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

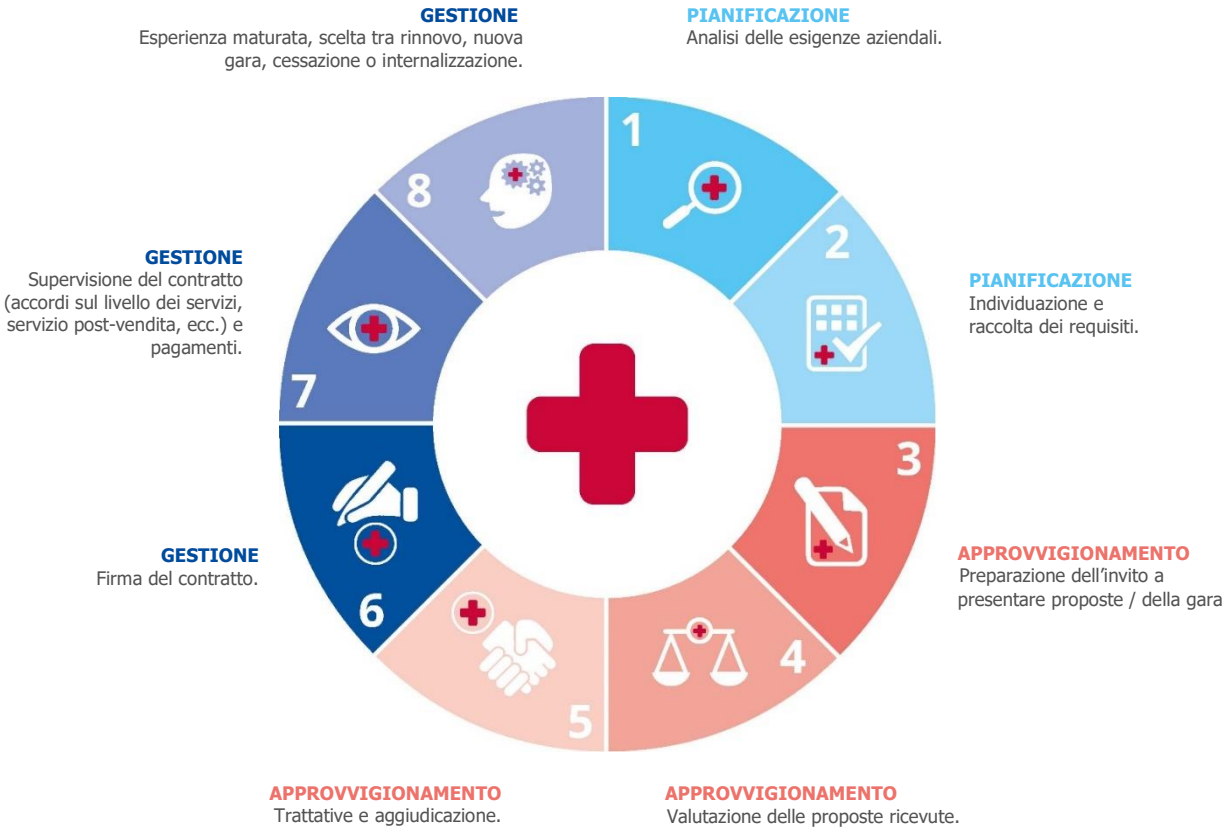
ORIENTAMENTI IN MATERIA DI APPALTI PER LA CIBERSICUREZZA NEGLI OSPEDALI

La relazione vuole essere una «guida» per gli operatori sanitari (molte prassi e raccomandazioni serviranno anche ad altre organizzazioni sanitarie, poiché le relative procedure di appalto possono essere molto simili) ed è utile per gli operatori che occupano posizioni tecniche negli ospedali, per esempio incarichi a livello dirigenziale (responsabili dei settori informatici, dei servizi informativi o della tecnologia, team informatici e funzionari preposti alla gestione degli appalti in organizzazioni sanitarie). Questo breve documento tratta i punti principali della relazione; per maggiori dettagli, il lettore dovrà consultare il testo ENISA Good Practices for the Security of Healthcare Services [Buone prassi dell'ENISA per la sicurezza dei servizi sanitari], pubblicato nel febbraio 2020.

LA PROCEDURA DI APPALTO

Poiché l'ecosistema ospedaliero consta di molte componenti informatiche, occorre esaminare la cibersicurezza separatamente nell'ambito di ognuna di queste diverse componenti; la cibersicurezza deve essere presente in tutte le varie fasi della procedura di appalto. In questa sezione presenteremo le fasi comuni della procedura di appalto per l'acquisizione di prodotti e servizi, ivi compresi dispositivi medici, sistemi di informazione e infrastrutture.

Figura 1: ciclo di vita della procedura di appalto per gli ospedali



- Fase di pianificazione: inizialmente l'ospedale analizza le proprie esigenze e raccoglie i requisiti delle varie divisioni a livello interno; per esempio, nel caso dell'acquisizione di un nuovo servizio cloud, il responsabile della tecnologia deve identificare le esigenze e comprendere il tipo di utilizzabilità che offrirà il servizio.

- Fase di approvvigionamento: in seguito, i requisiti vengono tradotti in specifiche tecniche e, in collaborazione con l'ufficio appalti, viene avviata la procedura di approvvigionamento (per esempio con la pubblicazione di una gara d'appalto). L'ospedale riceve le relative offerte, il comitato (comprendente il responsabile della tecnologia/dei servizi informativi e/o un membro del team informatico) le valuta e seleziona i prodotti più adeguati. Vengono condotte trattative con l'appaltatore e si procede all'aggiudicazione del contratto.

- Fase di gestione: infine, viene affidato il contratto di gestione e monitoraggio al titolare dell'impresa nell'ambito dell'ospedale. Il funzionario incaricato ha il compito di concludere la procedura di gara e ricevere i riscontri degli utenti in merito alla prestazione effettiva delle apparecchiature/del sistema/del servizio.

TIPI DI APPALTO NEGLI OSPEDALI

Tabella 1. Tipi di appalto (tassonomia delle risorse)

Tipo di appalto	Descrizione
Sistemi informativi clinici	Comprende l'acquisizione di qualsiasi tipo di software orientato all'assistenza medica
Dispositivi medici	Qualunque dispositivo hardware destinato al trattamento, al controllo o alla diagnosi delle malattie
Apparecchiature di rete	Cavi di rete (coassiali, ottici), gateway, router, interruttori, firewall, VPN, IPS, IDS, ecc.
Sistemi di teleassistenza	Strutture o dispositivi per fornire assistenza al di fuori dell'ambiente ospedaliero, in particolare quelli che oggi sono definiti «servizi di assistenza domiciliare all'interno dell'ospedale».
Dispositivi mobili client	Qualunque software che fornisca assistenza sanitaria o raccolga dati medici non direttamente collegati alla rete ospedaliera, per esempio app di telemedicina
Sistemi di identificazione	Sistemi che servono a identificare univocamente i pazienti o il personale medico (scanner biometrici, lettori di schede, ecc.) e a garantire l'identificazione e/o l'autorizzazione per accedere ai sistemi informatici.
Sistema di gestione degli edifici	Qualsiasi tipo di costruzione che possa contenere strutture mediche.
Sistemi industriali di controllo	Sistemi che controllano tutti gli aspetti fisici dei centri (sistemi di regolazione della potenza, sistemi di chiusura porte, sistemi di sicurezza a circuito chiuso).
Servizi professionali	Qualunque tipo di servizi, esternalizzati o meno, prestati da professionisti o aziende: servizi medici, trasporto, contabilità, progettazione, informatica, consulenza legale, manutenzione, pulizia, catering, ecc.
Servizi cloud	Qualsiasi sistema CIS per la gestione dei rapporti con i clienti o altro sistema informatico che non sia ubicato nella struttura medica o in un centro dati totalmente controllato dalla divisione informatica del centro medico.

TASSONOMIA DELLE MINACCE

Diversi tipi di appalto sono correlati a varie minacce per l'ambiente TIC di un ospedale. Si prega di consultare la tassonomia delle minacce presentata in questa sezione, oltre al proprio reparto informatico, ufficio di sicurezza o di gestione dei rischi, per individuare i tipi di minacce maggiormente pertinenti per la propria organizzazione. Quest'attività deve rientrare fra le attività informatiche svolte nell'ospedale, indipendentemente dal potenziale in materia di appalti.

Tabella 2. Tipi di minacce (tassonomia delle minacce)

Minaccia	Esempi
Fenomeni naturali	Incendi, alluvioni o terremoti
Interruzione della catena di approvvigionamento	Interruzione del provider di servizi cloud, interruzione del provider di rete, guasto di alimentazione, guasto di dispositivi medici / non responsabilità del loro produttore
Errori umani	Errore di configurazione del sistema sanitario, assenza di registri di verifica, controllo dell'accesso non autorizzato / assenza di procedure in materia, mancata conformità (BYOD), errore del personale medico / paziente
Atti dolosi	Malware (virus, ransomware, BYOD), furto di account (cryptojacking, medjacking), ingegneria sociale (phishing, baiting, clonazione di dispositivi), furto (dati, dispositivi), manomissione di dispositivi medici, clonazione di carte di credito, attacchi di tipo «denial of Service», attacchi dal web, attacchi alle applicazioni web, minacce interne, manipolazione fisica / danno fisico, furto d'identità, spionaggio informatico, danni meccanici ai componenti
Guasti di sistema	Avaria del software, firmware non aggiornato, guasto di un dispositivo, guasto dei componenti di rete, manutenzione insufficiente

BUONE PRASSI PER LA CIBERSICUREZZA IN MATERIA DI APPALTI

Il seguente elenco di buone prassi non è in alcun modo esaustivo, ma rappresenta un ottimo punto di partenza per l'operatore informatico sanitario responsabile per l'acquisto di apparecchiature ospedaliere. Questa serie di buone prassi è il risultato a livello collettivo di tutti i contributi degli operatori sanitari intervistati. Il lettore può adeguare l'elenco sulla base delle priorità della sua organizzazione.

BP 1. Coinvolgere il dipartimento informatico nelle varie fasi dell'appalto per garantire che si tenga conto delle competenze negli aspetti della cibersicurezza.

Fasi dell'appalto: tutte

Tipi di appalto correlati: tutti

Minacce correlate: tutte

BP 2. Attuare una procedura di identificazione e gestione delle vulnerabilità per garantire che queste ultime vengano prese in considerazione prima di acquisire nuovi prodotti o servizi e che vengano monitorati i difetti di prodotti/servizi esistenti per tutta la durata del loro ciclo di vita.

Fasi dell'appalto: tutte

Tipi di appalto correlati: sistemi informativi clinici, dispositivi medici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: tutte

BP 3. Sviluppare una policy per gli aggiornamenti hardware e software per verificare che siano state applicate le patch più recenti per OS e il proprio software e che l'antivirus sia aggiornato.

Fasi dell'appalto: tutte

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 4. Potenziare i controlli di sicurezza per la comunicazione senza fili, al fine di garantire che l'accesso alle reti wi-fi dell'ospedale sia limitato e rigorosamente controllato.

Fasi dell'appalto: tutte

Tipi di appalto correlati: dispositivi medici, dispositivi client remoti, sistemi di identificazione, servizi cloud

Minacce correlate: atti dolosi, errori umani

BP 5. Definire policy di collaudo per verificare che prodotti recentemente acquisiti o configurati siano sottoposti a un test anti-intrusione e vengano adottate misure correttive conformi ai parametri operativi dell'ambiente reale.

Fasi dell'appalto: tutte

Tipi di appalto correlati: sistemi informativi clinici, dispositivi medici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, guasti di sistema, errori umani

BP 6. Definire piani di continuità operativa per garantire che un guasto di sistema non causi l'interruzione dei servizi essenziali dell'ospedale e che il ruolo del fornitore sia ben definito.

Fasi dell'appalto: tutte

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 7. Tenere conto degli aspetti che riguardano l'interoperabilità per garantire l'assenza di divari in termini di sicurezza rispetto ai componenti già esistenti (struttura informatica preesistente).

Fasi dell'appalto: tutte

Tipi di appalto correlati: sistemi informativi clinici, dispositivi medici, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: guasti di sistema, errori umani, atti dolosi

BP 8. Collaudare tutti i componenti per garantire che siano all'altezza delle aspettative: verificare la facilità d'uso, la correttezza dei risultati sotto carico e le eventuali falle di sicurezza (politica delle password inadeguata, SQL injection).

Fasi dell'appalto: tutte

Tipi di appalto correlati: sistemi informativi clinici, dispositivi medici, dispositivi client remoti, sistemi di identificazione, servizi cloud, sistemi industriali di controllo, sistemi di teleassistenza, sistema di gestione degli edifici, dispositivi mobili client

Minacce correlate: atti dolosi, errori umani, guasti di sistema, interruzione della catena di approvvigionamento

BP 9. Consentire la verifica e la registrazione per tracciare gli hacker e l'entità delle informazioni perse/rubate una volta che il sistema sia compromesso.

Fasi dell'appalto: tutte

Tipi di appalto correlati: dispositivi medici, sistemi di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 10. Crittografare dati personali sensibili a riposo e in transito attraverso la definizione di una policy per i sistemi, i servizi o i dispositivi che trattano le categorie speciali di dati personali di cui all'articolo 9 del RGPD.

Fasi dell'appalto: tutte

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 11. Eseguire una valutazione dei rischi nell'ambito della procedura di appalto.

Fasi dell'appalto: pianificazione

Tipi di appalto correlati: tutti

Minacce correlate: tutte

BP 12. Pianificare in anticipo i requisiti di rete, hardware e licenza per stabilire se occorra effettuare aggiornamenti e/o acquisti supplementari prima dell'installazione ai fini dell'adeguamento al nuovo sistema.

Fasi dell'appalto: pianificazione

Tipi di appalto correlati: sistemi informativi clinici, apparecchiature di rete, sistemi di identificazione, sistemi industriali di controllo

Minacce correlate: interruzione della catena di approvvigionamento, guasti di sistema, fenomeni naturali, errori umani

BP 13. Identificare minacce correlate ai prodotti o ai servizi da acquisire e verificare che l'identificazione delle minacce sia costante lungo il ciclo di vita della procedura di appalto.

Fasi dell'appalto: pianificazione, gestione

Tipi di appalto correlati: tutti

Minacce correlate: tutte

BP 14. Segregare la propria rete per garantire la possibilità di isolarne / filtrarne il traffico, in modo da limitare e /o impedire l'accesso tra zone di rete.

Fasi dell'appalto: pianificazione, approvvigionamento

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 15. Determinare i requisiti di rete per garantire l'interoperabilità ed evitare scompensi dopo la creazione della rete e della topologia dei componenti

Fasi dell'appalto: pianificazione

Tipi di appalto correlati: sistemi informativi clinici, apparecchiature di rete, sistemi di identificazione, sistemi industriali di controllo, servizi cloud, sistemi di teleassistenza, dispositivi mobili client

Minacce correlate: interruzione della catena di approvvigionamento, guasti di sistema, fenomeni naturali

BP 16. Stabilire requisiti minimi di sicurezza e tradurli in criteri di ammissibilità durante la selezione dei fornitori.

Fasi dell'appalto: pianificazione, approvvigionamento

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 17. Preparare una richiesta di offerta apposita per l'appalto di servizi cloud che tenga conto dei requisiti normativi e programmatici.

Fasi dell'appalto: pianificazione, approvvigionamento

Tipi di appalto correlati: servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento

BP 18. Assegnare priorità all'appalto di risorse certificate in base a sistemi/standard di cibersicurezza.

Fasi dell'appalto: approvvigionamento

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 19. Condurre valutazioni d'impatto sulla protezione dei dati durante la pianificazione dell'appalto di un nuovo sistema o servizio.

Fasi dell'appalto: approvvigionamento

Tipi di appalto correlati: sistemi informativi clinici, dispositivi medici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, servizi professionali, servizi cloud

Minacce correlate: atti dolosi, errori umani

BP 20. Predisporre gateway che mantengano connessi i sistemi/macchinari preesistenti e prevedere un controllo di frontiera in caso di problemi all'interno di questi gruppi.

Fasi dell'appalto: approvvigionamento, gestione

Tipi di appalto correlati: dispositivi medici, sistemi di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 21. Fornire una formazione sulle prassi di cibersicurezza dell'organizzazione per garantire che il personale interno o i contraenti/consulenti esterni che lavorano in sede siano adeguatamente preparati.

Fasi dell'appalto: approvvigionamento, gestione

Tipi di appalto correlati: tutti

Minacce correlate: atti dolosi, errori umani

BP 22. Elaborare piani di risposta in caso di incidenti tenendo conto di prodotti o sistemi recentemente acquisiti.

Fasi dell'appalto: approvvigionamento, gestione

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 23. Coinvolgere il fornitore/produttore nella gestione degli incidenti e fissare termini chiari nella richiesta di offerta.

Fasi dell'appalto: approvvigionamento, gestione

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 24. Programmare e monitorare le operazioni di manutenzione per tutte le apparecchiature, in modo da garantire un adeguato livello di funzionalità e decidere l'applicazione di eventuali aggiornamenti/patch, ecc.

Fasi dell'appalto: approvvigionamento, gestione

Tipi di appalto correlati: sistemi informativi clinici, apparecchiature di rete, dispositivi medici, sistemi di gestione degli edifici, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: errori umani, guasti di sistema, fenomeni naturali

BP 25. L'accesso remoto deve essere ridotto al minimo e gestito in modo che le comunicazioni esterne con il fornitore siano limitate esclusivamente al dispositivo che deve controllare.

Fasi dell'appalto: approvvigionamento, gestione

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema, errori umani

BP 26. Richiedere l'applicazione di patch per tutti i componenti e includere informazioni in materia nella richiesta di offerta.

Fasi dell'appalto: approvvigionamento, gestione

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema

BP 27. Sensibilizzare il personale in merito alla cibersicurezza per garantire che sia conscio dei rischi connessi a prodotti o servizi recentemente acquisiti.

Fasi dell'appalto: gestione

Tipi di appalto correlati: tutti

Minacce correlate: tutte

BP 28. Eseguire l'inventario delle risorse e la gestione della configurazione per accertarsi che l'inventario sia opportunamente aggiornato quando viene aggiunto o rimosso un componente dall'ambiente TIC e verificare che siano impostate e adeguatamente gestite configurazioni minime di sicurezza.

Fasi dell'appalto: gestione

Tipi di appalto correlati: sistemi informativi clinici, dispositivi medici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione

Minacce correlate: atti dolosi, errori umani, guasti di sistema

BP 29. Stabilire meccanismi di controllo dell'accesso destinati a impianti per dispositivi medici che devono essere protetti anche fisicamente e accessibili solo al personale specializzato.

Fasi dell'appalto: gestione

Tipi di appalto correlati: dispositivi medici, sistema di gestione degli edifici, sistemi di identificazione

Minacce correlate: atti dolosi, errori umani

BP 30. Programmare test anti-intrusione con frequenza o dopo una modifica dell'architettura/del sistema e includere i relativi termini nella richiesta di offerta.

Fasi dell'appalto: approvvigionamento, gestione

Tipi di appalto correlati: dispositivi medici, sistemi informativi clinici, apparecchiature di rete, sistema di teleassistenza, dispositivi mobili client, sistemi di identificazione, sistemi industriali di controllo, servizi cloud

Minacce correlate: atti dolosi, interruzione della catena di approvvigionamento, guasti di sistema