ANEXO II – REQUISITOS NÃO FUNCIONAIS

1	A aplicação principal da solução deverá possuir arquitetura nativamente web, com acesso direto por meio de navegador, e permitir sua utilização dentro ou fora das unidades da Rede HU Brasil, por computadores e dispositivos móveis. O acesso por dispositivos móveis poderá ocorrer por interface web responsiva ou aplicativo móvel. Não serão admitidas soluções cujo acesso por navegador dependa de mecanismos intermediários de execução, virtualização, transmissão ou renderização de interface originalmente desenvolvida para ambiente desktop ou cliente-servidor.
2	A solução deve apresentar integração com sistema de gestão hospitalar, sistema HCM em uso pela Empresa, sistemas de ponto, visões e demais que se fizerem necessárias.
3	A solução deve apresentar portal de autosserviço responsivo
4	A solução deve permitir categorização de perfis de acesso da equipe de RH e de gestores/supervisores por lotação, vínculo funcional etc.
5	A solução deve permitir a delegação de funções pela chefia imediata aos supervisores, desde que previamente parametrizadas pela equipe de RH autorizada.
6	A solução deve possibilitar a interação colaborador/chefia/RH em todos os processos decorrentes de tempos, horários e escalas.
7	A solução deverá permitir a gravação de histórico de eventos ocorridos (inclusão, exclusão, alteração e outros), nas trilhas de auditoria. Todos os registros de histórico deverão apresentar o usuário e a data e hora da ocorrência do evento. Para os eventos de alteração de informações, a solução deverá registrar a situação da informação antes e depois da sua alteração
8	A solução deverá garantir integridade dos registros quando da atualização simultânea deles, provendo recursos de bloqueio e liberação de atualização de informações na plataforma Web.
9	A solução deverá prover mecanismos que garantam que a implementação de customizações e parametrizações sejam mantidas após o recebimento e aplicação de atualizações
10	A solução deverá garantir que uma única transação executada pelo usuário desencadeie todas as ações dela decorrentes, garantido que os processos estejam totalmente integrados, em tempo real, a fim de garantir a integridade das informações e, consequentemente, a confiabilidade e agilidade no processo de tomada de decisão.

11	A solução, com todos os componentes tecnológicos que a compõem, deverão estar aderentes à LGPD implantando como padrão o princípio de Privacy by Design/by Default. Como exemplo, mas não se limitando a esta funcionalidade, o sistema deverá implementar filtros e funcionalidades que delimitem níveis de acesso e responsabilidade, garantindo que dados pessoais e sensíveis só possam ser apresentados, manipulados ou exportados por pessoas devidamente autorizadas.
12	A solução deverá possuir controle de acesso, com atribuição de privilégios por perfil para seus componentes (telas, transações, áreas de negócio), regras de negócio e alçadas
13	A solução deverá sempre exigir autenticação para qualquer acesso à sua plataforma, seja por acessos individuais dos usuários ou por qualquer acesso demandado por processos de integração
14	A solução deverá possuir identificação única para cada usuário, por meio de login e senhas individualizadas, de forma a permitir auditoria, controle de erros e de tentativas de invasão
15	A solução deverá permitir a gestão centralizada de metadados. Os metadados deverão facilitar, para os usuários do sistema, o entendimento dos relacionamentos e a utilidade das informações armazenadas durante a construção de relatórios e consultas avulsas.
16	A solução deverá disponibilizar relatórios do uso diário das subscrições ativas. O relatório deverá informar o tipo de licença utilizada e o usuário. Também deverá ser possível quantificar o número de acessos simultâneos para cada tipo de licença.
17	A solução deverá ter, como o idioma padrão, o português (pt-br) para toda interface e as mensagens de interação com o usuário.
18	A solução deverá possuir interface responsiva que permita acesso aos módulos da ferramenta por dispositivos com resoluções diferentes. A solução deverá se adequar a interface garantindo a legibilidade para o usuário.
19	A solução deverá possuir ambiente de portal, onde o acesso de qualquer usuário utilize a mesma interface, possibilitando a customização desta interface única.
20	A solução deverá alertar o usuário por meio de mensagens em português (pt-br), a fim de que possa corrigir eventuais erros antes da conclusão de determinada função, caso haja divergência com alguma regra de negócio ou qualquer outra regra importante.
21	É desejável que a solução permita a configuração do tempo decorrido para sinalizar a ocorrência de transações demoradas.
22	possuir capacidade de autenticar usuários a partir da integração com o *Microsoft Active Directory.*
23	Possuir a capacidade de atribuir usuário único para cada colaborador, por meio de login e senha individualizados.
24	Possuir capacidade de ser integrada a outros sistemas utilizando webservices em padrão SOAP e/ou REST.

25	Possuir integração com serviços de Correio Eletrônico em padrão SMTP, permitindo a comunicação com *software* Microsoft Exchange.
26	Possuir capacidade de realizar importação massiva de dados a partir da integração com outros sistemas ou planilhas eletrônicas (xlsx, xls, csv) e arquivos texto (txt e xml).
27	Possuir a capacidade de exportar os dados dos relatórios nos formatos PDF, HTML, planilhas eletrônicas (xlsx, xls, csv) e arquivos de texto (txt).
28	Possuir capacidade de manter a rastreabilidade de operações para auditoria, garantindo a estruturação de um histórico de alterações.
29	Possuir capacidade de alteração da identidade visual a fim de caracterizá-la com cores e logo da empresa.
30	Conforme a IN Nº5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem e com a Norma Operacional - SEI nº 6/2022/SGTI/DTI-EBSERH que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pela Rede Ebserh, a solução deve possuir certificações ISO 27001, ISO 9001, TIER 2, SOC 2, SOC 3 ou similares. Alternativamente, pode demonstrar conformidade com todos os objetivos e controles dessas normas por meio da apresentação de políticas, procedimentos e outros documentos pertinentes.
31	A aplicação web deverá ser compatível com os principais navegadores, incluindo, no mínimo, as versões estáveis e suportadas de Google Chrome, Mozilla Firefox, Microsoft Edge e Safari, assegurando o adequado funcionamento das funcionalidades disponibilizadas por esse meio de acesso.
32	Possuir a capacidade de ser acessada através de dispositivos móveis, responsiva, para garantir uma experiência de usuário otimizada em dispositivos móveis ou possuir aplicativo gratuito disponibilizados nas principais lojas.
33	Deve ser acessível para consulta de seus registros através de API e/ou acesso direto à base de dados.
34	Os ambientes necessários ao funcionamento da solução, bem como os respectivos serviços de backup, deverão ser disponibilizados em ambiente de nuvem provido pela CONTRATADA e estar integralmente incluídos na prestação do serviço.
35	A CONTRATADA será responsável pelo dimensionamento dos ambientes necessários à prestação do serviço, de forma a assegurar o atendimento aos níveis de serviço estabelecidos, considerando o quantitativo de usuários contratado.
36	O sistema deverá ter banco de dados relacional
37	Para transações cujo processamento ultrapasse 60 (sessenta) segundos, a solução deverá informar ao usuário que a operação permanece em processamento, por meio de mensagem informativa ou indicação gráfica, evitando que a ausência de retorno seja interpretada como falha na execução

38	Permitir a atribuição temporária, a usuário formalmente designado como substituto, dos acessos e permissões necessários ao exercício das atribuições do usuário substituído, por período previamente definido, mantendo a identificação e a rastreabilidade das operações realizadas pelo substituto.