European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

ORIENTAÇÕES PARA OS CONTRATOS PÚBLICOS NO ÂMBITO DA CIBERSEGURANÇA NOS HOSPITAIS

O relatório tem como objetivo funcionar como um “guia” para os profissionais de saúde. Muitas das práticas e recomendações serão igualmente úteis para outros organismos responsáveis pelos cuidados de saúde, uma vez que os processos de contratação podem ser muito semelhantes. É útil para profissionais de saúde que ocupem cargos técnicos nos hospitais, ou seja, para profissionais com cargos diretivos: CIO, CISO, CTO, equipas de TI e diretores de compras em organismos responsáveis pelos cuidados de saúde. Este breve documento abordou os principais pontos do relatório. Para mais informações, consultar a publicação da ENISA: ENISA - "Good Practices for the Security of Healthcare Services" [Boas Práticas para a Segurança dos Serviços de Saúde], de fevereiro de 2020.

PROCESSO DE CONTRATAÇÃO PÚBLICA

Uma vez que o ecossistema hospitalar inclui vários componentes de TI, cada um deles deve ser independentemente analisado em termos de cibersegurança. A cibersegurança deve estar incluída em todas as diferentes etapas do processo de contratação. Nesta secção, apresentamos as etapas comuns do processo de contratação pública de produtos e serviços, incluindo dispositivos médicos, sistemas de informação e infraestruturas.

Figura 1: Ciclo do processo de contratação pública para os hospitais

- Fase de planeamento: Inicialmente, o hospital analisa as suas necessidades e faz um levantamento interno dos requisitos dos diferentes departamentos. Por exemplo, no caso da aquisição de um novo serviço na nuvem, o CTO deve identificar as necessidades e compreender que tipo de usabilidade este serviço irá proporcionar.

- Fase de adjudicação: Em seguida, os requisitos são traduzidos em especificações técnicas e, em colaboração com o departamento de Compras, inicia-se o processo de contratação (ou seja, é aberto um concurso público). O hospital recebe as propostas designadas, a comissão (incluindo o CTO/CISO ou qualquer membro da equipa de TI) avalia as propostas e seleciona os produtos mais adequados. É conduzido o processo de negociação com o contratante e o contrato é adjudicado.

- Fase de gestão: Por fim, o contrato (gestão e supervisão) é atribuído ao responsável da área de negócio no hospital. O responsável designado fica encarregado do encerramento oficial do concurso e da gestão de todo o feedback dos utilizadores quanto ao desempenho efetivo do equipamento/sistema/serviço.

TIPOS DE CONTRATAÇÃO NOS HOSPITAIS

Tabela 1: Tipos de contratação (taxonomia dos ativos)

Tipo de contratação	Descrição
Sistemas de informação clínica	Inclui a aquisição de qualquer tipo de *software* orientado para os cuidados médicos
Dispositivos médicos	Qualquer *hardware* dedicado ao tratamento, controlo ou diagnóstico de doenças
Equipamento de rede	Linhas de rede (coaxiais, óticas), *gateways*, *routers*, comutadores, *firewalls*, VPN, IPS, IDS, etc.
Sistemas de assistência à distância	Instalações ou dispositivos que disponibilizam cuidados fora do ambiente hospitalar, sobretudo o que atualmente é denominado como “Serviços de apoio domiciliário de base hospitalar”.
Dispositivos móveis para o cliente	Qualquer tipo de *software* que disponibiliza assistência médica ou que permite a recolha de dados médicos não diretamente ligado à rede do hospital; por exemplo: aplicações de telemedicina
Sistemas de identificação	Sistemas de identificação individual de doentes ou pessoal médico (scanners biométricos, leitores de cartões, etc.) e que garantem a identificação e/ou a autorização para aceder aos sistemas informáticos.
Sistemas de gestão técnica centralizada	Qualquer tipo de estrutura que possa alojar instalações médicas.
Sistemas de controlo industrial	Sistemas de controlam todos os aspetos físicos dos centros, tais como sistemas de regulação energética, sistemas de fecho de portas, sistemas fechados de segurança.
Serviços profissionais	Todo o tipo de serviços, subcontratados ou não, disponibilizados por profissionais ou empresas: serviços médicos, de transporte, contabilísticos, de engenharia, informáticos, jurídicos, de manutenção, limpeza, catering, etc.
Serviços na nuvem	Qualquer CIS ou outro sistema de informação não localizado no edifício médico ou numa unidade de centro de dados totalmente controlada pelo departamento de TI do centro médico.

TAXONOMIA DAS AMEAÇAS

Diferentes tipos de contratações estão associados a diferentes ameaças ao ambiente TIC de um hospital. Consulte a taxonomia das ameaças disponibilizada nesta secção em conjunto com o seu departamento de TI, de segurança ou de risco, para identificar quais as ameaças mais relevantes para a sua organização. Esta atividade deve fazer parte das tarefas de TI no hospital, independentemente do potencial de contratação.

Tabela 2: Tipos de ameaça (taxonomia das ameaças)

Ameaça	Exemplos
Fenómenos naturais	Incêndios, inundações ou eventos sísmicos
Falha na cadeia de abastecimento	Falha no fornecimento de serviços de computação em nuvem, falha no fornecimento de serviços de rede, falha no fornecimento energético, falha no serviço do fabricante de dispositivos médicos/não responsabilidade
Erros humanos	Erro na configuração do sistema médico, inexistência de registos de auditoria, controlo de acesso não autorizado/inexistência de processos, incumprimento (BYOD), erro de pessoal médico/doente
Ações maliciosas	*Malware* (vírus, *ransomware*, BYOD), controlo não autorizado (criptossequestro, *medjacking*), engenharia social (*phishing*, *baiting*, clonagem de equipamentos), furto (dados, equipamento), violação de dispositivos médicos, clonagem, negação de serviço, ataques baseados na Web, ataques a aplicação Web, ameaça interna, manipulação física/danos, usurpação de identidade, ciberespionagem, perturbação da mecânica de componentes
Falhas do sistema	Falha do *software*, *firmware* desatualizado, falha do dispositivo, falha dos componentes de rede, manutenção insuficiente

BOAS PRÁTICAS DE CIBERSEGURANÇA NA CONTRATAÇÃO

A lista de boas práticas que se segue não é de forma alguma exaustiva; porém, constitui uma vantagem significativa para o profissional de TI na área da saúde responsável pela compra de equipamento num hospital. O conjunto de boas práticas é o resultado coletivo de todos os contributos dados pelos profissionais de saúde questionados. O destinatário pode adaptar a lista com base nas prioridades do organismo a que pertence.

BP 1. Envolver o departamento de TI nas diferentes etapas da contratação, para garantir que são tidos em conta os aspetos relacionados com a cibersegurança.

Fases da contratação: Todas

Tipos de contratação relacionados: Todos

Ameaças relacionadas: Todas

BP 2. Implementar um processo de identificação e gestão de vulnerabilidades para garantir que estas são analisadas antes da contratação de novos produtos ou serviços e que as vulnerabilidades dos produtos/serviços existentes são monitorizadas ao longo do seu ciclo de vida.

Fases da contratação: Todas

Tipos de contratação relacionados: Sistemas de informação clínica, Dispositivos médicos, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Todas

BP 3. Desenvolver uma política para atualizações de *hardware* e *software* que garanta a aplicação das mais recentes correções no SO e no *Software* e a atualização do *Software* de antivírus.

Fases da contratação: Todas

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 4. Melhorar os controlos de segurança para comunicação sem fios para garantir que o acesso às redes Wi-Fi do hospital é limitado e rigorosamente controlado.

Fases da contratação: Todas

Tipos de contratação relacionados: Dispositivos médicos, Dispositivos à distância para o cliente, Sistemas de identificação, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Erros humanos

BP 5. Definir políticas de testes para garantir que os produtos recentemente adquiridos ou configurados são submetidos a um teste de penetração e que as ações corretivas adotadas estão em linha com os parâmetros operacionais do ambiente atual.

Fases da contratação: Todas

Tipos de contratação relacionados: Sistemas de informação clínica, Dispositivos médicos, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistema de gestão técnica centralizada, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falhas do sistema, Erros humanos

BP 6. Implementar planos de continuidade das atividades para garantir que a falha de um sistema não perturba os serviços básicos do hospital e que o papel do fornecedor está bem definido.

Fases da contratação: Todas

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 7. Considerar questões de interoperacionalidade para garantir que não existem vazios de segurança em relação aos componentes já existentes (TI legado).

Fases da contratação: Todas

Tipos de contratação relacionados: Sistemas de informação clínica, Dispositivos médicos, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Falhas do sistema, Erros humanos, Ações maliciosas

BP 8. Permitir a testagem de todos os componentes para garantir que atuam como previsto: verificar a facilidade de utilização, verificar a correção dos resultados sob carga e verificar a existência de falhas de segurança (política relativa a palavras-passe fracas, injeção de SQL).

Fases da contratação: Todas

Tipos de contratação relacionados: Sistemas de informação clínica, Dispositivos médicos, Dispositivos à distância para o cliente, Sistemas de identificação, Serviços na nuvem, Sistemas de controlo industrial, Sistema de assistência à distância, Dispositivos móveis para o cliente

Ameaças relacionadas: Ações maliciosas, Erros humanos, Falhas do sistema, Falha na cadeia de abastecimento

BP 9. Permitir auditorias e registos para rastrear atacantes e a quantidade de informação perdida/roubada quando o sistema fica comprometido.

Fases da contratação: Todas

Tipos de contratação relacionados: Dispositivos médicos, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 10. Encriptar dados pessoais sensíveis inativos e em circulação mediante a definição de uma política para sistemas, serviços ou dispositivos que processem as categorias especiais de dados pessoais constantes do Artigo 9.º do RGPD.

Fases da contratação: Todas

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 11. Realizar uma avaliação de risco integrada no processo de contratação.

Fases da contratação: Planear

Tipos de contratação relacionados: Todas

Ameaças relacionadas: Todas

BP 12. Planear antecipadamente os requisitos de rede, *hardware* e licenças para determinar a necessidade de atualizações e/ou aquisições adicionais antes da instalação para receber o novo sistema.

Fases da contratação: Planear

Tipos de contratação relacionados: Sistemas de informação clínica, Equipamento de trabalho em rede, Sistemas de identificação, Sistemas de controlo industrial.

Ameaças relacionadas: Falha na cadeia de abastecimento, Falhas do sistema, Fenómenos naturais, Erros humanos

BP 13. Identificar ameaças relacionadas com produtos ou serviços contratados e garantir a continuidade da identificação das ameaças durante a vigência do contrato.

Fases da contratação: Planeamento, Gestão

Tipos de contratação relacionados: Todos

Ameaças relacionadas: Todas

BP 14. Segregar a rede para garantir que é possível isolar e/ou filtrar o tráfego de rede para limitar e/ou impedir o acesso entre zonas de rede.

Fases da contratação: Planeamento, Adjudicação

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 15. Determinar requisitos de rede para garantir a interoperacionalidade e evitar lacunas após a criação da topologia da rede e dos componentes.

Fases da contratação: Planeamento

Tipos de contratação relacionados: Sistemas de informação clínica, Equipamento de trabalho em rede, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem, Sistemas de assistência à distância, Dispositivos móveis para o cliente.

Ameaças relacionadas: Falha na cadeia de abastecimento, Falhas do sistema, Fenómenos naturais

BP 16. Implementar requisitos de segurança de referência e traduzi-los em critérios de elegibilidade aquando da seleção dos fornecedores.

Fases da contratação: Planeamento, Adjudicação

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 17. Criar um RFP dedicado para a aquisição de serviços na nuvem, tendo em conta as exigências regulamentares e de políticas.

Fases da contratação: Planeamento, Adjudicação

Tipos de contratação relacionados: Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento

BP 18. Dar prioridade à aquisição de bens com certificação contra esquemas/normas de cibersegurança.

Fases da contratação: Adjudicação

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 19. Realizar avaliações do impacto da proteção de dados na planificação da aquisição de um novo sistema ou serviço.

Fases da contratação: Adjudicação

Tipos de contratação relacionados: Sistemas de informação clínica, Dispositivos médicos, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Serviços profissionais, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Erros humanos

BP 20. Definir *gateways* que mantenham a ligação entre os sistemas/máquinas legados e disponibilizem um sistema de contenção em caso de problemas no interior destes grupos.

Fases da contratação: Adjudicação, Gestão

Tipos de contratação relacionados: Dispositivos médicos, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 21. Disponibilizar formação em matéria de cibersegurança ao nível das práticas de segurança do organismo para garantir que o pessoal interno ou os contratantes/consultores externos que trabalham nas instalações estejam devidamente formados.

Fases da contratação: Adjudicação, Gestão

Tipos de contratação relacionados: Todos

Ameaças relacionadas: Ações maliciosas, Erros humanos

BP 22. Desenvolver planos de resposta a incidentes que abranjam produtos ou sistemas adquiridos recentemente.

Fases da contratação: Adjudicação, Gestão

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 23. Envolver o fornecedor/fabricante na gestão de incidentes e definir claramente os termos no RFP.

Fases da contratação: Adjudicação, Gestão

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 24. Agendar e monitorizar operações de manutenção de todo o equipamento para garantir um nível adequado de funcionalidade e decidir a adoção de atualizações/correções, etc.

Fases da contratação: Adjudicação, Gestão

Tipos de contratação relacionados: Sistemas de informação clínica, Equipamento de trabalho em rede, Dispositivos médicos, Sistemas de gestão técnica centralizada, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Erro humano, Falha do sistema, Fenómenos naturais

BP 25. O acesso remoto deve ser minimizado e realizado de forma a que as comunicações externas com o fornecedor sejam limitadas apenas ao dispositivo que este tenha de controlar.

Fases da contratação: Adjudicação, Gestão

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema, Erros humanos

BP 26. Solicitar correções para todos os componentes e incluir a informação no RFP.

Fases da contratação: Adjudicação, Gestão

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema

BP 27. Incrementar a sensibilização para a cibersegurança entre o pessoal para garantir que este está consciente dos riscos associados a produtos ou serviços recentemente adquiridos.

Fases da contratação: Gestão

Tipos de contratação relacionados: Todos

Ameaças relacionadas: Todas

BP 28. Realizar a inventariação dos bens e a gestão da configuração para garantir que o inventário está devidamente atualizado quando algum componente for adicionado ou retirado do ambiente TIC e para garantir que estão implementadas configurações de segurança de referência para componentes e que estas são adequadamente geridas.

Fases da contratação: Gestão

Tipos de contratação relacionados: Sistemas de informação clínica, Dispositivos médicos, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação

Ameaças relacionadas: Ações maliciosas, Erros humanos, Falhas do sistema

BP 29. Implementar mecanismos de controlo de acesso dedicados para instalações com equipamentos médicos, que devem ser também fisicamente protegidos e cujo acesso deve ser limitado apenas ao pessoal especializado.

Fases da contratação: Gestão

Tipos de contratação relacionados: Dispositivos médicos, Sistema de gestão técnica centralizada, Sistemas de identificação

Ameaças relacionadas: Ações maliciosas, Erros humanos

BP 30. Agendar testes de penetração frequentes ou após qualquer alteração na arquitetura/sistema e incluir os termos no RFP.

Fases da contratação: Adjudicação, Gestão

Tipos de contratação relacionados: Dispositivos médicos, Sistemas de informação clínica, Equipamento de trabalho em rede, Sistema de assistência à distância, Dispositivos móveis para o cliente, Sistemas de identificação, Sistemas de controlo industrial, Serviços na nuvem

Ameaças relacionadas: Ações maliciosas, Falha na cadeia de abastecimento, Falhas do sistema