SELEZIONE PUBBLICA, PER TITOLI E COLLOQUIO, PER IL CONFERIMENTO DELL'INCARICO DI DIRIGENTE DI SECONDA FASCIA PER L'AREA INFRASTRUTTURE PRESSO L'UNIVERSITÀ DEGLI STUDI DI BERGAMO, CON CONTRATTO DI LAVORO A TEMPO DETERMINATO DI TRE ANNI.
CODICE SELEZIONE USBer26DIR001
(avviso di selezione rep. n. 28/2026 del 13.02.2026 pubblicato sul sito istituzionale e sul Portale del reclutamento inPA in data 13.02.2026)

TRACCE DEI COLLOQUI

Traccia A (Traccia estratta)

1. La ricerca è uno degli ambiti principali degli Atenei. Spesso il supporto ai progetti di ricerca è decentralizzato e gestito direttamente dai Dipartimenti o da Centri di ricerca. Si descrivono pregi e difetti di una gestione centralizzata del supporto ICT alla ricerca discutendo anche le soluzioni organizzative e tecnologiche ipotizzabili per fornire un supporto centralizzato ICT ai ricercatori nella realizzazione delle attività di ricerca di un Ateneo di medie dimensioni.
2. La gestione del patrimonio immobiliare universitario richiede strumenti informativi integrati per supportare programmazione e controllo. Si descriva come sistemi informatici dedicati possano supportare la pianificazione degli interventi edilizi, la gestione degli immobili e il monitoraggio dello stato del patrimonio. Si evidenzi quali debbano essere gli elementi di attenzione per la programmazione di un aggiornamento costante delle competenze di utilizzo di sistemi informativi dedicati

Leggere e tradurre

The NIS2 Directive marks a significant step in enhancing cybersecurity across the European Union. It provides a clear and comprehensive approach to managing cyber risks, reporting incidents, and sharing information. The directive introduces enhanced security requirements for essential and important entities, while also reinforcing the supervisory responsibilities of national competent authorities. However, enhancing cybersecurity extends beyond policy — it requires the effective engagement of people. To implement the directive effectively, entities should define internal cybersecurity roles and responsibilities aligned with its requirements7.

Testo da
ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia B (Traccia non estratta)

1. Le modalità con cui vengono acquisiti i sistemi ICT incidono sempre di più su aspetti fondamentali per gli Atenei, come la sicurezza, la gestione delle informazioni e i costi. Si esaminino le diverse strategie di acquisizione del software per un Ateneo di medie dimensioni, considerando le soluzioni cloud, on-premise e ibride, e mettendo a confronto le alternative make (sviluppo interno) e buy (acquisto da fornitori esterni). Si illustrino le principali differenze tra questi approcci, evidenziandone vantaggi e svantaggi e analizzando le implicazioni dal punto di vista economico, gestionale e della sicurezza, anche in relazione ai più recenti modelli di lavoro agile.
2. La normativa sugli appalti pubblici prevede un crescente utilizzo di piattaforme digitali per la gestione delle procedure di gara. Si descriva come i sistemi informativi possano supportare la

gestione digitale delle procedure di gara, esplicitando come possano essere messi in atto i migliori meccanismi di coordinamento con l'Area Legale e Appalti.

Leggere e tradurre
This section introduces two articles of the NIS2 Directive, which outline several obligations for entities falling within its scope. Article 21 states that essential and important entities must apply proper cybersecurity risk management steps. This covers areas like dealing with incidents, securing the supply chain, and maintaining smooth business operations. Article 23 highlights the duty of these entities to report incidents. They must inform their competent authorities and/or Computer Security Incident Response Teams (CSIRTs) on time about any significant incidents.

Testo da
ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia C (Traccia estratta)

1. Sia l'attività dell'amministrazione che quelle della didattica e della ricerca dipendono sempre di più dalla disponibilità e dal corretto funzionamento dei sistemi informatici. Si descriva quale sarebbe la migliore organizzazione di un sistema di supporto utenti per i servizi informatici di un Ateneo di medie dimensioni distribuito su più sedi che offra supporto al personale docente e tecnico-amministrativo, oltre che agli studenti.
2. L'adozione dei modelli digitali delle opere rappresenta un elemento chiave nell'innovazione del settore edilizio pubblico. Si descriva il ruolo del BIM nella progettazione, realizzazione e gestione delle opere edilizie universitarie e i benefici lungo il ciclo di vita dell'edificio. Si definisca un piano di adeguamento delle competenze per l'adozione dei più recenti modelli digitali.

Leggere e tradurre
Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services and to prevent or minimise the impact of incidents on recipients of their services and on other services.
Taking into account the state-of-the-art and, where applicable, relevant European and international standards, along with the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed.

Testo da
ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia D (Traccia non estratta)

1. Considerando il processo amministrativo di trasferimento di uno studente da un altro Ateneo che parte dalla compilazione della richiesta da parte dello studente e si conclude con la

registrazione del trasferimento da parte della segreteria, si descriva come si dovrebbe procedere nel ridisegnare il processo. Si individui anche quali sono gli strumenti e le piattaforme nazionali che possono essere utilizzate in questo caso.

2. Le attività edilizie generano un'elevata quantità di documentazione tecnica e amministrativa. Si illustri come sistemi informatici di gestione documentale possano supportare la dematerializzazione dei fascicoli tecnici degli immobili e garantire tracciabilità e conservazione dei documenti e come favorire un adeguamento delle competenze del personale da dedicare alla costruzione di un sistema di dematerializzazione

Leggere e tradurre

Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred t in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not, in itself, subject the notifying entity to increased liability

Testo da

ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia E (Traccia non estratta)

1. Le università gestiscono grandi quantità di dati personali e sistemi esposti a molteplici rischi informatici. Si descriva quali sono i più rilevanti vincoli normativi e quali le principali misure organizzative e tecniche che un Ateneo dovrebbe adottare per garantire la sicurezza dei sistemi informativi e la protezione dei dati di studenti, docenti e personale. Si ipotizzi un modello organizzativo e di ruoli che possa rispondere alla gestione della complessità dei temi legati alla privacy.
2. La realizzazione di opere edilizie richiede strumenti efficaci di controllo su tempi, costi e avanzamento lavori. Si descriva come piattaforme digitali possano supportare il monitoraggio dei progetti edilizi e la rendicontazione verso gli organi di governo dell'Ateneo.

Leggere e tradurre

To make the NIS2 obligations and their mapping to ECSF role profiles more accessible and understandable for entities, the following sections present two scenarios illustrating how the ECSF can be leveraged to enhance cybersecurity maturity. Both scenarios are based on a medium-sized organisation with limited financial and human resources, characterised by informal, decentralised cybersecurity governance and a low maturity level. It is important to note, however, that this is not a one-size-fits-all approach. Every organization has a unique approach towards cybersecurity, and the implementation should be tailored accordingly, using the detailed mapping provided in Section 4 of this document.

Testo da

ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995

https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia F (Traccia estratta)

1. Gli Atenei utilizzano numerose piattaforme informatiche per la gestione delle attività didattiche, amministrative e di ricerca. Si descrivano strategie e strumenti utili a garantire l'integrazione e l'interoperabilità tra i diversi sistemi informativi presenti nell'università. Si definiscano i principali ruoli organizzativi da coinvolgere in un progetto integrazione dei sistemi informativi
2. Le attività dell'Area edilizia devono interagire con diversi sistemi informativi di Ateneo, come contabilità, gestione del personale e pianificazione strategica. Si descrivano le principali esigenze di integrazione tra i sistemi informatici dell'area edilizia e quelli amministrativi e gestionali dell'università.

Leggere e tradurre
As a first step to address tasks 1, 2, and 3, the senior management decided to appoint a cybersecurity manager responsible for developing the organisation's policy on the security of network and information systems, as well as topic-specific policies, procedures, processes, and plans to establish a security baseline.
This role is expected to provide strategic oversight of the entity's cybersecurity programme, underlining the senior management's commitment to cybersecurity. Given the size of the organisation, the role should also encompass responsibility for managing cybersecurity risks, including the identification of proposed remediation actions

Testo da
ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia G (Traccia non estratta)

1. Considerando il processo di presentazione della domanda di laurea per gli studenti di un Ateneo, si descriva come si dovrebbe procedere nel ridisegnare il processo, tenendo conto anche dei principali ruoli da coinvolgere. Si definiscano gli strumenti e le piattaforme nazionali che possano essere utilizzate in questo caso.
2. La programmazione dello sviluppo edilizio richiede analisi integrate su utilizzo degli spazi, costi e fabbisogni futuri. Si descriva come strumenti di analisi dei dati e sistemi informativi possano supportare i processi decisionali nella definizione del piano di sviluppo edilizio.

Leggere e tradurre
The IT and Systems Administrators were following different cybersecurity best practices and frameworks and worked mostly in an ad-hoc way without a strategy or structure. To address task 7, the CISO decided to upskill the IT and Systems Administrators through targeted training, utilising a list of key knowledge and skills from the ECSF10. This enabled them to securely implement, operate, maintain, and support technical solutions, including secure configuration, patch management and system testing. This upskilling also prepared the IT and Systems Administrators to participate effectively in incident response efforts, working in close collaboration with external specialists to address task 10.

Testo da

ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia H (Traccia non estratta)

1. La gestione dei dati rappresenta un elemento sempre più strategico per il governo degli Atenei. Si descriva come strumenti di data analytics, business intelligence e intelligenza artificiale possano supportare i processi decisionali attraverso una lettura integrata dei dati istituzionali. Si discuta inoltre come progettare sistemi informativi per il monitoraggio di politiche, strategie, processi e risultati e come un Ateneo di medie dimensioni possa strutturarsi per costruire un Data Analysis Team.
2. La manutenzione degli edifici universitari è fondamentale per garantire sicurezza e continuità delle attività istituzionali. Si illustri come sistemi informativi di facility e maintenance management possano supportare la pianificazione e il controllo delle attività manutentive.

Leggere e tradurre

To address tasks 9 and 10, the CISO decided to outsource the Cyber Incident Response, the Cyber Threat Intelligence and the Digital Forensics Investigation responsibilities to a specialised organisation able to provide continuous monitoring, advanced threat detection, digital forensics analysis and effective containment measures, ensuring a rapid and coordinated response.Service Level Agreements (SLAs) were clearly defined to set expectations around response times and quality of service. However, reporting obligations could not be delegated, so the CISO retained responsibility for reporting incidents in accordance with regulatory requirements. Recognising that successful incident response requires collaboration between internal and external teams, the CISO acknowledged the need to upskill internal IT and Systems Administrators- —a need that is addressed in Step 3.

Testo da

ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia I (Traccia estratta)

1. Dal 16 ottobre 2024 è in vigore anche in Italia il d.lgs. 4 settembre 2024, n. 138, che recepisce la Direttiva (UE) 2022/2555, conosciuta come NIS 2. Si discutano gli impatti tecnologici ed organizzativi della normativa NIS2 nello specifico caso dell'applicazione a un Ateneo descrivendo anche le principali attività da porre in essere, i portatori di interesse da coinvolgere, le risorse da utilizzare per predisporre e implementare un piano operativo di adeguamento alla nuova normativa.
2. La gestione del patrimonio edilizio universitario richiede interazioni frequenti con enti e amministrazioni esterne. Si descriva come i sistemi informativi possano supportare la gestione dei flussi informativi e documentali verso enti come ANAC, Comuni, Regioni, Vigili del Fuoco e Soprintendenze.

Leggere e tradurre

This use case illustrates how a medium-sized organisation can use the ECSF to develop a cybersecurity organisational framework, in order to work towards NIS2 Directive implementation. By

providing a comprehensive mapping of required responsibilities and skills, the ECSF enabled the organisation to systematically address its cybersecurity needs. The framework facilitated strategic organisational alignment, guiding the management in hiring a dedicated cybersecurity manager, upskilling existing staff, and outsourcing critical functions like threat intelligence and incident response and occasional tasks like conducting security audits, security scans and training.

Testo da
ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia L (Traccia non estratta)

1. Considerando il processo amministrativo di gestione dello stage di uno studente che parte dalla compilazione della richiesta da parte dello studente e si conclude con la registrazione della conclusione dello stage da parte della segreteria, si descriva come si dovrebbe procedere nel ridisegnare il processo e quali ruoli organizzativi sia importante coinvolgere. Si individui anche quali sono gli strumenti e le piattaforme nazionali o interne che possano essere utilizzate in questo caso.

2. Gli Atenei gestiscono spazi complessi destinati a didattica, ricerca e servizi agli studenti. Si descriva come sistemi informativi dedicati alla gestione degli spazi possano supportare la pianificazione dell'utilizzo degli edifici, il monitoraggio delle superfici e l'ottimizzazione delle risorse immobiliari e come un Ateneo possa garantire l'adeguamento delle competenze necessarie all'adozione dei più recenti sistemi informativi dedicati.

Leggere e tradurre
To meet the cyber incident response and reporting requirements, senior management established a team of skilled professionals. Recognising that, as a medium-sized company, they lacked the internal capacity, skills, or resources to fully staff a dedicated internal team, they leveraged three (3) pre-established roles, the CISO, a Cybersecurity Implementer, and the Cyber Legal, Policy and Compliance Officer, alongside the external specialised organisation providing Incident Response, Threat Intelligence, and Digital Forensics services. The team's objective was to ensure effective response and reporting of cybersecurity incidents, fully aligning with NIS2 compliance requirements.

Testo da
ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

Traccia M (Traccia estratta)

1. Considerando il processo amministrativo di presentazione delle delibere agli organi di Ateneo che parte dalla predisposizione di una proposta da parte del dirigente e si conclude con la registrazione nel repertorio corretto da parte degli addetti dell'ufficio Organi Collegiali si descriva come si dovrebbe procedere nel ridisegnare il processo. Si individui anche quali sono gli strumenti e le piattaforme che passono essere utilizzate in questo caso e come costruire un gruppo di lavoro dedicato a tale progetto.
2. La sicurezza degli edifici universitari richiede il coordinamento tra sistemi tecnologici e procedure organizzative. Si illustri come sistemi informatici possano supportare la gestione

delle informazioni relative alla sicurezza degli edifici, alla prevenzione dei rischi e al coordinamento con gli enti di controllo.

Leggere e tradurre
The Cybersecurity Implementer, a Systems Administrator who was upskilled to additionally fulfil this role, received an alert from their network monitoring system indicating a possible sign of a data exfiltration attempt. The Cybersecurity Implementer quickly called the CISO. The CISO collaborated and asked for support from the outsourced service to provide context and the potential impact of the detected activity. The team began their analysis remotely, identifying a sophisticated phishing attack that had bypassed initial defences and was likely responsible for the suspicious network behaviour.

Testo da
ENISA - Cybersecurity Roles and Skills For NIS2 Essential and Important Entities
ISBN 978-92-9204-706-1, doi: 10.2824/8870995
https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities