IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Il dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

in virtù della delega conferita con deliberazione N°327/2025

HA ASSUNTO LA PRESENTE DETERMINAZIONE

N. 639 del 27/06/2025

OGGETTO: AFFIDAMENTO, TRAMITE MEPA, AI SENSI DELL'ART. 50 COMMA 1 LETTERA B) DEL D.LGS. 36/2023, ALLA SOCIETA' CYBER-BEE SRL DEL SERVIZIO DI SUPPORTO PER LE ATTIVITA' DI FORMAZIONE AI FINI DELL'ACQUISIZIONE DELLE COMPETENZE IN MODALITÀ E-LEARNING, ANCHE NELL'AMBITO DELLE DIRETTIVA UE NIS 2, NECESSARIE ALLA GESTIONE DEL RISCHIO INFORMATICO DEGLI IFO PER IL PERIODO 01.07.2025 – 30.06.2026 - CIG: B75CE04031

Esercizi/o e conto 2025-2026 502020302 Centri/o di costo 1000115

- Importo presente Atto: € 73.200,00

- Importo esercizio corrente: € 36.600,00

Budget

- Assegnato: € -

- Utilizzato: € -

- Residuo: € -

Autorizzazione n°: 2025/2026 1 SIST INF

Servizio Risorse Economiche: **Livio Cardelli**

UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici Proposta n° DT-657-2025

L'estensore

Silvia Placidi

Il Responsabile del Procedimento

Giuseppe Navanteri

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Giuseppe Navanteri

La presente determinazione si compone di n° 8 pagine e dei seguenti allegati che ne formano parte integrante e sostanziale:
Allegato 1 e Allegato 2

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Visto il decreto legislativo 30 dicembre 1992 n. 502 e successive modificazioni ed integrazioni;
il decreto legislativo 16 ottobre 2003 n. 288 e il decreto legislativo 23 dicembre 2022 n. 200 di riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico;

Vista la legge regionale 23 gennaio 2006, n. 2;

Visto l'Atto Aziendale adottato con deliberazione n. 153 del 19 febbraio 2019 e approvato dalla Regione Lazio con DCA n. U00248 del 2 luglio 2019, modificato e integrato con deliberazioni n. 1254 del 02 dicembre 2020, n. 46 del 2 gennaio 2021 e n. 380 del 25 marzo 2021, approvate dalla Direzione Salute e Integrazione Sociosanitaria della Regione Lazio, con Determinazione n. G03488 del 30 marzo 2021;

Visto il Decreto del Presidente della Regione Lazio n. T00015 del 12 febbraio 2025 avente ad oggetto "*Nomina del Direttore Generale dell'Azienda Sanitaria Locale dell'IRCCS Istituti Fisioterapici Ospitalieri (Art. 8, comma 7 bis, della legge* regionale 16 giugno 1994, n. 18 e s.m.i.)";

Vista la deliberazione n. 160 del 18 febbraio 2025 di presa d'atto dell'insediamento del Direttore Generale dell'IRCCS Istituti Fisioterapici Ospitalieri Dott. Livio De Angelis;

Visto il D.M. del Ministero della Salute del 20 giugno 2024 di conferma del riconoscimento del carattere scientifico dell'IRCCS di diritto pubblico a Istituti Fisioterapici Ospitalieri (IFO) relativamente alla disciplina di "oncologia" per l'Istituto Nazionale Tumori Regina Elena (IRE) e alla disciplina di "dermatologia" per l'Istituto Santa Maria e San Gallicano (ISG);

Vista la deliberazione n. 446 del 27 maggio 2024 di attribuzione delle deleghe ai Dirigenti del Ruolo Professionale, Tecnico e Amministrativo degli IFO;

Visto il D.Lgs n.36 del 31 marzo 2023 s.m.i., avente ad oggetto "Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici";

Premesso che con l'entrata in vigore della Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148, meglio nota come NIS 2, l'Unione Europea ha dato avvio ad un aggiornamento cruciale nella legislazione dell'Unione Europea per la sicurezza delle reti e delle informazioni stabilendo una strategia comune di cybersecurity per tutti gli Stati membri ed elevando i livelli di sicurezza dei servizi digitali su scala europea;

che con il D.Lgs 138/2024 di recepimento della Direttiva NIS 2 il Governo ha stabilito misure volte a garantire un livello elevato di sicurezza informatica su tutto il territorio italiano, contribuendo così ad incrementare il livello comune di sicurezza nell'Unione europea;

Considerato che negli ultimi anni, nello scenario nazionale ed internazionale, si sta assistendo ad un incremento esponenziale degli attacchi informatici alle infrastrutture IT di tutte le organizzazioni sia private che pubbliche, rendendo imprescindibile la necessità di incrementare la capacità di resilienza rispetto al cyber-risk;

Constatato anche che l'accelerazione della digitalizzazione, dettata dal Piano triennale per l'informatica, amplifica ancor di più l'esigenza di assicurare una transizione cyber-resiliente, garantendo sicurezza ai dati e la continuità dei servizi digitali dei cittadini e delle imprese;

inoltre, che la sicurezza delle informazioni e la protezione dei dati, in particolare riferiti all'ambito dei servizi sociosanitari, rappresentano elementi fondamentali e abilitanti per innovare i servizi ed incrementare la produttività del Sistema Regionale nonché per migliorare la qualità della vita dei cittadini e la competitività delle imprese;

Dato atto che gli IFO hanno investito nel campo della sicurezza informatica raggiungendo un consistente livello di maturità a livello organizzativo, procedurale e tecnologico soprattutto nell'ambito della gestione ed erogazione di servizi digitali;

Verificato che la sempre più diffusa e capillare informatizzazione dei servizi e la sempre maggiore integrazione e interdipendenza dei sistemi in uso richiede di adottare misure di sicurezza tecnologiche ed organizzative sempre più sofisticate che consentano di prevenire attacchi informatici, preservare l'integrità dei dati e delle informazioni gestite nell'ambito dell'intero sistema sociosanitario regionale e assicurare la continuità dei servizi per i cittadini;

Ravvisata pertanto la necessità di adottare le dovute contromisure basate non solo sul potenziamento della infrastruttura tecnologica e sul rafforzamento del perimetro del rischio, ma anche sull'accrescimento della consapevolezza che i comportamenti umani rappresentano principalmente l'anello debole della Cyber Security;

Rilevata quindi l'esigenza di prevedere interventi di formazione nell'ambito della cybersecurity, volti a promuovere la cultura della sicurezza informatica e della

prevenzione dei rischi informatici prevedendo l'erogazione di specifici moduli formativi obbligatori rivolti a tutti i dipendenti orientati a trasformare efficacemente i comportamenti dei discenti rendendoli adeguati in termini di cognizione della minaccia e prontezza nell'agire correttamente;

Verificato che è stata individuata una soluzione per le attività di rafforzamento e rinnovo delle competenze digitali del personale degli IFO, attraverso un preciso e puntuale piano di formazione in grado di rafforzare il livello di consapevolezza dei rischi di Cyber Security;

che la soluzione in parola, denominata CYBER GURU, consente di tradurre gli adempimenti previsti dalla Direttiva NIS2 in un'opportunità strategica, fornendo strumenti operativi per supportare gli organi di amministrazione e i dirigenti delle pubbliche amministrazioni nel rafforzare la resilienza digitale dell'Ente, garantendo una protezione efficace dalle minacce cyber sempre più sofisticate e rendendoli in grado di:

- ✓Interpretare il contesto strategico della sicurezza informatica;
- ✓Analizzare l'evoluzione degli scenari nazionali e internazionali in materia di cyber security;
- ✓Identificare e comprendere i rischi cyber a cui è esposta la propria amministrazione;
- ✓Valutare e approvare strategie, piani, policy e procedure finalizzate alla mitigazione del rischio;

che tale sistema di e-learning, pensato specificatamente per il personale non specialistico delle organizzazioni pubbliche e private, viene fornita dall'Operatore Economico CYBER-BEE SRL, abilitato sul MePA di Consip;

Valutato che la scrivente Uosd ha effettuato un'informale indagine di mercato sul Mepa di Consip per verificare la sussistenza di altre società in grado di svolgere in

maniera equivalente, o superiore, le attività di training della piattaforma software Cyber Guru;

Dato atto che, a seguito di una valutazione tecnico-economica è stato valutato di procedere con la soluzione offerta dalla società CYBER-BEE S.R.L., azienda partner di Cyber Guru, accreditata dall'Agenzia per la Cybersicurezza Nazionale, in riferimento a quanto sopra esposto;

Letto l'art.50 comma 1 lett. b) del D. Lgs. 36/2023 per il quale "le stazioni appaltanti procedono all'affidamento di lavori, servizi e forniture […] con affidamento diretto dei servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a 140.000 euro, anche senza consultazione di più operatori economici";

Verificato che non sono attivi Accordi Quadro o Convenzioni Consip per l'affidamento in oggetto;

Considerato che, invece, il servizio di che trattasi è presente sul Me.PA di Consip sotto la categoria "Licenze software-Mepa Servizi" ed è inserito a catalogo dalla Società CYBER-BEE SRL;

Dato atto che, al fine di procedere all'affidamento del servizio in parola, la scrivente UOSD ha avviato sul Me.PA di Consip la Trattativa Diretta n. 5435533 per la fornitura delle due piattaforme in modalità e-learning denominate "CYBER GURU ENTERPRISE PLUS" e "BOARD TRAINING NIS2" (Allegato 1);

che, entro la data stabilita per la scadenza della ricezione dell'offerta, la società invitata ha provveduto a inviare un'offerta tecnico-economica d'importo pari a € 60.000,00 oltre Iva (Allegato 2);

Verificato che l'importo della suddetta offerta risulta congruo e in linea con gli importi di mercato relativi ad analoghi servizi e che, in conseguenza, è possibile procedere con l'affidamento della trattativa MEPA di che trattasi per un importo complessivo € 73.200,00 Iva inclusa alla società CYBER-BEE SRL a copertura del periodo 01.07.2025 - 30.06.2026 – CIG: B75CE04031;

Attestato che la complessiva spesa di € 60.000,00 oltre Iva al 22% (€ 73.200,00 Iva inclusa) può essere registrata come di seguito specificato:
- € 36.600,00 Iva inclusa sul conto economico 502020302 dell'esercizio finanziario 2025;
- € 36.600,00 Iva inclusa sul conto economico 502020302 dell'esercizio finanziario 2026;

che il presente provvedimento, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è ritenuto adeguato e sufficiente in relazione al principio del risultato di cui all'art.1 del Dlgs n.36/2023 ed è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 14 gennaio 1994, n. 20 e successive modifiche, nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 7 agosto 1990, n. 241, come modificata dalla legge 11 febbraio 2005, n. 15;

DETERMINA

Per i motivi esposti in narrativa e che si intendono integralmente confermati di:

- Affidare, ai sensi dell'art. 50 comma 1 lett. b) del D.lgs 36/2023, alla società CYBER-BEE SRL il servizio di supporto per le attivita' di formazione ai fini dell'acquisizione delle competenze in modalità e-learning, necessarie alla gestione del rischio informatico degli IFO anche nell'ambito delle Direttiva UE NIS2, a copertura del periodo 01.07.2025 - 30.06.2026 e per un importo complessivo di €60.000,00 oltre IVA al 22% – CIG: B75-CE04031;

- Attestare che la spesa complessiva di € 73.200,00 Iva inclusa può essere registrata come di seguito specificato:
  - € 36.600,00 Iva inclusa sul conto economico 502020302 dell'esercizio finanziario 2025;
  - € 36.600,00 Iva inclusa sul conto economico 502020302 dell'esercizio finanziario 2026;
- Trametterе apposito ordine NSO;
- Nominare DEC del presente affidamento l'Ing. Giuseppe Navanteri.

La UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici curerà tutti gli adempimenti per l'esecuzione della presente determinazione.

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Giuseppe Navanteri

Documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

acquistinretepa

SISTEMI DI E-PROCUREMENT

IDENTIFICATIVO DELL'RDO: 5435533

Tipologia di Rdo: Trattative Dirette

Si richiede la migliore offerta tecnico-economica per l'acquisto della piattaforma "CYBER GURU ENTERPRISE PLUS" comprensiva dei moduli:
1) Cyber Guru Awareness (CGA): piano di formazione basato su di una piattaforma di e-learning composto nel suo complesso di 3 cicli di 12 mesi.
2) Cyber Guru Phishing (CGP): Sistema di training esperienziale anti-phishing

e acquisito Piattaforma Board Training NIS2

Dati Principali

Numero RDO
5435533

Nome RDO
Richiesta di offerta per piattaforma "CYBER GURU ENTERPRISE PLUS" e "BOARD TRAINING NIS2"

Tipologia di contratto
Appalto di servizi

Tipologia di procedura
Affidamento diretto dei servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a 140.000 euro

Regolamento applicabile alla procedura telematica
Regolamento MEPA eProcurement Acquistinrete

Ruoli e Autorizzazioni

Stazione Appaltante
AMMINISTRAZIONI ENTI ED AZIENDE DEL S.S.N. > AZIENDE OSPEDALIERE, POLICLINICI, IRCCS e ISTITUTI ZOOPROFILATTICI > I.R.C.C.S. ISTITUTI FISIOTERAPICI

Ente Committente
AMMINISTRAZIONI ENTI ED AZIENDE DEL S.S.N. > AZIENDE OSPEDALIERE, POLICLINICI, IRCCS e ISTITUTI ZOOPROFILATTICI > I.R.C.C.S. ISTITUTI FISIOTERAPICI OS...

GN

Responsabile del procedimento

GIUSEPPE NAVANTERI
NVNGPP84P23D086R

Soggetto Stipulante/Soggetti Stipulanti

GIUSEPPE NAVANTERI NVNGPP84P23D086R

OSPITALIERI ROMA

GN

Date

Pubblicazione
12/06/2025 11:49

Inizio presentazione offerte
12/06/2025 11:49

Termine ultimo presentazione offerte
20/06/2025 12:00

Data limite stipula contratto
28/08/2025 12:00

Giorni dopo la stipula per consegna beni/decorrenza
5

Dettaglio

Criterio Aggiudicazione
Minor Prezzo

CIG
B75CE04031

CUP
-

CPV

Identificativo	Descrizione	Categoria	Fornitura
72500000-0	Servizi informatici	Licenze software-Mepa Servizi	100

Formulazione offerta economica
VALORE ECONOMICO

Decimali Offerta
2

Termini di pagamento
60 GG DATA RICEVIMENTO FATTURA

Importo base d'asta

€ 75.000,00

Dati consegna e fatturazione

Fatturazione: VIA ELIO CHIANESI 53 - PRESSO UO INFORMATICA CED ROMA (ROMA);Consegna: VIA ELIO CHIANESI 53 - PRESSO UO INFORMATICA CED ROMA (ROMA); Aliquote: secondo la normativa vigente

GN

GN

Documentazione Gara

Request REQUEST.xml

7.3 Kb

DGUE REQUEST

GN

Inviti

Partita IVA	Ragione sociale
14559061008	CYBER-BEE S.R.L.

GN

Oggetto: Descrizione piattaforma software Cyber Guru per:

- ✓ 2000 utenti
- ✓ Fino a 150 membri dell'organo direttivo

1) Descrizione Piattaforma Cyber Guru ENTERPRISE PLUS

Cyber Guru Enterprise Plus (di seguito CGE Plus) è una piattaforma di "e-learning" di cui Cyber Guru S.r.l. è proprietaria e titolare dell'uso esclusivo e del diritto di commercializzazione in favore di soggetti pubblici e privati.

CGE Plus si compone di tre sottosistemi:

1) Cyber Guru Awareness (CGA): piano di formazione basato su di una piattaforma di e-learning composto nel suo complesso di 3 cicli di 12 mesi.

2) Cyber Guru Phishing (CGP): Sistema di training esperienziale anti-phishing

3) Cyber Guru Channel (CGC): Serie TV a tema cyber

2) Descrizione Piattaforma Board Training NIS2

4) PA Training – NIS2 è un programma formativo in modalità e-learning, strutturato per supportare gli organi di amministrazione e direttivi delle pubbliche amministrazioni nell'acquisizione delle competenze necessarie alla gestione del rischio informatico.
5) La Direttiva NIS2 attribuisce una responsabilità diretta agli organi di governo delle istituzioni in materia di sicurezza cibernetica, introducendo specifici obblighi formativi volti a rafforzare la capacità di prevenzione e risposta alle minacce digitali.
6) Il percorso formativo è rivolto alle pubbliche amministrazioni rientranti nel perimetro di applicazione della Direttiva UE NIS2 incluse PA centrali, locali ed enti pubblici che erogano servizi critici, oltre a subappaltatori e fornitori coinvolti

La soluzione consente di tradurre gli adempimenti previsti dalla Direttiva NIS2 in un'opportunità strategica, fornendo strumenti operativi per supportare gli organi di amministrazione e i dirigenti delle pubbliche amministrazioni nel rafforzare la resilienza digitale dell'ente e garantire una protezione efficace dalle minacce cyber sempre più sofisticate, rendendoli in grado di:

- ✓ Interpretare il contesto strategico della sicurezza informatica;
- ✓ Analizzare l'evoluzione degli scenari nazionali e internazionali in materia di cyber security;
- ✓ Identificare e comprendere i rischi cyber a cui è esposta la propria amministrazione;
- ✓ Valutare e approvare strategie, piani, policy e procedure finalizzate alla mitigazione del rischio;
- ✓ Valutare le azioni di mitigazione (procedurali, organizzative e tecniche) più idonee

Struttura del documento

Il presente documento descrive l'offerta economica per il cliente in oggetto, in Allegato A riporta l'elenco dei moduli del percorso Awareness ed una breve descrizione di ognuno di essi, in Allegato B riporta l'elenco dei moduli della NIS2 ed una breve descrizione di ogniuno di essi.

7) Descrizione Piattaforma Cyber Guru Awareness (CGA)

Cyber Guru Awareness è un innovativo sistema di e-learning pensato specificatamente per il personale non specialistico delle organizzazioni pubbliche e private. Il primo sistema progettato interamente in Italia, che si fonda su metodologie di formazione che tengono conto delle modalità di apprendimento digitale che risultano maggiormente efficaci in Italia. CGA è stato progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, che si caratterizza per un approccio "a rilascio costante e graduale":

- la formazione impegna il partecipante per pochi minuti a settimana, ma con un percorso diviso in annualità, che mantiene elevata l'attenzione del partecipante ogni qualvolta interagisce con le tecnologie digitali;
- tutte le lezioni sono disponibili in formato multimediale, con la possibilità di fruire dei contenuti sia in formato video sia in formato testuale;
- il linguaggio utilizzato risponde a un criterio divulgativo, focalizzato sul personale non specializzato sulla Cyber Security;
- ogni lezione è corredata da test di valutazione del livello di apprendimento;
- il corso usa una metodologia di GAMIFICATION, corredata da premi e riconoscimenti, che stimola l'apprendimento e premia l'eccellenza;
- è prevista un'organizzazione in team che dà luogo ad una competizione tra team diversi;
- ogni modulo formativo è auto-consistente perché affronta uno specifico argomento;
- i moduli formativi sono in totale 12 e una loro sintetica descrizione è presente nell'Allegato A di questo documento;
- i moduli formativi vengono erogati con la frequenza di uno ogni mese.

8) Descrizione Piattaforma Cyber Guru PHISHING (CGP)

Cyber Guru Phishing (di seguito CGP) è una soluzione innovativa di training Anti Phishing che produce risultati efficaci grazie alla sua particolare metodologia addestramento esperienziale. Basato su automazione e machine learning, CGP è rivolto a tutto il personale delle organizzazioni pubbliche e private, esso consente di mantenere "allenate" due importanti caratteristiche difensive umane: la prontezza e la reattività. Questo risultato viene raggiunto mediante la simulazione di campagne di Phishing cui vengono sottoposti tutti gli utenti (una mail al mese). Mail diverse verranno mandate dal sistema ai diversi utenti ed il livello di difficoltà di ogni esercitazione varierà per ogni utente sulla base delle reali prestazioni di ogni utente.

CGP si propone come la naturale integrazione ai programmi formativi della linea Cyber Guru, aumentando la reattività dell'individuo di fronte a attacchi basati su tecniche di Phishing. Considerando che i maggiori pericoli per la sicurezza delle organizzazioni sono "in agguato" nelle caselle e-mail dei loro dipendenti e collaboratori, le simulazioni di attacco Phishing, messe in atto da Cyber Guru Phishing, "personalizzate" sulla base delle caratteristiche peculiari di ogni singolo utente, preparano dipendenti e collaboratori a modificare i comportamenti e ad individuare con prontezza mail di phishing.

9) Descrizione Piattaforma Cyber Guru CHANNEL (CGC)

Cyber Guru Channel è una piattaforma che pubblica su base mensile video di alta qualità, della durata di 5-8 minuti l'uno, che analizzano dei casi di attacchi/frodi cyber. I format utilizzati sono diversi (Cyber Detective, Break News, Sit-Com). Ogni video e' poi dotato di un documento di approfondimento che analizza più nel dettaglio il fatto cyber affrontato nel video.

10) Servizi Assistenza

GN

11) Il Servizio di Assistenza ai gestori si esplica mediante posta elettronica (casella support@cyberguru.it); risposte vengono garantite entro 8 ore lavorative dalla ricezione. L'assistenza viene fornita nella fase iniziale del servizio per tutte le attività di on-boarding degli utenti e, nel corso di validità dell'intero contratto, per tutte le tematiche di fruizione e disponibilità del servizio stesso.
12) CSM (Customer Success Management)
13) Viene offerto, compreso nel canone presentato a prescindere dall'opzione scelta, un servizio di CSM (Customer Success Management) che supporta il cliente nella corretta implementazione del servizio di training. Più precisamente al momento dello start-up del progetto, viene assegnato uno specialista di Cyber Guru che assiste il cliente, mediante videoconferenze, sia nella fase di avviamento del piano formativo (on boarding degli utenti, supporto alla suddivisione in team, ausilio alla comunicazione agli utenti, scelta dei template per phishing mail, analisi primi risultati,…), sia nel corso di esecuzione del piano, mediante riunioni mensili mirate all'analisi dei risultati.

Allegato A – Moduli Formativi CGA (12 mesi)

14) Descrizione dei moduli formativi

Di seguito la lista dei 12 moduli formativi. Benché ogni modulo è auto-consistente, la sequenza con cui sono stati organizzati è stata studiata per produrre dei "naturali" richiami ad argomentazioni già affrontate in precedenza, rafforzando in questo modo il livello di apprendimento e memorizzazione dei contenuti.

Anno 1

PHISHING

Il PHISHING è la più comune tecnica di attacco utilizzata dai criminali Cyber e utilizza la mail come principale veicolo di diffusione, anche se si va estendendo velocemente ad altri canali, come i più popolari canali di messaggistica e i canali social. È particolarmente subdola perché basata su un inganno, con cui si cerca di indurre la potenziale vittima a compiere un'azione che consente al criminale di sferrare il suo attacco. Questo modulo formativo fornisce gli elementi cognitivi per riconoscere un attacco PHISHING e per adottare le necessarie contromisure.

PASSWORD

Uno dei pilastri della Cyber Security è rappresentato dalla PASSWORD, la chiave di accesso a tutte quelle risorse informatiche a cui si deve garantire un accesso sicuro e riservato. La gestione delle proprie PASSWORD diventa quindi un elemento basilare delle strategie difensive, della persona e dell'organizzazione. Questo modulo formativo fornisce gli elementi cognitivi necessari ad una gestione sicura delle PASSWORD, mettendole al riparo da tentativi di violazione che potrebbero avere conseguenze disastrose.

SOCIAL MEDIA

I SOCIAL MEDIA rappresentano una nuova modalità di socializzazione basata sulle ampie possibilità che la tecnologia digitale mette oggi a disposizione. Ma allo stesso tempo sono anche fattori di rischio, dove si può arrivare a compromettere sia la privacy delle persone sia la sicurezza dei sistemi delle organizzazioni. Questo modulo fornisce gli elementi cognitivi per utilizzare in modo consapevole questi strumenti, proteggendo la persona e l'organizzazione dai rischi che la condivisione in rete di contenuti individuali e professionali può generare.

PRIVACY & GDPR

L'introduzione del nuovo regolamento europeo sulla protezione dei dati aumenta la sensibilità delle organizzazioni rispetto alla PRIVACY e alla protezione dei dati sensibili. Al di là dei ruoli specifici, è importante che tutti i membri di un'organizzazione acquisiscano maggiore sensibilità rispetto alla protezione dei dati.

Questo modulo fornisce gli elementi cognitivi per assumere un atteggiamento proattivo rispetto alla protezione dei dati, e per contribuire alla conformità dell'organizzazione rispetto alle nuove norme europee.

MOBILE & APP

I DEVICE MOBILI, soprattutto Smartphone e Tablet, sono strumenti che diventano ogni giorno più critici e che rappresentano la massima espressione della rischiosa sovrapposizione tra dimensione personale e professionale. Questo modulo fornisce gli elementi cognitivi per utilizzare i dispositivi mobili, siano essi personali o professionali, in modo consapevole, abilitando buone pratiche che siano in grado di aumentare il livello di sicurezza e di protezione dei dati.

FAKE NEWS

Le FAKE NEWS sono articoli redatti con informazioni inventate o semplicemente distorte, che hanno lo scopo di disinformare. Sono un fenomeno pericoloso, che se non controllato può avere ripercussioni negative sia per l'individuo sia per le organizzazioni. L'argomento viene spesso trattato dal punto di vista sociale e politico, ma ha anche una implicazione diretta con la Cyber Security. Questo modulo formativo fornisce gli elementi cognitivi necessari a riconoscere una Fake News, attivando alcuni processi di indagine che aiutano a sviluppare un atteggiamento corretto su qualsiasi informazione acquisita in rete.

USB DEVICE

Tutti i dispositivi USB, e in particolare i dispositivi di memorizzazione, possono diventare un punto critico rispetto alla necessità di proteggere le informazioni riservate, ed è per questa ragione che sono spesso oggetto di specifiche policy. Questo modulo formativo fornisce gli elementi cognitivi per riconosce tutti i rischi associati ai dispositivi USB, con particolare riferimento ai dispositivi di memorizzazione, abilitando buone pratiche per evitare di incorrere in fenomeni di sottrazione di dati.

EMAIL SECURITY

La MAIL è uno strumento sempre più importante, che nella vita professionale assume un ruolo centrale e particolarmente critico. Attraverso le MAIL vengono scambiate informazioni sensibili e quindi l'aspetto della sicurezza non può essere sottovalutato. Questo modulo formativo fornisce gli elementi cognitivi per le mail e le informazioni in esse contenute.

MALWARE & RANSOMWARE

I MALWARE in generale e il RANSOMWARE in particolare hanno conquistato velocemente gli onori della cronaca, mettendo in evidenza tutta la loro pericolosità. Le persone devono comprendere che i software antivirus non garantiscono la protezione totale rispetto a questi programmi maligni. Questo modulo formativo fornisce gli elementi cognitivi per ridurre il rischio di cadere vittima di questa particolare tipologia di software e per limitare le conseguenze negative in caso di violazione.

WEB BROWSING

La NAVIGAZIONE nel WEB presenta molti rischi e in quella che ormai sembra quasi un'attività scontata si presentano molti aspetti critici. Una buona conoscenza di alcune caratteristiche peculiari dei siti Web e dei browser può aiutare a ridurre notevolmente il livello di rischio. Questo modulo formativo fornisce gli elementi cognitivi su come navigare nel WEB in sicurezza.

CRITICAL SCENARIOS

Nell'interazione con il Cyber Spazio, esistono alcuni scenari critici: l'uso delle piattaforme Cloud, il viaggio di piacere o di affari, piuttosto che l'uso delle piattaforme di e-commerce, sia in ambito B2B che B2C. Sono scenari che risultano particolarmente esposti alla possibilità di subire attacchi da parte dei criminali Cyber, con rischi sia sul piano individuale sia sul piano professionale. Questo modulo vuole fornire elementi essenziali di consapevolezza che aiutano a comprendere le minacce, spesso sottovalutate, che sono collegate a questi particolari scenari di utilizzo delle tecnologie digitali.

SOCIAL ENGINEERING

Il social engineering, o ingegneria sociale, è la madre di tutte le strategie di attacco Cyber. È una strategia che punta sull'inganno e sulla manipolazione psicologica per perseguire finalità truffaldine. Per rendere più efficace

l'attacco, il nucleo di questa strategia è costituito dall'acquisizione di informazioni sulla vittima designata. Questo modulo fornisce elementi di consapevolezza sulle tecniche utilizzate dai Cyber Criminali, diventando di fatto la sintesi ideale di elementi già trattati nei moduli precedenti.

Allegato B – Moduli Formativi NIS2 (12 mesi)

Il corso sulla Direttiva UE NIS2 affronta il rischio cyber, un problema sistemico che minaccia la stabilità delle infrastrutture digitali. Mira a fornire conoscenze e competenze manageriali per mitigare i rischi, con focus sulla normativa, la gestione del rischio, la prevenzione degli attacchi e gli impatti di tecnologie emergenti come Cloud e AI. Il corso è rivolto a imprese nel perimetro NIS2 e alla supply chain di grandi gruppi industriali.

SEZIONE I – QUADRO NORMATIVO

Lezione	Titolo Lezione	Descrizione Lezione
1	Il contesto normativo	Il contesto normativo della cybersicurezza si è evoluto dal 2010 con tre fasi principali: frammentazione iniziale (pre-2012), coordinamento nazionale con la Legge 133/2012, e istituzione dell'Agenzia per la Cybersicurezza Nazionale (2021). La Direttiva NIS 2, in vigore dal 2024, amplia il perimetro di applicazione e rafforza i requisiti di sicurezza per proteggere il sistema produttivo europeo, richiedendo strategie nazionali e team di risposta agli incidenti. In Italia, la direttiva NIS è stata recepita nel 2018, con un incremento significativo del numero di Operatori di Servizi Essenziali.
2	La Direttiva NIS2 (1)	La Direttiva NIS-2 rafforza la sicurezza informatica nell'UE ampliando il perimetro a soggetti essenziali e importanti in settori critici. Introduce requisiti rigorosi per la gestione dei rischi, la supervisione aziendale e la segnalazione degli incidenti, con misure tecniche, organizzative e operative. Gli organi aziendali sono responsabilizzati nella gestione della cybersecurity, sottolineando un approccio organizzativo e multi-rischio per proteggere infrastrutture e servizi essenziali.
3	La Direttiva NIS2 (2)	La Direttiva NIS-2 richiede misure di sicurezza specifiche per la gestione dei rischi cyber, come policy sui rischi, gestione degli incidenti, continuità operativa e sicurezza della supply chain. Promuove un approccio multi-rischio che include rischi fisici, umani e tecnologici. Prevede notifiche obbligatorie di incidenti significativi entro 24 e 72 ore e introduce un quadro sanzionatorio dettagliato: fino a 10 milioni di euro o il 2% del fatturato per soggetti essenziali, e fino a 7 milioni o l'1,4% per soggetti importanti. L'obiettivo è migliorare consapevolezza, preparazione e resilienza.
4	Recepimento della NIS2	Il Decreto Legislativo 138/2024 recepisce la Direttiva NIS-2 introducendo criteri aggiuntivi per l'inclusione nel perimetro e specifiche nazionali per la gestione dei rischi e la divulgazione delle vulnerabilità. Gli organi direttivi e amministrativi sono responsabilizzati nella gestione della cybersecurity e obbligati a formazione specifica. Sanzioni e sospensioni sono previste per mancato adempimento, con multe fino allo 0,1% del fatturato globale. Entro il 28 febbraio 2025, le aziende potenzialmente incluse nel perimetro devono registrarsi presso l'ACN e ottemperare agli obblighi entro il 2026.

GN

Lezione	Titolo Lezione	Descrizione Lezione
5	Il modello organizzativo NIS2	La NIS-2 introduce un approccio multirischio alla gestione della cybersecurity, responsabilizzando gli organi direttivi e assegnando ruoli specifici per garantire conformità e sicurezza. Le aziende devono istituire una funzione di NIS-2 Compliance, un Comitato NIS-2 per monitorare le attività, e assegnare responsabilità ai Direttori di Linea di Business (LOB) e ai Risk Owner. Gli organi direttivi sono responsabili delle misure di sicurezza e della formazione continua, mentre il Compliance Manager coordina le attività, realizza report periodici, effettua verifiche di secondo livello e supervisiona il risk management. I Risk Owner nelle LOB gestiscono e validano le analisi del rischio cyber, operando sotto delega esplicita dei Direttori LOB. Il Comitato NIS-2 si riunisce trimestralmente per monitorare l'avanzamento delle attività e prendere decisioni strategiche. Questo modello garantisce chiarezza nei ruoli, controllo delle vulnerabilità e maggiore resilienza aziendale.

SEZIONE II – RISCHI CYBER

Lezione	Titolo Lezione	Descrizione Lezione
1	Il rischio cyber	La gestione del rischio cyber, parte integrante delle attività aziendali, richiede di valutare e mitigare i rischi derivanti da vulnerabilità digitali sfruttate intenzionalmente da malintenzionati. La riduzione del rischio si basa su due dimensioni: abbassare la probabilità di un attacco attraverso prevenzione e consapevolezza, e limitare l'impatto tramite asset resilienti e best practice tecnologiche. Le strategie di mitigazione includono mitigare, eliminare, accettare o trasferire il rischio, mentre per influenzare i comportamenti umani è essenziale formare e allenare il personale. Una gestione efficace richiede il coinvolgimento di amministratori e specialisti per integrare misure tecniche e organizzative.
2	L’analisi del rischio cyber	L'analisi del rischio è fondamentale per comprendere minacce, probabilità e impatti, e definire le contromisure. Seguendo standard come ISO o NIST, si articola in sei fasi: identificare il contesto e i rischi, analizzarli, definire priorità, predisporre risposte e monitorare continuamente. L'output principale è il Risk Register, che mappa i rischi cyber e non, essenziale per strategie di sicurezza multi-rischio come richiesto dalla NIS-2. Questo strumento può essere adattato a diversi ambiti aziendali, integrandosi nell'Enterprise Risk Management per garantire resilienza e controllo.
3	La misura del rischio	La valutazione del rischio consiste nell'analizzare probabilità e impatto di un evento avverso per prendere decisioni consapevoli. Le analisi possono essere qualitative, più semplici ma soggettive, o quantitative, più complesse ma precise e utili per giustificare investimenti in mitigazione. Misurare il rischio aiuta a scegliere le migliori strategie di trattamento, riducendo l'incertezza e superando le distorsioni legate alla percezione personale.

GN

Lezione	Titolo Lezione	Descrizione Lezione
4	I controlli di sicurezza	La gestione degli incidenti di sicurezza si basa sull'analisi dei log generati dalle infrastrutture digitali per identificare e prevenire situazioni critiche. Il Security Operations Center (SOC) elabora gli allarmi attraverso un flusso operativo strutturato articolato in tre fasi: analisi preliminare, analisi dettagliata e definizione delle azioni di contenimento e rimedio. L'uso dell'Intelligenza Artificiale (AI) aiuta a ridurre i falsi positivi, migliorando l'efficienza operativa. Gli incidenti vengono valutati in base a gravità e impatto, utilizzando una matrice di criticità per pianificare le risposte e, nei casi più gravi, attivare un'escalation ai vertici aziendali. L'analisi forense finale consente di trarre lesson learned per prevenire il ripetersi di eventi simili in futuro.
5	Il danno	L'impatto rappresenta il danno causato da un evento avverso, classificabile in diretto, da responsabilità civile, indiretto e consequenziale. Nel rischio cyber, i danni si distinguono in propri (interruzione attività, ripristino sistemi, gestione dell'incidente) e verso terzi (contenziosi, violazioni di dati). Mentre i danni materiali sono più facilmente stimabili, quelli immateriali richiedono valutazioni complesse, rendendo l'analisi dell'impatto una sfida cruciale per le aziende.

SEZIONE III – ATTACCHI CYBER

Lezione	Titolo Lezione	Descrizione Lezione
1	La dinamica di un attacco	La dinamica del rischio cyber segue un modello in cui una minaccia sfrutta un vettore e una tecnica per colpire una vulnerabilità, generando un danno. Comprendere minacce, vettori e tecniche è cruciale: le minacce spaziano da singoli a organizzazioni complesse; i vettori includono email, app malevole o botnet; le tecniche variano dal phishing al malware. La mail è il vettore più comune, mentre le botnet, composte da dispositivi compromessi, sono usate per attacchi massivi come il DDoS. La consapevolezza umana è essenziale per mitigare i rischi, soprattutto in un contesto in cui l'AI rende gli attacchi più sofisticati.
2	Le principali tecniche di attacco	Le tecniche di attacco cyber includono malware, sfruttamento di vulnerabilità e attacchi Distributed Denial of Service (DDoS). I malware, compresi gli zero-day, sfruttano vulnerabilità sconosciute, mentre le vulnerabilità esposte su Internet consentono di sottrarre dati e ottenere accessi privilegiati, spesso attraverso il social engineering. I DDoS sovraccaricano infrastrutture o applicazioni, rendendole inservibili. L'uso dell'AI generativa rende questi attacchi sempre più sofisticati, richiedendo contromisure avanzate.
3	Le vulnerabilità	Le vulnerabilità rappresentano un rischio solo se non sono mitigate da controlli tecnici o procedurali. Il loro ciclo di vita attraversa quattro fasi: scoperta, divulgazione, individuazione della contromisura e applicazione, con le prime due particolarmente critiche. La gestione efficace delle vulnerabilità richiede un processo industrializzato, basato su aggiornamenti costanti, inventari completi degli asset e una strategia di priorità che affronti prima le minacce più gravi e urgenti, riducendo l'esposizione complessiva ai rischi.

Lezione	Titolo Lezione	Descrizione Lezione
4	Gli incidenti di sicurezza	La gestione degli incidenti di sicurezza si basa sull'analisi dei log prodotti dalle infrastrutture digitali, utilizzati per identificare e prevenire situazioni critiche. Il Security Operation Center (SOC) processa allarmi attraverso un flusso operativo articolato in tre fasi: analisi preliminare, analisi dettagliata e definizione delle azioni di contenimento e rimedio. L'uso dell'Intelligenza Artificiale riduce i falsi positivi, migliorando l'efficienza. Gli incidenti sono valutati in base a gravità e impatto, utilizzando una matrice di criticità per pianificare le risposte e, in casi gravi, attivare il coinvolgimento dei vertici aziendali. L'analisi forense finale fornisce "lessons learned" per prevenire future occorrenze.

SEZIONE IV – CASI CYBER

Lezione	Titolo Lezione	Descrizione Lezione
1	Truffa del CEO	Un cyber criminale compromette o falsifica la mail del CEO o di un altro membro del Board e invia un'email urgente al CFO o a un dirigente finanziario, ordinando un bonifico di milioni di euro verso un conto estero.
2	Attacco Ransomware con ricatto	Un’azienda leader nel settore energetico subisce un attacco ransomware che blocca i sistemi IT e paralizza le operazioni. I criminali minacciano di pubblicare dati sensibili del Board se il riscatto non viene pagato.
3	Attacco alla Supply Chain	Un fornitore di servizi cloud utilizzato dall’azienda subisce un attacco. Gli hacker usano le sue credenziali per accedere ai dati riservati del Board e di clienti strategici.
4	Data Breach	Un attacco mirato sottrae dati finanziari e personali dei membri del Board. La stampa ne viene a conoscenza e l’azienda subisce un danno reputazionale, oltre ai rischi per mancata conformità alla NIS2 e al GDPR.

acquistinretepa

SISTEMI DI E-PROCUREMENT

DOCUMENTO DI OFFERTA ECONOMICA

NUMERO DI RDO: 5435533

Offerta Economica relativa a

Descrizione Richiesta di offerta per piattaforma "CYBER GURU ENTERPRISE PLUS" e "BOARD TRAINING NIS2"

RdO nr. 5435533

Numero lotto 0

Amministrazione titolare del procedimento

Ente acquirente	I.R.C.C.S. ISTITUTI FISIOTERAPICI OSPITALIERI ROMA		
Ufficio	TECNOLOGIE E SISTEMI INFORMATICI		
Codice fiscale	02153140583	**Codice univoco ufficio**	QL8R3J
Indirizzo sede	Via elio chianesi 53		
Città	Roma		
Recapito telefonico	+390652662991		
Email	informatica@ifo.it		
Punto ordinante	GIUSEPPE NAVANTERI		

Concorrente

Forma di partecipazione

Singolo operatore economico

Ragione sociale/Denominazione

CYBER-BEE S.R.L.

Partita IVA

14559061008

Tipologia societaria

Società a responsabilità limitata (SRL)

Oggetto dell'Offerta

Formulazione dell'Offerta Economica = Valore economico (Euro)

DATA DI GENERAZIONE DOCUMENTO: 19/06/2025

GN

Nome	Valore
Valore offerto	60000

Il Concorrente, nell'accettare tutte le condizioni specificate nella documentazione del procedimento, altresì dichiara:

- che la presente offerta è irrevocabile ed impegnativa sino al termine di conclusione del procedimento, così come previsto nella lex specialis;
- che la presente offerta non vincolerà in alcun modo la Stazione Appaltante/Ente Committente;
- di aver preso visione ed incondizionata accettazione delle clausole e condizioni riportate nel Capitolato Tecnico e nella documentazione di Gara, nonché di quanto contenuto nel Capitolato d'oneri/Disciplinare di gara e, comunque, di aver preso cognizione di tutte le circostanze generali e speciali che possono interessare l'esecuzione di tutte le prestazioni oggetto del Contratto e che di tali circostanze ha tenuto conto nella determinazione dei prezzi richiesti e offerti, ritenuti remunerativi;
- di non eccepire, durante l'esecuzione del Contratto, la mancata conoscenza di condizioni o la sopravvenienza di elementi non valutati o non considerati, salvo che tali elementi si configurino come cause di forza maggiore contemplate dal codice civile e non escluse da altre norme di legge e/o dalla documentazione di gara;
- che i prezzi/sconti offerti sono omnicomprensivi di quanto previsto negli atti di gara;
- che i termini stabiliti nel Contratto e/o nel Capitolato Tecnico relativi ai tempi di esecuzione delle prestazioni sono da considerarsi a tutti gli effetti termini essenziali ai sensi e per gli effetti dell'articolo 1457 cod. civ.;
- che il Capitolato Tecnico, così come gli altri atti di gara, ivi compreso quanto stabilito relativamente alle modalità di esecuzione contrattuali, costituiranno parte integrante e sostanziale del contratto che verrà stipulato con la stazione appaltante/ente committente.

ATTENZIONE: QUESTO DOCUMENTO NON HA VALORE SE PRIVO DELLA SOTTOSCRIZIONE A MEZZO FIRMA DIGITALE

GN

GN