AVVISO SELEZIONE PERMANENTE

Siamo alla ricerca di persone con competenze senior e/o junior da inserire nell'area ICT del consorzio, da assumere a tempo indeterminato CCNL commercio e terziario – Confesercenti.

L'inquadramento e il trattamento economico saranno definiti tenendo conto dell'esperienza professionale, delle competenze e della seniority accertate nell'ambito del processo di selezione.

LIVELLO	Range RAL
1	€ 35.852,18 – € 42.852,18
2	€ 31.962,00 – € 36.862,00
3	€ 28.341,32 - €32.651,32

CISIA è un consorzio nazionale al servizio del sistema universitario ed è una realtà in costante crescita ed evoluzione. Abbiamo creato nel tempo un ambiente di lavoro molto positivo e stimolante.

Se hai interesse a lavorare con noi puoi inviare un curriculum vitae, con l'autorizzazione al trattamento dei dati personali, al seguente indirizzo di posta elettronica certificata: selezionicisia@pec.it.

ENTRA A FAR PARTE DEL NOSTRO TEAM

La selezione è finalizzata a individuare professionalità con competenze ed esperienza in uno o più dei seguenti ambiti:

- sviluppo dei frontend
- sviluppo dei backend
- analisi software e requirement management
- IT project management
- infrastructure engineering
- cybersecurity engineering.

Gli ambiti sopra indicati non corrispondono necessariamente a profili distinti: la selezione è volta a individuare persone le cui competenze, anche trasversali, possano riguardare uno o più degli ambiti indicati.

CRITERI DI SELEZIONE

I curricula saranno selezionati secondo criteri di imparzialità e trasparenza.

Saranno analizzate sia le competenze tecniche specifiche, sia l'attitudine a ricoprire le posizioni necessarie tramite le più aggiornate e razionali metodologie e tecniche di valutazione, adottando oggettivi e trasparenti metodi di verifica del possesso dei requisiti.

Almeno ogni due mesi i curricula pervenuti saranno esaminati e valutati e, in funzione delle esigenze, si procederà alla comparazione e all'eventuale colloquio dei profili pervenuti.

Di seguito i requisiti e le competenze attese. Rispetto alle conoscenze e competenze indicate potranno essere valutate anche competenze ulteriori o diversamente articolate in coerenza con gli ambiti ricercati.

AMBITO SVILUPPO

SVILUPPO FRONTEND: REQUISITI

- Buona conoscenza dell'uso di strumenti come OpenAI ChatGPT e CODEX e di Anthropic CLAUDE e CLAUDE CODE
- ottima conoscenza del linguaggio PHP a partire dalla versione 7.4
- ottima conoscenza della programmazione funzionale e OOP
- conoscenza del paradigma di sviluppo MVC per comprendere la base dei più utilizzati framework PHP
- conoscenza approfondita di Drupal dalla versione 8 in poi, creazione e personalizzazione nuovi temi e site building
- conoscenza approfondita del linguaggio Javascript e del framework jQuery
- conoscenza approfondita di Angular a partire dalla versione 16.x
- conoscenza di VUEJs 2.x/3.x
- conoscenza dei fogli di stile CSS e del loro sviluppo con SASS
- conoscenza approfondita del tool di versionamento GIT e del workflow GitFlow.

SVILUPPO BACKEND: REQUISITI

- Buona conoscenza dell'uso di strumenti come OpenAI ChatGPT e CODEX e di Anthropic CLAUDE e CLAUDE CODE
- ottima conoscenza del linguaggio PHP a partire dalla versione 5.3
- ottima conoscenza della programmazione funzionale e OOP
- conoscenza del paradigma di sviluppo MVC per comprendere la base dei più utilizzati framework PHP
- conoscenza approfondita di Drupal dalla versione 8 in poi, personalizzazione interfaccia di amministrazione, creazione nuovi moduli custom
- conoscenza approfondita di MySQL, linguaggio, struttura, ottimizzazione e indicizzazione
- conoscenza approfondita di MongoDB, linguaggio, struttura, ottimizzazione e indicizzazione
- conoscenza approfondita di NodeJS a partire dalla versione 6.x in poi
- allestimento di ambienti di sviluppo locali, utilizzo della console e bash scripting
- conoscenza approfondita del tool di versionamento GIT e del workflow GitFlow.

ALTRE SKILL E ABILITÀ VALUTATE POSITIVAMENTE PER L'AMBITO SVILUPPO

- Conoscenza dell'applicativo MOODLE
- conoscenza linguaggio Python
- sviluppo di applicazioni mobile crossplatform
- conoscenza di strumenti per l'automazione dei test e2e
- competenze di Machine Learning o supervised learning, Generative AI

IL TITOLO DI STUDIO PREFERENZIALE RICHIESTO PER L'AMBITO SVILUPPO

- Laurea triennale (o magistrale) in ingegneria dell'informazione e similari
- laurea triennale (o magistrale) in informatica o similari
- laurea in ingegneria informatica o similari
- laurea in informatica umanistica o similari.

AMBITO ANALISI SOFTWARE E IT PROJECT MANAGEMENT

ANALISI SOFTWARE E REQUIREMENT MANAGEMENT: REQUISITI

- Comprensione dei processi organizzativi
- analisi dei bisogni
- capacità di raccogliere i vincoli di sicurezza, riservatezza e conformità
- raccolta dei requisiti, formalizzazione dei requisiti funzionali e non funzionali, modellazione dei requisiti, gestione della qualità dei requisiti
- prioritizzazione dei requisiti
- capacità di validazione e collaudo
- conoscenza del metodo di lavoro agile e padronanza di strumenti di implementazione del metodo
- capacità relazionali e comunicative, quali ascolto attivo, pensiero analitico, precisione nella scrittura, facilitazione e capacità di comunicare con interlocutori tecnici e non tecnici
- esperienza dimostrabile.

IT PROJECT MANAGEMENT: REQUISITI

- Saper impostare un progetto, definire la governance, gestire il perimetro
- saper fare la gestione economica, la gestione di rischi e dei problemi
- effettuare la pianificazione, il controllo dell'avanzamento, la gestione della qualità
- saper gestire l'adozione, la chiusura ed il passaggio all'esercizio
- gestire la comunicazione direzionale
- conoscenza del metodo di lavoro agile e padronanza di strumenti di implementazione del metodo
- esperienza dimostrabile.

IL TITOLO DI STUDIO PREFERENZIALE RICHIESTO PER ANALISI E IT PROJECT MANAGEMENT

- Laurea triennale (o magistrale) in ingegneria gestionale o similari
- laurea triennale (o magistrale) in materie scientifiche.

AMBITO INFRASTRUCTURE ENGINEERING

INFRASTRUCTURE ENGINEERING: REQUISITI

- Saper sviluppare e manutenere procedure di Infrastructure as Code
- saper automatizzare le attività sistemistiche e operative
- gestire e sviluppare playbook e ruoli Ansible
- supportare i processi di deploy e rilascio dei servizi
- gestire e automatizzare il ciclo di vita dei certificati digitali
- integrare servizi e piattaforme tramite API
- supportare le attività di amministrazione di sistemi Linux e servizi infrastrutturali
- produrre e aggiornare la documentazione tecnica.

IL TITOLO DI STUDIO PREFERENZIALE RICHIESTO PER INFRASTRUCTURE ENGINEERING

- Laurea triennale (o magistrale) in ingegneria informatica o similari
- laurea triennale (o magistrale) in materie scientifiche.

ALTRI REQUISITI UTILI

- Esperienza documentata di almeno 1 anno in uno o più dei seguenti ambiti:
    - amministrazione di sistemi Linux
    - automazione mediante Ansible
    - Infrastructure as Code tramite Terraform
    - utilizzo di sistemi di versionamento Git
    - scripting tramite Bash o linguaggi equivalenti
- conoscenza dei principali protocolli di rete e dei concetti base di sicurezza informatici
- capacità di problem solving
- orientamento al raggiungimento dei risultati
- capacità di lavoro in gruppo.

Verranno valutate ulteriori esperienze e competenze nei seguenti ambiti:

- esperienza nell'automazione di processi di deploy applicativo

- esperienza nella gestione e nel rinnovo di certificati digitali
- conoscenza di piattaforme di virtualizzazione
- conoscenza di tecnologie container e orchestrazione (Docker, Kubernetes, OpenShift)
- conoscenza di ambienti Cloud pubblici quali AWS o Microsoft Azure
- esperienza con strumenti CI/CD
- conoscenza della lingua inglese scritta e parlata.

AMBITO CYBERSECURITY ENGINEERING

I REQUISITI PER CYBERSECURITY ENGINEERING

- Amministrare e configurare le soluzioni di sicurezza, tra cui firewall, VPN, sistemi di protezione degli endpoint (EDR/XDR), piattaforme SIEM e strumenti di gestione delle vulnerabilità
- monitorare gli eventi di sicurezza, analizzare le segnalazioni e contribuire all'identificazione, al contenimento e alla risoluzione degli incidenti
- gestire le attività di verifica delle vulnerabilità, valutare le priorità di intervento e collaborare con i team tecnici alla loro risoluzione
- applicare e verificare le configurazioni di sicurezza dei sistemi Windows e Linux, curando l'hardening e la gestione degli aggiornamenti
- gestire identità, autorizzazioni e accessi privilegiati secondo il principio del minimo privilegio, contribuendo all'adozione dell'autenticazione multifattore
- automatizzare le attività ricorrenti di controllo e amministrazione mediante script e strumenti di orchestrazione
- predisporre e aggiornare la documentazione tecnica, le procedure operative e i report sulle attività di sicurezza
- supportare le verifiche di sicurezza e le prove di ripristino dei servizi in collaborazione con i gruppi responsabili.

Competenze richieste:

- esperienza nell'amministrazione di sistemi e strumenti di sicurezza in ambienti ICT strutturati
- conoscenza dei sistemi operativi Windows e Linux e delle relative tecniche di hardening
- conoscenza delle reti TCP/IP, dei principali protocolli di comunicazione e dei meccanismi di segmentazione e controllo del traffico
- competenze nella configurazione e gestione di firewall, VPN e soluzioni di protezione degli endpoint
- capacità di analizzare log, correlare eventi e svolgere una prima valutazione degli allarmi di sicurezza
- conoscenza dei processi di gestione delle vulnerabilità, aggiornamento dei sistemi e risposta agli incidenti
- familiarità con i sistemi di gestione delle identità, quali Active Directory ed Entra ID
- capacità di utilizzare almeno un linguaggio di scripting, preferibilmente PowerShell, Python o Bash
- conoscenza della lingua inglese adeguata alla consultazione della documentazione tecnica e all'interazione con fornitori e interlocutori internazionali

- esperienza nella protezione di ambienti cloud, virtualizzati e containerizzati
- familiarità con strumenti di automazione della risposta agli incidenti e gestione degli accessi privilegiati
- conoscenza dei framework e delle linee guida di sicurezza, quali NIST, CIS e ISO/IEC 27001
- possesso di certificazioni pertinenti al ruolo, in ambito sicurezza, networking o amministrazione di sistemi.

Completano il profilo:

- capacità di analisi e risoluzione dei problemi
- precisione operativa
- riservatezza
- attitudine al lavoro di squadra
- capacità di gestire le priorità anche in situazioni di emergenza.

IL TITOLO DI STUDIO PREFERENZIALE RICHIESTO PER CYBERSECURITY ENGINEERING

- Laurea triennale (o magistrale) in ingegneria informatica o similari
- laurea triennale (o magistrale) in materie scientifiche.

Informativa sulla privacy

I dati saranno trattati e conservati esclusivamente per finalità di selezioni presenti e future, garantendo i diritti di cui al D. Lgs. 196/2003 e al Regolamento (UE) 2016/679. Gli interessati sono invitati a leggere l'informativa sulla privacy.
Ai sensi dell'art. 13 del Regolamento (UE) 2016/679, si informa che il Consorzio, in qualità di titolare del trattamento, procede al trattamento dei dati dei partecipanti esclusivamente per le finalità di seguito indicate, nel rispetto della normativa in materia di protezione dei dati personali. I dati personali e quelli eventualmente appartenenti alle categorie particolari (come, ad esempio, l'informazione relativa all'appartenenza a categorie protette), sono trattati dal Consorzio al fine esclusivo di dare esecuzione alla procedura di selezione.
I dati sono conservati solo per il periodo necessario a dare esecuzione alla procedura di selezione, salvi obblighi di ulteriore conservazione previsti per legge.
I nominativi degli ammessi alle diverse fasi del processo di selezione e la graduatoria finale saranno pubblicati sul sito CISIA per la durata prevista dalla normativa (Art. 19 D.lgs. 33/2013 e Linee Guida ANAC approvate con determinazione n. 1134 del 08/11/2017).
I partecipanti alla selezione possono esercitare i diritti riconosciuti dalla vigente normativa in materia di protezione dei dati personali, tra cui il diritto di chiedere al titolare del trattamento l'accesso ai dati

personali e la rettifica o la cancellazione degli stessi, la limitazione o opposizione al trattamento, oltre al diritto alla portabilità dei dati, nei limiti di cui agli artt. 15-21 del Regolamento.
Ai sensi dell'art. 77 del Regolamento, qualora la figura partecipante alla selezione ritenga che il trattamento che lo riguarda violi la normativa in materia di protezione dei dati personali, ha diritto di proporre reclamo al Garante italiano per la protezione dei dati personali ovvero all'autorità di controllo dello Stato membro UE in cui risiede abitualmente, lavora ovvero del luogo ove si è verificata la presunta violazione.
Per l'esercizio dei suoi diritti, può rivolgersi al titolare del trattamento, inviando una comunicazione al seguente recapito: privacy@cisiaonline.it.
Il Consorzio ha designato il proprio Responsabile della Protezione dei Dati che può essere contattato per tutte le questioni relative al trattamento dei propri dati personali e all'esercizio dei propri diritti, al seguente riferimento: lavinia.vizzoni@hotmail.it.