PCSoftware

Sommario

PCSoftware

Il **Gruppo PCSoftware** vanta una pluriennale esperienza nelle soluzioni come **Servizi Digital Trasformation** e **Cybersecurity**, progettando soluzioni IT per le aziende in continua sinergia con gli innovativi orizzonti tecnologici contemporanei.
Il **Gruppo PCSoftware elabora nuovi processi informatici**, traducendo la modernità in chiave di sviluppo e di organizzazione per diverse linee di business e per i diversi settori dipartimentali della tua azienda.
Un partner unico in grado di **ottimizzare gli strumenti informatici aziendali**, di **rendere sicure le reti** delle imprese di **gestire flussi di informazioni e dati**, rispondendo alle esigenze del cliente con processi di massima efficienza.
Una guida sicura per il processo di **trasformazione digitale**, allo scopo di adeguare processi e skill alle nuove tecnologie e permettendo alla tua azienda di essere più reattiva in questo delicato passaggio, senza blocchi o ritardi nelle operatività.
L'alto grado di competenza dei professionisti che affiancheranno le vostre scelte è il nostro tratto distintivo. **Uniamo innovazione alla professionalità umana fatta di conoscenza e predisposizione all'ascolto**.

LETTURA

Il **fattore umano** per contrastare gli attacchi informatici

La **Cybersecurity** non è (solo) una questione di tecnologia.

A volte siamo indotti a prendere decisioni errate perché la nostra sfera emotiva prende il sopravvento su quella razionale.

Se il rischio di un cyber attacco è esponenzialmente aumentato, **come possiamo aumentare il nostro livello di protezione?**

La sicurezza è anche una **dimensione sociale**, fatta di cultura aziendale e di competenze utili a sviluppare **una corretta percezione del rischio**, al fine di aumentare in ogni individuo la sensazione di essere protetto, a casa come al lavoro.

La conoscenza e consapevolezza dei fattori che ci rendono vulnerabili può ridurre di molto la superficie di attacco e di conseguenza metterci in una **situazione di maggior protezione**.

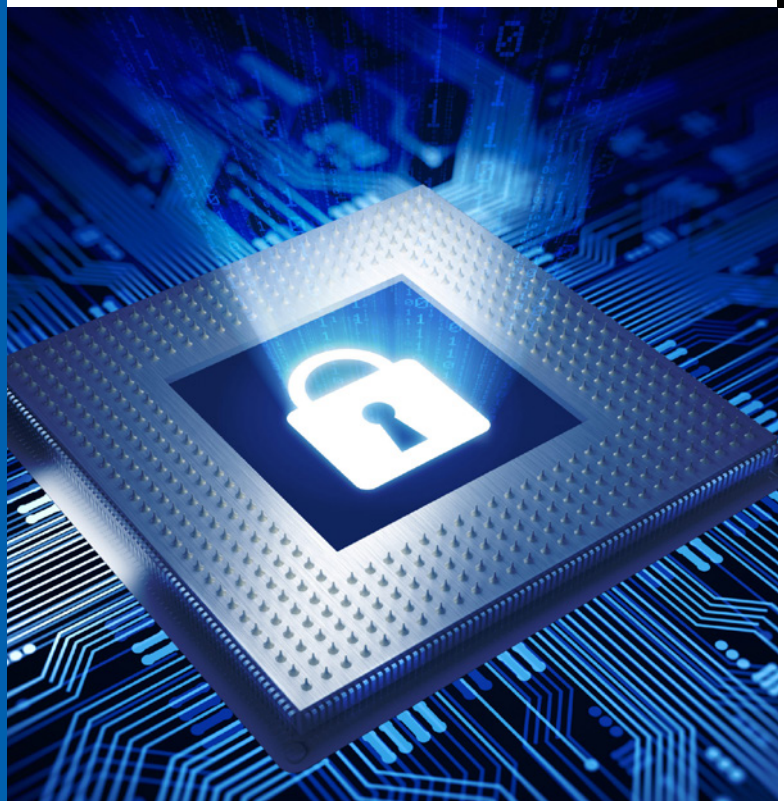
Stando all'ultima edizione del **Rapporto Clusit** (fonte https://clusit.it), il confronto tra gli incidenti di sicurezza più significativi avvenuti a livello globale nel corso del **primo semestre 2022** con i dati raccolti nei 4 anni precedenti indica un aumento significativo della loro incidenza.

Comparando i numeri del primo semestre 2018 con quelli del 2022, si evidenzia **una crescita degli attacchi pari al 53%** (da 745 a 1.141).

In 4 anni e mezzo **la media mensile di attacchi gravi a livello globale è passata da 124 a 190**.

Studi ci dicono inoltre che **un singolo attacco** su larga scala **può provocare danni per circa 120 miliardi di dollari** e che i cyber attacchi sono costati nel complesso qualcosa come tre trilioni di dollari (il 3% del Pil globale), cifra che è in sensibile aumento per gli anni futuri.

La gestione del rischio informatico e delle infrastrutture critiche è quindi una priorità per tutte le aziende, di qualsiasi settore e dimensione e il modello elaborato dal **NIST (National Institute of Standards and Technology)** è universalmente riconosciuto dagli esperti come una guida a cui fare riferimento per adottare standard e procedure di cybersecurity.



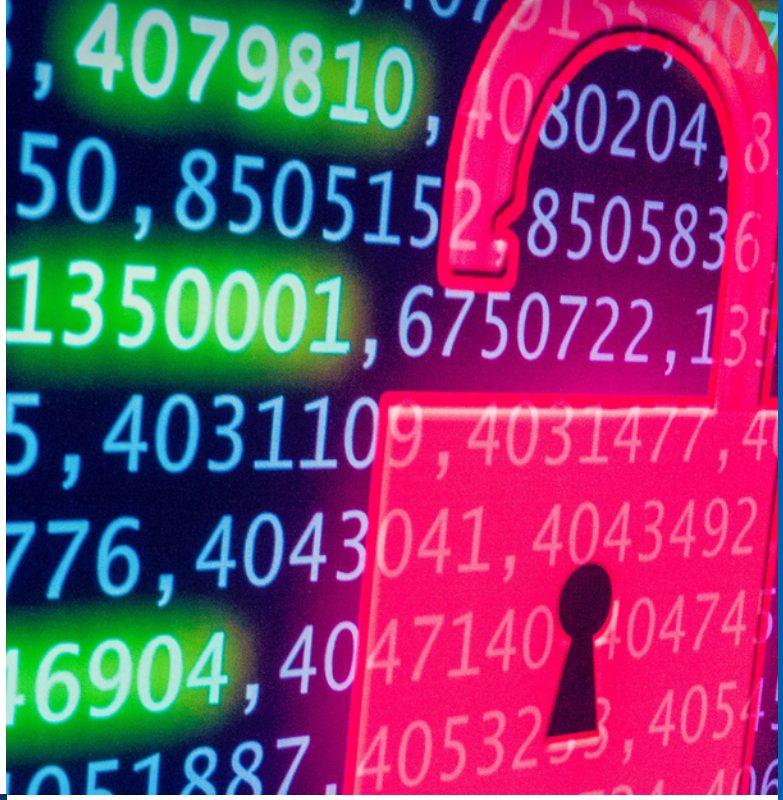
Sono cinque le funzioni di questo modello in continuo aggiornamento:

- **Identificare**
- **Proteggere**
- **Rilevare**
- **Rispondere**
- **Recuperare**

Scopo finale è quello di abilitare un **approccio "risk-based"** in ogni organizzazione, fornendo una tassonomia comune per definire le azioni necessarie per raggiungere il proprio obiettivo di cybersecurity.

La tecnologia ci rende più efficienti e produttivi e permette di aumentare la scalabilità di risorse e sistemi, ma contemporaneamente ci rende inconsapevolmente più vulnerabili.

Per questo **non è possibile delegare la protezione dei dati esclusivamente alla tecnologia** e solo a determinate figure ma **è necessario creare dei percorsi di formazione e sensibilizzazione verso i dipendenti** utili a mitigare gli errori derivanti dal fattore umano.



La cybersecurity, è un insieme di tre elementi; Hardware, Software e Uomini.

La conoscenza e coscienza di ciò che ci circonda e come affrontare le problematiche innalza il paletto della nostra protezione aziendale riducendo la superficie di attacco.

Certificazione
ISO 27001

Sistema di gestione della sicurezza informatica

Il **Sistema di Gestione della Sicurezza delle Informazioni** è un elemento di importanza basilare per lo sviluppo del business di un'azienda in quanto tutte le informazioni, anche i dati informatici, rappresentano un bene che le conferisce valore e costituiscono quindi un vero e proprio patrimonio da gestire in modo strategico, al fine di tutelare l'impresa stessa e il suo sviluppo.

È fondamentale proteggere questo patrimonio per garantire la crescita e il successo delle proprie attività.
Definire e mettere in atto un **Sistema di Gestione delle Informazioni** equivale a salvaguardare la riservatezza, l'integrità e la disponibilità dei dati di una organizzazione (in formato cartaceo, elettronico o intellettuale) e tutelare così il proprio patrimonio.

Al giorno d'oggi le **informazioni gestite, in particolare con mezzi informatici, sono oltre il 60% del capitale intellettuale delle aziende**, ed è quindi necessario avvalersi di un sistema che ne garantisca la gestione sicura anche dal punto di vista dei rischi informatici.

La sicurezza è un fattore strutturale che si ripercuote su tutta l'organizzazione aziendale, ed è fondamentale gestire in condizioni di sicurezza tutto il sistema delle informazioni aziendali, per salvaguardarne la riservatezza, l'integrità e la disponibilità e per non andare incontro a una perdita di competitività e riduzione delle quote di mercato.

Compiti del Consulente

- Definizione delle **politiche di sicurezza aziendali**.
- Definizione dell'**ambito di applicazione** del Sistema di Gestione per la Sicurezza delle Informazioni.
- **Analisi del rischio**.
- **Gestione del rischio**.
- Selezione degli **strumenti di gestione**.
- Stesura della **dichiarazione di applicabilità**.

Vantaggi della Certificazione **ISO 27001**

Scopi essenziali di un valido **Sistema di Gestione della Sicurezza delle Informazioni** sono:

Proteggere le informazioni.
È fondamentale **proteggere** questo patrimonio per garantire la crescita e il successo delle proprie attività.

Salvaguardare la riservatezza, l'integrità e la disponibilità dei dati.
Definire e mettere in atto un **Sistema di Gestione delle Informazioni** equivale a salvaguardare la riservatezza, l'integrità e la disponibilità dei dati di una organizzazione, per tutelare al meglio il proprio patrimonio.

Garantire la gestione sicura dal punto di vista dei rischi informatici.
Al giorno d'oggi le informazioni gestite, in particolare con mezzi informatici, costituiscono gran parte del capitale intellettuale delle aziende, ed è quindi necessario avvalersi di un sistema che ne garantisca la **gestione sicura** anche dal punto di vista dei rischi informatici.

Gestire in condizioni di sicurezza tutto il sistema delle informazioni aziendali.
La **sicurezza** è un fattore strutturale che si ripercuote su tutta l'organizzazione aziendale, ed è fondamentale gestire in condizioni di sicurezza tutto il sistema delle informazioni aziendali, per salvaguardarne la riservatezza, l'integrità e la disponibilità e per non andare incontro a una perdita di competitività e riduzione delle quote di mercato.

Dimostrare a terze parti di aver ottemperato ad obblighi di legge in materia di sicurezza delle informazioni.
Anche se non esiste un obbligo di legge, la **certificazione di sicurezza su base volontaria**, in particolare quella effettuata secondo lo standard **ISO 27001** può, in certi casi, trovare utilizzo per dimostrare a terze parti di aver ottemperato ad obblighi di legge in materia di sicurezza delle informazioni.

General Data Protection Regulation

Il nuovo Modello Organizzativo sul Trattamento dei Dati Regolamento Europeo Privacy Ue 2016/679

Il 4 maggio 2016, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) i testi del **Regolamento europeo in materia di protezione dei dati personali**.

Si tratta del passaggio finale per l'entrata in vigore del nuovo "**Pacchetto protezione dati**", l'insieme normativo che definisce un quadro comune in materia di tutela dei dati personali per tutti gli Stati membri dell'UE.

Il regolamento è entrato in vigore il 24 maggio 2016, ma ha trovato applicazione negli Stati solo alla data del 25 maggio 2018: le imprese e le pubbliche amministrazioni hanno avuto due anni (un periodo di tempo congruo ma non troppo ampio) per organizzarsi e adeguarsi alle nuove regole. Il che non significa che automaticamente è abrogato il nostro D.lgs 196/2003, quindi almeno per un po' di tempo le due norme convivranno.

È opportuno quindi mantenere attivo il DPS e verificare almeno una volta l'anno che

i requisiti richiesti dalla normativa (lettere di incarico ai responsabili dei trattamenti, archiviazione dei documenti contenenti dati sensibili, salvataggi costanti e protetti, rotazione delle password…) siano rispettati redigendo un rapporto dettagliato a disposizione degli organi di controllo.
Nel nuovo regolamento la definizione ***data protection*** ha preso il posto della parola ***privacy***.
Il termine scelto ha un significato molto più vasto e pone l'accento su un cambio di prospettiva: il problema di fondo non è semplicemente essere in possesso di dati sensibili, ma saperli gestire nel modo corretto.

Tra le principali novità

- L'obbligo di trattare i dati secondo la progettazione "**by design**" (cioè analizzando il trattamento per tutto il ciclo di vita dei dati.) e "**by default**" (cioè il partire da configurazioni "chiuse" dei sistemi informatici, per poi gradualmente ampliarle solo dopo avere valutato l'impatto di eventuali aperture).
- La nascita del **Data Protection Officer (DPO)**, che sarà obbligatorio nella Pubblica Amministrazione e nelle aziende private che processano dati a rischio (ad es.: il trattamento su larga scala di speciali categorie di dati quali quelli sensibili).
- L'obbligo di svolgere il **Data Protection Impact Assessment (DPIA)**, per i trattamenti delicati e ad alto rischio, tranne nel caso in cui il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche. In tal caso il responsabile dovrà preventivamente consultare l'Autorità di controllo.
- L'obbligo di rispettare il "**Data breach**", cioè la segnalazione al Garante e all'interessato di eventuali fughe o compromissioni di dati.

I soggetti coinvolti nel nuovo modello organizzativo sul trattamento dei dati

- Il **Titolare del Trattamento**, ora chiamato **Data Controller** o **Responsabile del trattamento**, dotato di un potere decisionale in ordine alle tecniche da adottare e alle misure organizzative,

al fine di garantire la conformità al Regolamento delle operazioni di trattamento dei dati.

- Il **Responsabile esterno del Trattamento/Amministratore di Sistema**, ora chiamato **Joint Controller** o **Co-responsabile del trattamento** (ad esempio ad un fornitore di servizi in Cloud).
- Il **Responsabile ed incaricato del trattamento**, ora chiamato **Data Processor** e Incaricato del Trattamento o più semplicemente **Data Handler**, sarà l'attuale responsabile e potrà procedere al trattamento dei dati solo su istruzione del responsabile.
- Il **Responsabile della sicurezza dei dati**, ora chiamato **Data Protection Officer (DPO)**.

Nel nuovo Regolamento generale sulla protezione dei dati, si nota subito un **cambio di definizioni**, laddove la figura del Responsabile del trattamento come prevista dall'art. 29 del D.Lgs. n. 196/2003 ha una nuova denominazione con nuovi compiti e funzioni (tra l'altro precisamente stabiliti nel testo europeo citato).

Per essere più chiari possibile, la figura dapprima denominata come **Titolare del trattamento**, con il citato Regolamento UE, ha assunto il nome di **Responsabile del trattamento**. Si aggiunga che la figura dell'**Incaricato del trattamento**, così come era prevista dall'art. 30 del D.lgs 196/2003, è scomparsa completamente.

Altra novità sarà la possibilità (in questo caso concessa al **Data Subject** o **Soggetto Interessato**) di esercitare i propri diritti nei confronti di ciascun **Data Controller** Congiunto del trattamento oppure al **Joint Controller**.

Un elemento cruciale differenzia un **Data Protection Officer** o **DPO** da un **responsabile privacy** ex art. 29: mentre il primo deve essere indipendente e autonomo, il secondo doveva agire seguendo solo e soltanto le istruzioni del titolare del trattamento, pertanto, un vincolo che impedisce di godere di ampia indipendenza, tipica invece del nuovo ruolo del DPO.

La nostra consulenza:

- **Analisi dei rischi**
- **Policy Sicurezza Informatica**
- **Accordo di Riservatezza**
- **Aggiornamento alla nuova documentazione**

Vulnerability Assessment

Vulnerability Assessment

Lo scopo del VA è quello di fornire una **valutazione complessiva del livello di sicurezza del sistema informativo aziendale** per poter poi intraprendere le opportune contromisure.
Il primo vantaggio è certamente la consapevolezza del livello di sicurezza dei propri sistemi e la conseguente opportunità di abbassare il livello di rischio verso lo zero.
Con una protezione alta, quindi con una politica di prevenzione degli attacchi, la continuità operativa dell'azienda è garantita e il pericolo di perdite economiche ridotto.
C'è però un altro fattore essenziale connesso alla sicurezza: quello della **reputation**.
Non c'è perdita peggiore, per un'azienda, di quella della reputazione. Perché un danno economico può essere recuperato. Un danno all'immagine, invece, è molto difficile da colmare, in quanto si lega alla percezione di fiducia che i Clienti hanno nei confronti di un'azienda.

Un servizio di consulenza di qualità

Il servizio di consulenza offerto comprende enormi benefici per le infrastrutture, quali:

- **Visibilità completa** e condivisione dei rischi di sicurezza.
- **Suggerimenti per l'implementazione di misure di protezione** adeguate alla valutazione dei rischi.
- **Gestione delle procedure di Risk Assessment** per effettuare verifiche sulle misure di protezione implementate.
- **Valutazione dei processi interni aziendali** per analisi approfondite e degli obiettivi prefissati in termini di sicurezza.
- **Programmazione di piani di intervento** per l'ottenimento dei requisiti richiesti dalla legge.

Tutto questo in linea con quanto previsto e richiesto dalla normativa GDPR.

Trasformazione digitale delle aziende

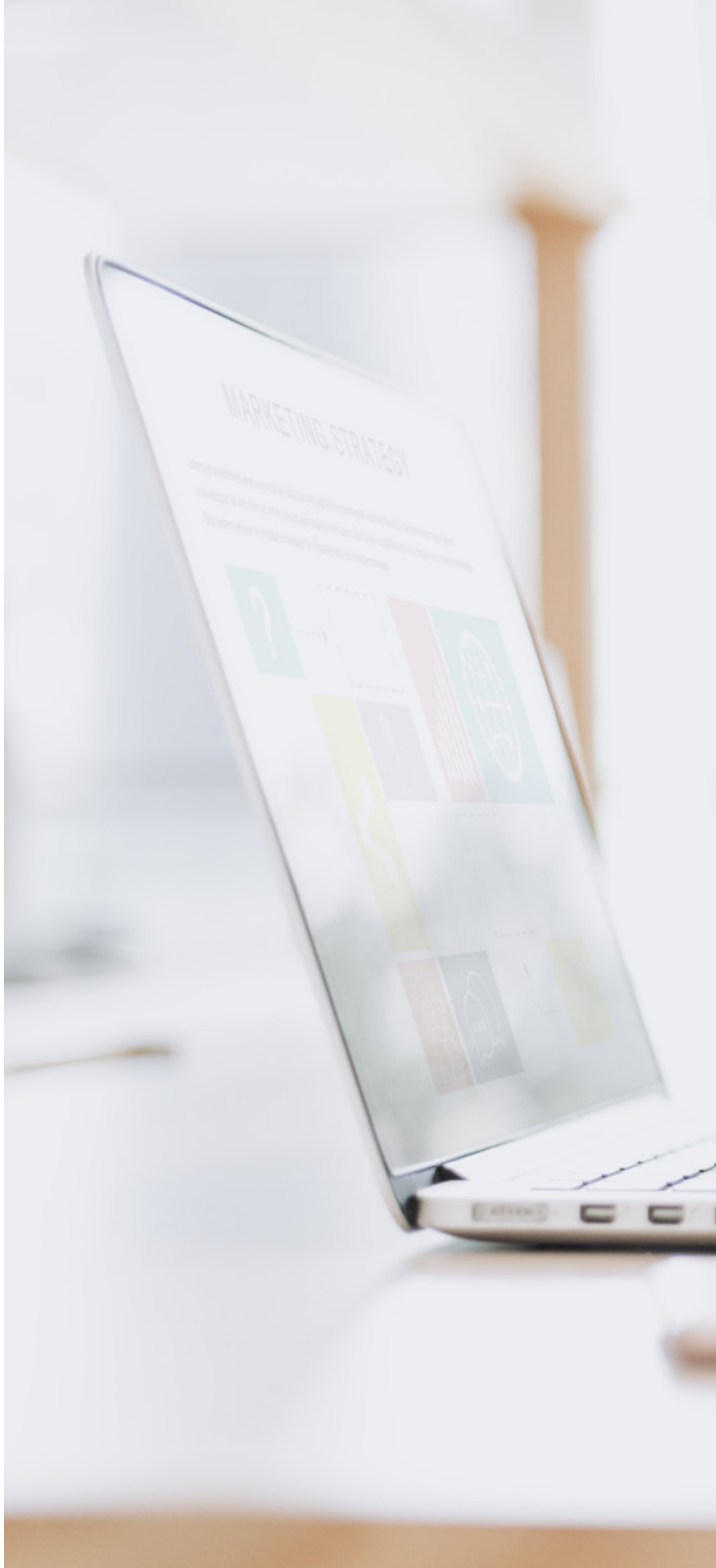
Siamo nell'era dell'**Industria 4.0**, presentiamo le nostre soluzioni di consulenza avanzate per la trasformazione digitale.
Efficienza, **risparmio** e **modernizzazione** delle Organizzazioni in generale sono stati i principali obiettivi perseguiti attraverso l'evoluzione della normativa di riferimento per la **Transizione Digitale** emanata nel corso degli ultimi anni in tema di gestione dei contenuti e dei processi digitali.
I punti significativi di questo processo:

Il nuovo protocollo informatico

Il **Protocollo Informatico** diventa il nodo di interoperabilità, con nuove regole di colloquio, requisiti di sicurezza, specifiche tecniche e funzionalità di cooperazione applicativa e comunicazione digitale.

Formazione dei documenti informatici

Il **documento digitale** non è rappresentato solo dal file elettronico ma è costituito da altre proprietà fondamentali come i metadati specifici, l'impronta (hash) ed altre proprietà da considerare in fase di formazione.



Gestione documenti e fascicoli digitali

Lavorare in modalità digitale significa ripensare ad attività e flussi documentali in una nuova ottica per non interrompere la catena del valore annullando la validità probatoria con la stampa di PEC o di documenti firmati digitalmente

Conservazione a norma

Il **sistema di conservazione** garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione e dalla normativa vigente, stabilire cosa deve essere trasmesso in conservazione fa parte dell'organizzazione aziendale

Formazione del personale

Il **processo di passaggio alla Trasformazione Digitale** comporta un importante e significativo cambiamento organizzativo della trasformazione delle classiche procedure con mezzi di tipo digitale. Questo perché cambiare la natura di un'organizzazione significa cambiare il modo in cui le persone lavorano. Quando un'organizzazione inizia un percorso di Trasformazione Digitale si rende conto di aver bisogno di **set di competenze diverse da quelle tradizionali**, per soddisfare le esigenze del cambiamento tecnologico. È un modo di lavorare completamente diverso, che richiede agli amministratori, ai dirigenti, ai reparti IT e persino ai dipendenti entry-level una mentalità diversa.

LETTURA

Una **consulenza su misura** per la trasformazione digitale

Offriamo una consulenza per la trasformazione digitale che sia su misura per le necessità specifiche della tua azienda.

i 4 step per una digitalizzazione di successo

Analisi e Informazioni preliminari
Valutazione delle necessità e soluzioni adeguate alla singola organizzazione. In questa fase preliminare è importante uno scambio di informazioni per definire le esigenze e impostare la consulenza. In questa fase cerchiamo di conoscere meglio il tuo business, i tuoi prodotti e i tuoi obiettivi.

Analisi e revisione delle strutture organizzative
Questo servizio permette di effettuare un **check-up della struttura organizzativa** al fine di individuare le attività che funzionano bene ma soprattutto quelle che potrebbero essere migliorate.

Analisi e revisione delle strutture organizzative

Studio e definizione degli obiettivi

Individuate le criticità, è più facile definire gli strumenti adatti per intervenire con successo ed ottenere i miglioramenti necessari, oltre a **ridisegnare la struttura organizzativa** e **implementare nuovi servizi** per la collettività.
Questa attività ricopre particolare rilevanza poiché legata a tre fattori di cambiamento:

- **implementazione dello smart working**, che richiede una mappatura delle attività e della loro gestione all'interno della organizzazione;
- **valutazione dell'impatto della digitalizzazione** sulla struttura organizzativa;
- **pensionamenti** che si sono verificati (e si verificheranno nei prossimi anni) che possano sbilanciare l'equilibrio dei servizi offerti.

Studio e definizione degli obiettivi

Una volta **approvato il progetto** ci mettiamo al lavoro per **definire strategie e obiettivi**.
In questa fase, normalmente, il Cliente ci fornisce dei **feedback** che utilizziamo per finalizzare il lavoro.

Report e misurazione dei risultati

Ultimata la consulenza forniamo le **soluzioni da implementare** sia a livello organizzativo che a livello di soluzioni tecnologiche per il passaggio alla Trasformazione Digitale.

CISO
Chief Information Security Officer

Tra le professioni più richieste da tutti, c'è sicuramente quella del **CISO, Chief Information Security Officer.**

Questa figura considerata il manager della sicurezza è in grado di definire la giusta strategia di protezione degli asset aziendali, di mitigare tutti i possibili rischi informatici.

Che cos'è e cosa fa il CISO

Governance

Definire, implementare, gestire e mantenere un programma di governance della sicurezza delle informazioni.

Security Risk Management, Controls, Audit Management

- **Identificare i processi operativi e gli obiettivi aziendali** per valutare il livello di tolleranza al rischio;
- **Progettare i controlli dei sistemi informativi** in linea con le esigenze e gli obiettivi operativi e condurre test prima dell'implementazione per garantirne l'efficacia e l'efficienza;
- **Identificare e selezionare le risorse necessarie** per implementare e mantenere efficacemente i controlli sui sistemi informativi;
- **Progettare e implementare controlli** sui sistemi informativi per mitigare il rischio.

Security Program Management & Operations

- **Definire le attività** necessarie per eseguire con successo il progetto per la sicurezza delle informazioni;
- **Sviluppare, gestire e monitorare il budget di programma** dei sistemi informativi, stimare e controllare i costi dei singoli progetti;
- **Identificare, negoziare, acquisire e gestire le risorse necessarie** per una corretta progettazione e implementazione del programma sui sistemi informativi (ad esempio, persone, infrastrutture e architettura).

Information Security Core Concepts

- **Identificare i criteri per un controllo di accesso ai dati** obbligatorio e discrezionale, comprendere i diversi fattori che aiutano nell'implementazione dei controlli di accesso e progettare un piano di controllo di accesso;
- **Identificare diversi sistemi di controllo dell'accesso**, come carte d'identità e biometria;
- **Comprendere diversi concetti di ingegneria sociale e il loro ruolo** negli attacchi che prendono di mira i dipendenti aziendali per sviluppare le migliori pratiche per contrastarli;
- **Elaborare un piano di intervento** in caso di furto d'identità.

Strategic Planning, Finance & Vendor Management

- **Eseguire analisi esterne** dell'organizzazione (ad esempio, analisi di clienti, concorrenti, mercati e ambiente industriale) **e interne** (gestione dei rischi, capacità organizzative, misurazione delle prestazioni) e utilizzarle per allineare il programma di sicurezza delle informazioni con gli obiettivi dell'organizzazione;
- **Valutare e adeguare gli investimenti IT** per garantire che siano sulla buona strada per supportare gli obiettivi strategici dell'organizzazione.

AI

PCSoftware

Your Consultant

Ing. Dott. Michele Lasorsa

Chief Information Security Officer (CISO)

+39 347 17 61 331

m.lasorsa@pcsoftware.it

pcsoftware.cloud