2018: L'ANNO DELLE OPPORTUNITÀ

L'aggiornamento della norma per la certificazione dei sistemi di gestione della qualità ISO 9001 e il nuovo regolamento UE sulla Privacy permetteranno alle aziende di raggiungere una maggiore padronanza dei processi finalizzati allo sviluppo del proprio business

Gabriele Pagani
Consulente in Tecnologie dell'Informazione e della Comunicazione, Ingegnere dell'Informazione Junior

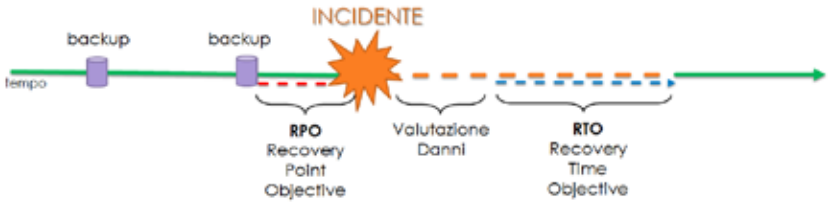

Fig.1 Dinamica post incidente

Nel 2018 diversi cambiamenti nelle procedure aziendali dovranno avere il loro compimento.
Entro il 14 settembre 2018 le organizzazioni certificate ISO 9001 sul sistema di gestione della qualità dovranno infatti adeguarsi alla nuova revisione della norma, passando dalla definizione di requisiti standard (UNI EN ISO 9001:2008) a un approccio che preveda l'identificazione dei rischi nei processi aziendali e delle misure appropriate da adottare per gestirli, oltre all'individuazione delle possibili soluzioni e contromisure per affrontarli (UNI EN ISO 9001:2015).
Un'opportunità per migliorare l'intero business aziendale, estendendo questi principi dello standard a tutti i rischi che possono mettere a repentaglio i processi produttivi e organizzativi, coinvolgendo aree come ambiente, sicurezza sul lavoro, impianti chiave, infrastrutture ICT.
Il 25 maggio 2018 entrerà inoltre in vigore il nuovo regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679) che, insieme alla Direttiva UE 2016/680, è stato definito il "Pacchetto europeo protezione dati". Le aziende dovranno adeguarsi alle nuove regole passando dal soddisfacimento meramente formale dei requisiti indicati nel disciplinare tecnico allegato al Decreto Legislativo n. 196 del 2003 (c.d. "Codice Privacy"), ad una valutazione e gestione del rischio, assumendosi la responsabilità di definire le misure di sicurezza idonee alla tutela dei dati personali trattati.
Il 2018 si presenta pertanto come un anno di cambiamento organizzativo, se non addirittura culturale all'interno delle aziende. Non è più richiesto semplicemente di assolvere ai requisiti stabiliti dalle norme, ma di definire un piano di Risk Assessment polisettoriale che studi strategie di gestione e identificazione dei rischi, stimandone conseguenze e gravità.
Nelle moderne organizzazioni il sistema informativo aziendale rappresenta la struttura dentro la quale la maggior parte dei processi produttivi e organizzativi sono gestiti. Risulta quindi prioritario garantirne la continuità di funzionamento e la tutela delle informazioni in esso contenute, anche in termini di "qualità del dato". Approfittando dell'adeguamento alle norme indicate precedentemente, le aziende hanno l'opportunità di implementare o migliorare il proprio sistema di protezione dei dati aziendali, sensibili non solo dal punto di vista legislativo ma in riferimento a quelle informazioni ritenute importanti e strategiche, anche indirettamente, la cui diffusione o perdita potrebbe cagionare danno all'azienda:

- La redazione di un regolamento interno sull'utilizzo dei dispositivi informatici, che permetta agli operatori di apprendere procedure certe a tutela delle operazioni svolte durante le attività lavorative.
- L'implementazione di procedure per la cancellazione sicura delle informazioni al fine di impedire che dati sensibili vengano estrapolati da dispositivi dismessi.

Non è sufficiente la semplice cancellazione di file o la classica formattazione del disco, che non sempre realizzano una vera cancellazione dei dati memorizzati, ma è necessario utilizzare software dedicati allo scopo e, nel caso il dispositivo elettronico non sia più funzionante, occorrerà procedere con la distruzione fisica o l'utilizzo di dispositivi di demagnetizzazione.

- Firewall e antivirus, sistemi di protezione ormai consolidati all'interno delle imprese, abbisognano di revisioni periodiche. Le necessità aziendali cambiano rapidamente ed è importante appurare che le politiche di gestione di questi sistemi siano correttamente interpretate e aggiornate, tenendo traccia di ogni nuova implementazione.
- Garantire la protezione dei PC portatili, supporti rimuovibili (chiavette usb), smartphone e tablet, applicando misure per limitare i danni in caso di furto o smarrimento quali la cifratura dei dispositivi, l'utilizzo di credenziali di accesso (anche su chiavette, cellulari e tablet). A novembre 2016 ESET, società che sviluppa software di sicurezza, ha presentato i risultati di una ricerca condotta su 500 lavanderie inglesi in cui sono stati ritrovati negli indumenti consegnati in un anno oltre 22.000 chiavette USB e oltre 950 cellulari, il 45% dei quali non è tornato in possesso dei legittimi proprietari.
- Impedire l'utilizzo di dispositivi personali o di provenienza incerta che potrebbero essere veicolo di infezioni che potrebbero propagarsi all'interno della rete aziendale. Una diffusa tecnica per tentare l'intrusione informatica è quella di lasciare chiavette USB contenenti virus nelle vicinanze dell'obiettivo designato e attendere che venga raccolta e collegata a un computer aziendale. Nel 2016 un gruppo di ricercatori dell'Università dell'Illinois ha pubblicato gli esiti di un esperimento che replicava lo scenario descritto, con il risultato che quasi la metà delle chiavette abbandonate è stato inserito in un computer connesso a Internet.
- Proteggere i sistemi e definire i comportamenti in caso di collegamento a hot spot pubblici (aeroporti, Internet-cafè, hotel e altri luoghi pubblici) per evitare l'intercettazione delle comunicazioni o essere reindirizzati su altri siti Web di natura fraudolenta.
- La definizione di un piano di "business continuity", documento che contempli tutte le misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi d'impresa, a fronte di imprevisti che ne intacchino la regolare attività. All'interno di questo documento deve essere presente anche il piano di *disaster recovery* con l'esplicita valutazione e definizione del "Recovery Time Objective", cioè del tempo previsto per il ripristino dei servizi (identifica la massima durata prevista o sopportata del tempo di fermo) e del "Recovery Point Objective", cioè della quantità di dati che il sistema può tollerare di perdere in caso di guasto improvviso (determina la frequenza e tipologia del backup).
- Una conoscenza completa delle politiche di backup e ripristino diventa cruciale per assicurare il riavvio completo in tempi brevi dell'infrastruttura IT. Questo si ottiene tramite operazioni tassative di verifica della congruità dei dati copiati, la predisposizione di processi multipli di backup anche in remoto o in Cloud, frequenze di esecuzione mirate definite nel Piano "Risk & Disaster Management", e l'uso di supporti di archiviazione diversi in base all'importanza e alla velocità di aggiornamento dei dati.

Ecco perché il 2018 si presenta davvero come l'anno delle opportunità: adeguando le organizzazioni agli adempimenti di legge si permetterà ai manager di conoscere più approfonditamente e migliorare i processi aziendali, ponendo le basi per una migliore governance in tutti i settori del proprio business. ■