W.TRAINING

ERIS CONSULTING

SICUREZZA DELLE INFORMAZIONI ALL'EPOCA DELLO SMART WORKING

MINI-MASTER PER RISPONDERE ALLE ESIGENZE DI SICUREZZA DELLE AZIENDE E PER PROTEGGERNE LE INFORMAZIONI

Una proposta di
W.Training

PRESENTAZIONE

La sicurezza delle informazioni quando si lavora in smart working dipende da aspetti tecnici (accessi remoti, tecnologie, ecc.), organizzativi (regolamenti, reingegnerizzazione dei flussi operativi e dell'interazione tra i dipendenti e gestione degli stessi), legali (norme relative, controlli, ecc.).

Per essere affrontato in maniera efficace, però, **il tema va inquadrato in un ambito più esteso, che comprenda e che traguardi l'intera organizzazione**, sia per quanto riguarda ovviamente organizzazione e legalità, ma anche la gestione della sicurezza delle informazioni nel suo complesso, non tanto dal punto di vista tecnologico, ma soprattutto da un punto di vista comportamentale.

L'innovativo percorso innovativo proposto da W.Training in collaborazione con **Eris Consulting**, società specializzata nella sicurezza e tutela del patrimonio informativo aziendale, ha un **taglio operativo**: alla teoria sarà concesso meno spazio rispetto al **fare concretamente** e i partecipanti al percorso formativo saranno chiamati a un ruolo da protagonisti.

I responsabili aziendali saranno inizialmente coinvolti dagli esperti di Eris Consullting in un **Light Assessment che individuerà le problematiche di sicurezza e i comportamenti più a rischio** all'interno della propria azienda.

A due seminari "introduttivi" sarà poi affidato il compito di avviare un **"percorso di consapevolezza" in azienda**, fornendo le indicazioni tecniche, organizzative e comportamentali necessarie per salvaguardare le informazioni.

Toccherà quindi ai dirigenti, durante **workshop condotti in assoluta autonomia**, senza la supervisione dei docenti - una sorta di **micro self-assessment** -, testare con i propri gruppi di lavoro il grado di consapevolezza riguardo la sicurezza dei dati in azienda e individuare eventuali rischi per l'organizzazione.

A questo punto, i dirigenti torneranno in aula virtuale per **approfondire la conoscenza delle normative legate alla sicurezza dei dati e al rispetto della privacy**, nonché gli **aspetti organizzativi, manageriali e della gestione del capitale umano** che soprattutto le imprese che operano in modalità "agile" si trovano ad affrontare.
I partecipanti alla formazione avranno poi modo, durante un altro **workshop condotto in autonomia** senza l'ausilio dei docenti, di applicare il **modello GROW**, una metodologia che consente di definire obiettivi condivisi e motivanti ed individuare il percorso reale per raggiungerli.
Durante l'**ultima giornata**, infine, i dirigenti e gli esperti di Eris Consulting **analizzeranno quanto emerso dal Light Assessment iniziale e dai vari workshop** effettuati in autonomia dai dirigenti per individuare le **criticità** e le relative **contromisure**.

L'investimento richiesto è di 12.500 euro
e potrà essere interamente finanziato
con l'Avviso 1/2021 di Fondirigenti.

DETTAGLI DEL PERCORSO FORMATIVO

Affiancamento e Light assessment

Questa fase si compone di due momenti distinti, ma integrati, durante i quali ci si confronterà con i dirigenti dell'azienda analizzando ad alto livello l'organizzazione ed i processi aziendali, sia per le attività svolte all'interno dell'azienda, sia per quelle svolte da remoto; questo confronto ha l'obiettivo, inoltre, di aiutare il management a focalizzarsi sulle peculiarità dei due modi di lavorare ed iniziare ad introdurre alcuni concetti sulla sicurezza.

- **Snapshot sull'organizzazione e verifica dei processi IT**

Uno sguardo all'organizzazione ed ai processi IT con particolare riguardo alla gestione della sicurezza delle informazioni, sia per chi opera in azienda, sia per i lavoratori remoti o in smart-working. L'attività consiste in una serie di interviste che saranno principalmente rivolte alla Direzione dei Sistemi Informativi, alla Direzione del Personale, al Responsabile della Sicurezza, al Direttore di Produzione, alla Direzione Generale, al Direttore Ricerca e Sviluppo, al responsabile della gestione degli asset... ad un paio di utenti presi a campione, e nella raccolta della documentazione presente (Policy, procedure, organigrammi, nomine, ecc.).

- **Osservazioni comportamentali**

Come ormai è risaputo, la sicurezza non è una questione di prodotti e tecnologie ma di processi, e i comportamenti sono il fulcro di questi ultimi. A nulla servono infatti procedure e regolamenti se poi questi non sono conosciuti o se ancor peggio vengono disattesi, spesso inconsapevolmente, talvolta volutamente, magari per creare una facile scorciatoia nello svolgere le proprie attività. Questa parte del percorso formativo ha l'obiettivo di osservare i comportamenti delle persone in azienda (talvolta interagendo con i dipendenti tramite piccole attività di social engineering), osservando come si relazionano con i principi base sulla sicurezza, con quale attenzione trattano le informazioni riservate, comprese quelle cartacee (non è infrequente fare, ad esempio una verifica di cosa si trova nei cestini a fine giornata lavorativa) e quelle verbali. L'obiettivo è quello di fornire indicazioni sui comportamenti per eventualmente rilevare la necessità di creare maggiore consapevolezza, o rafforzare la diffusione delle politiche di sicurezza.

Seminari

Persone consapevoli, informazioni più sicure

L'obiettivo di questa parte del percorso formativo è quello di informare e sensibilizzare i partecipanti in merito alla sicurezza delle informazioni e ai principali aspetti e rischi ad essa connessi. Saranno prese in esame anche le diverse tipologie di attacco più comuni, comprese quelle di tipo "social engineering", ecc.
Il modulo aiuta a creare consapevolezza negli impiegati, che sono in genere chiamati alle funzioni più operative, e a sensibilizzare i responsabili ed i manager a porre la giusta attenzione al fenomeno degli attacchi informatici e delle frodi finanziarie, all'importanza di adottare opportuni accorgimenti per la protezione delle informazioni aziendali.

Lo smart working e la sicurezza

Operare in smart working comporta necessariamente variazioni nel modo di operare e soprattutto nel modo in cui ci si approccia alle informazioni dell'azienda ed alle tecnologie che le gestiscono.
Le informazioni aziendali sono a rischio quando i dipendenti che lavorano in modalità "agile" utilizzano una connessione privata che nella quasi totalità dei casi dispone di livelli di sicurezza molto inferiori a quelli delle reti aziendali, così come pericoloso è l'utilizzo da parte dei lavoratori dei propri strumenti che, non essendo sotto il dominio IT aziendale, sono molto difficilmente gestibili e monitorabili, costituendo pertanto un vero e proprio tallone di Achille.
L'obiettivo di questo modulo, da un lato è quello di fornire qualche indicazione tecnica e organizzativa, dall'altro quello di fornire le indicazioni comportamentali per poter operare in maggior sicurezza.

Workshop svolti in autonomia, singolarmente

La consapevolezza sulla sicurezza in azienda dal punto di vista del personale

Obiettivo

- Comprendere il livello di consapevolezza di dipendenti e collaboratori in merito alla sicurezza delle informazioni
- Trasferire in Azienda alcuni dei concetti discussi durante il Seminario sulla sicurezza delle informazioni

Modalità

Incontro/intervista con i propri collaboratori e con i dipendenti in genere; ogni dirigente incontrerà singolarmente almeno 5 persone del proprio reparto, discuterà con loro dei concetti di sicurezza cercando di comprendere se i dipendenti conoscono le regole aziendali in merito alla sicurezza delle informazioni, con particolare riferimento allo smart-working, se le seguono, se conoscono, anche per linee generali i rischi relativi alla sicurezza delle informazioni e quali sono i loro comportamenti.

Ogni dirigente riporterà in formato tabellare quanto emerso dagli incontri e lo spedirà al coordinatore del corso.

Durante l'ultima giornata del corso i risultati degli incontri saranno discussi collegialmente.

Come traccia generale viene fornita una lista di domande che possono essere utilizzate per l'incontro con i dipendenti.

Uno sguardo dall'alto sui rischi per l'organizzazione e per il business

Obiettivo

Fermarsi un momento e fare una riflessione sulla propria organizzazione e sul proprio business, con particolare riferimento alla sicurezza delle informazioni, cercando di focalizzare quali sono gli elementi principali che fanno funzionare l'azienda, quali sono le minacce ai quali questi elementi sono sottoposti e quali contromisure sono state implementate per limitare i rischi.

Modalità

Si tratta di una sorta di micro self-assessment; utilizzando come spunto le domande fornite, fare una riflessione sui vari argomenti, esponendo le peculiarità di ogni area/macro-servizio, dando una prima stima della sua criticità in Azienda (cosa succederebbe se questo elemento smettesse di funzionare? Per quanto tempo posso accettare che questo elemento non funzioni senza che il funzionamento o il business dell'azienda ne risenta seriamente? Ecc.)

Durante l'ultima giornata del corso i risultati degli incontri saranno discussi collegialmente.

Come traccia generale viene fornita una lista di domande da usare come spunto per la riflessione.

Prepararsi a discutere domande quali: cosa avete fatto/state facendo per contrastare questa minaccia? Cosa sarebbe opportuno fare?

Seminari

Smart working e normativa applicabile rispetto agli strumenti informatici

L'obiettivo del modulo è quello di focalizzare in maniera sintetica e pratica gli aspetti legali che consentono di conciliare lo smart working con i diritti dei lavoratori e al tempo stesso con una governance "conforme" degli strumenti informatici.

Le principali tematiche: Decreti di urgenza attuali e smart working: principi ed applicazioni pratiche **|** Come cambia la regolamentazione interna rispetto alle primarie normative in ambito informatico **|** Il dipendente ed il diritto alla disconnessione **|** Casi pratici: presenza di MDM, tracciabilità dell'operato, SIEM attivi

Come gestire sotto il profilo legale la privacy in smart working

Il GDPR ci ha insegnato che la normativa non rappresenta un mero vincolo a cui adempiere, ma soprattutto un driver per la crescita aziendale e l'aumento della competitività, un'opportunità da cogliere in ottica di innovazione di processi, prodotti, servizi e di relazione con i propri clienti, partner e fornitori. Questi ultimi assumono un ruolo centrale nel processo di evoluzione dell'impresa. Il modulo è dedicato al tema dell'applicazione del Regolamento europeo in smart working: cosa porre all'attenzione, cosa modificare e come gestire gli adempimenti per rispettare la normativa.

Le principali tematiche: La gestione degli obblighi documentali **|** Le procedure in accountability che devono essere adottate tenuto conto del nuovo assetto organizzativo **|** Il privacy by design applicato a distanza **|** Audit fornitori a distanza: come effettuare l'audit e che cosa deve essere dimostrato in caso di controllo

Workshop svolto in autonomia, in gruppo

L’applicazione del modello GROW

Obiettivo

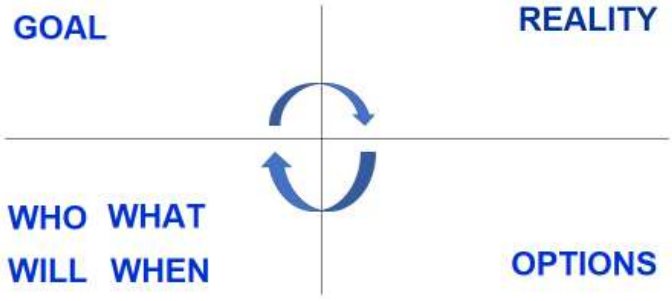
Prendere dimestichezza ed esercitarsi con una metodologia in gruppo che consenta di definire obiettivi condivisi e motivanti ed individuare il percorso reale per raggiungerli.

Modalità

Il responsabile come anello forte o debole della catena tra azienda e collaboratori. Le competenze morbide sono da tempo considerate irrinunciabili ma oggi lo sono divenute ancora di più per effetto dei mutamenti imposti dalla pandemia.

Se consideriamo che, per creare scambi significativi in azienda, come in qualunque organizzazione collettiva, si può fare affidamento a 4 meta-competenze significative:

Su questi presupposti di consapevolezza e di conseguente assunzione di responsabilità e facendo riferimento alle competenze morbide, si può utilizzare una metodologia in gruppo che consente di definire obiettivi condivisi e motivanti e individuare il percorso reale per raggiungerli.
Si tratta della metodologia G.R.O.W. (Goal, Reality, Options, hat/When/Who/Will). Un percorso in gruppo che: definisce il Goal; ne considera gli aspetti di Realtà nel bene e nel male; ne considera le possibili Opzioni per la soluzione migliore; pone da ultimo la Volontà di fare, ossia il piano di azione del cosa si farà, quando e chi.
Nei due quadranti Goal e Reality si nutre la consapevolezza, nei due quadranti Options e WWWW si assumono responsabilità.



Ultima giornata

Analisi e discussione di quanto emerso dal Light Assessment, dai risultati dei workshop e indicazioni delle eventuali contromisure

Questa sessione prevede un momento di affiancamento e un confronto con i dirigenti ed il management dell'Azienda per operare in maniera congiunta una analisi delle evidenze raccolte durante le interviste e dei workshop effettuati in autonomia dai dirigenti, per discuterne, per approfondire eventuali punti e per individuare eventuali azioni correttive e/o evolutive da adottare per migliorare il livello di sicurezza, sia per l'azienda, sia per i dipendenti.

I DOCENTI

Franco Prosperi

Ha maturato la propria esperienza professionale nel settore dell'Information Technology e della consulenza presso grandi clienti, a partire dal 1987, in una primaria società multinazionale statunitense. Nel 2003, costituisce la **Eris Consulting Srl**, di cui è tuttora socio ed amministratore, con l'obiettivo di proporre servizi consulenziali rivolti al Management e alla proprietà aziendale sulle tematiche di Sicurezza e tutela del patrimonio informativo, Information Governance, prevenzione e contrasto frodi, Risk Management e Business Continuity.
Nel corso degli anni ha conseguito le seguenti certificazioni professionali:

- CISA (Certified Information System Auditor) e CISM (Certified Information Security Manager) rilasciate da ISACA (Information System Audit and Control Association);
- CFE (Certified Fraud Examiner) rilasciata da ACFE (Association of Certified Fraud Examiner);
- Lead Auditor ISO/IEC 27001:2005 rilasciata da BSI (British Standard Institution).

Romano Castagnara

Dopo una esperienza di oltre 20 anni in una multinazionale dell'informatica, con diverse mansioni e lavorando spesso con gruppi internazionali, nel 2001 passa in un'azienda italiana di servizi informatici (outsourcing, consulenza e progetti) dove per oltre 10 anni ha ricoperto il ruolo di dirigente responsabile della progettazione di soluzioni di sicurezza e dell'erogazione di servizi per Top Customer.
Attualmente è socio e amministratore di **Eris Consulting** e svolge attività di consulenza manageriale e formazione in ambito di information governance e security, di processi di gestione di servizi informativi, sicurezza fisica.

Gianni Spulcioni

È un Management Consultant che si occupa di gestione del personale, di formazione, di governance all'interno delle imprese e di sistemi di controllo interno, di sistemi di gestione della sicurezza sul lavoro. Ha maturato la propria esperienza professionale all'interno di aziende di diversi settori, tra cui Assicurativo, Farmaceutico e Energia.
È stato Condirettore Generale Controlli e Vice Direttore Generale per servizi e risorse in HDI Assicurazioni, Responsabile Gestione Risorse Umane in Menarini Group, Responsabile Gestione/Sviluppo Risorse Umane in Fondiaria-SAI, responsabile HR\Relazioni Industriali Formazione Sviluppo in Italgas\FiorentinaGas spa.
Al suo attivo diverse pubblicazioni edite da Aracne Editrice e Franco Angeli.