ELENA VACIAGO
VINCENZO SANSONETTI
MARIA GRAZIA FILIPPINI

PROFESSIONI 4.0

La trasformazione digitale delle imprese e dei ruoli

Introduzione di Stefano Colli-Lanzi

SOIEL INTERNATIONAL
Informazione - Innovazione - Imprese

1 Sicurezza e valutazione dei rischi

di Claudio Pantaleo

1.1 Premessa

Tutte le imprese hanno in comune l'esigenza di proteggere il proprio business e i beni vitali con processi operativi ed organizzativi trasversali alle diverse strutture di cui si compone la loro organizzazione. La globalità di tale impostazione, che potremmo definire "a tutto campo", deve essere in grado di superare le tradizionali barriere legate alle tipicità del settore produttivo di appartenenza e alla frammentazione dei ruoli e delle responsabilità interne in tema di sicurezza [tipicamente: safety (sicurezza in senso lato), vigilanza delle aree, ICT Security & Protection (sicurezza e protezione di tutte le tecnologie dell'informazione e della comunicazione), R&D (ricerca e sviluppo), nuove tecnologie ecc.]. Si consente così di armonizzare gli interventi individuati come necessari e di elevare il grado di conoscenza e di coinvolgimento del personale nei processi di protezione degli asset aziendali. Tale impostazione può essere peraltro ritrovata anche nelle Norme internazionali di Sicurezza quali, ad esempio, la Norma Italiana UNI 10459 («Funzioni e profilo del professionista della Security Aziendale»), che nella sua prima edizione del 1995 già così sintetizza il concetto di Security: «Studio e attuazione delle strategie, delle politiche e dei piani

CLAUDIO PANTALEO

Senior Corporate Security Executive, Certified Chief Security Officer, Maestro del Lavoro, ha ricoperto il ruolo di Direttore Sistemi e Tecnologie a Protezione del Patrimonio, in ATM Milano, azienda leader, in Italia e all'estero, nel Trasporto Pubblico Locale. Precedentemente è stato il Direttore Sicurezza Aziendale per l'Italia e il Sud Europa della BAT - British American Tobacco, primaria azienda multinazionale nel mondo del tabacco. La sua prima esperienza lavorativa di durata trentennale è stata in IBM, multinazionale leader mondiale nel settore informativo, dove ha ricoperto ruoli tecnici nelle nuove tecnologie e ruoli commerciali, terminando come Direttore Sicurezza Aziendale. Attualmente effettua consulenze direzionali ed attività di docenza personalizzate alle necessità del richiedente.

operativi volti a prevenire, fronteggiare e superare eventi, in prevalenza di natura dolosa e/o colposa, che possono colpire le risorse umane, materiali, immateriali ed organizzative di cui l'azienda dispone o di cui necessita per garantirsi un'adeguata capacità concorrenziale nel breve, nel medio e nel lungo termine». È evidente, tuttavia, che lo studio e l'attuazione di strategie, politiche e conseguenti piani operativi porta la funzione di Security aziendale ad espletare un'attività molto ampia, totalmente integrata e coerente con le strategie e le politiche del management.

1.2 Il Security manager

Nell'espletamento delle proprie attività, la Security è orientata e chiamata a garantire la possibilità di realizzare i propri obiettivi attraverso la riservatezza, la disponibilità e l'integrità di tutte le risorse di proprietà e interesse dell'impresa. Ne consegue un posizionamento organizzativo tale da prevedere – necessariamente – la dipendenza diretta della funzione Security dai massimi vertici aziendali. Tale posizionamento, oltre che garantire adeguata visibilità alla funzione Security, presenta aspetti estremamente proficui e qualificanti per l'impresa. Il top management ha infatti una visione chiara, non deformata o mediata di tutte le problematiche dell'impresa; il rapporto diretto con la Security consente di acquisire anche una maggiore sensibilità sui problemi di sicurezza interna, oltre che favorire l'immediatezza dei contatti, la rapidità decisionale, ove necessaria, nonché la contenuta distribuzione delle informazioni riservate secondo il principio del *need-to-know*. Il soggetto designato alla gestione di una funzione così impegnativa e complessa dovrà possedere, all'interno dell'impresa, un ruolo organizzativo rilevante, che consenta lo svolgimento delle funzioni attribuite con incisiva autorevolezza nei confronti del Top management e di tutte le funzioni aziendali. Si tratta, in sostanza, di una posizione dirigenziale di alto livello, il cosiddetto Security manager: figura altamente specializzata e polivalente, che possa cooperare direttamente con i vertici aziendali. Al Security manager spetterà l'adozione di strumenti e metodologie finalizzate alla protezione delle risorse dell'impresa, intesa come spazio operativo, fisico e tecnologico, e dovrà quindi avere spiccate competenze tecniche e tecnologiche, investigative, relazionali e di comunicazione.

1.3 Le "qualità" del Security manager

Le attività traversali della Security dovranno essere poste in essere mediante interventi organici e con il contributo di personale identificato all'interno delle singole funzioni aziendali, opportunamente formato e che riporti funzionalmente al Security manager le tematiche qui elencate.

1) **Information Security-Cyber Security** (sicurezza delle informazioni e sicurezza informatica). È l'insieme delle misure finalizzate a tutelare il patrimonio informativo dell'impresa, su qualunque supporto risiedano le informazioni sensibili (informatico, trasmissivo, cartaceo), e a proteggere i sistemi elaborativi complessi da attacchi di criminalità informatica.
2) **Risk Management**. Individua i criteri di identificazione e analisi del rischio per gli asset tradizionali e non, anche in relazione a tendenze massimaliste.
3) **Auditing**. È la definizione e verifica del corretto utilizzo delle procedure e delle norme di Security all'interno e all'esterno dell'impresa, con eventuale correzione di situazioni anomale.
4) **Risorse umane**. Si tratta della promozione dell'intelligence (investigazione) interna, individuazione di comportamenti anti aziendali, predisposizione di politiche combinate su fenomeni di disagio, analisi di possibili minacce terroristiche e di conflitti violenti a sfondo contestativo o eversivo.
5) **Safety**. È l'integrazione della gestione del rischio e delle emergenze.
6) **Finanza.** Può essere utile la collaborazione con attività di intelligence per l'individuazione di fenomeni di inquinamento di circuiti finanziari.
7) **Servizi Generali**. Occorre infine collaborare alla scelta e al controllo dei fornitori, delle imprese di manutenzione e del personale di vigilanza e custodia (sia interno che in outsourcing, in appalto a una società esterna); selezione, utilizzo e gestione dei servizi di sicurezza in outsourcing.

Dalla complessità delle operazioni richieste alla funzione di Security, appena sinteticamente delineate, e dalle conseguenti macroscopiche implicazioni, emerge con chiarezza l'esigenza, non più differibile, di adeguare ed estendere l'interpretazione della Security, già significativamente recepita in molti settori industriali nei quali la "parcellizzazione" delle attività di sicurezza e la conseguente mancata unitarietà hanno evidenziato

gravi manchevolezze. Tale sviluppo dovrebbe andare di pari passo con la crescita della consapevolezza del valore acquisito e del ritorno di investimento e di immagine legato alla maggiore protezione dell'impresa; il processo potrà essere ulteriormente potenziato attraverso il perfezionamento degli strumenti già adottati e lo sviluppo di nuove metodologie, con specifica attenzione alla tutela delle performance (prestazioni) e dei processi aziendali (business, partnership, opportunità, know-how, immagine, buon nome ecc.). Il piano operativo di Security avrà precipuamente tale funzione e dovrà risultare il più possibile preventivo. Esso dovrà tener conto, con scientifica sistematicità, di metodi operativi all'avanguardia e dell'ingresso sempre più spinto delle tecnologie dell'informazione e della comunicazione, proponendo linee di condotta e procedure adeguate e trasferendo a tutti gli attori coinvolti il processo di formazione necessario per migliorare i singoli comportamenti e per la completa armonizzazione dei processi d'impresa.

1.4 Sicurezza e valutazione dei rischi

Le minacce ai sistemi e alle infrastrutture critiche sono in forte crescita. Minacce che possono essere portate in modo involontario o intenzionale e possono provenire da una varietà di fonti esterne [ad esempio cracker (pirati informatici), clienti, competitor, service provider, consulenti, business partner, hacktivist (sabotatori in segno di protesta), crimine organizzato, terroristi, governi], ma anche dall'interno [ad esempio insider, dipendenti scontenti, collaboratori]. Tutti questi soggetti tendono a sfruttare le vulnerabilità presenti nell'organizzazione, nei processi e nei sistemi, e le tecniche di "attacco" possono essere diversificate e integrate tra loro. La consapevolezza dei rischi rappresenta, quindi, uno dei punti di forza di un'impresa, che in tal modo è cosciente sia delle minacce che incombono sulle proprie informazioni, sia (elemento questo ancor più rilevante) delle proprie vulnerabilità. Vulnerabilità su cui l'impresa deve concentrarsi per annullare o portare a un livello accettabile il rischio di un attacco che possa sfruttarle. La stima del livello di rischio e l'impatto che deriva dalla sua materializzazione, consentono di sviluppare una serie di piani operativi per adottare controlli di tipo logico, fisico e organizzativo al fine di ridurre, trattenere, evitare o trasferire i rischi. È compito del Security manager, nell'ambito delle proprie responsabilità e utilizzando

professionalità a tale scopo formate (es. CISO, Chief Information Security Officer – responsabile della sicurezza delle informazioni –, nell'ambito dell'Information Security), eseguire periodicamente un'attività di analisi del rischio, utilizzando tutte le informazioni che provengono dall'esterno (ad esempio, intelligence) o dall'interno (ad esempio, incidenti), adottando specifiche metodologie che seguono standard di sicurezza. Una frase tipica di sicurezza è quella che afferma: «Non "se ci attaccheranno", ma "quando ci attaccheranno"»; passando cioè da una vaga probabilità a una possibile certezza. Ed è proprio per essere pronti a una tale eventualità che la valutazione del rischio assume un'importanza vitale per la salvaguardia della mission aziendale. I rischi per l'impresa sono, ahimè, sempre in agguato.

1.5 Test di vulnerabilità e di inclusione

Un'altra modalità per avere visibilità dei rischi è l'esecuzione di specifici test di vulnerabilità e di intrusione (sia logica, a livello dei sistemi informativi, sia fisica, a livello degli strumenti utilizzati per garantire la safety delle infrastrutture e delle persone). Queste verifiche hanno l'obiettivo di trovare le vulnerabilità nel sistema e nell'organizzazione. I test rappresentano un modo per controllare se le contromisure applicate sono efficaci e quindi essi sono orientati a rilevare non solo le vulnerabilità fisiche e logiche dei sistemi e dei dispositivi adottati, ma anche quelle di tipo organizzativo. L'esecuzione di tali test obbliga l'impresa a non stare semplicemente sulla difensiva, ma a pensare come un "attaccante". Tali test possono avere un livello di "aggressività" variabile in termini di invasività e sono portati fino al livello di dimostrazione "tangibile" della vulnerabilità, potendo simulare le attività di un potenziale attaccante per acquisire informazioni [ad esempio utilizzando tecniche di ingegneria sociale (studio del comportamento individuale), trashing o intrusione fisica]. Queste attività, tipiche delle funzioni di IT, Information Technology, e Audit, revisione (ma oggi anche di altri segmenti aziendali, in ottica di governance e Risk Management d'impresa), forniscono report dettagliati sullo stato dei sistemi e sull'organizzazione e consentono di impostare specifici piani di rientro per la rimozione delle vulnerabilità evidenziate.

1.6 Imparare dagli incidenti

Un incidente può essere considerato la materializzazione di un rischio e in tal senso aiuta a comprendere quali siano stati i fattori che lo hanno provocato. Esso inoltre aiuta a diminuire il rischio di un futuro attacco. E stimola una serie di domande.

- La probabilità di un attacco era stata sottostimata o ignorata?
- La capacità dell'attaccante, le sue motivazioni all'attacco, le vulnerabilità dell'impresa erano state tutte analizzate?
- Che cosa si doveva e poteva fare per evitare l'attacco?
- La reazione è stata efficace per mitigare il danno?
- Esiste capacità dell'impresa di analizzare l'incidente in tutte le sue fasi?

Quelle sopracitate sono alcune delle domande che ci aiutano a valutare il rischio di una "sottostima" o di una "cattiva gestione" del rischio. Domande che consentono di compiere una valutazione del proprio livello di sicurezza. L'obiettivo è la salvaguardia delle informazioni aziendali e, in tal senso, il Security manager deve conoscere in ogni momento i rischi che incombono sugli asset aziendali. Spesso l'adozione delle contromisure è un'attività abbastanza lunga a causa di processi interni lenti e complicati, o per indisponibilità di budget adeguati. La velocità di attuazione, tuttavia, rappresenta un fattore vincente e il Security manager deve rendere evidente al proprio management che ogni giorno di ritardo rappresenta un'esposizione a quel rischio, così come deve collaborare e rendere più celere possibile l'attuazione delle contromisure da parte delle funzioni aziendali coinvolte. Il rischio, in estrema sintesi, non va mai ignorato.

1.7 La tecnologia

Così come gli "attaccanti" utilizzano la tecnologia per attuare le loro attività criminali, così anche l'impresa necessita di tecnologie di sicurezza efficaci per attuare strategie di prevenzione, rilevazione e contrasto. La tecnologia di sicurezza, come qualsiasi tipo di tecnologia, è affascinante e spesso l'impresa l'acquisisce con la convinzione che l'adozione di tale tecnologia possa risolvere tutti i suoi problemi. Le statistiche sugli incidenti ci dimostrano che ciò non è vero, e quindi bisogna dedurre che la tecnologia – da sola – non rappresenta la soluzione. L'adozione di una soluzione tecnologica richiede sempre la definizione di ruoli e responsabilità asso-

ciati, la pubblicazione di specifiche procedure e la sensibilizzazione e formazione del personale e, molto spesso, anche una stretta integrazione con altre strutture aziendali. Ciò anche al fine di evitare i rischi dovuti alla generazione di un "falso senso di sicurezza" che l'adozione tecnologica può portare. Organizzazione e cultura quindi diventano complementari e consentono di aumentare l'efficacia di una tecnologia di sicurezza. Il presidio delle nuove tecnologie di sicurezza dovrebbe essere un'attività che coinvolge le aree tecniche della Security per gli aspetti strategico/funzionali e tecnologici. È importante anche sottolineare il mantenimento delle competenze tecniche. I gap formativi possono diventare una minaccia in caso di attacco a causa dell'impreparazione o dell'incapacità a reagire. In tal senso, come in un'esercitazione militare, sono importanti le integrazioni con le attività di penetration test, per verificare la capacità reattiva tecnico/organizzativa delle persone preposte alla gestione e controllo dei sistemi. Ciò è ancora più vero qualora tali attività vengano erogate in cloud/outsourcing. In definitiva, la tecnologia di sicurezza va presidiata per avere sempre la migliore soluzione tecnologica, ma non vanno mai trascurate tutte le componenti aziendali che, nell'utilizzo della stessa, contribuiscono a fornire il corretto livello di protezione delle informazioni dell'impresa.

1.8 Il controllo e la compliance (conformità)

Oltre alle attività più squisitamente tecniche e operative, sono molto importanti verifiche e controlli (procedurali, organizzativi e tecnologici) che mirino a determinare l'effettiva conformità alle politiche aziendali, alle procedure e alla definizione organizzativa. La funzione di Auditing lavora a stretto contatto con la Security aziendale per adeguare o mantenere l'intero sistema di sicurezza al livello richiesto dagli standard aziendali. La funzione di compliance, o quei settori dell'impresa che si occupano di compliance, verificano invece appunto la conformità agli standard di sicurezza e alle normative di legge. Queste ultime prevedono, in caso di non conformità, anche sanzioni di tipo civile o penale e possono avere impatti sul livello di credibilità che l'impresa riesce a trasmettere verso il mercato. Esistono diversi standard e normative di legge (Legge 262/05, Decreto legislativo 231/01, Decreto legislativo 196/03, ISO 27001, SOX, PCI DSS ecc.), che talvolta necessitano di visioni organizzative diverse. Anche in

questo caso la Security aziendale assume un ruolo di guida, per adottare un approccio basato sull'integrazione delle attività afferenti a normative diverse e che possiedono elementi similari. Da tale approccio si ottiene il catalogo dei processi, dei rischi e dei controlli opportunamente condiviso tra le diverse compliance. Esso, inoltre, consente di:

- **operare un'ottimizzazione e velocizzazione delle operazioni**, permettendo di svolgere attività di testing (analisi) sui controlli una volta sola per le diverse esigenze di compliance, coprendo contemporaneamente i diversi rischi;
- **diminuire il rischio globale di compliance e facilitare il dialogo** dei diversi attori del sistema di controllo interno, preposti alla gestione della compliance. Va tuttavia sottolineato in modo molto chiaro che compliance non significa sicurezza, ed essere certificati o conformi a una normativa non significa necessariamente essere sicuri. La Security aziendale è chiamata a garantire la conformità agli standard di sicurezza e alle normative vigenti avendo sempre, in ogni caso, un approccio verso un'analisi efficace delle minacce e dei rischi, piuttosto che verso una mera verifica di checklist (lista di controllo).

1.9 Il fattore umano

La sicurezza delle informazioni è responsabilità di tutti e il fattore umano, i rischi a esso associati, rappresentano una tra le variabili più critiche per la gestione di un sistema di sicurezza. Le migliori politiche e tecnologie di sicurezza possono essere rese totalmente inefficaci se le risorse umane non comprendono quale sia il loro ruolo e le loro responsabilità nella salvaguardia degli asset aziendali. Le persone possono eseguire azioni non intenzionali (errori, omissioni) o azioni deliberate (frodi, sabotaggi, vandalismo) o possono avere un atteggiamento passivo, di non esecuzione (nel caso di mancanza di competenze appropriate o in mancanza di indicazioni specifiche) in una situazione che invece richiederebbe un'azione. Tutte queste attività sono tali da comportare seri rischi. Il Security manager, anche in questo caso, deve disegnare e rendere operativa l'esecuzione di un'operazione di tipo "culturale", che ha l'obiettivo di diffondere la "cultura della sicurezza" in modo pervasivo e continuativo sulle risorse umane, per evitare comportamenti inadeguati e non in linea con le politiche e la

missione di business dell'impresa. Con tale obiettivo, la preparazione di un programma di sensibilizzazione sul sistema di gestione della sicurezza delle informazioni (Information Security Awareness) è un'attività ciclica e continua, vitale a maggior ragione se l'impresa appartiene alle infrastrutture critiche, cioè l'insieme delle attività e dei sistemi strategici ritenuti essenziali per una nazione, perché forniscono servizi primari per i cittadini e la struttura economica e industriale (energia, sicurezza, telecomunicazioni, risorse idriche, sanità, trasporti, banche e servizi finanziari ecc.).

1.10 Attuare cicli di sensibilizzazione

Il programma di sensibilizzazione va preparato in funzione di parametri interni ed esterni, che necessitano di attenzione da parte dei dipendenti e deve essere contestualizzato in relazione alle tecniche, alle tecnologie e ai contenuti, per essere più conforme possibile alla cultura aziendale. I contenuti dovranno essere in linea con l'emissione di politiche, procedure e processi di sicurezza presenti nell'impresa, a cui poter fare riferimento; e sono necessarie anche metriche di misurazione pre e post formazione, per misurare il livello di apprendimento e, in sostanza, il livello di "rischio disinformazione", che può portare all'adozione di comportamenti non in linea con le direttive manageriali.

1.11 Come cambiare il finale a storie già scritte

Stiamo vivendo oggi una realtà estremamente difficile e gli scenari di rischio cambiano molto velocemente, in relazione alle diverse condizioni esterne e interne all'impresa, che rendono necessarie una continua attenzione e gestione del problema. Con l'avvento della mobilità spinta e dell'informatica distribuita, grazie ai computer portatili, agli smartphone, all'Internet of Things (o Internet delle Cose), assieme ai concetti di estrema flessibilità sanciti dal "connetti il tuo device qualunque esso sia" nella mia rete informatica (BYOD - "Bring Your Own Device"), si è tremendamente innalzato il livello di minaccia agli asset personali dell'impresa, in quanto tutti questi "grappoli" di oggetti attaccati alla stessa rete, rappresentano più porte, più o meno aperte, verso il mondo esterno. Porte che sempre più spesso, una volta violate, possono metterci nella condizione di "noi o i nostri devices", usati come porti di partenza di attacchi importanti e

devastanti verso le risorse e gli asset di altri utenti del web. Per cambiare il finale a storie che appaiono già scritte, e difendersi in modo corretto, occorre tener presente che è aumentata la superficie di attacco alla nostra impresa, e gli attacchi malevoli possono avere origine da singole persone, da strutture di cyber criminali, da organizzazioni criminali e non ultimo da Stati sovrani. Il cyber spazio, sempre più complesso e articolato, è stato creato dall'uomo, tramite l'unione di milioni di reti, dati e stratificazioni di software (di base e applicazioni) che interconnettono cose e persone nel pianeta (e non, vedasi le sonde spaziali); e l'uomo, che è all'origine di tutto ciò, vista la grande vastità dello scenario, velocemente ne sta perdendo cognizione e controllo. Tutto sempre connesso e costantemente on line, dalla tecnologia individuale a quella aziendale, a quella politica o governativa, supportato da tecnologie abilitanti, rendono la nostra vulnerabilità dinamica, variabile e rinnovata nel tempo. Tecnologie abilitanti sempre più spinte e complesse (Cloud e Cloud ibrido, banda larga e ultralarga, Big Data, robotica, droni, intelligenza artificiale, Internet of Things, apprendimento automatico), ci impongono di restare al passo con i tempi e di considerare la sicurezza non come una destinazione, un punto di arrivo, ma come un viaggio continuo, che non finisce mai.

1.12 Un vademecum in sei punti

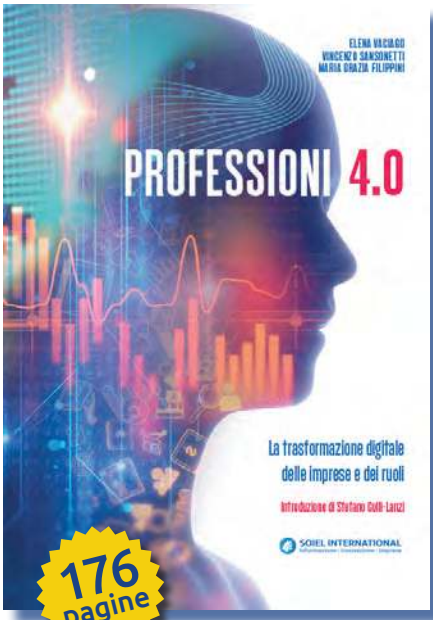
La conoscenza approfondita sia delle realtà che possono portare minacce che delle proprie vulnerabilità, e l'apprendimento, la lezione che proviene dal verificarsi degli incidenti, rappresentano aspetti fondamentali per capire quale strategia difensiva adottare per proteggere gli asset e i processi legati al business aziendale. Gli attacchi continueranno infatti a sfruttare i punti di debolezza presenti nell'organizzazione, nella tecnologia e nei processi. Perciò il successo di un'impresa nel campo della sicurezza delle informazioni va perseguito tenendo presenti alcuni punti essenziali. Eccoli.

1) **Avere una organizzazione di Security solida**, con velocità di attuazione, competenze sempre aggiornate e un presidio costante e integrato di tutte le attività inerenti alla gestione dei rischi. La mancanza di esperti nel settore è sempre più un danno diretto alle attività dell'impresa attuali e future.
2) **Sviluppare la Security come un processo** e non come una lista di voci da verificare.

3) **Valutare il rischio cyber e conoscere tutti i propri "punti oscuri"**, le proprie vulnerabilità e lavorare per ridurli mettendo in atto tutte le contromisure e azioni necessarie.
4) **Pensare come un "attaccante"**, prestando anche attenzione ad aspetti di ingegneria sociale, avendo cura di non trascurare la componente umana.
5) **Diffondere la cultura della sicurezza a tutti i livelli**, in modo tale che le persone rappresentino "gli occhi e le orecchie" dell'impresa e le azioni siano coerenti e coordinate. Creare quindi sensibilità sul problema Cyber Security, alzando il livello di awareness, di consapevolezza, in tutti gli addetti e presso il grande pubblico.
6) **"Imparare ad imparare" dagli incidenti che accadono su scala planetaria**; domani potrebbero presentarsi anche a noi, facciamo così in modo che ci trovino con le difese già pronte e adeguate. In tal senso, la Security aziendale rappresenta l'anello di congiunzione tra il business e l'impresa, pensando, attuando e verificando tutte le attività necessarie a protezione degli asset e del patrimonio aziendale e diventando il fulcro di un'azione efficace per l'aumento, nel tempo, del valore dell'impresa sul mercato.

PROFESSIONI 4.0

La trasformazione digitale delle imprese e dei ruoli



UN LIBRO PER PREPARARSI ALLA SFIDA DEL FUTURO

Come le aziende e i loro dirigenti stanno affrontando le straordinarie trasformazioni tecnologiche che cambieranno per sempre il mondo del lavoro? I mutamenti in corso pongono davanti a scelte difficili e a responsabilità nuove, che richiedono una adeguata preparazione. Il libro Professioni 4.0, frutto di un confronto a tutto campo e ad alto livello, analizza per la prima volta questa sfida così urgente e attuale grazie alle testimonianze di prestigiosi manager, che raccontano le loro esperienze e l'impatto della quarta rivoluzione industriale sul proprio ruolo. Il volume è la sintesi di una serie di tavole rotonde che si sono tenute presso Fondazione Gi Group e si rivolge innanzitutto a manager aziendali, consulenti e imprenditori, ma anche a docenti e studenti universitari e a tutti coloro che sono interessati ai cambiamenti in atto. Imperdibile per chi vuol capire come le imprese stanno preparandosi al futuro.

ELENA VACIAGO, VINCENZO SANSONETTI, MARIA GRAZIA FILIPPINI
Professioni 4.0. - La trasformazione digitale delle imprese e dei ruoli (introduzione di Stefano Colli-Lanzi)

SOMMARIO

NOVITÀ

Il libro "Professioni 4.0" può essere richiesto in SOIEL INTERNATIONAL S.r.l. mandando una mail a abbonamenti@soiel.it o accedendo al sito www.soiel.it compilando il form di richiesta.

Il prezzo di copertina di euro 19,00 comprende anche le spese di spedizione.

SOIEL INTERNATIONAL
Informazione - Innovazione - Imprese

Via Martiri Oscuri, 3 • 20125 Milano • Tel. 02 26148855 • Fax 02 26149333
att.ne Lina Prestia • abbonamenti@soiel.it • www.soiel.it