- Possuir capacidade de conexão entre vários departamentos de forma a resolver as reclamações dos clientes com maior rapidez, deve ainda possuir de forma nativa funcionalidade onde todos os departamentos atrelados a reclamação monitorem e rastreiem o status dessa reclamação, desde o início até a resolução.
- Possuir funcionalidade de gerenciamento de empréstimos para todos os tipos de público, exemplo: pessoa física ou jurídica.
- Deve possuir visão 360 do cliente, com gerenciamento e supervisão do ciclo de vida do cliente de forma a fornecer fluxos de trabalho simplificados para coletar informações, verificar a documentação de identidade e aprovar contas.
- Possuir capacidade de priorizar, resolver e reduzir as reclamações de forma controlável e auditavel.

19. HIPERAUTOMAÇÃO DE PROCESSOS (RPA)

- Fornecer uma orquestração centralizada para implantar, monitorar, gerenciar, medir e verificar a conformidade de todos os robôs em nível enterprise, ou seja, em execução nas diferentes áreas e departamentos da organização
- Fornecer automações baseadas em elementos e APIs que interagem entre os vários aplicativos de negócios, podendo emular ações do usuário e eliminar atividades humanas mundanas e repetitivas.
- Permitir criar dois tipos de automações usando robos e executá-los com o de modo autônomo (Unattended) ou Automação assistida (Attended Robot).
- Permitir que as autenticações dos usuários nos robos possam ser feitas utilizando ao menos duas formas: instalação de certificados de usuário ou exportando o certificado do Active Directory.
- Permitir criar e utilizar robôs de forma autônoma, onde possa usar esse tipo de automação para tarefas altamente repetitivas. Por exemplo, em um sistema de CRM, as tarefas de copiar e colar podem ser executadas pelo robô autônomo em um arquivo do Excel sem qualquer intervenção humana.
- Permitir criar e utilizar robôs de automação assistida, onde possa usar esse tipo de automação com supervisão humana. Por exemplo, em uma central de atendimentos, robôs são usados como assistentes de usuário. Eles são instalados nas estações de trabalho do operador e são acionados por operadores humanos sob demanda.
- Permitir a modularização de robôs criados previamente na solução, para a integração/utilização desses robôs em fluxos de trabalhos maiores;
- Possuir integração com framework de segurança capaz de garantir a seguridade dos dados sensíveis armazenados na solução;

- Fornecer interface para desenvolvimento de processos automatizados sem a necessidade de utilização de nenhuma linguagem de programação (No-code/Low-code), sendo possível executar testes funcionais do processo, sempre que necessário.
- Fornecer interface web de administração dos robôs, processos, pacotes, filas, regras de alertas e parâmetros;
- Possuir capacidade de gerenciar a automação assistida e autônoma podendo exibir os robôs autônomos e assistidos e o trabalho que eles executam, de modo a governar, gerenciar e supervisionar os robôs de um local centralizado.
- Possuir a capacidade de agendamento da execução de um processo automatizado;
- Prover a capacidade de desenvolvedores, usuários de suporte, gerentes e administradores poderem utilizar um aplicativo centralizado do RPA para iniciar e interromper um processo de bot, executar habilidades, exibir o código de hash de uma versão de pacote e desativar um processo de bot , pacote e os robôs.
- Possuir painel centralizado com capacidade de gerenciar itens da fila de trabalho com mais eficiência, podendo exibir os itens da fila de trabalhos, marcá-los como concluídos e reatribuir um item da fila de trabalhos.
- Permitir, depois que um processo de bot está publicado, em manutenção ou em um estágio descontinuado, verificar o status de todos os estágios do ciclo de vida para os processos de bot assistidos e autônomos.
- Permitir criar uma habilidade para fornecer automações pré-criadas e integrações plug-and-play para os processos de negócios complexos, podendo criar um projeto de tipo de habilidade que pode ser usado em outras automações.
- Possuir a capacidade de implementação de segurança para os robôs sem supervisão humana, podendo-se gerar certificados de autenticação para esses robôs, na própria solução;
- Permitir implantar, monitorar, gerenciar, medir e verificar a conformidade de todos os robôs em um nível empresarial, ou seja, várias áreas e/ou departamentos, a partir de um local centralizado.
- Gerenciar os metadados que incluem robôs, pacotes, processos, filas, programações, parâmetros compartilhados e alertas.
- Disponibilizar as análises dos robôs em gráficos, apresentando no mínimo: Resumo do processo de bot, seção de utilização do robô, resumo dos trabalhos e processos executados, resumo das filas de tarefas dos robôs, principais áreas de negócios executando robôs, painel do licenciamento contando robôs autônomos e assistidos.
- Possuir modelos de processos automatizados para cópia e reuso, caso necessário;
- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita a contagem de número inteiros, gerando contadores para incremento ou decremento de números.
- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita configurar o e-mail a ser usado para executar as ações de e-mail padrão, como enviar e-mail, marcar e-mails como lidos e recuperar e-mails, ler o último e-mail recebido na caixa de entrada de um objeto de e-mail, retornar os detalhes do e-mail e salvar anexos;

- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita validar e efetuar a leitura de log, escutar de diferentes origens e gravar eventos e mensagens personalizadas no Microsoft Event Viewer.
- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita executar várias ações em servidores FTP. Por exemplo, carregar ou baixar arquivos de um servidor FTP. O conector deve fornecer vários métodos que executam essas ações como parte de uma automação.
- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita conectar ao Internet Explorer (IE) permitindo que execute várias ações no navegador IE, aplicativos e seus elementos de tela no navegador. Por exemplo, executar um método para abrir um site, clicar em um botão, identificar elementos em tela, capturar caixa de diálogo de contexto e etc.
- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita conectar ao Microsoft Excel permitindo que execute várias ações em um documento do Microsoft Excel como parte de um Robotic Process Automation. Por exemplo, abrir um arquivo Microsoft Excel e exportá-lo para o formato PDF, capturar dado da planilha (célula, range, nome da planilha, tipo de gráfico, cor, nome da coluna, caminho do arquivo, fórmula e etc).
- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita conectar ao MS Windows permitindo que execute várias ações nos aplicativos Windows e seus elementos de interface do usuário, como fechar janela do aplicativo ativo, recuperar o ID da janela ativa do aplicativo, obter nome da janela ativa e definir o diretório de trabalho do aplicativo para todas as operações de arquivo por meio do aplicativo a serem executadas no diretório especificado.
- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita conectar ao Microsoft do Word permitindo que execute várias tarefas em um documento do Microsoft Word por meio de seus métodos. Por exemplo, adicionar um rodapé a um documento, adicionar cabeçalho, copiar e colar células, obter e excluir tabela, exportar para PDF, obter texto, adicionar coluna, linhas e demais itens em tabelas, inserir imagem ou texto, salvar e etc.
- Na interface de desenvolvimento dos projetos dos robôs, deve apresentar método que permita conectar ao Microsoft Outlook permitindo automatizar ações padrão no aplicativo Microsoft Outlook como parte de uma automação. Por exemplo, automatizar o envio ou a resposta a e-mails.
- Fornecer por padrão, interface web com visão unificada da situação atual de execução dos processos, robôs e filas;
- Possuir funcionalidade capaz de capturar a navegação do usuário através do Browser e, através dessa captura, salvar um processo que poderá ser atribuído a um robô posteriormente;
- Possibilitar a exportação dos processos criados em arquivos XML;
- Possibilitar a criação de credenciais de forma unificada, para utilização dos processos nos acessos aos computadores da rede;
- Possuir a capacidade de criação de grupos de acesso para segregar os acessos e permissões nos processos;
- Possuir log contendo informações das fases de execução dos processos;

- Possuir a capacidade de criação de variáveis globais, permitindo assim a utilização dessas variáveis em mais de um processo;
- Possuir a capacidade de criação de regras de alerta de notificação para robôs e processos agendados;
- Possuir funcionalidade capaz de incluir nos processos tarefas capazes de transformar os dados, possibilitando o desenvolvimento de scripts de transformação dos dados nas linguagens VB.NET, C# e Javascript;
- Possibilitar a execução de robôs com certificados para que não dependam de usuários em serviços de diretórios como AD e etc;

a. CENTRO DE AUTOMAÇÃO

- Possuir módulo para controlar ciclos de vida de automação (RPA) de vários fornecedores de ponta a ponta e em um só lugar. Agregando painéis em tempo real, métricas, gerenciando e medindo a integridade da automação e evitando falhas de automação em vários fornecedores.
- Deve ser capaz de se integrar a qualquer aplicativo RPA de terceiros que não o da solução contratada, usando API, permitindo que se crie os seguintes tipos de eventos na sua plataforma:
    - Robôs - agentes de software que executam um processo de bot. Os robôs de RPA podem ser executados com ou sem supervisão.
    - Processo: instância de um RPA em um robô específico. Ele é responsável por executar trabalhos. Para identificar exclusivamente um processo, deve ser possível especificar a ID do processo e o ID do robô.
    - Execução: tarefa específica a ser executada em um processo do robô, como copiar informações de um recurso e copiá-las para outro, como ao copiar informações de e-mails para uma planilha.
- Permitir que se crie uma meta de automação para gerenciar o andamento e estimar os resultados de uma solicitação de automação, permitindo associação de objetivos e metas.
- Permitir que as solicitações de automação possam ser criadas enviando uma solicitação de automação usando o formulário do Catálogo de Serviço da solução.
- Permitir que se modifique o layout do formulário de solicitação de automação do Catálogo de Serviços da solução para personalizá-lo de acordo com os requisitos do CONTRATANTE.
- Permitir criar tarefas de automação para gerenciar com eficiência as atividades associadas à solicitação de automação.
- Permitir exibir uma lista de robôs disponíveis para fins de referência.
- Permitir gerenciar e revisar suas execuções de automação, incluindo seus estados, para garantir que elas estejam no caminho certo.

*20. **DEVOPS***

- Integrar com ferramentas de monitoração viabilizando a abertura e fechamento de registros de incidentes de forma automática, conforme estado de eventos e integrar com ferramentas de *Application Performance Management* – APM.
- Possuir plataforma DevOps que deve fornecer insights de dados, facilitar o processo de mudanças e aumentar a visibilidade do ambiente DevOps usando um único sistema.
- Permitir a coleta dados em todo o conjunto de atividades do ciclo de vida para fornecer visibilidade para que as equipes DevOps possam controlar o processo de ponta a ponta (planejar, desenvolver, construir, testar, implantar e operar), minimamente integrando-se aos seguintes aplicativos DevOps: Azure DevOps Boards, Jira, Azure DevOps Repos, GitHub, Bitbucket Server, GitLab SCM e Azure DevOps Pipelines, Jenkins e GitLab CI/CD
- Permitir extrair e visualizar a progressão do estágio do pipeline e os detalhes de cada aplicativo (GitLab SCM, Azure DevOps Pipelines, Jenkins e GitLab CI/CD) no Módulo DevOps.
- Permitir que o Módulo DevOps acesse as ferramentas listadas com as credenciais corretas e obter a URL do webhook para retorno de informações, funcionando em duas vias.
- Permitir que o Módulo DevOps descubra, automaticamente, todas as informações da ferramenta, como: Planos de aplicação da ferramenta de planejamento, repositórios de ferramentas de codificação, tarefas e pipelines de ferramentas de orquestração.
- Permitir configurar a URL do webhook na ferramenta de origem para que as notificações da aplicação integrada possam ser recebidas pelo Módulo DevOps.
- Permitir importar todos os dados da ferramenta e permitir o rastreamento, sendo minimamente: dados do item de trabalho do plano de aplicativo da ferramenta de planejamento (e versões do plano, recursos), ramificação do repositório de ferramentas de repositório de códigos e dados de commit, dados de execução de tarefas da ferramenta de orquestração.
- Permitir criação de política de repetição de requisição HTTP para os aplicativos de integração para repetir automaticamente as solicitações com falha quando uma etapa encontrar um problema de conexão, como uma falha de rede ou limite de taxa de solicitação.
- Permitir que todas as conexões de ferramentas de planejamento, codificação e orquestração suportem o modo de configuração manual, por exemplo, quando o usuário não tiver privilégios de administrador em uma das ferramentas a serem integradas para configuração do webhook.
- Permitir que seja feita a associação do Commit na ferramenta de gestão de código por meio de comentários na plataforma de gestão de código Git, informando a história de usuário utilizando por exemplo: Commit da história #STRY00048 em produção.
- Permitir criar solicitações de mudança no módulo de ITSM automaticamente em qualquer estágio para implantações que requerem controle de mudança no ambiente.
- Permitir ao Módulo DevOps a criação automática de solicitação de mudança em seu pipeline utilizando políticas de aprovação de mudança para automatizar a aprovação sob certas condições.
- Permitir a criação de mudanças no Módulo DevOps no mínimo para: Azure, Jenkins e GitLab.
- Permitir que as solicitações de mudança sejam automaticamente aprovadas para mudanças de baixo risco, quando o risco e o impacto calculados estão abaixo dos valores limite (definido por formulário para o pipeline).

- Permitir que os valores calculados de risco e impacto quando estiverem nos valores limite ou acima, a mudança normal permaneça no estado Avaliação, ou similar, até ser aprovada manualmente.
- Permitir que Políticas de Aprovação de Mudanças sejam mapeada para a Política de Mudanças DevOps integradas ao módulo de ITSM.
- Permitir visualizar, graficamente, o pipeline extraído das ferramentas como Azure, Jenkins etc, em formato semelhante ao da ferramenta de origem.
- Possuir painéis de análise de performance para obtenção do ambiente DevOps com no mínimo: Total de alterações DevOps enviadas anualmente, tempo médio para fechar as mudanças de DevOps nos últimos 30 dias, Taxa média de sucesso de mudança do DevOps para solicitações de mudança nos últimos 30 dias, volume de solicitações de mudança criadas para DevOps nos últimos 7 dias, Número de solicitações de mudança que não foram fechadas para cada pipeline, Número de alterações DevOps aguardando aprovação por intervalo de datas, Número de alterações não DevOps aguardando aprovação por intervalo de datas, Número de implantações de produção bem-sucedidas em um mês, Tempo médio de resolução para um incidente causado por uma mudança de DevOps nos últimos 30 dias.
- Permitir visualizar os resultados do teste de compilação para ver quais testes foram aprovados ou reprovados na interface do módulo de DevOps.
- Permitir obter uma visão rápida de como tudo está conectado para ver exatamente o que está acontecendo com o pipeline e quando, podendo acessar a UI do Pipeline e ver rapidamente os commits, os committers e outros detalhes da solicitação de mudança em um só lugar.
- Permitir usar políticas de aprovação de mudança para automatizar a aprovação de solicitação de mudança no módulo de ITSM para continuar a implantação por meio do pipeline de execução automaticamente.
- Permitir que integrações possam ser criadas pelo usuário do Módulo DevOps com ferramentas adicionais de planejamento, codificação e teste não incluídas nas integrações fornecidas com o Módulo DevOps padrão.
- Permitir criar um subfluxo para coletar e transformar dados da ferramenta que está sendo integrada, sem a necessidade de código (no code/low code).
- Permitir criar configurações de rotação de banco de dados e limpeza de tabela para os dados importados no Módulo Devops, não comprometendo dessa forma a performance.
- Deverá permitir a coordenação de atividades de backend através da possibilidade de integração com múltiplas ferramentas e processos (ex.: gerenciamento de acesso para solicitações de acesso, sistemas de gerenciamento de portfólio para solicitações de projetos ou melhorias, sistemas externos à TI como ordens de serviço de manutenção e instalações prediais);
- Plug-ins nativos para as seguintes ferramentas APM (Application Performance Monitoring):
    - Datadog.
    - Dynatrace.
    - Cisco (AppDynamics).
    - New Relic.

- Plug-ins nativos para as seguintes ferramentas de monitoramento:
    - Zabbix.
    - VMware vRealize Operations e Wavefront.
    - Splunk.
    - Oracle Enterprise Manager.
    - Microsoft System Center Operations Manager (SCOM).
    - Microsoft Azure Monitor.
- Deve possuir conector ou gateway que permita a integração a redes de telefonia PSTN (Public Switched Telephone Network) e VoIP por computador, permitindo que o aplicativo de atendimento aos usuários ofereça suporte a chamadas telefônicas de entrada e saída (inbound and outbound telephone calls). Uma vez configurada esta integração, é possível aos atendentes:
    - Realizar chamadas para algum dos números telefônicos de contato de usuários clientes, de fornecedores ou pontos focais de equipes de atendimento.
    - Receber uma chamada de qualquer terminal de telefonia convencional, celular ou VoIP (SIP).
    - Transferir uma chamada para outro atendente dentro do sistema.
    - Ativar ou desativar, na chamada, o modo mudo.
    - Definir se está disponível para contatos telefônicos ou não.
- Deve permitir a integração com as seguintes fontes ou protocolos de identidades e diretórios:
    - Microsoft Active Directory.
    - Azure Active Directory.
    - Bancos de dados via ODBC ou JDBC.
    - Open Lightweight Directory Access Protocol (Open LDAP).
    - Secure Lightweight Directory Access Protocol (SLDAP).
    - Security Assertion Markup Language (SAML) 2 e superiores.
    - Provedores OAuth 2.0 e superiores.
- Deve suportar a integração com servidores de e-mail via protocolo SMTP e IMAP, tanto para leitura como para o envio de mensagens.
- Deve permitir integrações com outras ferramentas por meio de execução de comandos em CLI, scripts e macros.
- Deve integrar-se nativamente, no mínimo, às seguintes ferramentas e protocolos de comunicação e colaboração:
    - Microsoft Teams.
    - SMS gateway.

- WhatsApp for Business.

- Deve permitir a migração de registros de solicitações mantidas nas ferramentas em uso pelo contratante por meio de um processo não manual (ou seja, lote, script, arquivo texto etc.).
- Deve ser possível a integração com sistemas ITSM de terceiros para abrir tickets automaticamente, rastrear seu status e gerenciar seu ciclo de vida.

21. DESCOBERTA DE ITENS DE CONFIGURAÇÃO (ITOM)

- Prover a descoberta de toda a infraestrutura, Itens de Configuração e seus respectivos relacionamentos de forma automática sem agentes instalados em ambiente *on-premises* ou em nuvem, para a população do BDGC.
- A descoberta deve permitir encontrar computadores/notebooks, servidores, impressoras, uma variedade de dispositivos habilitados para IP e as aplicações executadas neles, atualizando, se necessário, o BDGC com os dados que coleta.
- Prover a descoberta dos serviços de negócio "*top down*" e criar um mapa abrangendo todos os dispositivos, aplicações e perfis de configuração referente a estes serviços de negócio.
- A descoberta *top-down* deve permitir que o Mapeamento de serviço usado para localizar e mapear ICs que fazem parte dos serviços de negócios, como um serviço de e-mail. Por exemplo, a descoberta de cima para baixo (*top-down*) pode mapear um serviço de negócios do site da Web, mostrando os relacionamentos entre um serviço de servidor da web Apache Tomcat, um servidor Windows e o banco de dados MSSQL que armazena os dados para o serviço de negócios
- Possuir uma base única de gerenciamento de ativos e itens de configuração podendo gerenciar tais itens independentemente da metodologia ou processo e que permita sua população de forma automatizada e manual.
- Prover a informação de configuração do serviço na linha do tempo, possibilitando a visualização das diferenças entre o período atual e a data selecionada.
- Permitir a fácil visualização no mapa do impacto causado por eventos e/ou problemas associados que lhe causam impacto, permitindo a rápida visualização dos ICs e seus relacionamentos em estrutura de árvore de serviço.
- Permitir inventariar e mapear serviços de negócio hospedados em nuvem privada, pública, híbrida ou em recursos locais.
- Permitir a configuração de informações de cada tipo de ativo, permitindo adicionar e remover campos de informações de gestão do ativo.
- Permitir o acesso seguro e controlado à base de dados do gerenciamento da configuração.
- Permitir o armazenamento do histórico de mudanças dos IC para fins de auditoria.
- A solução deve implementar e seguir corretamente o fluxo de Gerenciamento de Configuração e Ativos de Serviço conforme prescrito na biblioteca ITIL V4 e deve permitir no mínimo:
    - Manter atualizadas características da configuração de ativos;
    - Manter atualizadas características da configuração de componentes de ativos;
    - Manter atualizados os relacionamentos entre ativos com possibilidade de representação gráfica destes relacionamentos;

    - A representação gráfica do relacionamento entre ativos deve permitir o *drill down* de informações, para obter detalhes do ativo, seus relacionamentos, seus usuários, ou seus componentes;
- A solução deve oferecer a capacidade de carga a partir de fontes externas e extração por outras aplicações de informações do CMDB, para população de dados e consultas;
- A solução deve permitir a criação manual de itens de configuração a partir de modelos pré-definidos *(templates)*, para agilizar o preenchimento de informações e criação de relacionamentos entre ativos;
- Permitir a criação livre de itens de configuração, para o registro e controle de itens que não se aplicam sob um padrão;
- Permitir a criação manual de itens de configuração para aqueles tipos de ativos que não sejam eletronicamente inventariáveis;
- Permitir o complemento de informações de um ativo, que não puderam ser eletronicamente inventariadas ou que não estavam disponíveis;
- Permitir também o cadastro de itens não técnicos, como mobiliário, equipamentos que não pertençam à TI, dentre outros, sem prejuízo à capacidade de relacioná-los com outros itens, técnicos ou não, para a representação gráfica dos relacionamentos;
- A solução deve permitir o gerenciamento de todo o ciclo de vida do ativo, de acordo com as definições da biblioteca ITIL V4 ou conforme necessidades.

g. GERENCIAMENTO E INVENTÁRIO DE CERTIFICADOS

- Permitir a descoberta, inventário e gerenciar proativamente todos os seus certificados TLS da organização.
- Permitir que o processo de descoberta verifique automaticamente os certificados em portas específicas (portas padrões como 443, 8443, 636, etc e cadastro de outras) por meio de seus agendamentos de descoberta baseados em CI existentes.
- Permitir criar agendamentos de descoberta para verificar URLs específicas.
- Permitir o cadastramento do certificado como um item de configuração no CMDB e manter informado sobre expirações iminentes.
- Deve automaticamente criar tarefas de certificado por meio de fluxos para renovar certificados expirados.
- Deve automaticamente criar incidentes para certificados já expirados.
- Solicitações de certificado e incidentes devem ser criados automaticamente quando certificados próximos a vencer e expirados são descobertos.
- Solicitações e incidentes de renovação de certificados devem ser criados automaticamente quando os certificados estão prestes a expirar ou expiraram.
- Solicitações podem ser criadas manualmente usando o Catálogo de Serviços.
- As tarefas para renovações de certificados devem ser geradas automaticamente 60 dias antes da expiração e deve permitir parametrização da quantidade de dias.
- Se já houver uma tarefa de certificado para o certificado atual, nenhuma tarefa adicional deverá ser criada.
- Para tarefas e incidentes de certificado de renovação, vários campos devem ser pré-preenchidos automaticamente com base no IC do certificado (validade, número de série, subject common name etc).
- Permitir que os Itens de Configuração criados a partir dos certificados identificados possam ser priorizados em relação a importância do certificado.
- Permitir descobrir a cadeia de certificados para cada uma das URLs no lote e armazenar as informações da cadeia de certificados para cada certificado.

- Permitir a descoberta diretamente na CA Authority utilizando chamadas de API REST de acordo com o padrão da CA específico (minimamento para GoDaddy, DigiCert, Entrust, Sectigo Certificate Authority).
- Deverá permitir o cadastro das credenciais junto a API da CA (API Key/Secret Key etc).
- Permitir importar os certificados SSL em massa para economizar tempo e recursos utilizando arquivo .xlsx contendo informações como: root issuer, issuer, subject comman name, issuer common name, fingerprint, issuer distinguisged name, validade, algoritimo de assinatura, tamanho da chave e estado (exemplo: instalado, revogado, retired ou outros).
- Permitir a descoberta de certificado por meio da importação de arquivo de certificado armazenado em uma pasta de um servidor na rede, minimamente nos seguintes formatos: .cert, .pem, .txt e .der.
- Permitir que os certificados descobertos sejam relacionados com servidores, aplicativos ou serviços de negócio existentes no CMDB, identificando todos os locais onde os certificados estão instalados.
- Possuir painéis de gerenciamento de certificados exibindo um resumo de todos os certificados e tarefas de certificados criadas.

h. GESTÃO E RELATÓRIOS DE REGRAS DE FIREWALL

- Permitir descobrir e fazer um inventário de todas as políticas de segurança de firewall, dispositivos de firewall, grupos de dispositivos de firewall e informações do gerenciador de firewall e mantê-las no CMDB.
- Permitir consultar e realizar auditoria de políticas de segurança de firewall por um período de tempo específico.
- Permitir durante processo de descoberta, todos os firewalls junto com suas políticas, versões de firmware e outros atributos de hardware.
- A descoberta deve ocorrer fazendo uso de integração com APIs REST e SNMP para conectar a plataforma de descoberta ao inventário de firewall e às políticas de firewall.
- Permitir configurar uma auditoria aleatória para medir a segurança na política e propriedade do firewall, bem como realizar auditorias proativas regularmente.
- Permitir a disponibilização de painéis Dashboards agrupando segurança e riscos vinculados às tarefas, alterações e solicitações. Permitir acompanhar o progresso e gerenciar o ciclo de vida geral do inventário de firewall neste painel unificado, podendo validar histórico de auditorias e acompanhar o andamento das tarefas atuais e das não concluídas.

i. MAPEAMENTO AUTOMÁTICO DE SERVIÇOS

- Permitir criar e manter o mapa de serviço que apresenta os componentes de TI e suas dependências com uma abordagem de cima para baixo (*Top-Down*);
- Permitir verificar o tráfego de rede, descobertas e mapas de relacionamento entre os componentes, mesmo que dinâmicos, ou em ambientes virtualizados.;
- Possuir capacidade de mapear continuamente as mudanças no ambiente para atualizar os mapas de serviços em tempo real, provendo uma fotografia em tempo real do impacto no serviço de forma a identificar problemas proativamente.

22. GERENCIAMENTO DE EVENTOS E ALERTAS

- Consolidar, correlacionar e analisar eventos de todas as ferramentas de monitoração para apresentar em tempo real informações sobre a saúde dos serviços de negócio e sua infraestrutura;
- Possuir separação entre eventos e alertas. Eventos serão as notificações informadas por uma ou mais fonte externa/ferramentas de monitoração (Zabbix, Nagios, Openview, vCenter, Trap SNMP, email, etc) as quais indicam algo que ocorreu no ambiente que necessita ser registrado, como logs, warning ou erro. Alertas serão um ou mais eventos que serão destacados que possuem relevância para ser tratados e gerenciados, pois requerem mais atenção.

j. EVENTOS

- Deve integrar, nativamente, com as ferramentas de monitoração de mercado utilizando os seguintes tipos de conexão: REST API, SNMP ou JavaScript customizado.
- Possuir a função de criar um servidor intermediário para conectar os monitores à aplicação de gerenciamento de eventos, possuindo as formas de pull (coletar os eventos de alguma fonte) ou push (listeners).
- Possuir interface para criar conectores, porém já possuir conectores nativos, no formato pull, para: Microsoft SCOM, Nagios, vCenter, vRealize e Zabbix).
- Possuir conectores nativos, formato push (listener), para: AWS, Azure, SNMP Traps, Email.
- Possuir uma arquitetura que permita separar os eventos recebidos, classificar e identificar para quais dos eventos serão criados Alertas que realmente necessitam de atenção do time de operação. Evitando excesso de trabalho no volume de eventos das diversas fontes de informação.
- O evento original deve ser mantido para revisão ou remediação.
- Deve possuir pelo menos os seguintes campos em um evento: Fonte do Evento, Nó que ocorreu o evento (FQDN, endereço IP ou endereço MAC), Tipo do Evento, Recurso relevante (ex. Disco, CPU, processo, serviço, Mensagem chave, Tipo do IC, Severidade, estado do evento (pronto, processado, ignorado ou com erro), estado de resolução (novo ou fechado), hora/minuto e dia que o evento ocorreu, Indicador que um alerta foi criado com o número do alerta, descrição do evento, informações adicionais do evento, log de processamento do evento.
- Possuir mecanismos para ver todos os eventos que estão vindo de fontes de monitoração ou de outras fontes, como Traps SNMP e email.
- Permitir um mapeamento de-para dos campos do evento de origem para a base de evento do sistema, permitindo padronizar diversos tipos de fontes de eventos.
- Possuir mecanismo nativo dentro da solução para gerar eventos e poder realizar testes, sem a necessidade de criar scripts e de forma amigável.
- Permitir criar regras de eventos para gerar alertas. Cada regra de evento de possuir:
    - Informações sobre a Regra: Nome, Fonte do evento, Ordem dessa regra frente a todas outras regras e descrição);
    - Filtro em que essa Regra do Evento será aplicada (Condições que serão verificadas para que seja aplicada essa regra a esse evento);
    - Quais as informações serão utilizadas para transformar este evento e compor alerta. Deverá permitir alterar e criar novas.

- Possuir mecanismo que gerencie "*storm*" de eventos e eventos intermitentes, pelo menos com seguintes campos: Tipo de storm, número de ocorrências e duração em segundos.
- Deverá permitir criar uma regra de evento diretamente de sobre um evento já existente, trazendo todas as informações para a criação da regra.
- Por padrão deverá associar um evento a um IC, porém deve permitir ajustar a regra para sobrepor esse padrão para associar um evento a um alerta de um tipo de IC diferente.
- Permitir a configuração de deduplicação de eventos.
- Quando um evento passar por uma regra de evento que deverá gerar um alerta, um alerta deverá ser criado. Cada alerta deverá possuir um número identificador único e um workflow específico para seu ciclo de vida;
- As descobertas devem ser executadas através dos protocolos dos componentes que serão mapeados. Ao menos os seguintes protocolos devem ser contemplados:
    - Criar relacionamentos *upstream e downstream* entre os componentes interdependentes;
    - Descobrir e mapear relacionamentos do tipo virtual-virtual e virtual-físico;
    - Descobrir e mapear relacionamentos em ambientes virtualizados instalados, como Vmware;
    - Descobrir e mapear relacionamentos onde os componentes estão dentro de um único host virtual ou espalhados por vários hosts virtuais;
    - Descobrir e mapear todos os componentes e relacionamentos de TI que suportam um serviço, incluindo aplicativos, middleware, servidores, storage e equipamentos de rede;
    - Descobrir e mapear todos os componentes e relacionamentos de TI que suportam uma aplicação, incluindo outras aplicações, servidores, middlewares, storage e equipamentos de rede;
    - Descobrir os componentes de TI individualmente, bem como todas as conexões diretas entre componentes adjacentes;
    - Descobrir, documentar e mapear dependências de aplicações instaladas em Docker e Kubernetes, suportando as APIs dessas tecnologias;
    - Descobrir, documentar e mapear dependências de recursos utilizados pelo CONTRATANTE nos serviços de nuvem da AWS, Azure, Google, através das APIs desses fornecedores.
- Disponibilizar filtros para cadastros manuais de componentes que devem ser ignorados nos processos de descoberta;
- Disponibilizar graficamente mapas com toda topologia dos serviços identificados;
- Disponibilizar interface para cadastro manual de serviços, componentes e transações;
- Fornecer filtros para seleção das informações que serão coletadas durante as ações de descoberta;
- Fornecer templates customizáveis para realização de descobertas pelos seguintes critérios:
    - Gerar mapas atualizados com a identificação dos componentes e os relacionamentos que suportam os serviços;
    - Identificar graficamente nos mapas os componentes que impactam na qualidade e disponibilidade dos serviços;
    - Identificar portas de entrada e processos utilizados em servidores e que tenham relação com os serviços mapeados; e
    - Ignorar de forma proativa componentes e relacionamentos que não fazem parte do serviço.

- Manter os mapas de serviços atualizados periodicamente, bem como as informações das aplicações e de todos os componentes de rede. O período de atualização pode ser customizável;
- Validar periodicamente as relações de dependência das aplicações com componentes de rede e de infraestrutura;
- Montar mapas de dependências e de topologia, automaticamente, a partir do cadastro de pontos de entrada como URLs, componentes, serviços e transações;
- Permitir a descoberta e obtenção de informações sobre softwares ou outros componentes não suportados nativamente através da customização e extensão de sensores;
- Permitir o mapeamento manual de componentes e serviços;
- Permitir o uso de tags personalizadas para os componentes descobertos;
- Realizar a descoberta de forma híbrida, com e sem o uso de agentes;
- Registrar as seguintes métricas para os relacionamentos entre todos os componentes descobertos e mapeados:
    - Registrar informações de IP e subnets associadas aos componentes descobertos e mapeados;
    - Usar aprendizado de máquina para detectar automaticamente os componentes e detectar anomalias nos serviços mapeados.

k. GESTÃO/CORRELACIONADOR DE ALERTAS

- Um Alerta dever possuir, pelo menos, os seguintes campos: Número, Fonte do Evento, Nó que ocorreu o alerta, Tipo, Recurso (Ex. CPU, Disco 1, etc), item de configuração, Atividade (ex. Incidente, Mudança ou Problema), nome da métrica, descrição, Severidade, estado (aberto, reaberto, intermitente ou fechado), Reconhecido (Acknowledged), manutenção, dia/hora que foi atualizado, alerta pai, contagem de eventos, instancia fonte, nome do usuário que fez a última atualização, alertas correlacionados;
- Para cada alerta dever possuir além dos campos indicados, informações adicionais com as seguintes abas: Serviços impactados, histórico, atividades (registros dos trabalhos realizados);
- O Alerta deve possuir a função de seguir um alerta (following), para seu acompanhamento e colaboração na sua resolução;
- Possuir a função de resposta rápida, permitindo abrir uma janela que possua as atividades de executar uma remediação ou abrir alguma aplicação específica;
- Possuir integração nativa com CMDB, possuindo a capacidade de reduzir os alertas irrelevantes, removendo informações duplicadas, sem perda de contexto ou de criticidade, facilitando para os analistas responder primeiro aos alertas de alta prioridade;
- Possuir painéis intuitivos de saúde que apresentem o estado de todos os serviços de negócio, permitindo à equipe de gerenciamento de eventos realizar o “drill down” em mapas de serviços interativos para determinar a causa raiz do problema;
- Possuir pesquisa contextual na base de conhecimento para identificar artigos que possam ser utilizados para orientar a resolução ou atividades para um Alerta;
- Possuir a funcionalidade de responder automaticamente a um alerta, por meio de configuração de regras, para determinar a resposta adequada a um alerta (por exemplo: Abrir um incidente, base de conhecimento, abrir uma tarefa específica, variações de remediação, entre outras);
- As regras devem ser executadas toda vez que um alerta é aberto ou atualizado, baseado em filtro de condições;
- Deve possuir pelo menos os seguintes subfluxos de remediação: marcar um alerta que já está reconhecido, mudar o alerta para “Em manutenção", fechar um alerta e criar um incidente;

- Permitir criar subfluxos de remediação customizados;
- Permitir que possa criar separação de domínios de alertas, o qual deve incluir a separação de dados, processos e atividades administrativas em grupos lógicos chamados de domínios;
- Possuir a capacidade de agregação de alertas e análise de causa raiz (RCA) com análise de alertas e agregação para serviços técnicos, serviços de aplicativos e grupos de alertas. Fornecer análise de causa raiz (RCA) para serviços de negócios no CMDB;
- Possuir funcionalidade de Agregação de Alerta, associando alertas similares, mas não necessariamente idênticos, baseado também em quão próximo foram os alertas, avaliando alertas passados, identificando padrões de relacionamento e utilizando técnicas probabilísticas para sugerir padrões;
- Permitir habilitar e desabilitar a identificação de causa raiz;
- Possuir funcionalidade de validar o gerenciamento de eventos após uma mudança de configuração ou uma atualização;
- Possuir pelo menos os seguintes papeis de operação de eventos: Administrador, Operador, Usuário e Integrador;
- Possuir SLA integrado que permita monitorar e gerenciar a qualidade dos serviços de negócio, por exemplo, contabilizar o tempo que um IC ou um serviço está no estado crítico até o momento que retorna para um estado aceitável;
- Permitir criar um grupo baseado em serviços técnicos, ou seja, um grupo dinâmico baseado em um critério comum (Ex. Servidores Web do Edifício Sede ou switches da Filial 1, etc);
- Deverá possuir mecanismo para determinar por quanto tempo um alerta ficará ativo, mesmo quando fechado, permitindo que caso um evento ocorra após um alerta fechado ele possa reabrir o alerta ou criar um novo alerta;
- Possuir funcionalidade de cálculo de impacto mostrando a magnitude de um alerta para um IC, serviços de negócio, serviços de aplicação e grupos de alertas, sendo baseado nos seguintes fatores: regras de impacto, número de alertas relacionados, histórico do IC afetado, relacionamento entre o IC e o Serviço (Aplicação ou de negócio);
- Deverá ter funcionalidade de excluir a análise de impacto quando o IC sob alerta possuir uma mudança programada de manutenção;
- Possuir um dashboard com a informação do status dos serviços de negócio e dos grupos de alertas, permitindo de forma rápida navegar de um para outro, ver apenas os serviços/grupos críticos, e poder pesquisar um serviço específico por meio de um campo de pesquisa. Nesse dashboard o tamanho do quadro que representa o serviço/grupo deverá ser de acordo com sua prioridade (relacionada ao Negócio, Severidade ou Custo);
- Possuir de forma gráfica, baseado em árvore de serviço, a situação de cada IC do Serviço. Permitindo que ao clicar em um item de configuração na árvore, apresente os alertas referentes ao IC no mesmo painel. Esse painel deve incluir o histórico de alerta desse serviço;
- Possuir uma console de alertas, que apresente os alertas e mostre se houve relacionamento entre um alerta e outros alertas, informando se esse agrupamento foi automatizado por uma regra, automaticamente pelo sistema, pelo relacionamento de CMDB ou Manual;
- Possuir mecanismo para criar regras de correlacionamento de alertas automáticas, definindo qual tipo de alerta será primário que quais serão secundários;
- Possuir forma de correlacionar manualmente alertas que são relacionados, apresentado os primários e os secundários;
- Apresentar um relatório de apresente o percentual de alertas que estão sendo correlacionados durante um período de tempo;
- Possuir abas de inteligência (Insights), para alertas, com pelo menos as seguintes informações: Alerta repetidos e fechados com a mesma chave de mensagem, Alertas similares, Incidentes com o mesmo IC, Problemas com o mesmo IC, Requisições de Mudanças com o mesmo IC;

- Possuir um ambiente configurado para o Operador.

23. GESTÃO E PROVISIONAMENTO DE NUVEM

- Permitir o uso em uma única interface para acessar recursos de nuvem, publicar ofertas de nuvem em um catálogo e gerenciar o uso desses recursos.
- O gerenciamento de serviços em núvem deve ser integrado a provedores de nuvem privada e pública, minimamente Amazon Web Services, Microsoft Azure e ofertas de VMware.
- Permitir atribuir funções de provisionamento e governança em nuvem a grupos de usuários e usuários individuais com base nas atividades e responsabilidades do usuário.
- Disponibilizar capacidade de manter uma conta de serviço como sendo um registro seguro na instância que vai armazenar a credencial e as informações de acesso para a conta de provedor de nuvem.
- Permitir criar rotinas de trabalho agendado para, regularmente, baixar os dados de faturamento do provedor.
- Permitir salvar os dados em uma tabela de custos e usar as informações para gerar relatórios.
- Permitir analisar toda a gama de custos associados aos ativos em nuvem e utilizar os dados para identificar oportunidades, economizar dinheiro e otimizar operações.
- Permitir chamar uma API do provedor de nuvem, AWS por exemplo, e usar as credenciais permanentes de uma conta mestre (da organização) para assumir a função de uma ou mais contas-membro.
- Permitir execução de Descoberta de Itens de Configuração, downloads de faturamento, provisionamento de máquinas virtuais e execução de operações de ciclo de vida em máquinas virtuais.
- Permitir usar os recursos de governança da plataforma para restringir o provisionamento de recursos de nuvem incluindo cotas e políticas.
- Permitir configurar fluxo de trabalhos de aprovação que deve ser usado depois que um usuário solicita um recurso de nuvem.
- Possuir Portal com consolidação e visualização de todas as atividades da nuvem.
- Disponibilizar no portal monitoramento da cota, custos, orçamento, ciclo de vida de eventos, stack-health e solicitações.
- Permitir que por meio do portal seja possível solicitar stacks do catálogo de serviços e rastrear as solicitações.
- Permitir que por meio do portal seja possível solicitar operações de ciclo de vida para stacks e recursos (por exemplo, parar, iniciar ou desprovisionar).
- Permitir que por meio do portal seja possível criar e rastrear incidentes dos serviços em nuvem.
- Permitir que ao solicitar um item no catálogo de serviços do Portal do usuário da nuvem o sistema provisione a stack automaticamente ou passe por um processo de aprovação.
- Permitir o controle do limite de cota e caso exceda para o usuário ou seu grupo de usuários, uma mensagem de erro será exibida ou o sistema acionará um fluxo de trabalho de aprovação com base em políticas.
- Permitir visualizar os limites de cota para ver quantos recursos foram consumidos pelo usuário e quantos pode provisionar com base nos limites de cota definidos para o usuário ou grupo de usuários.
- Possuir, minimamente, os seguintes tipos de recursos predefinidos no sistema e que podem ter limites de cota definidos para um usuário ou grupos de usuários: Contagem de Stack, Cotagem de VMs, Contagem de vCPUs, Contagem do volume de Storage, Contagem de recursos de rede (Network).

- Permitir que sejam executadas operações como Start/Stop, Deprovision e Execute Script nos stacks ou recursos da nuvem.
- Permitir que, por meio do portal, sejam visualizadas e gerenciadas as seguintes atividades de ações na nuvem: Solicitações realizadas, pedidos de mudança, incidentes para stack e seus recursos, tarefas de catálogo para quando uma solicitação de stack/recurso falhe, operações de arrendamento (lease) com operações que estão se aproximando das datas de término do aluguel, visualizar as chaves SSH existentes atribuídas ou gerar uma chave.
- Permitir que para provedores de nuvem que não possuem conexão nativa na plataforma possam ser realizados por meio de chamadas REST, como PUT, GET, POST e DELETE.

24. INTELIGÊNCIA OPERACIONAL

- Possuir a habilidade de capturar, explorar e analisar métricas operacionais que podem promover alertas, fazendo o mesmo aparecer na console de alertas e no dashboard de saúde dos serviços;
- Possuir mecanismo de análise de métricas para identificar desvios/eventos baseados em estatísticas de comportamento (Ex. Faixa de uso comum de CPU, faixa de uso comum de memória). Cada desvio do comportamento padrão deverá ser classificado como um evento anômalo;
- O mecanismo estatístico deve ser baseado em dados históricos e para cada métrica irá identificar o limiar superior e inferior;
- Cada evento anômalo deverá receber uma classificação (score) para demonstrar o grau de desvio;
- Possuir inteligência para identificar eventos anômalos e alertas anômalos, promovendo-os para alertas de TI caso esteja fora de um comportamento normal;
- Possuir um mapa de anomalias que mostra uma visão geral de anomalias por IC, apresentando o histórico de anomalias por item de configuração e cores desse histórico por score (grau de anomalia);
- Poder navegar por cada IC onde será apresentado a métrica coletada, o gráfico de comportamento do IC frente a métrica, as anomalias detectadas e o score (grau da anomalia) durante o tempo;
- Realizar a exclusão dos dados de métricas quando o IC estiver no modo de manutenção;
- Possuir uma funcionalidade para testar/avaliar a detecção de anomalias, podendo comparar os resultados do teste aos resultados esperados. Permitir fazer ajustes até que parâmetros atinjam um valor ótimo.

25. MANIPULAÇÃO DE DADOS E FORMULÁRIOS EXISTENTES E/OU NOVOS

- Possuir recursos gráficos de workflow interativos para criação de processos e rotinas operacionais, que permita operações como arrastar-e-soltar para o desenho dos fluxos de trabalho;
- Apresentar componente próprio para a modelagem gráfica e a automação de processos /fluxos de trabalho na solução;
- Permitir a criação dessas aplicações sem uso de código, para que toda a empresa possa desenvolver e atualizar novas aplicações integradas à plataforma;

- Possuir um estúdio integrado (IDE) para desenvolvimento de aplicações integradas a plataforma;
- O IDE deve possuir wizard que automaticamente crie as aplicações web e para aplicativo mobile;
- As novas aplicações deverão gerar tabelas independentes das outras aplicações. Isto é, independente de outros módulos da solução;
- Uma nova aplicação deverá conter no mínimo:
    - Tabelas;
    - Elementos gráficos de interface do usuário: Menus, Módulos, Listas e Formulários;
    - Arquivos da Aplicação: Regras de Negócio, Workflows, Ações gráficas (comportamento da tela ou de algum de seus componentes);
    - Integrações: Rest Web Services, JSON Data Format, SOAP, e outras possíveis integrações dessa aplicação;
    - Dependências: Tabelas de tarefas, Gerenciamento de SLA, Base de Usuários e seus respectivos acessos;
    - Permitir a construção, independente, de menus, telas, módulos para a mesma aplicação em dispositivo móvel (iOS e Android) em aplicativo fornecido nativamente pela solução;
    - Integrar com gerenciador de código fontes (GIT).
- Permitir que os desenvolvedores de aplicativos se integrem a um repositório de controle de origem (GIT), salvem e gerenciem várias versões de um aplicativo em ambiente desenvolvimento e/ou homologação;
- O sistema deve gerar um arquivo de controle de integridade (checksum) no repositório GIT para determinar se algum arquivo do aplicativo foi alterado fora da IDE de desenvolvimento. Quando o valor da soma de verificação do arquivo corresponde ao valor da soma de verificação atual, a integração ignora o processo de validação e sanitização. Quando os valores da soma de verificação não correspondem, a integração valida e limpa os arquivos do aplicativo como parte da operação de controle de origem;
- Permitir a automação de fluxos de trabalho de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código-fonte;
- Possuir ferramenta de criação de formulários com campos específicos de cada processo e fluxo de trabalho, a fim de personalizar a inserção de informações e controles de acordo com a necessidade do CONTRATANTE, sem a necessidade de programação ou alteração do código-fonte;
- Dispensar a necessidade de criação, de forma manual (usando scripts e programação), de tabelas, colunas e campos de banco de dados na solução, tornando estas atividades, quando necessárias, transparentes aos administradores da solução;
- Permitir a customização de menus, formulários, labels, automações de fluxos de trabalho e processos do CONTRATANTE, desenvolvidos e implementados na solução, permitindo a adequação às necessidades de uso de cada usuário, sem a necessidade de programação ou alteração do código fonte;
- Permitir a configuração de ciclos de vida específicos para fluxos de trabalho ou processo automatizados na solução;
- Permitir que os processos e fluxos de trabalho automatizados na solução possuam as mesmas funcionalidades nativas disponibilizadas na solução, como por exemplo: requisitos de usabilidade da lista de registros, citados nesta especificação técnica, ferramentas de

colaboração como chat e notificações, permitindo comunicação entre clientes e provedor de serviços, personalização de menus, regras de aprovação de fluxos, relacionamento entre processos, painéis e dashboards automatizados;

- Deve possuir o conceito de segregação de aplicações ou escopo de aplicações. Funções dentro do escopo só poderão ser acessadas ou manipuladas por aqueles que possuem acesso. Ex. Escopo de aplicações do Jurídico, Escopo de Aplicações do RH, etc;
- Possuir o conceito de hierarquia de escopo de aplicações;
- Possuir controle de dependências entre aplicações e privilégios de acesso;
- Permitir o compartilhamento de aplicações entre outras instâncias, sejam de desenvolvimento, teste ou em produção;
- Possuir mecanismo de teste automatizado de versões de aplicações, dentro da própria solução, o qual permite criar e executar testes automatizados para confirmar se a instância funciona após fazer uma alteração. Por exemplo, após uma atualização, durante o desenvolvimento do aplicativo ou ao implementar configurações de instância com conjuntos de atualização, permitir revisar os resultados do teste com falha para identificar as mudanças que causaram a falha;
- Permitir que sejam criados vários testes e fiquem disponíveis para futuros testes de upgrade ou mudanças nas aplicações, podendo ser reutilizados;
- Permitir pelo menos os seguintes testes:
    - Testar operações básicas de um formulário;
    - Fazer referência a um valor de uma etapa anterior em um workflow. Ex.: Testar atribuição a um campo de formulário do valor de uma variável de saída de uma etapa anterior;
    - Testar uma regra de negócio que deva ser aplicado em alguma etapa;
    - Testar o workflow de um processo.
- Após a configuração de uma aplicação permitir visualizar como a aplicação funcionaria no Tablet, em um computador ou em um dispositivo celular;
- Permitir que possa utilizar/estender as tabelas de uma determinada aplicação para criar outras aplicações;
- Permitir a comunicação em tempo real entre clientes, usuários e atendentes dos serviços;
- Incluir anotações nos registros da solução, possibilitando aos operadores atendentes publicar e tornar visível ou não para os usuários;
- Registrar toda comunicação entre usuários e atendentes dos serviços nos registros da plataforma;
- Permitir comunicação entre as partes interessadas e envolvidas nos processos e em atendimentos dos serviços;
- Possibilitar a inserção de notificações automatizadas em qualquer momento de fluxo de trabalho e processos automatizados na solução;
- Configurar as notificações automáticas de alertas para reiterar chamados técnicos abertos;
- Enviar notificações com informações contendo dados de qualquer parte do registro de um fluxo de trabalho ou processo implementado na solução;
- Enviar notificações baseadas em condições e eventos da solução.

26. GESTÃO DE ATIVOS (ITAM/SAM)

- Deverão ser fornecidos e instalados todos os módulos e/ou ferramentas para atender aos requisitos de Gestão de Ativos, que estará sempre associado ao processo de GERENCIAR

CONFIGURAÇÃO E ATIVOS DE SERVIÇO. As informações dos ativos devem ser integradas ao CMDB (*Configuration Management Database*, Base de Dados do Gerenciamento de Configuração);

- A solução deve permitir a gestão do inventário e licenciamento de software de forma integrada com os demais processos ITIL, suportando automação de workflows para a instalação de software mediante fluxo prévio de autorização e gerando relatórios de consumo que permitam a gestão e controle do uso das licenças;
- Deverá fornecer identificação única do Item de Configuração - IC;
- Deverá possibilitar o registro e atualização, de forma manual e automática, dos ICs e de seus atributos, permitindo o ajuste e adaptação (personalização) das informações do IC;
- Deverá permitir copiar um IC e seus atributos para criar um IC com uma identificação distinta;
- Deverá fornecer modelos de ativos e itens de configuração predefinidos e permitir a criação de modelos customizados, contendo campos pré-populados desses itens, como classificação, descrição, local, usuários, clientes e etc;
- Deverá fornecer funcionalidades de inventário dos ativos de TIC;
- Deverá permitir a associação e visualização da dependência lógica e física entre ativos e itens de configuração;
- Deverá permitir o controle de licenciamento de software, fornecendo uma visão do número total de licenças, o número de licenças em uso e a localização das licenças em uso de cada software;
- Deverá controlar o fim de vida de suporte das principais aplicações de mercado;
- Deverá permitir o gerenciamento de contratos e ordens de compra dos ativos e itens de configuração;
- Deverá permitir inventário de todas as estações de trabalho do CONTRATANTE, coletando informações parametrizáveis pelos administradores da solução. Após esse passo, deve possibilitar a abertura de ticket para qualquer alteração no ativo;
- Deverá permitir consulta das informações das estações com os parâmetros pretendidos;
- Deverá permitir associação de cada item de configuração a um grupo de usuários responsáveis, com permissão para editar seus atributos e relacionamentos;
- Deverá permitir a definição de permissões para cada campo do IC com, no mínimo, as seguintes opções: nenhum acesso, somente visualização e alteração;
- Deverá permitir o gerenciamento dos fornecedores dos ativos e itens de configuração;
- Deverá permitir visualizar facilmente a quantidade de requisições, incidentes, problemas e solicitações de mudanças relacionadas ao ativo ou item de configuração;
- Permitir que os dados sejam compartilhados de forma nativa e inteligente com outros aplicativos da plataforma;
- Permitir monitorar o pico de uso e definir parâmetros para evitar ajustes dispendiosos;
- Permitir que usuários consigam reservar ativos temporários e rastrear os estágios de atendimento e ajuda para prever os níveis de estoque;
- Fornecer suporte para gerenciamento de dispositivos móveis e tablets;
- Permitir suporte à autorização de devolução de mercadoria (RMA) com fluxos de trabalho automatizados;

27. GERENCIAMENTO INTEGRADO PARA GOVERNANÇA DE RISCOS E CONFORMIDADE (IRM)

- SEGURANÇA, RISCOS E CONFORMIDADE

- Deverá possuir solução integrada para Processos, Governança, Riscos e Compliance, que deverá permitir controle e gestão do cumprimento às normas internas da CONTRATANTE de regulamentações ou instruções normativas externas, visão integrada dos riscos da CONTRATANTE vinculados a processos, produtos, serviços ou canais, gestão de riscos operacionais e seus planos de ação;
- Solução que forneça aos usuários acessar qualquer legislação, normas, políticas e padrões e repositório de controles;
- A solução deverá possuir taxonomia comum e estruturada para identificar, medir e monitorar riscos, vulnerabilidades e ameaças mantendo em repositório centralizado;
- A solução deverá possuir taxonomia para processos de conformidade e para conteúdo de governança (políticas, padrões e controles);
- A solução deverá possuir workflow para governança das informações de controles associados aos processos;
- Permitir a gestão de riscos com a possibilidade de identificação, análise, avaliação, monitoração, proposição de controles e acompanhamento do tratamento dos riscos;
- Todas as características abrangidas na solução devem ser funcionalidades da solução ofertada, não havendo necessidade de instalação de outros produtos para criação de relatórios, painel, conectores, mobile, dentre outras características;
- Possibilitar a criação de painéis de indicadores que permitam a visualização completa de todas as soluções abrangidas pela plataforma (exemplo: Risco, Conformidade e etc.), e que permita a definição de controles de acesso diferenciados a cada painel;
- Possibilidade de registro em hierarquia para gerenciamento de estrutura organizacional;
- Possuir log completo de atividade de usuários dentro da plataforma com armazenamento irrestrito dessas informações;
- Manter trilha de auditoria referente às transações realizadas na solução;
- Permitir a inclusão, vinculação e parametrização para classificação de controles; marcação de controles-chave, tipo de controle, execução do controle; frequência do controle; dono do controle; resposta do controle; adequação do desenho do controle; registro de avaliação de efetividade; marcação de controles anticorrupção; marcação de controle preventivo de conflito de interesses;
- Permitir catalogar riscos;
- Permitir identificar, analisar, avaliar, monitorar, gerenciar e reportar riscos de maneira integrada com todos os demais módulos da solução, adequado a diversas categorias de riscos, como por exemplo: Capital, Compliance, Contágio, Crédito, Estratégia, Liquidez, Mercado, Reputação ou de Imagem, Legal ou Jurídico, Operacional, Cibernético e Socioambiental;
- Permitir a busca de informações em banco de dados externos;
- Permitir a avaliação periódica do risco, monitorando a sua evolução analiticamente e graficamente – emissão de relatórios, mantendo histórico das avaliações de cada processo;

- Manter o cadastro histórico e acompanhamento das alterações (revisionamento) dos mapas de risco;
- Permitir a elaboração e parametrização de mapas de riscos;
- Possibilitar a aprovação dos mapas de riscos ao final do planejamento e a revalidação dentro de frequência preestabelecida;
- Descrever e associar controles existentes (processos e normas internas) aos riscos identificados, fatores de riscos, causa ou origem, consequências ou impactos;
- Permitir a classificação do controle (ex.: manual ou automático; implementado, parcialmente implementado, não implementado; adequado ou não adequado);
- Permitir associar eventos ao controle como Incidentes, Problemas ou Workflows;
- Permitir alimentar atributos e informações adicionais ao controle, conforme a necessidade da CONTRATANTE;
- Permitir a visualização global de todos os riscos cadastrados, independente do componente ao qual estão relacionados;
- Permitir classificação de impacto e vulnerabilidade dos riscos mapeados, com agrupamentos por classificação por processos, tipo de risco, unidade responsável, dentre outros;
- Permitir pesquisar no repositório de riscos usando filtros como categoria, impacto, probabilidade, vulnerabilidade, classificação do risco; componente associado e etc;
- Permitir a atribuição de pesos para cada aspecto de risco avaliado;
- Permitir a elaboração de matriz de riscos (da companhia, por unidade, por processo);
- Permitir visualização da Matriz de Risco, de forma a agrupar quantitativamente as avaliações, bem como de identificar os riscos dentro dos quadrantes utilizados no método de avaliação;
- Selecionar a natureza e categoria do risco identificado;
- Identificar responsável pela identificação e análise do risco;
- Permitir a definição de responsáveis por processos, riscos, controles e planos de ação;
- Definir medidas saneadoras ou de mitigação de fragilidades (Planos de Ação) de acordo com padrão estabelecido;
- Permitir o acompanhamento da execução dos planos de ação;
- Identificar data de cadastro das informações, data de início e de conclusão das ações propostas;
- Permitir visualização do status da ação proposta de acordo com padrão estabelecido;
- Permitir o estabelecimento de alçadas para assunção a riscos e/ou autorização para prorrogações de prazos de planos de ação;
- Oferecer um painel customizável aos donos dos riscos e controles (1ª linha de defesa) com a situação dos riscos sob sua responsabilidade, bem como dos apontamentos e obrigações a ele imputadas;
- Permitir a criação de painel interativo e extração de relatório em que seja possível que os usuários vejam os controles sob sua responsabilidade e possam executar ações sobre eles (avaliações, testes e revisões);
- Definir prazos dos planos de ação em função da classificação do risco e/ou da assunção de Risco pela Alta Administração, com registro para cada caso;

- Permitir a criação de painéis dos indicadores de risco, de compliance e de controles internos;
- Permitir inclusão de novos eventos de risco pelos usuários;
- Permitir selecionar os eventos de risco para cada atividade do processo;
- Permitir que os eventos de risco possam ser associados a mais de um processo, mas que sejam analisados e documentados individualmente para cada processo;
- Permitir descrever as causas para cada evento de risco;
- Permitir descrever os efeitos/consequências para cada evento de risco;
- Permitir selecionar a categoria do risco identificado/selecionado;
- Permitir selecionar a natureza do risco identificado, a partir da categoria do risco;
- Medir o grau de exposição aos riscos e permitir acompanhar sua evolução;
- Permitir a notificação parametrizável para pessoa ou grupos no cadastramento de eventos;
- Permitir a identificação e cadastramento de riscos e ausência/deficiência de controles por todos os usuários com restrição de acesso por perfil, inclusive anonimamente;
- Permitir agendar avaliações periódicas dos riscos e controles, com notificação controlada pela solução e painel de visualização dos riscos e controles a serem revisitados.

- COMPLIANCE E INTEGRIDADE

  - Identificar, a partir da norma capturada, quais as normas que sofreram alteração em todo ou em parte;
  - Rastrear nas normas internas aquelas que fazem referência às normas que estão sofrendo alteração, gerando relatório para a área de compliance com o resultado do rastreamento;
  - Distribuir automaticamente as normas aos gestores de produtos, serviços e canais de forma a permitir o acesso ao conteúdo completo da mesma, permitir o registo de sua análise bem como o registro da manifestação de impacto;
  - Oferecer um repositório legislativo de fácil acesso aos usuários;
  - Permitir a integração da legislação aplicável aos negócios e dos instrumentos de controles vinculados (Normas Internas e Processos);
  - Permitir a criação de obrigações de compliance (requisitos e compromissos);
  - Permitir que a área de compliance tenha acesso as informações prestadas pelos gestores e possa questionar eventuais manifestações das áreas;
  - Permitir implementar em plataforma única, indicadores do Programa de Compliance e Integridade, por meio de módulos interativos e de fácil
  - compreensão, adequando os elementos e as ações correlatas estabelecidas no programa;
  - Permitir a análise e diagnóstico de processos críticos a par r da sua relação com riscos e eventos de perda associados, podendo ser realizado ainda o envio de notificações;
  - Permitir mapear os riscos de compliance e de integridade (riscos de fraude e corrupção) aos quais a empresa está sujeita;

- Permitir a avaliação periódica do risco de integridade, mantendo histórico das avaliações de cada processo;
- Enviar alertas e notificações periodicamente ou em casos de mudanças de cenários (novas legislações);
- Apresentar interface gráfica que permita a rápida visualização de vínculos diretos e indiretos entre administradores, colaboradores e fornecedores.

- MONITORAMENTO DE ATIVIDADES DE COMPLIANCE EM TEMPO REAL

    - Verificar cumprimento das recomendações/determinações de auditorias internas e externas, fiscalizações de órgãos reguladores apresentando Relatório de Pendências;
    - Mapeamento de violações de integridade com integração das denúncias e correição (canal de denúncias, investigações e punições).

28. GERENCIAMENTO DE DEMANDAS DE OUVIDORIA E CORREGEDORIA

- Executar testes de auditoria em cada elemento (pilar) do Programa de Compliance e Integridade;
- Permitir a criação/edição de normas corporativas;
- Permitir a inclusão de texto, controles e recomendações de normas internas;
- Permitir a aprovação da norma com alçada compartilhada;
- Permitir atualização das normas com envolvimento dos responsáveis.

29. GERENCIAMENTO DE PRIVACIDADE (Privacy Management – PRM)

- Possuir integrado nativamente ao módulo de Governance, Risk, and Compliance um segmento/módulo de Gestão de Privacidade para ajudar a proteger clientes, funcionários e fornecedores com soluções integradas de risco de privacidade de dados e gerenciamento de conformidade e privacidade por conceitos de design.
- O gerenciamento de privacidade deve gerenciar vários regulamentos de privacidade, como a LEI Nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), Geral Regulamento Geral de Proteção de Dados (GDPR), a Lei de Privacidade do Consumidor da Califórnia (CCPA) e a Lei de Privacidade Australiana.
- Possui capacidade de gerenciar estruturas como o Instituto Nacional de Padrões e Tecnologia (NIST) e ISO 27001, permitindo implementar políticas de privacidade e reconhecimentos para lidar com dados pessoais de clientes e funcionários.
- Permitir gerenciar os programas de privacidade, como, por exemplo, de programas de privacidade de conformidade regulatória de privacidade, avaliações de impacto na privacidade, gerenciamento de política de privacidade e etc.
- Permitir a criação de um inventário de processos de negócios críticos, aplicativos e fornecedores para avaliações de privacidade.

- Possui capacidade de configurar o conteúdo da biblioteca de privacidade, como documentos de autoridade, citações, objetivos de controle, declarações de risco e políticas.
- Deve fazer o gerenciamento das avaliações de impacto na privacidade.
- Deve fazer o gerenciamento das avaliações de risco de privacidade
- Descobrir atividades de processamento que processam informações pessoais.
- Gerenciar atividades de processamento para rastrear sua postura de risco e conformidade com monitoramento contínuo e recursos de gerenciamento de problemas.
- Compreender e analisar a postura geral de privacidade da organização com vários painéis e relatórios.
- Possui capacidade de mapear as atividades de processamento, como sendo um registro que processa dados pessoais. Exemplos de tais registros podem ser um processo de negócios ou um aplicativo de negócios que possui informações pessoais. As atividades de processamento permitem que as equipes de gerenciamento de privacidade entendam como as informações pessoais estão sendo processadas ou usadas.
- Possui capacidade de gerenciar os programas de privacidade, usando qualquer processo de negócios ou aplicativo de negócios que esteja disponível como inventário ou registros no Configuration Management Database (CMDB) da aplicação para criar um registro de atividade de processamento. Cada processo de negócios ou aplicativo é uma atividade de processamento separada.
- As atividades de processamento mapeadas devem possuir minimamente as seguintes informações: Nome e informações de contato do controlador de dados e do processador de dados; Finalidade para a qual uma atividade de processamento está processando dados pessoais. Por exemplo, base legal, obrigações legais e assim por diante; Categorias de titulares de dados e categorias de dados pessoais em tratamento. Exemplos de titulares de dados são clientes ou funcionários; Destinatários com quem os dados pessoais são compartilhados. Por exemplo, fornecedores ou terceiros e sistemas internos; Terceiros em outros países e organizações internacionais que recebem os dados pessoais; Regulamentos de privacidade, políticas, riscos, controles e questões relacionadas a cada atividade de processamento; As principais partes interessadas da atividade de processamento, como os proprietários da entidade e outras pessoas envolvidas na atividade de processamento.
- Possui capacidade de gerar avaliações de privacidade que serão usadas para coletar informações dos proprietários de processos na organização. Essas informações ajudam as equipes de privacidade a entender como as informações pessoais (PI) estão sendo usadas ou armazenadas em uma atividade de processamento.
- Deve possuir a capacidade de configurar vários tipos de avaliações e enviar essas avaliações para os proprietários do processo de negócios ou do aplicativo de negócios para coletar suas respostas.
- Essas avaliações a serem enviadas devem possuir, no mínimo: Avaliações iniciais de triagem de privacidade, Avaliações de impacto de privacidade (PIA), Avaliações de prontidão de privacidade.
- Os recursos para criar a avaliação de privacidade devem ter propriedades para que as respostas gerem avaliações automáticas dos processos dos sistemas, fornecendo no mínimo as seguintes opções de configuração: Configurando vários tipos de perguntas usando uma

interface de usuário simples; Configurando a criação de atividades de processamento usando as respostas das avaliações; Controles de mapeamento para respostas de perguntas para determinar as respostas que mapearão automaticamente os controles para as atividades de processamento; Configurar objetos de informação [PI] para respostas para mapear automaticamente os objetos de informação para uma atividade de processamento; Mapeamento de respostas de perguntas para campos de atividade de processamento para preencher automaticamente os dados necessários na atividade de processamento.

- Possui a capacidade de criar objeto de informação, onde seja possível descrever logicamente o tipo de dados que são trocados entre uma aplicação e um banco de dados.
- Permitir criar objetos de informações e mapear para aplicações de negócios ou processos de negócios. Esta atividade ajuda as equipes de gerenciamento de privacidade a descobrir os objetos de informação que processam dados pessoais. Alguns exemplos de objetos de informação [PI] no gerenciamento de privacidade são: Endereços de e-mail do cliente, Números de contas bancárias do cliente, Detalhes educacionais do funcionário, Endereço de e-mail pessoal do funcionário.
- Permitir que objetos da informação sejam criados manualmente ou por meio de integração com aplicativos externos de data collect/data mapping.
- Caso os objetos de informação não estiverem mapeados para as aplicações ou processos de negócios, o sistema deve poder enviar avaliações de privacidade iniciais para todas as entidades e usar suas respostas para determinar se os dados pessoais estão sendo processados.
- Deve criar Avaliação de criticidade: fornecendo a postura de risco no nível da atividade de processamento, avaliando os fatores no nível da atividade de processamento.
- Deve ter a capacidade para quando uma atividade de processamento é criada ou atualizada, uma avaliação de criticidade deve ser executada na atividade de processamento para entender a pontuação de risco de alto nível ou a pontuação de criticidade.
- Deve criar Avaliação de risco de privacidade: as avaliações de risco de privacidade são avaliações detalhadas que são realizadas se a pontuação de criticidade for alta.
- Deve ter a capacidade de avaliar cada risco associado à atividade de processamento e mapear a pontuação de risco agregada na atividade de processamento.
- Possuir capacidade para avaliar os riscos de privacidade, visualizar a postura de risco de privacidade no mapa de calor de risco.
- Possuir mapas de calor para fornecer informações detalhadas sobre riscos inerentes e residuais.

30. SEGURANÇA DA INFORMAÇÃO

- Permitir implementar as fases ou etapas de Gestão de Segurança da Informação definidas na Norma ISO 27001;
- Prover ferramentas de segurança e integridades dos dados armazenados na nuvem fornecida para armazenamento da solução;
- Permitir detecção e reporte tempestivo de incidentes de TI;
- Permitir suporte a gestão de incidentes e continuidade de negócios de TI;

- A solução deve oferecer suporte à criptografia de campos específicos de forma que seja garantida a confidencialidade das informações neles presentes, incluindo o acesso aos administradores do banco de dados;
- Permitir a extração de relatórios que comprovem a segurança da informação da ferramenta com evidências de testes de segurança, por exemplo, teste de intrusão;
- Permitir resguardo dos dados e entrega da base de dados dos processos e atividades com informações do CONTRATANTE quando do fim da vigência contratual, sem possibilidade de utilização das mesmas pela CONTRATADA.

a. SOAR - orquestração, automação e resposta de segurança (Security Incident Response)

- Possuir um mecanismo de orquestração, automação e resposta de segurança que usa os recursos da plataforma, incluindo fluxos de trabalho inteligentes, priorização e uma conexão profunda com a TI e seus serviços de atendimento;
- Possuir capacidade para que antes que o incidente seja atribuído a um analista, o ativo afetado seja comparado com o Banco de Dados de Gerenciamento de Configuração (CMDB) da plataforma para determinar a prioridade com base na importância do ativo para a camada de negócios, verificando a existência ou não de itens do ITIL como mudanças, incidentes e ou problemas;
- Deve correlacionar dados de inteligência de ameaças e automatizar a análise usando orquestração para realizar verificações adicionais de malware ou extrair processos em execução de um endpoint afetado;
- Possuir funcionalidade de solução de orquestração de segurança e resposta de automação (SOAR), simplificando a identificação de incidentes críticos e fornecendo ferramentas de fluxo de trabalho e automação para acelerar a correção. Os dados das ferramentas de segurança existentes na ORGANIZAÇÃO ou no Security Information and Event Manager (SIEM) possam ser importados por meio de APIs ou integrações diretas para criar automaticamente incidentes de segurança priorizados;
- Permitir visualizar e rastrear facilmente as tarefas de resposta que são executadas em paralelo dentro da plataforma e permitir que o sistema notifique os responsáveis se suas tarefas não forem concluídas no prazo de acordo com os limites de ANS (SLA) ou escalar as tarefas, se necessário;
- Permitir aos analistas obterem uma visão centralizada dos dados de fluxo de trabalho de segurança existentes usando o painel do Security Operations Center (SOC) com gráficos e painéis consolidados, usando dados do CMDB, ITSM ou outra aplicação criada usando os recursos internos da plataforma (low-code/no-code) ou externos que são monitorados usando ITOM;
- Permitir acelerar a resposta permitindo que o Security Incident Response automatize muitas tarefas, incluindo solicitações de aprovação, varreduras de malware e enriquecimento de ameaças;
- Possuir pacotes de orquestração para produtos de segurança integrados, facilitando ações comuns, como solicitações de bloqueio de firewall, de dentro das Operações de Segurança;
- Possuir capacidade de geração e manutenção de base de conhecimento de segurança (KB) usando informações adicionais e

artigos relevantes da base de conhecimento e permitir automaticamente associação a incidentes que possuam referência;

- Possuir capacidade de resposta a incidentes de segurança com priorização e triagem rápidas de ameaças por meio de uma abordagem proativa e orientada por dados. Por exemplo, recursos de Inteligência devem usados para phishing relatado pelo usuário para ajudar a identificar rapidamente e-mails de phishing suspeitos, organizar sua fila de incidentes com classificação integrada para identificar casos de alto impacto e diminuir o MTTR (tempo médio para resolver) para incidentes de phishing;
- Todas as atividades em um ciclo de vida de incidentes, desde a análise e investigação até a contenção e remediação, devem ser rastreadas na plataforma;
- Possuir capacidade para que depois que um incidente seja encerrado, as avaliações sejam distribuídas por toda a equipe e uma revisão pós-incidente (PIR), com carimbo de data/hora, seja criada automaticamente como um registro histórico, de modo que possa ser utilizado para auditoria;
- Possuir capacidade para Gerenciamento de Eventos onde seja possível fornecer uma camada adicional para realizar o ajuste de correlação, filtragem e limite na plataforma. Deve ajudar a reduzir drasticamente a quantidade de incidentes de segurança, empregando mais pontos de contato para filtrar notificações desnecessárias e falsos positivos, lidando com dezenas de milhares de eventos por dia, oferecendo a capacidade de lidar com dados de vários SIEMs ou ferramentas de terceiros;
- Deve ser possível definir permissões de acesso a usuários e grupos na ferramenta de modo a liberar acessos a pessoas e grupos específicos, garantindo o máximo de segurança e privacidade das informações;
- Mesmo usuários com perfil de administração da plataforma não devem acessar as funcionalidades da solução de Resposta a Incidentes de Segurança;
- Mesmo usuários com perfil de administração da plataforma não devem conseguir alterar senhas de qualquer usuário com perfil de administração da solução de Resposta a Incidentes de Segurança;
- Deve ser capaz de registrar incidentes de segurança de forma manual ou através de integração com softwares de terceiros;
- Sobre o registro de incidentes de segurança, a solução também deve ser capaz:

- Registrar incidentes a partir de eventos gerados internamente ou criados por monitoramento externo ou sistemas de rastreamento de vulnerabilidade por meio de regras de alerta. A integração com ferramentas alerta e monitoramento deve ocorrer através de API REST;
- Registrar incidentes a partir do catálogo de serviço;
- O formulário de incidente de segurança deve permitir relacionar qualquer combinação de vulnerabilidades, incidentes, mudanças, problemas, atividades realizadas no item de configuração e/ou nos grupos de itens de configuração afetados de modo a melhorar a análise da ocorrência;
- Deve ser possível customizar o formulário e/ou tabela que armazena os registros de incidente de segurança de modo que dados novos e/ou não mapeados possam ser adicionados e persistidos pela solução;
- A solução deve ser capaz de identificar malware, vírus e outras áreas de vulnerabilidade fazendo referência cruzada ao banco de dados do National Institute of Standards and Technology (NIST) ou outro software de detecção de terceiros;
- A solução deve permitir que, à medida que os incidentes de segurança são resolvidos, qualquer incidente seja usado para criar um artigo da base de conhecimento de segurança para referência futura;
- Deve ser possível realizar análises adicionais usando um mapa de serviços de negócios para localizar outros sistemas ou serviços de negócios afetados que podem ser/estar infectados;
- A solução deve possuir a capacidade de criar e atribuir tarefas a outros departamentos da organização com o objetivo de acelerar a contenção, erradicação e/ou recuperação do serviço ou item de configuração afetado. Através de um mapa de serviço de negócios deve ser possível criar tarefas, problemas ou mudanças para todos os sistemas, documentos, atividades, mensagens SMS, serviços de chamadas ou qualquer outro item de configuração afetado;
- Deve ser possível gerar, automaticamente, relatório de revisão de resolução de incidente pode ser gerado automaticamente, incluindo:
    - Resumo do que foi feito;
    - A linha do tempo;
    - O tipo de incidente de segurança encontrado;
    - Todos os incidentes relacionados, incluindo, pelo menos, as mudanças, problemas, tarefas e item de configuração;
    - Os detalhes da resolução;

- Deve permitir gerar e enviar pesquisa automatizada de revisão de incidentes de segurança para todos os usuários atribuídos a um incidente de segurança com o objetivo de coletar dados sobre o tratamento. Os dados desta pesquisa podem ser adicionados a uma base de conhecimento que contenha as lições aprendidas a serem seguidas para resolver futuras ocorrências;
- A solução deve ser capaz de oferecer, a provedores de serviço, separação de domínio de forma a padronizar os procedimentos de resposta a incidentes de segurança de acordo os diversos clientes e/ou usuários relacionados, reduzindo custos operacionais e gerando maior qualidade de serviço. Assim, deve ser capaz de criar áreas de trabalho separadas para fluxos de trabalho, painéis, relatórios e assim garantir que os dados do cliente sejam separados e nunca expostos a outros clientes.
- Deve ser possível criar incidentes de segurança a partir de um formulário ou lista de incidentes de segurança, catálogo de serviço de segurança, gerenciamento de evento ou item de vulnerabilidade;
- Deve possuir capacidade de criar incidente de segurança a partir da sinalização, por parte o usuário, de e-mail de phishing. Deve possuir recursos para agregação (retirar duplicidades) e extração do conteúdo, cabeçalho e origem do e-mail;
- Deve ser possível, a partir de um incidente de segurança registrado, criar uma solicitação de mudança, incidente ou problema;
- Possuir capacidade de criação de mapas de campos (de/para) caso seja necessário a transformação de um Security Incident Response (SIR) em um caso de atendimento ao cliente ou mesmo um incidente/problema/mudança relacionando as equipes de TI diretamente na plataforma, de forma nativa, e sem necessidade de integração;
- Deve permitir a criação de tarefas de resposta para rastrear outras ações a serem executadas para responder a um incidente de segurança criado;
- A solução deve utilizar algoritmos e recursos de predição para, baseado em dados históricos, realizar a triagem e priorização de incidentes de phishing reportados pelos usuários;
- A solução também deve ter capacidade de dar ao analista de segurança o veredito final sobre as suspeitas de phishing. Para isso, deve haver interface que demonstre de forma clara as condições que foram avaliadas pela funcionalidade de predição. Deve ser facultado ao analista de segurança alterar o veredito atribuído automaticamente;

- Deve conter interface clara para definição das regras e parâmetros a serem utilizados para treinar o modelo de predição;
- A solução deve permitir a atribuição manual dos incidentes de segurança para agentes ou analistas de segurança;
- A solução deve permitir a atribuição dos incidentes de segurança baseada em fluxo de trabalho de modo a padronizar o processo de resolução dos incidentes;
- A solução deve permitir a atribuição automática dos incidentes de segurança para agentes ou analistas de segurança. Neste cenário, a solução deve levar em conta, pelo menos, os seguintes parâmetros: habilidades profissionais, local, fuso horário e área de cobertura do grupo. Caso haja empate nos pesos anteriores, deve ser ponderada a carga de trabalho dos agentes ou analistas de segurança. Deve ser possível, também, alterar os pesos dos critérios de atribuição automática;
- Deve permitir a criação de requisições de entrada para realização de atividades de menor prioridade;
- Deve ser possível gerenciar observáveis. Observáveis são artefatos encontrados em uma rede ou sistema operacional que provavelmente indicam uma intrusão. Os observáveis típicos são endereços IP, hashes MD5 de arquivos ou URLs de malware ou nomes de domínio;
- Deve ser possível visualizar informações de índice de comprometimento, como observáveis e resultados de pesquisa associados a um incidente de segurança;
- Deve permitir a requisição de pesquisa de comprometimento a partir de um incidente de segurança, seja quando um observável é adicionado a um incidente ou através da solicitação em um catálodo de serviço;
- Deve permitir a requisição de pesquisa de vulnerabilidade a partir de um incidente de segurança, seja quando um observável é adicionado a um incidente ou através da solicitação em um catálogo de serviço;
- Deve ser possível associar incidentes de segurança usando relações do tipo pai e filho. Adicionalmente, deve ser possível propagar notas de trabalho inseridas no incidente pai para o(s) incidente(s) filho(s) e, caso um incidente pai seja cancelado ou fechado, os incidentes filhos também devem ser cancelados ou fechados;
- Deve ser possível visualizar itens de configuração, tarefas de resposta e eventos associados a incidente de segurança;
- A solução de permitir o cálculo da severidade de um incidente de segurança cadastrado através de regras pré-definidas;

- Deve permitir gerenciar, pesquisar, conceder aprovações e excluir e-mails de phishing em servidores de e-mail. A exclusão de e-mails de phishing pode ajudar a reduzir a exposição a um ataque específico;
- Deve permitir escalar incidentes de segurança;
- Deve fornecer a capacidade de gerenciar atividades pós-incidente de segurança. Deve ser possível pelo menos:
- Atribuir perfis de revisão pós-incidente;
- Configurar gatilho para avaliação (assessment);
- Criar questionários de revisão pós-incidente;
- Criar regras de atribuição pós-incidente de segurança;
- Relatório de revisão pós-incidente;
- A solução deve possuir um espaço de trabalho para os analistas de segurança que os assista com pelo menos as seguintes funcionalidades:
- Configurar filtros rápidos para visualização de incidentes;
- Permitir visualizar vários incidentes ao mesmo tempo;
- Visualizar a pontuação de risco dos incidentes filtrados;
- Permitir visualizar no espaço de trabalho as principais informações de um incidente, evitando várias mudanças de tela;
- Criar novos incidentes diretamente do espaço de trabalho;
- Fornecer ações rápidas sobre os incidentes, incluindo, pelo menos: editar o registro, gerenciar anexos, visualizar detalhes e enviar e-mail;
- Acessar manuais de apoio ao tratamento de incidentes de segurança;
- É necessário possuir manuais interativos que apoiem os analistas de segurança a realizar as atividades de tratamento de incidentes de segurança. Os manuais devem ser disponibilizados em formato de fluxo de trabalho, sendo possível criá-los e customizá-los de forma rápida. Deve ser possível também que lições aprendidas possam associadas aos manuais para futuras referências;
- Deve conter a capacidade de gerar relatórios para equipe gerencial e também para o time de analistas de segurança. Deve conter, no mínimo:
- Funcionalidade que forneça uma visão executiva de incidentes de segurança, com gráficos de tendência e relatórios, além de fornecer a possibilidade de detalhar as informações apresentadas, se necessário;
- Capacidade de exibir as informações adaptadas ao perfil dos usuários;

- Apresentar mapas de incidentes de segurança por localização geográfica;
- Fornecer mapas do tipo árvore para visão geral da resposta a incidentes de segurança, com a possibilidade de manter categorias e indicadores;
- Deve ser possível incluir, se necessário, gráficos de vulnerabilidade à visão executiva de incidentes de segurança;
- A solução deve conter funcionalidades dedicadas ao tratamento de incidentes de grande porte, com, pelo menos, as seguintes características:
- Conter espaço de trabalho dedicado a gerenciar incidentes de segurança de grande porte, adaptáveis ao perfil de usuário;
- Permitir gerenciar tarefas de resposta utilizando incidentes de segurança 'filhos';
- Possibilitar automatizar a criação de pastas de colaboração e canais de comunicação de bate-papo para apoiar e acelerar as atividades neste tipo de incidente;
- Possuir, por meio de integração com o Microsoft SharePoint, componente explorador de arquivos de modo a organizar e rastrear artefatos (arquivos) relacionados ao incidente de segurança de grande porte;
- Gerenciar canais de bate-papo e componentes de fluxo de atividades de comunicações para vários grupos de TI e/ou da área de negócio por meio de uma integração com o Microsoft Teams;
- A solução deve oferecer a possibilidade de gerenciar tarefas relacionadas a incidentes de segurança através de aplicativo móvel compatível com a plataforma Android ou iOS. O aplicativo deve conter as seguintes funcionalidades, pelo menos:
- Visualizar, editar e atribuir incidentes de segurança e tarefas de resposta;
- Receber notificações detalhadas para incidentes de segurança e tarefas que atendem aos critérios de notificação predefinidos;
- Visualizar agrupamentos de incidentes de segurança ou tarefas com base em um conjunto predefinido de consultas ou filtros;
- Visualizar as notas de trabalho e listas relacionadas de incidentes de segurança;
- Atualizar incidentes de segurança e adicionar notas de trabalho ou anexos;
- Deve conter a capacidade de orquestrar atividades e processos que interajam e recuperem dados sistemas operacionais Windows ou

UNIX usando processos de trabalho. Esta capacidade deve responder, pelo menos, às seguintes demandas:

- Popular a base de dados de itens de configuração (CMDB);
- Possuir pelo menos 10 modelos adaptáveis de fluxos de trabalho pré-definidos para tratamento de incidentes de segurança de modo a facilitar a implantação das atividades de resposta a incidentes de segurança;

b. Threat Intelligence:

- A aplicação Threat Intelligence permite o acesso e fornecimento de um ponto de referência para os dados de Expressão de Informação de Ameaça Estruturada (STIX™) da sua empresa. Incluído no Threat Intelligence está a aplicação Security Case Management, que fornece um meio para analisar ameaças à sua organização apresentadas por campanhas direcionadas ou atores estatais.
- A solução deve permitir o acesso e fornecimento de um ponto de referência para os dados de STIX™ da empresa contratante.
- A solução deve incluir um aplicativo de gerenciamento de casos de segurança para análise de ameaças apresentadas por campanhas direcionadas ou atores estatais.
- STIX é uma linguagem para descrever informações de ameaças cibernéticas de maneira padronizada e estruturada. Usando dados de STIX e perfis de Intercâmbio Automatizado Confiável de Indicadores de Informação (TAXII™), os profissionais de segurança podem usar informações de ameaças cibernéticas compartilhadas para isolar ameaças que foram identificadas previamente pela empresa contratante e de outras fontes. TAXII torna possível a ampla troca automatizada de informações de ameaças cibernéticas.
- A solução deve suportar as versões 1.1, 2.0 e 2.1 de STIX™ e perfis de TAXII™.
- A solução deve permitir a troca automatizada de informações de ameaças cibernéticas.
- A solução deve suportar as versões 1.1, 2.0 e 2.1 de STIX™.
- A solução deve estar em conformidade com as marcas registradas da The MITRE Corporation para STIX™ e TAXII™.
- A solução deve suportar a importação de informações relacionadas a ameaças através de STIX e TAXII.
- A solução deve fornecer uma linguagem padronizada e estruturada para representar informações de ameaças cibernéticas, incluindo

indicadores de atividade comprometida e informações contextuais de ameaças.

- A solução deve fornecer informações sobre como as empresas contratantes podem melhorar a defesa contra ameaças cibernéticas.
- A solução deve permitir a troca automatizada de informações de ameaças cibernéticas entre organizações e limites de produtos/serviços para detecção, prevenção e mitigação de ameaças cibernéticas.
- A solução deve fornecer um repositório para compartilhamento de informações formatadas em STIX. A solução deve permitir a configuração de coleções ou feeds TAXII.
- A solução deve permitir o uso dos campos Indicator, Indicator Type, Attack Mode/Method e Observable Type, conforme especificado pelo cliente.
- A solução deve suportar processadores de fonte de ameaça personalizados para usar esses campos de acordo com a estratégia definida pelo cliente.
- A solução deve permitir a criação de perfis TAXII para compartilhar informações formatadas em STIX. Cada perfil deve ter a capacidade de conter uma ou mais coleções ou feeds TAXII.
- O repositório IoC deve ser capaz de armazenar objetos STIX que contenham informações específicas.
- O sistema deve permitir a combinação de objetos STIX por meio de relacionamentos para permitir representações fáceis ou complexas de CTI.
- O repositório IoC deve suportar as versões 1.1, 2.0 e 2.1 do STIX.
- O sistema deve permitir a representação de modos e métodos de ataque, também conhecidos como Táticas, Técnicas e Procedimentos (TTPs), que descrevem como adversários cibernéticos se comportam, incluindo níveis crescentes de detalhamento. Esses modos e métodos de ataque se aplicam à versão 1.1 do STIX.
- O sistema deve ser capaz de armazenar e representar indicadores de comprometimento (IoCs), que são artefatos observados em uma rede ou sistema operacional que podem indicar uma intrusão. Esses IoCs se aplicam às versões 1.1 e 2.x do STIX.
- O sistema deve permitir a representação de observáveis, que são propriedades estatais (como o hash MD5 de um arquivo ou o valor de uma chave de registro) ou eventos mensuráveis (como a criação de uma chave de registro ou a exclusão de um arquivo) pertinentes

à operação de computadores e redes. Esses observáveis se aplicam às versões 1.1 e 2.x do STIX.

- O sistema deve permitir a representação de padrões de ataque, que são um tipo de TTP que descreve os métodos que os adversários tentam usar para comprometer alvos. Esses padrões de ataque se aplicam à versão 2.x do STIX.
- O sistema deve permitir a representação de campanhas, que são um grupo de comportamentos adversários que descrevem um conjunto de atividades maliciosas ou ataques que ocorrem ao longo do tempo contra um conjunto específico de alvos. Essas campanhas se aplicam à versão 2.x do STIX.
- O sistema deve permitir a representação de cursos de ação, que são ações tomadas para prevenir ou responder a um ataque em andamento. Esses cursos de ação se aplicam à versão 2.x do STIX.
- O sistema deve permitir a representação de identidades, que podem ser indivíduos reais, organizações ou grupos, ou classes de indivíduos, sistemas ou grupos. Essas identidades se aplicam à versão 2.x do STIX.
- O sistema deve permitir a representação de infraestrutura, que é um tipo de TTP que descreve quaisquer sistemas, serviços de software e recursos físicos ou virtuais associados destinados a suportar algum propósito de um ataque. Essa infraestrutura se aplica à versão 2.x do STIX.
- O sistema deve permitir a representação de conjuntos de intrusão, que são conjuntos agrupados de comportamentos e recursos adversários com propriedades comuns, geralmente envolvendo uma única organização. Esses conjuntos de intrusão se aplicam à versão 2
- O sistema deve ser capaz de armazenar e exibir informações de Localizações que representem locais geográficos relevantes para a segurança cibernética.
- As Localizações devem ser usadas principalmente para dar contexto a outros objetos STIX.
- O sistema deve permitir a criação, edição e exclusão de Localizações de forma fácil e intuitiva.
- O sistema deve ser capaz de armazenar informações sobre Malwares, que representam códigos maliciosos inseridos em um sistema de forma dissimulada.
- Deve ser possível vincular Malwares a outros objetos STIX, como Atores de Ameaças e Técnicas de Ataque.

- O sistema deve permitir a criação, edição e exclusão de objetos Malware de forma fácil e intuitiva.
- O sistema deve ser capaz de capturar e armazenar metadados e resultados de uma análise de Malware.
- As informações de análise devem estar vinculadas aos objetos Malware correspondentes.
- O sistema deve permitir a criação, edição e exclusão de informações de análise de Malware de forma fácil e intuitiva.
- O sistema deve ser capaz de armazenar e exibir informações de Dados Observados sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes.
- As informações de Dados Observados devem ser representadas usando objetos STIX Cyber-observable (SCO).
- O sistema deve permitir a criação, edição e exclusão de informações de Dados Observados de forma fácil e intuitiva.
- O sistema deve ser capaz de armazenar informações sobre Atores de Ameaças, que são indivíduos, grupos ou organizações que agem com intenções maliciosas.
- Deve ser possível vincular Atores de Ameaças a outros objetos STIX, como Técnicas de Ataque e Ferramentas.
- O sistema deve permitir a criação, edição e exclusão de objetos Atores de Ameaças de forma fácil e intuitiva.
- O sistema deve ser capaz de criar e gerenciar objetos de Agrupamento de Ameaças, que afirmam explicitamente que os objetos STIX referenciados têm um contexto compartilhado.
- Deve ser possível vincular objetos STIX a um objeto de Agrupamento de Ameaças para indicar que eles compartilham um contexto comum.
- O sistema deve permitir a criação, edição e exclusão de objetos de Agrupamento de Ameaças de forma fácil e intuitiva.
- O sistema deve ser capaz de criar e gerenciar objetos de Definição de Marcação, que representam uma marcação específica.
- As Definições de Marcação são usadas para fornecer informações adicionais sobre os objetos STIX.
- O sistema deve permitir a criação, edição e exclusão de objetos de Definição de Marcação de forma fácil e intuitiva.
- O sistema deve ser capaz de armazenar e exibir informações de Notas de Ameaças, que fornecem texto informativo para fornecer análises adicionais não contidas nos objetos
- A solução deve conter suporte para Locations, para representação de localizações geográficas relevantes para a análise de ameaças.

- A solução deve conter suporte para Malware, para representação de códigos maliciosos.
- A solução deve conter suporte para Malware Analysis, para captura de metadados e resultados de análises de malware.
- A solução deve conter suporte para Observed Data, para a transmissão de informações sobre entidades de segurança cibernética, como arquivos, sistemas e redes, usando os objetos observáveis de segurança cibernética (SCOs) do STIX.
- A solução deve conter suporte para Threat Actors, para a representação de indivíduos, grupos ou organizações que agem com intenções maliciosas.
- A solução deve conter suporte para Threat Groupings, para afirmar explicitamente que os objetos STIX referenciados possuem um contexto compartilhado.
- A solução deve conter suporte para Marking Definitions, para representar uma marcação específica.
- A solução deve conter suporte para Threat Notes, para fornecer texto informativo que forneça análises adicionais não contidas nos objetos STIX, objetos de definição de marcação ou objetos de conteúdo de idioma aos quais a nota se refere.
- A solução deve conter suporte para Threat Opinions, para avaliação da precisão das informações em um objeto STIX produzido por uma entidade diferente.
- A solução deve conter suporte para Threat Reports, para coleções de inteligência de ameaças focadas em um ou mais tópicos.
- A solução deve conter suporte para Sightings, para indicar que um indicador ou objeto foi visto. Os objetos podem ser um malware, ferramenta, ator de ameaça, etc.
- A solução deve conter suporte para Tools, para representação de software legítimo usado por atores de ameaças para realizar ataques.
- A solução deve conter suporte para Vulnerabilities, para representação de fraquezas ou defeitos em componentes de software ou hardware que são explorados por atacantes.
- A solução deve conter suporte para Relationships, para vincular dois SDOs ou STIX Cyber-observable Objects (SCOs) e descrever como eles se relacionam entre si.
- A solução deve conter suporte para STIX Visualizer, para representar visualmente a estrutura do objeto STIX e suas relações.
- Integração do MISP com o Security Operations para permitir investigações de incidentes de segurança, utilizando busca de

avistamentos (sightings searches) e enriquecimento de observáveis (observable enrichment).

- Capacidade de criar e atualizar eventos no MISP a partir do Security Operations.
- Suporte a compartilhamento de informações e inteligência de ameaças (threat intelligence) através do MISP com comunidades confiáveis, sejam elas privadas ou abertas.
- Capacidade de receber informações do MISP sobre ameaças e indicadores de comprometimento (IoCs) relevantes para investigações de incidentes de segurança.
- Melhoria da taxa de detecção de ataques direcionados e redução do número de falsos positivos no ambiente de segurança.
- Garantia de segurança e confidencialidade das informações compartilhadas através do MISP.
- A solução deve conter a aplicação Trusted Security Circles, que permita à equipe de segurança identificar atividades de rede suspeitas e consultar outros membros do círculo se já foram observadas. Isso deve incluir uma consulta anônima enviada aos outros membros do círculo e uma busca de observáveis suspeitos.
- A solução deve permitir que a equipe de segurança determine imediatamente se um incidente de segurança em investigação está afetando seus pares, fornecedores ou parceiros. Isso inclui uma capacidade de detecção que proteja os ativos de TI de outros membros do Trusted Security Circle e proteja a cadeia de suprimentos.
- A solução deve permitir a criação de canais de comunicação Trusted Security Circle que conectem conjuntos de clientes Trusted Security Circle que possuam algum tipo de relacionamento subjacente, como Trusted Security Circle (todos os usuários), Serviços Financeiros, Saúde, Localização e Fornecedores da em comum. O Trusted Security Circle pode ser composto por grupos de organizações dentro do mesmo ramo de negócio, divisões da mesma corporação ou hierarquia corporativa, ou grupos de organizações que desejam compartilhar inteligência de ameaças. A única exigência para que as organizações pertençam a um círculo é que elas tenham um perfil organizacional válido.
- A solução deve permitir o compartilhamento de mensagens ou observáveis entre os membros do Trusted Security Circle, com notificações enviadas a cada membro.
- A solução deve incluir perfis Trusted Security Circle. Os perfis devem definir como você, ou mais precisamente, sua instância do Trusted

Security Circle, é identificado para outros membros do círculo. Por padrão, um perfil rotulado como "anônimo" é criado automaticamente quando um plugin básico ou avançado do Trusted Security Circle é instalado pela primeira vez. Esse perfil também é automaticamente inscrito como membro do Trusted Security Circle global, referido como a instância central.

- A solução deve incluir uma instância central do Trusted Security Circle, que é um aplicativo com escopo hospedado pelo sistema que protege as identidades dos participantes e gerencia o comportamento dos perfis Trusted Security Circle. A instância central deve ser responsável por gerenciar processos como registrar um perfil de compartilhamento de inteligência de ameaças, atualizar e desativar um perfil, criar um círculo e listar círculos. A instância central deve autenticar todas as solicitações para garantir que apenas perfis de clientes sistema válidos possam acessá-la.
- O acesso à instância central deve ser restrito e só pode ser feito por meio do aplicativo e dos módulos instalados pelo plugin de compartilhamento de inteligência de ameaças.

c. Mitre-Att&ck:

- A solução deve conter um conhecimento abrangente das táticas, técnicas e procedimentos (TTP) comuns descritos no framework MITRE-ATT&CK.
- A solução deve permitir que a equipe de inteligência de ameaças da organização desenvolva modelos de ameaças específicos com base nas informações fornecidas pelo MITRE-ATT&CK.
- A solução deve documentar e rastrear as técnicas adversárias utilizadas durante diferentes estágios de um ataque cibernético, de acordo com o framework MITRE-ATT&CK.
- A solução deve permitir a coordenação de respostas a ataques cibernéticos por parte da comunidade de inteligência de ameaças.
- A solução deve permitir a conexão com um servidor TAXII para ingestão de dados de ameaças e inteligência de ameaças relevantes para o contexto da organização.
- A solução deve permitir a integração com os dados de ameaças fornecidos por um gerenciador de informações e eventos de segurança (SIEM), incluindo a associação desses dados com técnicas relevantes descritas no framework MITRE-ATT&CK.

- A solução deve permitir a busca automática de informações relevantes de ameaças e o envio dessas informações para fontes terceirizadas, como EDR, Sandbox ou TIP, para análise adicional.
- A solução deve permitir a extração de informações sobre as técnicas do framework MITRE-ATT&CK a partir de fontes terceirizadas, para enriquecer os dados na ferramenta de inteligência de ameaças.
- A solução deve permitir que a equipe de segurança revise as técnicas exploradas em resposta a vulnerabilidades, como parte da resposta à vulnerabilidade.
- A solução deve incluir matrizes de táticas e técnicas adversárias para permitir que a equipe de segurança compreenda a sequência de táticas usadas pelos adversários durante um ataque cibernético.
- A solução deve permitir que a equipe de segurança antecipe as próximas etapas do ataque adversário e interrompa a cadeia de ataques.
- A solução deve permitir a detecção e contenção de ameaças automatizadas, usando um playbook baseado no framework MITRE-ATT&CK.

d. Solução Data Loss Prevention - DLP

- A aplicação deve permitir a integração com múltiplas soluções de DLP de terceiros para obter uma visão unificada dos incidentes na plataforma Now.
- A aplicação deve permitir a monitorização e atribuição de incidentes aos utilizadores finais, de forma a agilizar a gestão de incidentes DLP.
- A aplicação deve disponibilizar modelos de e-mail personalizados e notificações para coaching de funcionários em relação a cada incidente, bem como um resumo geral.
- A aplicação deve permitir a escalada de incidentes DLP em atraso dos utilizadores finais para os seus gerentes.
- A aplicação deve disponibilizar relatórios de resumo de incidentes abertos por política, gravidade, principais causadores, entre outros.
- A aplicação deve permitir o acompanhamento de tendências de incidentes DLP, tendências de falsos positivos e tendências de remediação.
- A aplicação deve disponibilizar um espaço de trabalho para utilizadores finais ou funcionários, onde possam analisar e responder aos incidentes atribuídos de DLP.

- A aplicação deve disponibilizar um espaço de trabalho para gerentes, onde possam rever os incidentes DLP escalados e agir sobre eles de forma apropriada.
- A aplicação deve disponibilizar um espaço de trabalho unificado onde a equipa de operações DLP possa acompanhar as tendências dos incidentes abertos, principais causadores, incidentes por origem de digitalização, bem como visualizar, editar, atribuir e fechar incidentes DLP em múltiplas fontes (endpoints, redes e e-mail).
- A aplicação deve permitir o controlo administrativo da definição de modelos de e-mail para coaching e comunicação com os utilizadores finais, regras de atribuição para atribuição automática de incidentes, regras de escalonamento automático e delegação para respostas de incidentes.

e. Vulnerability Response

- Deve fornecer uma visão abrangente de todas as vulnerabilidades que afetam um determinado ativo ou serviço, bem como o estado atual de todas as vulnerabilidades que afetam a organização;
- Deve ser capaz de gerenciar de forma centralizada as vulnerabilidades no nível da infraestrutura e de aplicação;
- Deve ser capaz de usar o CMDB da plataforma de modo que as respostas de vulnerabilidades possam priorizar ativos vulneráveis por impacto nos negócios, usando uma pontuação de risco calculada para que as equipes possam se concentrar no que é mais crítico para a organização;
- A pontuação de risco pode incluir vários fatores em seu cálculo, incluindo a pontuação CVSS da vulnerabilidade e se a vulnerabilidade pode ser facilmente explorada, usando dados do scanner de vulnerabilidade importados para a plataforma;
- Deve ser possível definir permissões de acesso a usuários e grupos na ferramenta;
- Deve permitir a integração com sistemas de varredura (dos principais fornecedores, como Tenable, Qualys, Microsoft Threat & Vulnerability Management, Rapid7, Veracode e Fortify) ou bases de conhecimento (itens de vulnerabilidade) de terceiros de modo a facilitar o processo de importação de dados e descoberta/mitigação de vulnerabilidades. Deve ser possível importar dados do NVD (National Vulnerability Database), CPE (Common Platform Enumeration), CVE (Common Vulnerabilities and Exposures) e CWE (Common Weakness Enumeration);
- Deve ser possível, após a importação de dados de vulnerabilidade:
- Comparar os dados relacionados às vulnerabilidades de aplicação, se uma vulnerabilidade for encontrada em uma aplicação;

- Gerenciar itens de vulnerabilidade de aplicação. Cada vulnerabilidade representa uma entrada de vulnerabilidade no CWE (Common Weakness Enumerations) ou em bibliotecas de terceiros;
- Relacionar uma única vulnerabilidade de terceiros a várias entradas no CWE e encontrar o CWE primário para a vulnerabilidade na determinação do risco;
- Usar registros CWE, baixados do banco de dados CWE ou importados de sistemas (scanners) terceitos, para referência ao decidir se uma vulnerabilidade deve ser escalada. Cada registro CWE também deve incluir, para referência, um artigo de conhecimento associado que descreve a fraqueza;
- Deve permitir importar o escaneamento dinâmico de aplicações customizadas (DAST) com o objetivo de encontrar vulnerabilidades no comportamento geral da aplicação;
- Adicionalmente, o escaneamento dinâmico deve permitir:
- Relacionar cada vulnerabilidade dos resultados da verificação a algum tipo de item de configuração;
- Relacionar os resultados da verificação a um aplicativo existente, quando houver um registro no CMDB ou uma integração de terceiros;
- Relacionar os resultados da verificação a um aplicativo recentemente inserido e verificado quando um novo aplicativo não tiver sido identificado e/ou armazenado anteriormente no CMDB;
- Armazenar os resultados da verificação para o CMDB mesmo que as aplicações sejam gerenciadas em um produto diferente;
- Armazenar os resultados da verificação para o CMDB caso tenha sido personalizado anteriormente para alguma outra finalidade;
- Criar um aplicativo como repositório de código-fonte manualmente;
- Deve permitir importar o escaneamento estático (código) de aplicações customizadas (SAST) com o objetivo de encontrar vulnerabilidades causadas pela forma que o código foi escrito.
- Adicionalmente, o escaneamento estático deve permitir, no processo de importação:
- Identificar o ponto (linha de código) onde a vulnerabilidade foi encontrada;
- Relacionar cada vulnerabilidade dos resultados da verificação a algum tipo de item de configuração;
- Criar um item de configuração para o repositório de código-fonte manualmente;
- Armazenar os resultados da verificação mesmo que não exista um serviço de aplicativo relacionado;
- Deve permitir que resultados de verificação sejam armazenados considerando a release da aplicação alvo. Com isso, deve ser possível identificar a qual release cada vulnerabilidade pertence. Caso uma vulnerabilidade identifica não seja mais encontrada, ela deve permanecer vinculada ao resumo da última varredura onde ela foi vista. Caso a aplicação seja removida do CMDB, todas as vulnerabilidades a ela associadas devem ser fechadas;

- Deve ser possível verificar, de forma gráfica, o relacionamento entre as versões das aplicações verificadas, os itens de vulnerabilidade encontrados e os itens de configurações relacionados à aplicação;
- Deve permitir realizar pesquisa automática dos dados das vulnerabilidades de aplicação para encontrar correspondências na base de itens de configuração (CMDB);
- Deve ser possível atribuir/definir, automaticamente, responsável pelo tratamento das vulnerabilidades das aplicações com base em grupos de usuários, campos de grupos de usuários definidos para um item de configuração existente no CMDB ou scripts;
- Deve permitir priorizar e classificar automaticamente o impacto (risco e severidade) dos itens de vulnerabilidade de aplicação usando algoritmos, com base em qualquer critério, e filtros de condição;
- Deve ser possível determinar o impacto nos negócios, especificando condições variadas usando filtros, aplicando cálculos simples ou usando um script;
- Deve ser possível calcular automaticamente os valores iniciais para campos em itens de vulnerabilidade de aplicação. As entradas de vulnerabilidade possuem gravidade de origem e gravidade normalizada (com base no mapeamento de gravidade);
- Deve permitir criar regras para definição do período de tempo esperado para corrigir um item de vulnerabilidade de aplicação (regras de remediação);
- Deve ser possível gerar relatórios com o parecer sobre condutas de segurança da organização, tendências de correção e os 10 principais aplicativos ou unidades de negócios com os itens de vulnerabilidade de aplicação mais críticos;
- Deve conter um fluxo de trabalho (workflow) para tratamento ou remediação do item de vulnerabilidade de aplicação. Este fluxo e seus estados devem ser passíveis de customização.
- Deve conter painéis e relatórios para os usuários envolvidos na gestão, monitoramento e tratamento dos itens de vulnerabilidade com gráficos e ações que permitam a execução de todas atividades pertencentes a atribuição de cada perfil;
- Deve prover uma solução analítica e de relatórios para apresentar métricas que permitam avaliar e gerenciar o processo de gerenciamento das vulnerabilidades. Deve ser possível criar painéis de gestão, geração de relatórios de indicadores (KPIs) e métricas. Deve ser, com isso, capaz de responder as questões chave do negócio de modo a aumentar a qualidade da ação e reduzir custos;
- A solução deve ser capaz de gerar e armazenar métricas e indicadores acerca das avaliações de vulnerabilidade realizadas provendo, assim, meios para que seja possível comparar as métricas de diferentes avaliações;
- A solução deve possuir, por padrão, indicadores que ajudem a identificar o progresso das ações de remediação e quais itens de vulnerabilidade precisam de maior atenção. Estes indicadores devem

estar disponíveis em um painel e sua visualização deve ser condicionada a liberação de perfil específico;

- Deve conter fluxo de trabalho (workflow) para solicitação, revisão, preparação, teste, correção e geração de relatórios de penetração. A execução deste fluxo de trabalho deve ser condicionada a liberação de perfil específico;
- A solução deve conter recurso que permita gerenciar e tratar itens de vulnerabilidades de contêineres Docker. Uma imagem de contêiner deve poder ser verificada quanto a vulnerabilidades antes ou após a sua implantação;
- Adicionalmente, o escaneamento de contêiner deve permitir:
- Ser capaz detectar e gerenciar vulnerabilidades em contêineres Docker através do escaneamento de uma imagem do Docker correspondente ao contêiner em execução;
- Ser possível configurar a granularidade de itens de vulnerabilidade a serem rastreados na imagem, cluster Kubernetes, namespace ou nível de serviço;
- Rastrear novas versões de imagem para identificar vulnerabilidades corrigidas. Em tempo de execução, quaisquer vulnerabilidades relatadas em versões mais antigas devem ser resolvidas automaticamente quando novas versões de imagem são implantadas;
- Rastrear itens de vulnerabilidade nas imagens base separadamente das imagens de aplicação de forma a permitir a correção independente;
- Gerar solicitações de exceção ou informes de falsos positivos para que sejam revisados por meio de um processo de aprovação de vários níveis;
- Ser possível definir e gerenciar regras de exceção para adiar itens de vulnerabilidade automaticamente;
- Visualizar, através de painéis, gráficos e indicadores as vulnerabilidades que estão presentes nos contêineres escaneados;
- Ser capaz de gerenciar patches e implantações de patches para vulnerabilidades críticas e para grandes grupos de ativos usando dados de importações programadas de integrações de soluções de terceiros, fornecedores de patches como Microsoft, BigFix e scanners de vulnerabilidade, dentre outros;
- Possuir capacidade de organização de dados, permitindo que a organização conclua as etapas do ciclo de correção de vulnerabilidade, desde o processo de identificar vulnerabilidades, depois aplicar patches e atualizações e, finalmente, fechar os itens vulneráveis usando dados de scanner de terceiros, tudo de dentro da plataforma;
- Possuir capacidade para resposta à vulnerabilidades identificadas e correlacionadas na plataforma, de modo a pode ajudar a organização a a responder com mais rapidez e eficiência às vulnerabilidades, conectar as equipes de segurança e de TI e fornecer visibilidade em tempo real;