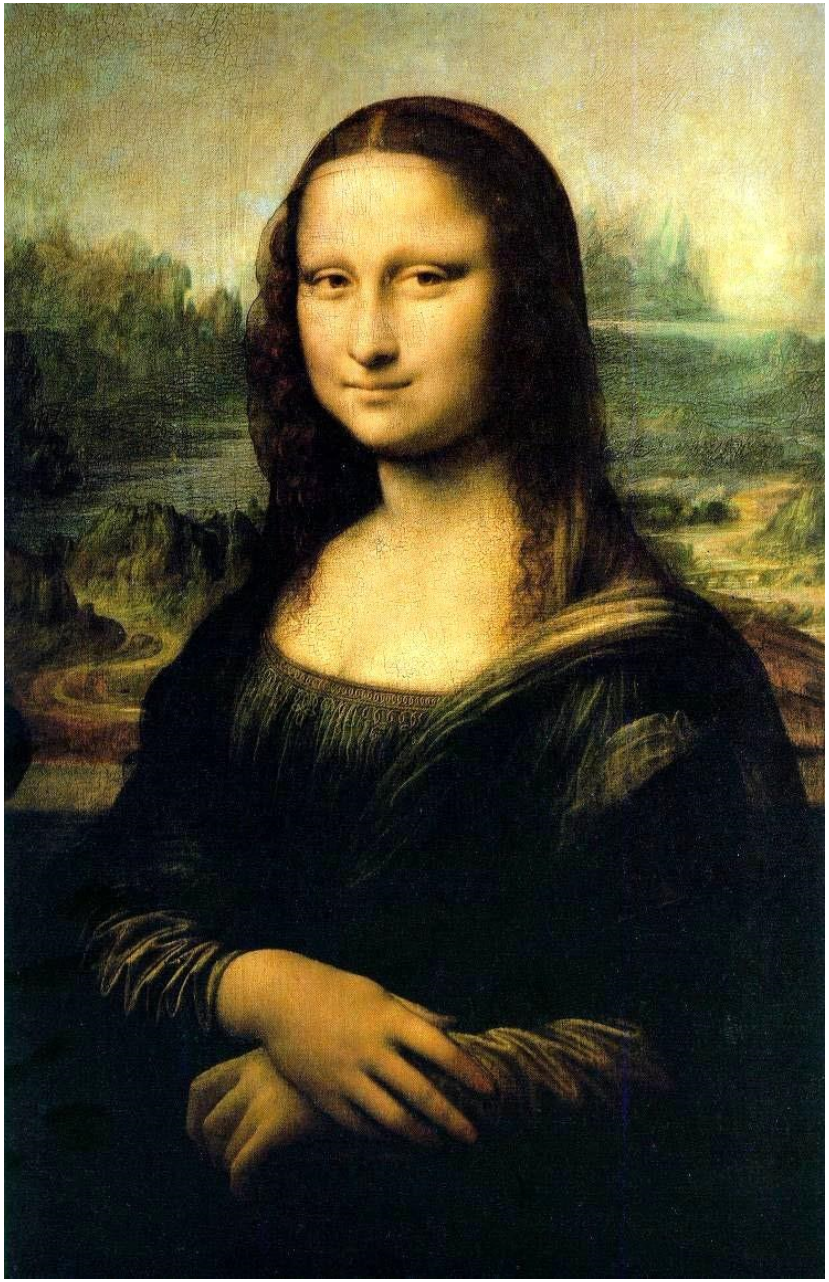


Maturità, sensibilità al rischio e consapevolezza delle risorse umane in azienda

Pierluigi Ascani,

Presidente del CDA *Format Research Srl*

Milano, 26 maggio 2016

agenda

- premessa
- processo logico
- considerazioni generali di sintesi
- i risultati della ricerca
- aspetti di metodo

In questo documento sono presentati i risultati di alcuni lavori svolti da Format Research sul tema della **sicurezza delle informazioni in azienda**.

Realizzati con la tecnica dell'indagine di campo, gli studi avevano l'obiettivo di analizzare la **maturità, la sensibilità al rischio e la consapevolezza** dei dipendenti di alcune aziende private italiane, con riferimento al tema della sicurezza aziendale….

- *ex ante,* identificandone il **livello di partenza**
- *ex post,* analizzandone i progressi …

a seguito delle **azioni di comunicazione e formazione** svolte presso le imprese su tale problematica.

L'obiettivo ultimo è stato quello di misurare l'efficienza e l'efficacia dell'attività di comunicazione in termini di **additività:** valore aggiunto prodotto delle azioni di comunicazione e formazione che si concretizzano con il livello di *awareness* delle risorse umane presenti in azienda.

È stato così possibile distinguere il «naturale» incremento della consapevolezza (dovuta al passare del tempo), rispetto a **quello che non avrebbe potuto svilupparsi senza le azioni di comunicazione e formazione svolte appositamente** (vero e proprio valore aggiunto).

processo logico | gli *step* della ricerca…

Di seguito è riportato il processo logico alla base del flusso di lavoro che ha caratterizzato l'indagine…

Sono state **selezionate** n. 30 imprese alto performanti, con fatturato superiore a 2,5 mln €

È stato somministrato un questionario ***EX ANTE*** alle risorse operative nelle aziende (dipendenti, ad esclusione dei dirigenti).

Alcune delle imprese selezionate hanno lanciato azioni di comunicazione e formazione interna circa le policy per la sicurezza aziendale.

È stato somministrato lo stesso questionario ***EX POST*** alle medesime risorse intervistate *ex ante*.

Sono stati analizzati i risultati in termini di **additività** del personale coinvolto nella ricerca.

Il livello di **consapevolezza delle componenti** nelle quali si articola la **sicurezza aziendale**, a giudizio dei dipendenti delle imprese coinvolte nella ricerca, risulta «alto» prevalentemente circa la salvaguardia delle **password** personali (è così per il 47,1% delle risorse intervistate), riguardo la **documentazione non digitale** (40,3%), la **posta elettronica** (38,4%). Meno con riferimento alle *policy* aziendali in generale e alla gestione delle non conformità, intese come eventi avversi (incidenti, malfunzionamenti). D'altra parte, questi ultimi due aspetti risultano anche tra quelli ritenuti meno «rischiosi» da parte dei lavoratori dipendenti. Al contrario, è percepito come «**elevato**» il livello di **rischio relativamente all'utilizzo delle password**, alla gestione delle **informazioni e dei dati**, alla sicurezza dei **terminali e dei device**.

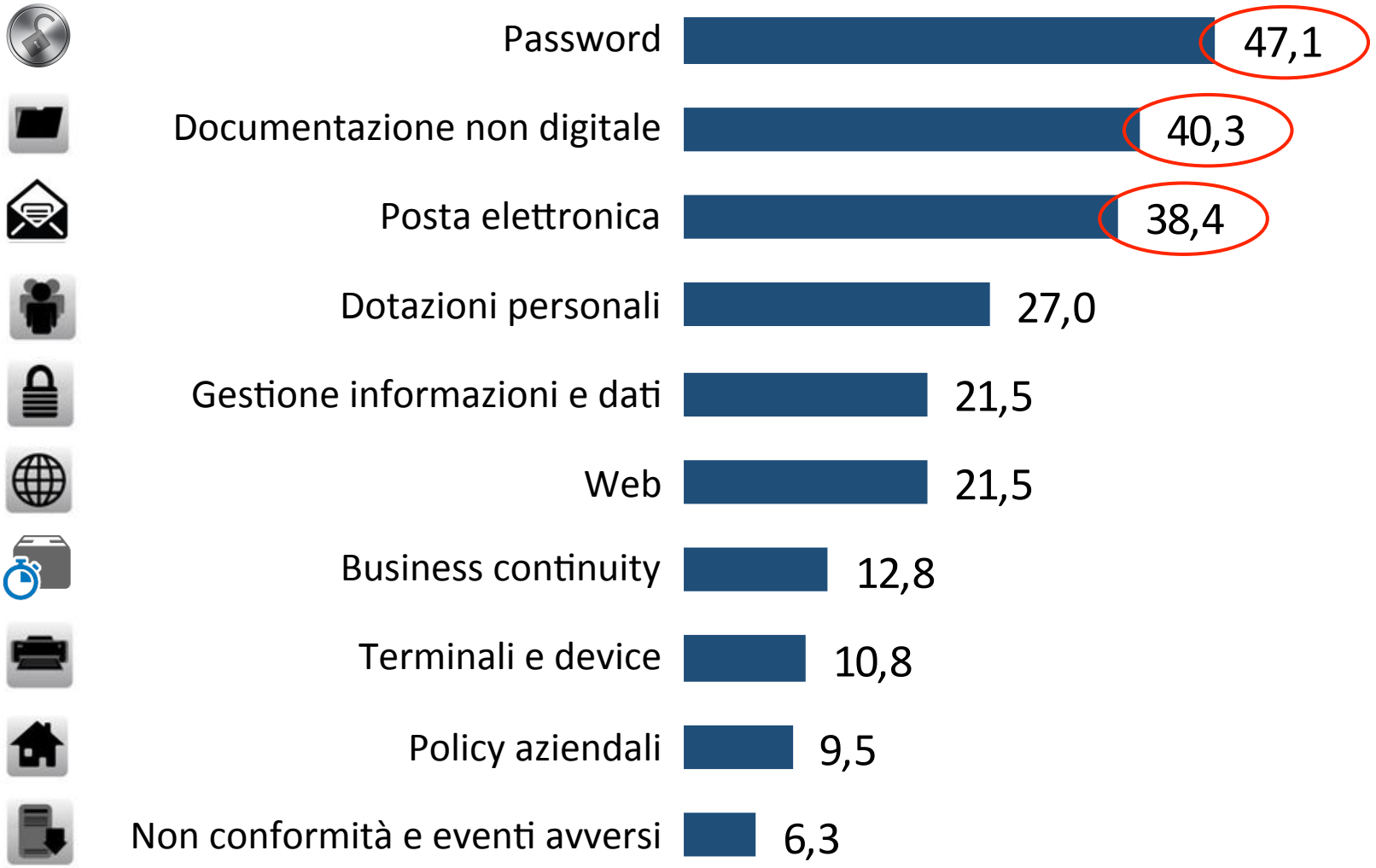
Analizzando il campione in funzione dell'avvenuta (o meno) effettuazione di **azioni mirate a sensibilizzare il personale su temi inerenti la sicurezza aziendale**, si evince come il segmento di coloro che hanno partecipato a tali iniziative evidenzi un livello di conoscenza delle *policy* di sicurezza aziendale decisamente più elevato rispetto a quanto non si registrasse prima della suddetta azione. Questo si traduce in un rilevante incremento dell'**additività** su quasi tutti gli aspetti analizzati, superiore a quello «naturale» che si sarebbe avuto con il semplice passare del tempo.

In linea generale, **un'azione di comunicazione e formazione sembrerebbe rivelarsi assai efficace** se organizzata sotto forma di **corsi di formazione** nell'ambito di un **sistema di qualità aziendale «normato»**, che si concretizza nella messa a disposizione di tutto il personale di **documenti e policy strutturate in materia di sicurezza.**

i risultati della ricerca | la consapevolezza delle componenti nelle quali si articola la sicurezza aziendale secondo il giudizio dei dipendenti

A Suo avviso, quali sono le **aree** nelle quali si articola la **sicurezza in azienda**?

(risposte spontanee, post-codificate)



i risultati della ricerca | il livello di rischio «alto» associato alle diverse componenti della sicurezza

Potrebbe indicarmi il **livello di rischio** per l'azienda associato ad ognuna delle aree appena descritte?

(Scala da 1=min rischio, a 4=max rischio. Sono riportate le aree con livello di rischio «4»)

Password	71,9
Gestione informazioni e dati	69,0
Terminali e device	62,3
Posta elettronica	56,7
Dotazioni personali	54,5
Documentazione non digitale	50,1
Web	35,5
Policy aziendali	35,0
Non conformità e eventi avversi	27,8
Business continuity	24,5

Password

In ambito informatico e crittografico, una password (dall'inglese «parola di accesso») è una sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica (computer, connessione internet, casella e-mail, reti, programmi, basi dati, ecc.) o per effettuare operazioni di cifratura. È consigliato ai dipendenti di un'azienda di non trascrivere mai (né comunicare ad altri) la propria password, provvedere a cambiarla periodicamente ed assicurarsi che sia costituita da caratteri alfanumerici che la rendano il più complessa possibile.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza delle password?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	3,0	20,5	20,5	**55,9**
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	0,0	4,6	23,5	**71,9**

Gestione informazioni e dati

Le informazioni e i dati aziendali rappresentano gli asset dell'impresa, ovvero un bene per ciascuna risorsa.
Le informazioni hanno carattere riservato e sensibile e devono essere distrutte quando non più necessarie.
Non possono essere trasferite dai locali aziendali senza autorizzazione o in contrasto con la policy di record management e devono essere solitamente conservati in apposite cartelle adibite esclusivamente a questo.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza della gestione di informazioni e dati?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	1,5	2,2	13,0	**83,3**
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	0,0	5,8	10,8	**83,4**

Terminali e device

Un terminale, in campo informatico, è un dispositivo hardware elettronico o elettromeccanico che viene usato per inserire dati in input ad un computer o di un sistema di elaborazione e riceverli in output per la loro visualizzazione.
Le norme di sicurezza consigliano solitamente di non installare software personali sui terminali e sui device aziendali, di prestare la massima attenzione ogniqualvolta si utilizzano dispositivi esterni mobili e di trasferire immediatamente sul server i dati più importanti importati dall'esterno.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza di terminali e device?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	5,8	8,6	28,8	**56,7**
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	0,3	5,5	32,3	**61,9**

Posta elettronica

La posta elettronica (e-mail o email, dall'inglese electronic mail) è una posta digitale grazie alla quale ogni utente abilitato può inviare e ricevere dei messaggi utilizzando un computer o altro dispositivo elettronico connesso in rete attraverso un proprio account di posta registrato presso un provider del servizio.
È necessario evitare di aprire e-mail di origine sconosciuta (es. Spam) e diffidare dalle mail che richiedono l'inserimento di credenziali (anche qualora il mittente sembri legittimo).

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza della posta elettronica?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	2,2	6,7	24,4	**66,7**
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	0,0	3,3	21,2	**75,5**

Dotazioni personali

Le dotazioni personali sono documenti confidenziali che devono essere ben custoditi e riposti sotto chiave quando la risorsa che ne detiene la proprietà si allontana dalla postazione di lavoro o a fine giornata.
È necessario evitare di lasciare sulla scrivania fogli con dati e/o informazioni aziendali o personali non adeguatamente custoditi.
Lo stesso vale per i materiali di carattere informatico (portatile, telefono aziendale, etc).
È sempre bene proteggere le proprie dotazioni personali (se possibile) con una chiave di cifratura.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza delle dotazioni personali?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	4,2	11,3	20,8	**63,7**
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	1,5	12,1	13,5	**72,9**

Documentazione non digitale

I documenti cartacei contenenti dati personali e riservati devono essere riposti in armadi o cassetti (chiusi a chiave) dopo il loro utilizzo.
È necessario assicurarsi di non lasciare mai incustodite informazioni sensibili (es. dati su lavagne) e non rivelare in alcun modo dati e informazioni a persone la cui identità non sia effettivamente verificata.
Lo stesso, vale per le comunicazioni telefoniche, che devono evitare di trattare tematiche inerenti il lavoro se si è al di fuori della propria postazione.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza della documentazione non digitale?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	5,0	14,1	14,1	**66,8**
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	0,0	7,5	7,8	**84,7**

i risultati della ricerca | il livello di conoscenza delle policy aziendali in merito alla sicurezza della *navigazione sul web* secondo il giudizio dei dipendenti

Web

Il World Wide Web (letteralmente «rete di grandezza mondiale»), abbreviato Web, è uno dei principali servizi di Internet che permette di navigare e usufruire di un insieme vastissimo di contenuti amatoriali (multimediali e non) collegati tra loro attraverso legami (link), e di ulteriori servizi accessibili a tutti o ad una parte selezionata degli utenti di Internet. Le norme di sicurezza consigliano di verificare sempre la correttezza di un indirizzo web che si intende visitare, non accettare alcuna richiesta di installazione, non rivelare informazioni aziendali e/o dati sensibili.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza nella navigazione sul web?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	0,0	0,0	25,0	**75,0**
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	0,0	0,0	14,0	**86,0**

Policy aziendali

La policy aziendale è un regolamento adottato dall'impresa che determina i comportamenti da tenere con riferimento all'uso del computer, della navigazione su internet, della posta elettronica, ecc.
Dette disposizioni sono unilaterali e disciplinano le modalità di utilizzo degli strumenti informatici in dotazione ai propri dipendenti per lo svolgimento dei compiti assegnati.
Vengono vietate alcune condotte oppure vengono dettati tempi e modi di utilizzo degli apparati informatici anche per fini personali.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza delle policy aziendali?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	**50,0**	6,7	7,4	35,9

	basso	medio	alto	molto alto
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	1,7	9,8	33,0	**55,5**

Non conformità e eventi avversi

Qualora si verificassero eventi avversi o non conformi alle politiche di sicurezza dell'azienda, è necessario avvisare tempestivamente il servizio di help desk (se esistente) o l'IT Security Manager.
La gestione di tali aspetti è dirimente e deve avvenire anche in via cautelativa, pur se in presenza esclusivamente di un'ipotesi di anomalia o di un apparente malfuzionamento informatico.
In caso di incidenti, è consigliato seguire sempre le procedure aziendali.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza delle non conformità e eventi avversi?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	10,0	20,0	30,0	**40,0**

	basso	medio	alto	molto alto
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	0,0	10,2	21,2	**68,6**

Business continuity

Per gestione della continuità operativa o continuità aziendale (business continuity) si intende la capacità dell'azienda di continuare ad esercitare il proprio business a fronte di eventi avversi che possono colpirla. In caso di emergenza è necessario attenersi in modo scrupoloso alle procedure di sicurezza preventivamente comunicate dall'azienda.
È importante affidarsi al servizio di help desk (se esistente) per il backup continuativo dei dati, evitando di memorizzare informazioni su CD e DVD se non autorizzato espressamente dall'azienda.

Qual è il suo livello di conoscenza delle policy aziendali in merito alla sicurezza della business continuity?

	basso	medio	alto	molto alto
*Imprese che **non hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	5,5	15,4	25,9	**53,2**
*Imprese che **hanno effettuato** azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale nel 2014-2015*	1,2	7,2	13,5	**78,1**

i risultati della ricerca | indice sintetico di efficienza delle azioni, iniziative di formazione e comunicazione

Di seguito è riportato l'esito delle azioni e/o iniziative di formazione e/o comunicazione in termini di **efficienza sui singoli aspetti**:

ALTA ADDITIVITÀ

- Password
- Terminali e device
- Documentazione non digitale
- Dotazioni personali
- Non conformità e eventi avversi
- Business continuity
- Policy aziendali

BASSA ADDITIVITÀ

- Web
- Gestione informazioni e dati
- Posta elettronica

 le azioni, le iniziative di formazione e comunicazione in materia di sicurezza aziendale ritenute più efficaci dai dipendenti

Azioni e/o iniziative di formazione e/o comunicazione in materia di sicurezza aziendale ritenute **più efficaci**:

89,5 Corsi di **formazione** specifici organizzati dall'azienda

85,0 **Sistema di qualità** dell'impresa
(documenti e policy strutturate dell'impresa in materia di sicurezza)

76,5 **Eventi, seminari, convegni** partecipati dai dipendenti

73,0 Informazioni reperibili nella **intranet aziendale**
(documentazione da fonti esterne ma conservata e indicizzata nella intranet dell'impresa)

73,0 Discussioni tra colleghi sul **social network aziendale**

61,2 **Comunicazioni aziendali interne** in materia di sicurezza aziendale

Al fine di conseguire gli obiettivi dello studio descritti in apertura di questo documento, si è proceduto ad un doppio intervento di ricerca (***ex ante***, ovvero prima della campagna di comunicazione ed ***ex post***, ovvero dopo la campagna di comunicazione).

Nell'ambito di ciascun intervento sono stati intervistati, tramite un questionario strutturato, dipendenti di imprese con fatturato superiore ai 2,5 mln €, a loro volta distinti in due *cluster*, omogenei al proprio interno in funzione del livello di conoscenza presunto verso le *policy per la sicurezza aziendale*:

- **Gruppo «A»:** soggetti con un livello medio alto/alto di conoscenza verso le *policy per la sicurezza aziendale;*
- **Gruppo «B»:** soggetti con un livello medio basso/basso di conoscenza verso le *policy per la sicurezza aziendale.*

Per garantire la possibilità di confrontare i risultati di rilevazioni svolte in momenti diversi nel tempo, il campione è stato costituito da un vero e proprio «**panel**» (sono stati intervistati i medesimi individui nel corso delle differenti rilevazioni dati).

La metodologia utilizzata ha permesso di misurare l'effettivo impatto della campagna di comunicazione sui dipendenti delle imprese oggetto dell'analisi, definendo con precisione lo scostamento avvenuto in termini di *awareness* presso ciascun gruppo («A» e «B»), delineando i risultati reali in termini di efficacia e soprattutto di additività.

Per ottenere questo risultato, è stato costruito un apposito indicatore in grado di monitorare in modo «longitudinale» l'evoluzione del livello di consapevolezza presso ciascun cluster e per ciascun aspetto indagato.

Stimatore dell'efficacia della campagna

Fattori componenti policy per la sicurezza	**Indagine ex ante**		**Indagine ex post**		**Stimatore χ**
	Gruppo "A"	Gruppo "B"	Gruppo "A"	Gruppo "B"	
Fattore n. 1					
Fattore n. 2					
Fattore n. …					
Valore complessivo					

Questo documento è la base per una presentazione orale, senza la quale ha limitata significatività e può dare luogo a fraintendimenti.

format research s.r.l.
via ugo balzani 77, 00162 roma, italia
tel +39.06.86.32.86.81, fax +39.06.86.38.49.96
info@formatresearch.com
cf, p. iva e reg. imp. roma 04268451004
rea roma 747042, cap. soc. € 10.340,00 i.v.

unità operativa - via sebastiano caboto 22/a
33170 pordenone, italia - rea 99634/pn

www.formatresearch.com

Membro: Asseprim, Assirm, Confcommercio, Esomar, SIS