



Struttura richiedente: **DIREZIONE GENERALE - Ufficio di Staff Sicurezza ICT**

Sede di lavoro: Via Giuseppe Colombo n. 46 - Milano (MI)

| | |
|---|---|
| Categoria D | CODICE 1 |
| Unità di personale: 1 | Area tecnica, tecnico-scientifica ed elaborazione dati |
| Titolo della posizione: Componente del Team “tutela dati” | |
| Competenze professionali richieste: <ul style="list-style-type: none">• Capacità di amministrazione dei sistemi operativi più diffusi (flavour di Unix e/o Windows), con particolare riguardo agli aspetti di sicurezza.• Conoscenza dei protocolli e delle tecnologie di rete (suite TCP/IP).• Conoscenza dei principali standard di sicurezza informatica.• Conoscenza della normativa nazionale ed europea sulla Sicurezza ICT, sulla protezione dei dati personali e continuità operativa nelle P.A. con particolare riguardo al nuovo GDPR e Misure minime di sicurezza per le PA.• Capacità ed esperienza nella produzione di politiche e procedure.• Conoscenza dei temi di analisi e gestione dei rischi in ambito Sicurezza.• Tecnologie, soluzioni e metodi per la protezione dei dati critici (riservatezza, integrità, disponibilità). | |
| Contenuti della posizione: <p>La persona sarà inserita nel team di Tutela dei dati che si occupa di:</p> <ul style="list-style-type: none">• Progettazione e gestione di progetti su temi relativi alla tutela dei dati, alla conformità normativa e ai regolamenti interni in materia di Sicurezza ICT.• Partecipazione al processo di valutazione e gestione del Rischio.• Partecipazione alla definizione e elaborazione di Policy-AUP (acceptable user policy) di sicurezza, di best practice e promozione delle azioni utili alla corretta applicazione in Ateneo.• Individuazione delle aree di intervento e delle azioni di adeguamento per il miglioramento del livello di conformità dell'Ateneo.• Identificazione e promozione delle misure tecniche finalizzate alla tutela dei dati (riservatezza, integrità, disponibilità).• Progettazione e assistenza di II livello dei processi di digitalizzazione (PA digitale) per gli aspetti di sicurezza.• Analisi e interpretazione dal punto di vista tecnico delle nuove disposizioni in materia di sicurezza, contestualizzandole nella realtà dell'Ateneo.• Collaborazione nell'individuazione dei vincoli e requisiti circa le misure di ICT Security nella scrittura dei contratti con i fornitori.• In relazione al Regolamento UE 2016/679, collaborazione alla progettazione di nuovi servizi IT, nuove tecnologie o all'adeguamento di quelli esistenti per assicurare la «security by design, security by default», partecipazione alle attività di Data Privacy Impact Assessment, al processo di analisi e gestione del Rischio legato alla Sicurezza e alle attività connesse ai casi di Data Breach.• Individuazione delle metriche di monitoraggio e di misurazione del livello di Sicurezza e di conformità normativa. | |



| | |
|--|--|
| Categoria D | CODICE 2 |
| Unità di personale: 2 | Area Tecnica, Tecnico-Scientifica ed Elaborazione Dati |
| Titolo della posizione: Team per la “Protezione Infrastrutture, Sistemi, Servizi” | |
| Competenze professionali richieste: <ul style="list-style-type: none">• Capacità di amministrazione dei sistemi operativi più diffusi (flavour di Unix e/o Windows), con particolare riguardo agli aspetti di sicurezza.• Conoscenza di base dei sistemi di virtualizzazione.• Conoscenza dei protocolli e delle tecnologie di rete (suite TCP/IP).• Conoscenza ed esperienza in materia di sicurezza ICT con particolare riguardo a:<ul style="list-style-type: none">- componenti (Firewall, IDS, SIEM, Antivirus...), tecniche e metodologie per la protezione delle reti, dei sistemi e dei servizi;- architetture di rete a supporto della sicurezza (LAN Virtuali, zone demilitarizzate (DMZ), indirizzamento e tecniche di instradamento, NAT/PAT, ecc.);- Conoscenza delle principali tecniche di attacco e sfruttamento vulnerabilità e relative contromisure;- meccanismi per l'identificazione e gestione di un incidente di sicurezza;- normativa in ambito sicurezza ICT.• Conoscenza di almeno un linguaggio di programmazione (preferibilmente Perl, e/o PHP o python); in particolare nell'ambito del trattamento dei file testuali (regular expression), dell'interazione con le basi di dati e dell'automazione dell'amministrazione di sistema.• Esperienza nella gestione di progetti.• Buone capacità di interrelazione con le strutture dell'Ateneo. | |
| Contenuti della posizione: <p>La persona sarà inserita nel team di Protezione Infrastrutture, Sistemi, Servizi che si occupa di:</p> <ul style="list-style-type: none">• Identificazione dei sistemi, delle soluzioni tecnologiche e degli opportuni meccanismi da mettere in essere per il potenziamento, miglioramento ed evoluzione della sicurezza dell'Ateneo, gestione e verifica della loro corretta implementazione della sicurezza ICT di Ateneo.• Partecipazione nella progettazione e implementazione di nuovi servizi IT o nuove tecnologie per la corretta e completa identificazione dei requisiti di sicurezza, la loro valutazione e il loro recepimento nelle soluzioni sviluppate.• Configurazione, gestione e monitoraggio della sicurezza di Ateneo attraverso l'implementazione, personalizzazione e evoluzione di tutti gli strumenti di sicurezza gestiti già in dotazione (Firewall, SIEM, Antivirus).• Implementazione di meccanismi per l'integrazione delle diverse piattaforme tecnologiche e servizi infrastrutturali per l'automazione dei processi in ambito sicurezza.• Early Warning verso strutture di Ateneo al fine di identificare, analizzare e notificare tempestivamente vulnerabilità tecnologiche emergenti e fornire suggerimenti per la loro mitigazione.• Raccolta di dati statistici sulla gestione della Sicurezza, produzione report, individuazione dei trend e delle metriche di monitoraggio.• Assessment di sicurezza e vulnerabilità su sottoreti, host o servizi; valutazione del livello di pericolosità, attuazione, in collaborazione con i gestori dei servizi, dei piani di rientro.• Gestione giornaliera degli incidenti di sicurezza in Ateneo per l'intero ciclo di vita mediante l'uso degli strumenti in dotazione ed attività di analisi attiva o passiva.• Progettazione e gestione dei Servizi VPN e Antivirus.• Identificazione e gestione delle informazioni relative ai Server e agli Asset di Ateneo.• Partecipazione, nel proprio ambito di competenza, all'attività di analisi, valutazione e gestione del Rischio legato alla Sicurezza.• Esperienza nella gestione di progetti.• Buone capacità di interrelazione con le strutture dell'Ateneo. | |