ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Gruppo di Lavoro
SICUREZZA INFORMATICA
Assintel

Metti al sicuro il tuo

BUSINESS

Vademecum per la sicurezza dei dati aziendali

Unione
CONFCOMMERCIO
IMPRESE PER L'ITALIA
MILANO · LODI · MONZA E BRIANZA

Ringraziamenti:

Si ringrazia per la stesura del Vademecum il Gruppo di Lavoro Sicurezza Informatica di Assintel nelle persone di:

Elio Arena: *CEO, Omicron Sistemi - www.omicronsistemi.it*

Michele Barbiero: *General Manager, CREAplus Italia - www.creaplus.it*

Alessandro Bottonelli: *CEO & Technical Director, AxisNet - www.axis-net.it*

Carlo Buzzi: *IT Security Consultant, Present Systems - www.it-present.com*

Paolo Calvi: *Privacy Consultant - www.privacymilano.it*

Stefani Galbusera: *CoCreatore, SeInTe Recuperodati.it - www.seinte.it*

Paola Generali: Managing Director, GETSOLUTION; *Vice Presidente Assintel; Coordinatrice Gruppo di Lavoro Sicurezza Informatica Assintel - www.getsolution.it*

Carlo Guastone: *Vicepresidente Business Development, Sernet - www.sernet.it*

Vincenzo Monteforte: *CoFondatore, Technical Engineer e Chief Evangelist, SOS Recuperodati - www.sosrecuperodati.it*

Maurizio Moroni: *Director of Sales - Head of Cybersecurity, Partner Data - www.partnerdata.it*

Vittorio Orefice: *Amministratore Delegato, Digiway - www.digiway.it*

Dino Sacco: *Security Delivery Unit Manager, Present Systems - www.it-present.com*

Franco Stolfi: *Responsabile metodologie e processi, Partner PRS Plannig Ricerche e Studi - www.prsmonitor.eu*

20121 Milano – C.so Venezia 47
Tel. 02 7750.231 • 02 7750 235 • Fax. 02 7752 500 • www.assintel.it

Indice

INTRODUZIONE

Le PMI e la sicurezza delle informazioni

In questo "vademecum" non troverete lunghi discorsi teorici; vogliamo invece dare agli imprenditori delle PMI concrete indicazioni sulle cose da fare (e non fare) per difendere il business da possibili "violazioni" della sicurezza delle informazioni aziendali. Tutte le PMI di ogni settore, infatti, nella gestione quotidiana creano, consultano, gestiscono informazioni con strumenti informatici aziendali (propri o in *Outsourcing* o anche in *Cloud*). Molte informazioni sono riportate anche su documentazione cartacea e richiedono adeguate misure di sicurezza, come previsto specificamente dalle Normative Privacy.
Ma in cosa consiste la sicurezza delle informazioni? La risposta è molto semplice a livello di enunciato: sicurezza significa in pratica riservatezza, disponibilità e integrità delle informazioni. Le PMI, come tutte le imprese e le altre organizzazioni, devono pertanto porsi una domanda fondamentale: quali sono i rischi di business e di conformità alle normative di legge che bisogna fronteggiare nei trattamenti delle informazioni (gestione delle attività commerciali, produttive e amministrative, partnership con altre aziende, innovazione dei prodotti-servizi, per citare solo alcune tipologie di informazioni trattate in azienda)?

E' evidente che ogni PMI presenta diversi livelli di rischio relativi alla sicurezza delle informazioni. La cosa importante è che ogni imprenditore conosca la propria esposizione al rischio e promuova le azioni più adeguate per fronteggiare (mitigare) i rischi considerando le minacce che possono pregiudicare la sicurezza delle informazioni, i possibili danni a fronte di violazioni di sicurezza, e, soprattutto, le "contromisure" da adottare. Ogni imprenditore conosce la sua azienda più di ogni altro e deve pertanto definire il livello di rischio accettabile per il business aziendale.
Senza voler generalizzare, è ragionevole sottolineare che sono maggiormente esposte ai rischi relativi alla sicurezza delle informazioni le aziende che:

- non hanno mai valutato la propria esposizione ai rischi,
- trattano informazioni che possono condizionare la competitività sul mercato,
- possono essere oggetto di frodi,
- sono interconnesse in via telematica con clienti e fornitori,
- trattano informazioni "critiche" in termini di conformità alle normative,
- ricorrono alla terziarizzazione dei servizi senza adeguati controlli,
- fanno un utilizzo significativo delle nuove tecnologie (web, social, dispositivi mobili), anche in area produttiva (es. Web 4.0).

Il Gruppo di lavoro Sicurezza Informatica di Assintel ha promosso la realizzazione e divulgazione del presente "vademecum" per sensibilizzare e per fornire un supporto pratico alle PMI nella valutazione delle misure relative alla sicurezza delle informazioni più adeguate alle specifiche realtà aziendali, in termini economici, gestionali, tecnologici ed organizzativi, in coerenza con le indispensabili valutazioni di rischio.

Struttura del Vademecum

Nel Capitolo 1 "**I sistemi informativi aziendali**" si accenna all'ambito nel quale la sicurezza delle informazioni dovrebbe trovare una concreta applicazione, con alcuni approfondimenti relativi alle tecnologie emergenti, che hanno inevitabilmente "innalzato" il livello di rischio, se la loro adozione non è accompagnata da adeguate misure di protezione.

Nel Capitolo 2 "**La sicurezza dei Sistemi informativi**" si descrivono gli aspetti fondamentali relativi alla sicurezza dei Sistemi Informativi, con accenni ad alcune tematiche di grande attualità quali la sicurezza dei servizi in outsourcing e le esigenze emergenti di conformità alla normativa.

Nel Capitolo 3 "**La gestione dei rischi**", che è il "cuore" del vademecum, sono descritte le principali misure di protezione che consentono di ricondurre i rischi a livelli accettabili, facendo riferimento ai principali ambiti nei quali la sicurezza delle informazioni assume grande rilevanza. Si fa riferimento, in particolare, alle attività degli utenti, alla protezione dai codici maligni, alla sicurezza della navigazione Internet, alla gestione dei siti Web e del Mobile, ai servizi di rete, ai servizi in outsourcing e in cloud, alle politiche aziendali di sicurezza e alla stipula di contratti con le indispensabili clausole sulla sicurezza. Infine si accenna alle principali problematiche tecnico-organizzative relative alla sicurezza, come la gestione degli incidenti, la sicurezza fisica, la disponibilità delle informazioni.

Nel Capitolo 4 "**Le norme vigenti in materia**" si affrontano le relazioni fra adempimenti richiesti dalla leggi e la sicurezza delle informazioni, focalizzandosi sulle normative attuali di grande attualità anche per le PMI, come il nuovo Regolamento europeo sulla Data Protection, il Provvedimento del Garante sui cookies, la legge sul Crimine Informatico (Computer Crime), il Decreto legislativo 231/2001, che prevede, fra l'altro, il reato di criminalità informatica e la frode informatica verso la PA, e il Codice dell'amministrazione digitale.

Nel Capitolo 5 "**Standard internazionali per la gestione dei sistemi informativi**" si fa riferimento alle principali Normative volontarie, certificabili da Enti accreditati, relative alla "Sicurezza delle Informazioni", alla "Gestione della continuità operativa" e alla "Gestione dei Servizi IT".
Tali standard, alcuni dei quali di larga diffusione a livello internazionale e nazionale, possono costituire, anche per le PMI, un importante e valido strumento metodologico e organizzativo, che può apportare positivi impatti gestionali e, inoltre, favorire una risposta efficace ai requisiti di conformità alla normativa.

Capitolo 1

I SISTEMI informativi aziendali

1.1 Cosa s'intende per sistemi informativi

Un sistema informativo può essere definito come un insieme di componenti interconnesse che raccoglie, elabora, memorizza e distribuisce le informazioni necessarie per supportare i processi produttivi, decisionali e di controllo di un'organizzazione.
Comprende tutte le informazioni utilizzate dall'azienda, inclusi i supporti che le contengono, gli strumenti che permettono di crearle, modificarle, cancellarle o trasmetterle e le persone, che sono sempre "fonti di informazioni" e contemporaneamente possono essere attori e fruitori del sistema stesso.
In un moderno sistema informativo aziendale buona parte di esso è composta dal sistema informatico, ossia quella parte del sistema informativo che fa uso delle tecnologie informatiche (computer, programmi, Internet, ecc.) a supporto dei processi aziendali.
Rientrano nel sistema informativo anche tutte quelle informazioni che risiedono su altri supporti non informatici, come ad esempio gli archivi cartacei, le fotocopie, le stampe e qualsiasi altro supporto che non viene gestito attraverso sistemi computerizzati.

1.2 Ruolo del sistema informativo

Il Sistema informativo gioca un grande ruolo nella competitività e nello sviluppo di un'azienda e le tecnologie costituiscono un elemento determinante (abilitante) nel raggiungimento degli obiettivi aziendali.
Difatti esiste una stretta correlazione tra la capacità di un'azienda di saper usare le tecnologie dell'informazione e la sua capacità di generare eccellenza operativa, sviluppare prodotti e servizi innovativi, incrementare la fidelizzazione dei propri clienti, migliorare i processi decisionali e aumentare il vantaggio competitivo.
Le aziende più dinamiche, cioè quelle che hanno una maggiore capacità di intercettare i cambiamenti tecnologici e utilizzarli proficuamente nei propri sistemi informativi, sono quelle che presentano i maggiori tassi di crescita, una migliore presenza sul mercato e una maggiore solidità economica.
La tecnologia però non è statica, ma in continua evoluzione; essa offre continuamente nuovi spunti e nuove opportunità per rivedere e aggiornare il sistema informativo aziendale.

Ma quali possono essere le aree tecnologiche che maggiormente potrebbero generare impatti benefici sui sistemi informativi?
Considerando i positivi risultati già riscontrati e traguardando ad un futuro nemmeno troppo lontano, le aree che hanno prodotto impatti positivi sui Sistemi Informativi aziendali possono riguardare:

- l'utilizzo sempre più diffuso del "*Cloud Computing*",
- la disponibilità di piattaforme basate su tecnologie mobile (Smartphone, Tablet, e più in generale sistemi *touch*),
- il dilagare del fenomeno dei *Social Network*,
- la diffusione dell'*IoT*,
- l'opportunità fornita dai "*Big Data*" e dalla "*Sentiment Analysis*" (Analisi delle emozioni espresse sui Social Media) di poter analizzare, interpretare ed estrarre nuove informazioni dalla grande quantità di dati raccolti ed elaborati per supportare i processi decisionali e le strategie di sviluppo aziendali.

Nella seguente Tabella 1 sono riepilogate le citate aree tecnologiche innovative e le tipologie di opportunità/benefici che possono fornire alle aziende.

Tabella 1

AREE TECNOLOGICHE E RELATIVE OPPORTUNITÀ

CLOUD COMPUTING **(nuvola informatica)**	La componente tecnologica del sistema informativo può essere esternalizzata consentendo all'azienda di concentrarsi sul proprio business. Rispetto al tradizionale outsourcing consente di disporre di risorse praticamente illimitate, continuamente aggiornate senza l'onere delle gestione operativa. Sotto il profilo economico consente di ridurre i costi delle infrastrutture tecnologiche, evitando preventivi e massicci investimenti, legandoli direttamente ai volumi delle attività aziendali.
MOBILE **(Dispositivi mobili)**	I dispositivi mobili (*mobile*) quali Smartphone, Tablet e più in generale i dispositivi con schermo tattile (*touch*) hanno superato sia in quantità che come modalità d'uso i Notebook e i Laptop e sempre di più consentono di poter svolgere qualsiasi operazione (navigare, ricercare, acquistare, comunicare, collaborare, etc.). In questo contesto il sistema informativo deve essere in grado di fornire funzionalità agli utenti che intendono mettersi in contatto con l'azienda per qualsiasi tipo di operazione sia di tipo informativo, ma anche per acquistare, comunicare o colloquiare con l'azienda. In questo modo aumentando il livello di interazione tra l'azienda e i propri clienti possono crescere il livello di fidelizzazione e le opportunità commerciali.
SOCIAL BUSINESS **(affari tramite i social)**	I canali social (Facebook, Twitter, Instagram, etc.) possono consentire all'azienda di approfondire il livello di interazione con i propri clienti al fine di incrementare sia in termini quantitativi che di segmentazione del mercato le proprie proposte commerciali. Ovviamente lo stesso strumento consente all'azienda di fornire in modo tempestivo e in una modalità non formale qualsiasi risposta ad eventuali chiarimenti e/o reclami. Il tutto nell'ottica di intensificare il livello di fidelizzazione e aumentare il numero dei contatti.
INTERNET OF THINGS **(Internet delle cose - IoT)**	I dati provenienti dai sensori dei diversi dispositivi possono essere la fonte di preziose informazioni che, opportunamente elaborate, possono consentire di rimodulare le strategie e gli orari di vendita, nonché la segmentazione della clientela per addivenire alla formulazione di strategie commerciali sempre più incisive e personalizzate.
BIG DATA **(Alti volumi di dati)**	Le nuove tecnologie consentono di intercettare gli alti volumi di dati connessi al traffico web, ai messaggi di posta elettronica, ai contenuti dei Social Network, ai dati dei sensori connessi a vari dispositivi *(IoT - Internet of Things)*; questa grande quantità di dati opportunamente elaborata può essere fonte di preziosi informazioni per indirizzare opportunamente sia le strategie commerciali che per fidelizzare i propri clienti ed acquisirne di nuovi.
SENTIMENT ANALYSIS **(Analisi delle opinioni)**	La *sentiment analysis* è l'ascolto di quello che gli utenti pensano e la rielaborazione di queste informazioni, vale a dire l'analisi delle opinioni senza sollecitarle. Il tutto si traduce in un metodo efficace che permette di avere campioni molto vasti (*Big Data*).

1.3 Outsourcing e Cloud

Che cos'è il "*Cloud Computing*"? È un modello in cui le infrastrutture tecnologiche (server, macchine virtuali, data base, piattaforme software, posta elettronica, applicazioni software e altri servizi) sono fornite da un provider come un pool di risorse virtualizzate condivise che possono essere rese disponibili a richiesta.
Dette risorse possono essere dislocate su aree geografiche differenti e possono essere accedute via internet in qualsiasi momento (*everytime*) da un qualsiasi dispositivo e da qualsiasi luogo (*everywhere*).
Le risorse possono essere incrementate o decrementate in funzione delle esigenze dell'azienda e il pagamento è strettamente correlato alla quantità, alla tipologia delle risorse e al periodo di tempo in cui vengono utilizzate. Le principali caratteristiche che contraddistinguono il *Cloud Computing* sono:

- **flessibilità**, intesa come la capacità di adattarsi alle diverse tipologie di esigenze;
- **elasticità**, intesa come la capacità di far fronte a improvvise variazioni di volumi;
- **servizi su richiesta** (*On Demand*), intesi come la capacità di rendere disponibile in modo semplice i servizi richiesti

Ci sono diverse tipologie di risorse e di servizi che possono essere utilizzati in Cloud; nella seguente Tabella 2 sono riepilogate le tre principali categorie di servizi *Cloud*[1].

Tabella 2

TIPOLOGIE DI SERVIZI *CLOUD*

RISORSE INFRASTRUTTURALI **(IaaS - Infrastructure as a Services)**	Rientrano in questa categoria server fisici, macchine virtuali, dischi per la memorizzazione dei dati (storage), reti e altri servizi (per esempio salvataggio degli archivi), messi a disposizione da un provider e sui quali l'utente manda in esecuzione le applicazioni del proprio sistema informatico.
PIATTAFORME SOFTWARE **(PaaS - Platform as a Services)**	Rientra in questa categorie l'insieme degli ambienti software e gli strumenti di programmazione necessari per sviluppare applicazioni. L'aggiornamento tecnologico e la manutenzione di tali ambienti e dei linguaggi è a carico del provider.
APPLICAZIONI SOFTWARE **(SaaS - Software as a Services)**	Rientra in questa categoria la possibilità di utilizzare software applicativi messi a disposizione dal provider. Possono rientrare in questa categoria le applicazioni di carattere gestionale (gestione del personale, contabilità, magazzini, etc.), i sistemi di gestione documentale e del protocollo, i sistemi di posta elettronica, etc. A dette applicazioni si può accedere da qualsiasi dispositivo e in qualsiasi momento; l'elaborazione e gli archivi di tali applicazioni non sono collocati presso l'azienda ma nei siti del provider.

[1]*Secondo la classificazione del NIST (National Institute of Standard and Technology)*

Il modello *Cloud* si presenta come una soluzione particolarmente adatta per le micro, piccole e medie imprese per i motivi che seguono.

- Consente una sensibile **riduzione dei costi**: permette alle aziende, soprattutto di piccole e medie dimensione di disporre di risorse tecnologicamente avanzate, sempre aggiornate a costi estremamente contenuti.
- Migliora la **flessibilità degli investimenti ICT**: utilizzare risorse e soluzioni in Cloud permette di contenere gli investimenti ICT e al contempo di ridurre i costi di gestione. Difatti, la continua e veloce evoluzione della tecnologia, da una parte rende gli investimenti IT velocemente obsoleti e dall'altra richiede un continuo aggiornamento di competenze tecniche che per le piccole e medie imprese possono costituire un problema economicamente significativo o in alcuni casi insormontabile.
- Migliora il ***time to market***: la pronta disponibilità di risorse ICT consente di ridurre il tempo di latenza per l'adeguamento dell'infrastruttura ICT alle strategie o alle evoluzioni commerciali dell'azienda. Elemento questo che diventa particolarmente rilevante anche nella ipotesi di contrazione della domanda, le cui risorse possono essere immediatamente rilasciate senza continuare a sostenere inutili costi.

Ci sono comunque alcuni elementi negativi da considerare nell'utilizzo dei servizi *Cloud*.
I dati e le applicazioni conferite in *Cloud* sono in genere collocate presso i siti del fornitore (provider) che, per la stessa definizione di *Cloud*, possono essere distribuiti su aree geografiche diverse; questo comporta che l'azienda non ha il pieno controllo delle risorse che sta utilizzando.
Eventuali situazioni di blocco del sito del provider, come pure una non efficiente gestione delle risorse, potrebbe portare ad un decadimento dei livelli di prestazione del servizio a discapito dell'operatività dell'azienda, con effetti potenzialmente dannosi sul business (si pensi all'impatto che la non disponibilità di risorse potrebbe avere su un sito di commercio elettronico *e-Commerce*).

In termini molto generali, nell'affidarsi a soluzioni basate su *Cloud Computing* occorre porre attenzione a:
- la **scelta del provider**: va selezionato opportunamente tra soggetti noti che presentano requisiti di maturità e affidabilità;
- la **verifica delle condizioni contrattuali**: bisogna cercare di non stipulare contratti a scatola chiusa, esaminare attentamente le clausole, eventualmente negoziarle e, se non fosse possibile, cercare provider alternativi;
- la **verifica di livelli di servizi** che tutelano l'azienda da possibili situazioni di degrado delle prestazioni; bisogna esaminare i livelli di servizio che garantiscono soprattutto la qualità delle prestazioni focalizzando l'attenzione soprattutto su quelli che possono avere il maggiore impatto sui processi critici dell'azienda;
- la **gestione del fine contratto**, lasciandosi aperta sempre la via di uscita; tutti i rapporti prima o poi hanno una fine e per quell'evento occorre garantirsi un passaggio ad un altro provider possibilmente senza interruzioni di servizio e senza perdita di dati.

1.4 Internet delle cose (*IoT*)

L'infrastruttura Internet è da sempre costituita di "cose" (*things*): server, router e PC usati e governati direttamente da uno o più umani; l'esempio tipico è chi è seduto davanti al proprio PC e legge le sue email, naviga nel Web o scrive un documento.
Quando si parla specificamente di *IoT* (*Internet of Things*) ci si riferisce a "cose" che scambiano dati via internet in modi e per finalità previsti dai programmatori del dispositivo, ma non necessariamente del tutto noti e/o controllabili dal suo utilizzatore umano, quando esiste. Qui di seguito si elencano alcuni dispositivi di tipo "*IoT*": pacemaker, navigatori satellitari, termostati, frigoriferi, televisori, sensori stradali, semafori, distributori di bevande o sigarette, sismografi, caselli autostradali automatizzati, video camere di sorveglianza, geolocalizzatori, allarmi di intrusione per fumo o fuoco o allagamento, ecc.
La *IoT* solo recentemente ha guadagnato la visibilità del grande pubblico, ma è "vecchia". Fu concettualizzata e messa in opera ancora nel 1982 alla Carnegie Mellon University utilizzando un distributore di bibite modificato, che manteneva l'inventario locale e lo notificava al fornitore perché potesse programmare con buon anticipo i rifornimenti.
Siamo già nella *IoT*, nessuno escluso. Coscienti o meno, i sistemi informativi aziendali sono già nella *IoT*, a diversi possibili gradi, come di seguito illustrato.

Oggetti occasionalmente IoT

Ci sono dispositivi in una "area grigia" che non appartengono strettamente alla *IoT*; per esempio PC, smartphone, server, router e punti di accesso WiFi all'occasione si comportano come *IoT*. Senza il vostro intervento essi si collegano ai produttori per verificare la presenza di aggiornamenti di software e fornire altre informazioni, le cui finalità non sono spesso note e chiare, anche perché le spiegazioni date dai produttori non sono sempre un trionfo di trasparenza!

Oggetti IoT anche se non sembrano tali

Qualcosa nella rete aziendale può appartenere a questa categoria. Video camere di sorveglianza, Unità Disco di Rete (o NAS: *Network Attacched Storage*) e Stampanti di Rete solitamente non si limitano a connettersi al produttore per verificare la presenza di aggiornamenti di software. Cosa altro "raccontano"? Serve andare sui siti dei produttori alle sezioni "Politiche sulle Privacy" (*Privacy Policy*) e/o "Termini del servizio" (*Terms of Service*) per avere una chiara e trasparente, si spera, dichiarazione di quali dati il produttore raccoglie dal dispositivo e, soprattutto, per quali finalità.

Oggetti strettamente IoT

Appartengono a questa categoria dispositivi come Smart TV, sensori vari, geolocalizzatori, macchine di controllo industriali, pacemaker, tornelli d'ingresso e timbratrici. Il più delle volte si collegano col produttore e/o col fornitore di servizi per molto di più che la semplice verifica di aggiornamenti di software.
Una Smart TV quasi certamente comunicherà le vostre abitudini e preferenze per poter indirizzare in modo mirato le inserzioni pubblicitarie. Un pacemaker per sua natura e per progetto comunica ad un centro di controllo i dati cardiaci del suo portatore. A chi, per dirgli cosa e per quali finalità altri oggetti (ad es. pressa, sensore antifumo, pompa idraulica, geolocalizzatore, robot industriale, ecc.) si connetteranno dipende dalla natura dell'oggetto.

Nella Tabella 3 che segue sono descritte le implicazioni di sicurezza della *IoT*.

Tabella 3

IMPLICAZIONI DI SICUREZZA DELLA *IoT*

Responsabilità	***Coscienza di quali dati la "cosa" scambia, con chi e perché***
1. L'Azienda è il responsabile ultimo di un proprio trattamento dati davanti alla Legge.	1. Bisogna leggere e capire i "Termini del Servizio" (*Terms of Service*) e la "Politica sulla Privacy (*Privacy Policy*)" del produttore, possibilmente prima di acquisire la "cosa" (NAS, PC, sensore, router, video camera, ecc.). Se qualcosa non è convincente bisogna chiedere spiegazioni; spesso la risposta arriva, ma se nessuno risponde o la qualità e/o trasparenza della risposta sono scarse conviene cambiare produttore!
2. Non essere coscienti di quali dati le "cose" nella propria rete scambiano con chi e per quali finalità: •non è una attenuante, •anzi è un'aggravante, •non sposta a terzi la responsabilità del trattamento (*v. note 1 e 2*)	2a. Il più delle volte è possibile disabilitare la funzionalità di scambio di informazioni fra "cosa" e produttore. Conviene disabilitare tale comunicazione; ma se questo non è possibile o se farlo implica perdere delle funzionalità importanti (per esempio l'aggiornamento del software) conviene cambiare produttore! 2b. Se non è necessario che la "cosa" parli con l'esterno, con tecniche di filtraggio (*firewalling*) e/o instradamento del traffico (*routing*), conviene: • isolarla all'interno della propria rete impedendole di "uscire" verso internet, • selezionate con chi la "cosa" può comunicare: per esempio non il produttore, ma un partner commerciale o industriale.
Affidabilità	***Cura nel progetto e nella gestione della rete aziendale***
3. Molti dei dati che legittimamente le "cose" trasmettono hanno scopi importanti o addirittura vitali: •per l'azienda (sensori di acqua o fumo, cctv, geolocalizzazione); •per un essere umano (pacemaker ed altri sensori medici).	3. Bisogna curare la propria rete aziendale e la sua interconnessione con internet; esse devono essere progettate e gestite con cura, con un occhio di riguardo a: • confidenzialità, • affidabilità, • resistenza ad eventi ordinari e straordinari, • continuità.
Da pochi dati a tanti dati (Big Data)	***Valutazione del rischio***
4. Le "cose" della *IoT* generano: • singolarmente un flusso quasi costante di pochi dati (*small data*); • che vanno ad alimentare tanti dati (i *big data*).	4. Se si trattano dati sensibili (come da definizione di Legge) e/o comunque importanti e/o critici per l'azienda, ad esempio proprietà intellettuale e/o materiale proprio e/o di altri con i quali si hanno obblighi di riservatezza, bisogna: • valutare il beneficio di usare "la cosa" per trattare tali dati; • rispetto al rischio che tali dati finiscano nelle mani sbagliate, accertarsi che le "cose" usate per lavorare tali dati: ▪ non comunichino con l'esterno o ▪ comunichino solo con chi è autorizzato a trattare tali dati.

Nota 1 - Se l'impresa A in qualità di fornitore, cliente o dipendente è lesa dall'uso improprio di dati che aveva fornito all'impresa B:
a) l'impresa A ha un contratto o comunque una relazione (de jure o de facto) con l'impresa B e non col produttore della "cosa",
b) l'impresa A aveva fornito i propri dati all'impresa B per fini precisi;
c) se dall'impresa B i dati sono finiti in mano al produttore della "cosa", il problema è fra l'impresa B ed il produttore, non fra l'impresa A ed il produttore.
Nota 2 - ""Termini del Servizio": in essi il produttore della "cosa" che l'utente ha messo in rete ha certamente incluso clausole in cui l'utente lo autorizzava all'uso di quei dati. Sarà difficile contestare al produttore d'aver fatto qualcosa che l'utente aveva autorizzato a fare.

1.5 Big data

Internet è fatta di persone e di "cose" (*things*); le persone comunicano fra loro e/o con le "cose" e/o per tramite delle "cose" e le "cose" comunicano con altre "cose" o con le persone.
In ogni momento tutti noi creiamo relazioni con altre persone ed oggetti. Ora che proprio tutto è interconnesso queste relazioni generano un flusso costante di piccoli dati (*small data*) che, come tanti piccoli torrenti e fiumiciattoli e fiumi affluenti, vanno ad alimentare progressivamente un enorme "Rio delle Amazzoni" dei dati (*Big Data*).
È importante essere consapevoli che esistono, e che un giorno potrebbero essere digitalizzati anche dati di natura analogica, per esempio: agende, fatture, ricevute cartacee.
Da ogni relazione uomo/uomo, uomo/macchina, uomo/macchina/uomo, macchina/macchina nasce un flusso costante di dati di varia natura.
Nelle realtà aziendali questi dati assumono dimensioni importanti: computer, cellulari, centraline elettriche o telefoniche, rifiuti, consulenti, dipendenti e ogni altro oggetto/soggetto producono dati.
Questi dati, ben classificati, raccolti, strutturati e sintetizzati graficamente possono migliorare l'operatività e l'efficienza di un apparato aziendale: il vostro apparato e/o quello dei vostri clienti, fornitori e... sfortunatamente anche quello dei vostri concorrenti!
I Big Data già riguardano tutti, chiunque li stia usando! Per quanto ci si possa sentire "piccoli", chiunque è uno dei rivoli (o torrenti o fiumi, dipende dalla specifica realtà aziendale) che alimenta il "Rio delle Amazzoni" dei dati (*Big Data*).

Fonti

I big data sono alimentati principalmente da queste fonti:
• la *Internet of Things*;
• i *Social Media*, incluso quel che ognuno scrive della sua Azienda e/o di se stessi;
• le fonti pubblicamente consultabili su internet, incluso il sito web della propria azienda;
• altre aree "grigie", quali: email, dischi virtuali e altri servizi (apparentemente) gratuiti o a basso prezzo.

Scopi

Multinazionali, governi, agenzie di marketing, servizi di sicurezza, la propria azienda e altre aziende possono estrarre e strutturare a livello macro prima, particolare poi, informazioni per scopi: nobili, utili, leciti, discutibili o decisamente illeciti!

Esempi di finalità:
• nobili: prevenire infezioni nei reparti di neonatologia;
• utili: identificare la ragione della scarsa qualità di una linea di produzione (v. sotto);
• leciti: verificare la solidità finanziaria della propria o altrui azienda;
• discutibili: profilare, con scarsa trasparenza, un utente o la propria azienda per poi venderne il profilo ad altri;
• illeciti: sottrarre un brevetto o usare il profilo della propria azienda per sottrarle i clienti e/o screditarla.

Chi

Qualcuno sicuramente usa i *Big Data* per analizzare la vostra impresa (sempre per finalità che possono andare dal nobile all'illecito). Si può e si deve limitare il flusso di dati che esce dalla propria azienda e va ad alimentare i *Big Data*, ma non si può fermarlo.
Visto che dei *Big Data* non ci si libera, tanto vale che ognuno li usi, naturalmente, per scopi nobili, utili e leciti.
Se ad esempio un produttore di sfere d'acciaio nota dei picchi di scarti che da una media dell' 1% passano al 4%, può tentate una analisi (tipo *Big Data*) per scoprire a quale altro fatto è legato questo picco:

1. succede quando si usa l'acciaio del fornitore X,
2. succede quando l'acciaio (di qualunque fornitore) lo consegna il trasportatore Z,
3. succede quando Mario, Rosa e Francesco sono di turno insieme sulla linea di produzione,
4. succede in corrispondenza di ritardi di pagamento al fornitore Z,
5. succede quando la temperatura esterna è oltre i 30° C,
6. ecc.

Attenzione: la relazione "fatto >> picco di scarti" è una cosa, il **significato** della relazione è un'altra cosa.
Se il picco è legato a quando Mario, Rosa e Francesco sono sulla linea di produzione, le spiegazioni potrebbero essere tante; una "relazione a tre", un conflitto proprio fra loro tre, un fatto medico, ecc. Per esempio se Mario, Rosa e Francesco soffrono tutti e tre di deficit d'attenzione, quando sono di turno con altri il loro deficit è compensato dagli altri loro colleghi, mentre quando sono di turno loro tre insieme il loro deficit si somma!
Potrebbe anche non interessare il perché: se si evita di mettere Mario, Rosa e Francesco nello stesso turno ed i picchi di scarti scompaiono, questo potrebbe bastare. Si saranno usati i *Big Data* per uno scopo utile all'azienda e del tutto lecito, invece che essere usati da altri per scopi tutti da definire.
Nella Tabella 4 presente nella pagina seguente sono descritte le implicazioni di sicurezza dei *Big Data*.

Tabella 4

IMPLICAZIONI DI SICUREZZA DEI *BIG DATA*

Responsabilità

1a. L'azienda è il responsabile ultimo di un proprio trattamento dati davanti alla Legge.

1b. Se dati dell'azienda o, peggio, di altri, messi in rete sono usati da **chiunque** per scopi dal discutibile all'illecito:
- potrebbe essere danneggiata la reputazione dell'impresa,
- o peggio, l'impresa potrebbe essere coinvolta in un contenzioso civile,
- o molto peggio, l'impresa potrebbe essere coinvolta in una causa penale (se del caso).

1c. Non essere coscienti di quali dati si lasciano in giro per la rete non sposta e non attenua la responsabilità dell'azienda.

Coscienza dei canali attraverso i quali si alimentano i big data

Bisogna fare attenzione:
- alla *Internet of Things*,
- a cosa si scrive sui *Social* o sul proprio sito web.

Per ogni informazione che s'intende pubblicare si deve:
- valutare la stessa nel contesto e non per il suo valore singolo;
- valutare come questa informazione possa essere incrociata con altre per scopi discutibili, illeciti o comunque scopi che possano danneggiare l'impresa.

Se non è necessario o dovuto pubblicare qualcosa:
- conviene astenersi dal pubblicarlo;
- ricordare che ciò che dell'azienda finisce in rete:
  - rimarrà per sempre in rete,
  - potrebbe essere, e quindi sarà, usato contro la stessa.

Bisogna dotarsi di una politica aziendale, che, per quanto semplice, stabilisca:
- chi è autorizzato a pubblicare in nome dell'azienda,
- le linee editoriali,
- i tipi di informazione "pubblicabili",
- i tipi di informazione che richiedono l'approvazione (di chi?) per essere pubblicate,
- i tipi di informazione esclusi da qualunque pubblicazione.

Non consapevolezza

2a. Molti servizi "gratuiti" ed anche alcuni non gratuiti vanno ad alimentare i *Big Data*:
- email,
- archiviazione (*drive*, *storage*),
- social,
- web.

2b. Non esiste un "pasto gratuito"; il fornitore non è un ente di beneficenza.

2c. Nei "Termini del Servizio" c'è l'autorizzazione per il fornitore del servizio:
- ad usare i dati per altri scopi,
- in alcuni casi c'è anche la cessione dei "Diritti Intellettuali" su quello che passa per i suoi servizi!

2d. Quindi non gli si può contestare di aver fatto qualcosa che era autorizzato a fare! (v. par. su *IoT*).

Consapevolezza del valore dei dati sparsi per la rete

2. Bisogna leggere e capire i "Termini del Servizio" per i servizi usati e:
- se del caso, usare altri servizi di altri fornitori,
- se possibile, rinegoziate i termini (vale per i servizi a pagamento!).

Si deve comprendere il valore dei propri dati e/o di quelli sotto la propria responsabilità:
- il valore per se stessi,
- il valore per gli altri!

L'approccio deve essere minimalista: far "uscire" dalla propria rete aziendale:
- solo ciò che è dovuto; ad es. il bilancio se obbligati per Legge,
- solo ciò che è necessario;
- solo ciò che soddisfi tutte queste altre caratteristiche:
  - utile... a se stessi,
  - inutile... ai vostri concorrenti,
  - lecito (questo esclude la maggioranza dei dati non propri),
  - nella misura "minima e sufficiente" ai propri scopi.

Ineluttabilità

3. Pur con tutte le attenzioni e precauzioni di cui sopra, comunque si alimenteranno, poco o tanto, i *Big Data*, in modi:
- utili a se stessi,
- utili ai propri concorrenti,
- utili a scopi discutibili o illeciti, attraverso canali:
  - nuovi ed imprevedibili,
  - fuori dalla propria oggettiva possibilità di controllo.

Difendibilità

3. Se sono state prese le dovute precauzioni si sarà in grado:
- di usare i *Big Data* per scopi utili a se stessi,
- di limitare l'utilità dei propri dati per i concorrenti,
- di dimostrare, se dovesse servire, la propria buona fede* a chi ne abbia titolo:
  - soci/azionisti,
  - consiglio d'amministrazione,
  - autorità giudiziaria, ecc.

Anche a questo servono le politiche aziendali di cui sopra ed ogni altra documentazione e comportamento utili a dimostrare che:
- si è agito al meglio consentito dallo "stato dell'arte",
- per quanto possibile l'azienda ha beneficiato dei *Big Data* invece di esserne vittima,
- quel che è "sfuggito", non era oggettivamente controllabile.

**ovvero: per limitare le conseguenze, tutto quello che era possibile fare è stato fatto!*

1.6 Continuità operativa (*Business Continuity*)

La condizione basilare perché un'azienda possa raggiungere i propri obiettivi è avere continuità nelle sue attività operative. Ma in realtà quotidianamente le aziende devono fare i conti con eventi che potrebbero interrompere o condizionare pesantemente il loro normale funzionamento: minacce più o meno naturali (incendi, alluvioni, terremoti o altri disastri), interruzioni di corrente, attacchi cibernetici, interruzione dei servizi IT, etc.
Spesso un problema si presenta come un normale incidente (v. ad esempio il non funzionamento di un router, di un server, etc.) da trattare con le normali procedure di manutenzione; diventa un problema di continuità operativa quando l'interruzione va oltre i tempi accettabili (per es. per mancanza delle parti di ricambio) e l'interruzione rischia di creare problemi al normale funzionamento dell'organizzazione.
In questi casi bisogna trovare una soluzione alternativa (per es. sostituire temporaneamente il server guasto con un server di scorta su cui far girare le applicazioni critiche); questa può essere una soluzione di continuità operativa.

Per continuità operativa o *Business continuity*, quindi, si può intendere l'insieme delle azioni messe in atto da una organizzazione per assicurare un determinato livello di operatività o la capacità di ripristinare l'operatività in un ragionevole lasso di tempo qualora dovessero verificarsi eventi dannosi (incidenti o disastri). L'ambito quindi non è limitato alle solo componenti IT ma coinvolge tutte le attività aziendali.

Quando si parla di *Business continuity* in genere si fa riferimento ad alcuni elementi fondamentali:

- **resilienza**, intesa come la capacità dei processi critici e/o delle relative infrastrutture, tra cui quelle IT, di far fronte (resistere) a incidenti o eventi dannosi;

- **recupero/ripristino**, intesa come la capacità di un'organizzazione di recuperare o ripristinare l'operatività (com'era prima del danno) dei processi critici e/o infrastrutture bloccati/danneggiati da incidenti o eventi disastrosi;

- **riserva**, intesa come la possibilità di un'azienda di far fronte a incidenti o eventi disastrosi previsti o meno facendo ricorso a risorse di riserva; in genere si attiva la riserva quando sia la capacità di resilienza che quella di recupero/ripristino non sono state in grado di fronteggiare l'evento dannoso.

Come si può immaginare gli eventi dannosi non sono statici, ma cambiano dinamicamente nel tempo sia in termini di probabilità del loro verificarsi che in termini di impatto anche considerando lo stato di salute dell'organizzazione.

Di conseguenza la continuità operativa non può essere un processo statico, ma deve essere considerato un processo continuo e sistematico finalizzato a valutare la probabilità del verificarsi dell'evento dannoso e il danno che può causare alle attività critiche che generano valore per l'azienda e per i soggetti ad essa interessati (*stakeholder*).

Lo strumento più efficace per analizzare e gestire gli eventi dannosi è rappresentato dalla gestione del rischio, che in genere viene articolata nei seguenti passi:

1. **Analisi** dei rischi finalizzata alla comprensione dell'evento dannoso in termini di causa che lo può generare e modalità che lo rende manifesto;

2. **Valutazione** della probabilità che si possa verificare e dell'impatto (danno) che può causare ai processi critici aziendali; mettendo in relazione la probabilità di accadimento dell'evento con il danno si può di stabilire un ordine di importanza per il rischio, in modo da concentrare l'attenzione sui rischi di maggiore importanza;

3. Individuazione delle **contromisure** da adottare in funzione dell'importanza del rischio; per rischi di elevata importanza normalmente si tende a prevedere:

- misure **preventive** da attivare prima che l'evento dannoso si manifesti e che possono o insistere sulla riduzione della probabilità di accadimento dell'evento (cosa non sempre possibile, soprattutto quando l'evento non rientra nella sfera di azioni dall'azienda) o sulla riduzione dell'impatto, adottando strategie che tendono a ridurre il danno (per esempio duplicando i server di una piattaforma di *e-Commerce*, se vitale per l'azienda);

- misure **correttive** da attivare quando si manifesta l'evento dannoso; solitamente si tratta di piani di emergenza (per es. piani di recupero da disastro o disaster recovery).

Qualora, anche prevedendo un certo insieme di contromisure, il rischio residuo fosse ritenuto elevato, allora si possono attivare delle misure di **trasferimento** del rischio (v. ad esempio l'accensione di polizze assicurative).

4. **Sorveglianza/monitoraggio** dei rischi, consistente nell'attivazione delle adeguate contromisure e nel valutare lo stato di attuazione dei singoli rischi: eliminare i rischi non più attuali, perché oramai si è sicuri che l'evento dannoso non si manifesterà, ed eventualmente aggiungerne di nuovi.

I passi di cui sopra vanno compiuti periodicamente al fine di aggiornare con continuità e sistematicità il portafoglio dei rischi, questo perché nel tempo i rischi possono mutare sia nella probabilità (che può aumentare o diminuire - si pensi ad esempio al rischio neve che in inverno ha un'alta probabilità mentre diminuisce sino ad azzerarsi nell'estate) che nell'intensità del danno che possono causare; nel tempo alcuni rischi perdono di validità ed altri se ne possono presentare: per entrambe le tipologie vanno ripetuti i passi di cui sopra.
Le modalità di gestione della continuità operativa di norma vanno descritte nel "Piano della continuità operativa" (*Business Continuity Plan*), un prezioso strumento finalizzato a supportare la continuità operativa delle attività aziendali e rafforzare la sopravvivenza dell'organizzazione.

1.7 *e-Commerce e Social Business*

In un mondo globalizzato diventa una necessità vitale per le aziende, soprattutto per le piccole e medie imprese, aumentare il numero dei contatti, incrementare il vantaggio competitivo e migliorare la marginalità delle vendite. Questo può avvenire consentendo alle aziende di aprirsi ad un mercato molto più ampio del ristretto ambito locale e territoriale e cercando di pensare a prodotti e servizi sempre più in linea con le aspettative dei consumatori.
Lo strumento principale a disposizione delle aziende, soprattutto per le piccole e medie imprese, che può consentire di affacciarsi ad un mercato più ampio di quello locale e territoriale, è costituito dall'*e-Commerce*, cioè dalla possibilità di effettuare attività commerciale attraverso una piattaforma web, in modo da poter raggiungere direttamente il cliente finale in tutte le parti del mondo.
Ma fare *e-Commerce* non è semplice, né si improvvisa; non basta realizzare un sito o una piattaforma web; occorre definire una strategia di vendita individuando il segmento di mercato target e definendo le migliori modalità di commercializzazione dei prodotti.

In misura maggiore rispetto al commercio tradizionale, l'*e-Commerce* richiede che prodotti e servizi siano presentati secondo offerte personalizzate che tengano conto dei profili e delle caratteristiche di gruppi di clienti.

Per poter costruire offerte personalizzate sono necessari due ingredienti fondamentali:

- strutturare processi aziendali adeguati a trattare con soluzioni di e-commerce dove la rapidità, la trasparenza, la qualità sono elementi fondamentali per la sopravvivenza di un'azienda; visto che la diffusione delle informazioni in internet è impressionante, aspetti negativi dell'azienda si potrebbero diffondere con una tale rapidità da condizionare il business aziendale;

- tracciare, rilevare, analizzare e comprendere le esigenze e i gusti del mercato in modo da anticipare le esigenze del mercato confezionando offerte di prodotti e servizi sempre più tarati sulle esigenze e sui gusti dei clienti.

In questo secondo ambito rientra l'utilizzo delle "reti sociali" (Social Network quali Facebook, Twitter, Instagram, etc.) quali strumenti di contatto con la clientela. La parola chiave è "conversazione"; chi usa i *Social Network* si sente libero di esprimere idee, sensazioni, di manifestare opinioni, di conversare su qualsiasi argomento.
La naturalezza delle conversazioni potrebbe rappresentare una fonte informativa preziosissima per le aziende che fossero in grado di saperla intercettare e analizzare.
Dalle conversazioni, dai messaggi (post), dalle foto, dai video, etc. è possibile capire cosa pensa il cliente in merito ad un prodotto o servizio, cosa gli piacerebbe acquistare o cosa non acquisterebbe affatto; dove andrebbe in vacanza, con chi e quando. In pratica si tratta di feedback molto più realistici di qualsiasi indagine di soddisfazione del cliente (*Customer Satisfaction*) o di ricerca di mercato.

A quanto sopra va aggiunto il potenziale a disposizione di un'azienda che decide di utilizzare il *Social Network*, quale canale di dialogo con la propria clientela.
Attraverso il *Social Network* il cliente può esprimere desideri, giudizi, suggerire miglioramenti oppure inoltrare reclami. L'azienda a sua volta può usare il canale *Social* per sondare la reazione su nuovi prodotti o strategie aziendali oppure promuovere il lancio di una nuova iniziativa, e così via.
Tutto questo serve a facilitare e rafforzare il legame con la propria clientela o più in generale con il proprio mercato di riferimento perché, come si può immaginare, con pochi click si possono raggiungere migliaia se non milioni di utenti.

Ma come ogni medaglia anche questo potentissimo mezzo ha il suo risvolto.
Non serve aprire un canale *Social* se non si ha una chiara strategia di marketing e se non si è disposti a investire su tale canale mantenendo attivi i contatti con i seguaci (*followers*). Sarebbe ancor più dannoso disporre del canale *Social*, ma aggiornarlo raramente oppure non rispondere tempestivamente alle sollecitazioni che vengono continuamente dai clienti.
Peggio ancora se si risponde in maniera poco trasparente; il passa parola negativo sul web si diffonde con una rapidità incredibile.
Pertanto l'*e-Commerce* come pure i canali *Social* sono una potente risorsa a disposizione delle piccole e medie imprese perché semplici da usare e molto economiche, ma richiedono inventiva e impegno per gestirlo in modo ragionato e con una forte visione prospettica.

Capitolo 2

LA SICUREZZA
dei sistemi informativi

2.1 Il valore delle informazioni per l'azienda

I computer, nati come semplici calcolatori, sono diventati col tempo dei potenti strumenti per memorizzare, elaborare e analizzare informazioni.
Tutti i giorni aziende ed organizzazioni generano dati di ogni genere e tipo.
Tutti i soggetti coinvolti nella vita aziendale traggono da queste informazioni «***valore***» per fare scelte migliori e operare in modo più produttivo ed efficiente. Un'azienda per erogare il proprio servizio, ha bisogno di informazioni, senza informazioni non potrebbe richiedere i pagamenti, pagare i propri dipendenti, non avrebbe un proprio bagaglio di conoscenze (*know-how*), un sito aziendale etc.
L'informazione in un'azienda ha valore in quanto potenzialmente utile per i suoi molteplici scopi: nell'informazione infatti è spesso contenuta conoscenza o esperienza di fatti reali vissuti da altri soggetti e che possono risultare utili senza dover necessariamente attendere di sperimentare singolarmente ogni determinata situazione.
Uno degli errori più comuni che commettiamo è di percepire il valore delle informazioni solo nel momento in cui non sono più disponibili; per esempio il furto di un portatile deve far pensare ai dati in esso contenuti e non al valore dell'oggetto. È importante proteggere i dati adeguatamente (**integrità**) ed evitare di non averli più disponibili (**disponibilità**) oltre ad evitare che possano essere utilizzati o venduti (**riservatezza**).
Per proteggere il proprio patrimonio informativo sarà quindi basilare conoscere la propria realtà aziendale, individuare le informazioni da salvaguardare e le situazioni di pericolo che potrebbero impattare l'azienda.
Una volta identificate le situazioni di pericolo e i rischi ad esse connessi, occorrerà individuare le misure necessarie atte a prevenire il verificarsi di determinati eventi e/o modificarne le cause.

A titolo indicativo, possiamo riassumere nella successiva Tabella 5 i danni e i costi derivanti dal furto e/o dalla perdita di dati aziendali critici.

Tabella 5

DANNI DERIVANTI DAL FURTO E/O DALLA PERDITÀ DI DATI AZIENDALI CRITICI

PROPRIETÀ INTELLETTUALE	È uno dei danni più insidiosi e più difficili da valutare: • in primo luogo, non bisogna confondere i costi di ricerca e sviluppo con le perdite dovute a un furto di proprietà intellettuale; • in secondo luogo il valore stesso della proprietà intellettuale (soprattutto quando è ancora a livello di ideazione e progetto) è di complessa determinazione; • in terzo luogo perché, sia a livello di Stato sia a livello di singola azienda, la consapevolezza del furto avviene quasi sempre in un lasso temporale successivo al momento in cui è realmente accaduto. Sarà difficile avere la certezza dell'entità del danno subito; per esempio, nel caso di un progetto, l'entità del danno dipenderà dal punto in cui si trovava il progetto quando il furto è stato effettuato.

PERDITE FINANZIARIE	I *crimini finanziari*, ossia il furto diretto di denaro (per esempio attraverso la clonazione delle carte di credito), rappresenta la seconda fonte di perdita causata dal crimine informatico (*cybercrime*).
FURTO DI INFORMAZIONI DI BUSINESS E MANIPOLAZIONE DEL MERCATO	Secondo il Center for Strategic and International Studies (Csis), il furto di informazioni di business rappresenta la terza fonte di guadagno per il crimine informatico. Tra i più perpetrati c'è il furto di informazioni relative ai clienti dell'azienda quali, ad esempio, il tipo e il numero di ordini effettuati, le modalità e i termini di pagamento.
PERDITA DI BUSINESS	Un attacco informatico può impattare la realizzazione immediata di un affare e aumenta il rischio di allontanare per sempre i clienti. Pensiamo, ad esempio, a un sito di commercio elettronico che subisce un attacco DDoS (Dos-Denial of Service): in questo caso l'azienda non può vendere i propri prodotti/servizi per il periodo in cui il sito non funziona; la fiducia dei clienti verso tale sito viene impattata ed è probabile che questi si rivolgano ad altri attori di mercato per effettuare i loro acquisti.
COSTI DI NOTIFICA	Al costo per la notifica delle violazioni subite, sia ai soggetti che ne sono stati impattati che alle autorità governative competenti (si considerino le spese in call center, comunicazione, eventuali specialisti ingaggiati ad hoc ecc.), bisogna aggiungere le risorse finanziarie e umane necessarie per le azioni da porre in essere in risposta all'incidente di sicurezza subito.
COSTI PER LA PERDITA DI PRODUTTIVITÀ	C'è il costo per la perdita di produttività dei dipendenti interni che vengono distolti o interrotti dalle loro normali mansioni.
IMPLICAZIONI GIURIDICHE	Ci sono i costi per le eventuali cause legali, soprattutto se la violazione ha riguardato il furto di informazioni riservate dei clienti.
SANZIONI NORMATIVE	Bisogna considerare eventuali costi per le sanzioni normative soprattutto in quei settori che trattano dati sensibili e che sono soggetti a regole di protezione stringenti (per es. informazioni sui pagamenti o sullo stato di salute dei propri dipendenti/clienti).
SOLUZIONI POST ATTACCO	Infine si avranno costi derivanti dai nuovi requisiti di sicurezza e di audit per proteggere l'azienda nel rispetto delle disposizioni che regolamentano la protezione dei dati, quali ad esempio l'adozione di processi, procedure e strumenti tecnologici specifici.
BRAND REPUTATION E AWARNESS	E per ultimo ci sarà la ricostruzione della reputazione del marchio (*brand reputation*) e della sua notorietà (*brand awarness*), per riparare al danno d'immagine subito e per riconquistare la fiducia del mercato.

2.2 Cosa si intende per sicurezza delle informazioni

La sicurezza delle informazioni attualmente rappresenta una tematica di notevole importanza ed è doveroso definirne il concetto.
Per **sicurezza dell'informazione s'intende** l'adozione di misure idonee a salvaguardare le informazioni sensibili.

Nella tabella che segue sono delineate le tendenze principali che riguardano il furto e/o la perdita di dati.

Tabella 6

TENDENZE PRINCIPALI RIGUARDANTI IL FURTO E/O LA PERDITA DI DATI

CAMBIANO LE MOTIVAZIONI	**Prima le azioni criminali erano finalizzate a soddisfare l'autocompiacimento degli attaccanti, oggi soprattutto mirano all'acquisizione di grandi somme di denaro.**
VARIANO I METODI	Si prediligono gli attacchi multivettore e del tipo "basso e lento" (*low and slow*); dal sistema colpito vengono estratti i dati per un lungo periodo senza che la vittima sia in grado di rilevare l'attività malevola.
I TARGET SONO SELEZIONATI ACCURATAMENTE	Esistono ancora gli attacchi in massa, ma si tende sempre di più ad avere obiettivi specifici.
GLI STRUMENTI DI ATTACCO SONO AUTOMATIZZATI	Si usa l'invio massivo di email sfruttando spesso l'intervento di persone inconsapevoli; per esempio, si chiede alla vittima di cliccare su un link malevolo all'interno di una chat o di una mail apparentemente ricevuta da un contatto amico; questo può accadere anche sulla posta certificata PEC!
CRESCE L'IMPATTO DELLE VIOLAZIONI	Possono implicare danni diretti sul business (costi di bonifica o *remediation*, mediazione con i clienti eccetera), il pagamento di sanzioni, licenziamento del management, etc.
LA DISPONIBILITÀ DI CRIMEWARE KIT	Ci sono veri e propri set di codice malevolo in vendita, facilmente accessibili, che non richiedono profonde competenze IT e sono in grado di generare molteplici varianti di uno stesso software dannoso (*malware*).
CAMBIANO GLI OBIETTIVI	Si spostano dalle infrastrutture IT alle applicazioni e alle risorse (*asset*) strategiche.
SI AMPLIANO LE VULNERABILITÀ	Le terze parti (i business partner o i *service provider*) diventano una potenziale vulnerabilità, perché potrebbero avere accesso ai sistemi informativi dell'azienda ma non adottare adeguate misure protettive.

La realizzazione di una sicurezza dell'informazione è garantita da un processo, che, oltre a misure tecniche, comprende anche misure aziendali e organizzative per la protezione dell'informazione.
Le finalità in termini di raggiungimento degli obiettivi prefissati nell'ambito della sicurezza dell'informazione sono essenzialmente riassumibili in due tronconi:

1. salvaguardia delle informazioni sensibili garantendo i requisiti di **disponibilità**, **riservatezza** ed **integrità**;
2. salvaguardia del proprio sistema informativo garantendone i requisiti di **sicurezza**, **funzionalità e semplicità di utilizzo**.

Qualunque programma/processo che si occupi della sicurezza delle informazioni, deve tutelare i concetti sopra citati.

Disponibilità

La **disponibilità** è probabilmente il concetto più semplice e più facile da capire della triade di sicurezza; tuttavia non deve essere trascurato.
Si riferisce ai sistemi e dati di comunicazione pronti per l'uso quando gli utenti legittimi ne hanno bisogno. Molti metodi sono utilizzati per la disponibilità, a seconda che si tratti di un sistema, di una risorsa di rete o di dati, ma tutti devono garantire che quando si necessita di un sistema o di dati, questi siano accessibili solo a personale autorizzato.
Garantire la disponibilità delle informazioni significa invece garantire che esse siano sempre disponibili quando ce n'è la necessità.

Riservatezza

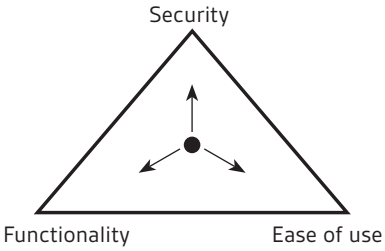
Indirizzare la segretezza e la **riservatezza** delle informazioni, significa prendere le misure idonee per prevenire la divulgazione di informazioni o dati a persone o sistemi non autorizzati.
Garantire la riservatezza significa evitare che persone, volontariamente o involontariamente, possano accedere a una o più informazioni senza che ne abbiano l'autorizzazione.
La riservatezza delle informazioni è d'obbligo per un individuo, la divulgazione potrebbe comportarne il furto di identità, le frodi e la perdita di denaro.

Integrità

L'**integrità** si riferisce ai metodi e alle azioni intraprese per proteggere le informazioni da alterazioni o revisioni non autorizzate.
Le misure di integrità garantiscono che i dati inviati dal mittente al destinatario arrivino senza alterazioni.
Garantire l'integrità delle informazioni vuol dire invece evitare che queste possano essere modificate, cancellate o spostate.

La sicurezza, la funzionalità e la facilità d'uso

Un'altra triade importante da ricordare è il paradigma **sicurezza**, **funzionalità** e **facilità d'uso**, rappresentata con un triangolo. È la rappresentazione grafica di un problema che affrontano i professionisti della sicurezza da un'eternità: più qualcosa è sicuro, più diventa meno fruibile e funzionale.



In un grafico in cui un punto rappresenta la nostra combinazione fra **Sicurezza**, **Funzionalità** e **Facilità d'uso**, il triangolo ci fa chiaramente intuire che se ci avviciniamo alla massima sicurezza, siamo allo stesso tempo nel punto più lontano da funzionalità e facilità d'uso; viceversa se ci avviciniamo al massimo alla facilità d'uso o alla funzionalità, ci allontaniamo al massimo dalla sicurezza.

2.3 Protezione dei dati personali

L'esigenza di prevenire incidenti ma anche semplicemente di erogare servizi porta alla raccolta di informazioni ed in particolare di dati personali (Vedi anche capitolo 4).
Questa necessità di informazioni deve seguire modalità strutturate di qualità per garantirne la **riservatezza**. La salvaguardia e la tutela delle informazioni personali è controllata dalla **privacy**.
Oggetto della normativa sulla privacy sono i dati personali, cioè "*qualunque informazione relativa a persona fisica, identificata od identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*".

Oggi le informazioni abbondano in rete e gli utenti sono inondati da dati. Internet ha dato vita ad una moltitudine di opportunità e servizi tra cui la contrattazione, vendita e acquisto di informazioni.
Il trattamento delle informazioni ha come cardine la necessità del consenso per il trattamento dei dati personali, che deve essere libero e consapevole.
La normativa prevede una serie di adempimenti e di misure minime che occorre mettere in pratica.

L'organo preposto al controllo relativo alla corretta applicazione della normativa in materia di privacy, è il Garante per la protezione dei dati personali, che opera un controllo preventivo e successivo sulle attività di trattamento di dati personali svolte in Italia.
Il Garante ha poteri istruttori, consultivi e sanzionatori, e costituisce il primo grado per il ricorso amministrativo contro eventuali violazioni della normativa.

2.4 Sicurezza informatica (*Cyber security*)

Per **sicurezza informatica (*cyber security*)** s'intende quell'insieme di tecnologie, processi e metodologie progettati per proteggere reti, sistemi, programmi e dati da attacchi, danni o accessi non autorizzati.
Numerose sono le prove che dimostrano come queste minacce stiano rapidamente evolvendo ed abbiano ormai raggiunto livelli di elevata pericolosità e complessità.
Le problematiche della sicurezza informatica comprendono sia la protezione dei dati trattati dai sistemi informatici che quella delle persone e/o beni da essi controllati/gestiti.
Ormai non si ragiona più sul "**se succederà**", ma sul "**quando**". Oggi molte PMI non seguono neppure le regole per la conformità normativa, incorrendo non solo in rischi operativi, ma anche legali, al contrario delle grandi aziende più sensibili e attente a tale tema. Con questi presupposti, è evidente la maggiore difficoltà delle organizzazioni più piccole nel fare fronte alle nuove minacce, che vengono ad esempio dall'uso di dispositivi mobili, dai *Social Media* e dalle applicazioni di condivisione di file; tali minacce sono spesso portate in azienda dagli utenti e difficilmente controllabili.
L'approccio delle PMI è incentrato sull'operatività e, durante la fase di sviluppo dei progetti IT, la sicurezza viene considerata un elemento accessorio, piuttosto che essenziale.
In questi contesti il referente difficilmente è un informatico e per i partner tecnologici, produttori o consulenti, diventa davvero problematico trasmettere determinati concetti. Anche quando si arriva a far comprendere il rischio e ad identificare la soluzione, non sempre si riesce a convincere il management ad allocare gli investimenti necessari sulla sicurezza, seppure a fronte di costi banali.

Queste preoccupazioni non sono legate alle dimensioni di un'azienda, ma sono spesso critiche per quelle di medie e piccole dimensioni che operano con risorse e staff limitati.
Prendiamo in considerazione l'esempio di un rivenditore di piccole dimensioni che è stato vittima di un devastante **furto di dati** che lo ha quasi costretto a chiudere l'attività.

Gli hacker sono stati in grado di accedere al sistema POS del negozio **sfruttando uno username e una password deboli** e hanno installato il software, che ha acquisito e copiato le informazioni delle carte di credito, prima che venissero inviate per essere elaborate.
Questo software è stato scoperto e rimosso un anno più tardi, ma solo dopo avere comportato una spesa di $22.000 per individuare la fonte della violazione e predisporre un potenziamento della sicurezza.
Questo tipo di violazione dei dati è diffuso e causa tipicamente perdite come conseguenza di inattività (*downtime*), ammende, perdita di privilegi nel trattamento del credito, nonché di danni alla fidelizzazione del cliente e al valore del marchio.

Prima si conosce la minaccia prima ci si può porre rimedio.

La Tabella 7 che segue riporta un elenco di tipologie di attacchi informatici che le aziende potrebbero subire.

Tabella 7

TIPOLOGIE DI ATTACCHI INFORMATICI

GUERRA DELLE INFORMAZIONI **(Cyber Warfare)**	Termine proveniente dall'ambiente militare, che sta ad indicare l'intercettazione, alterazione e distruzione di informazioni di comunicazione e/o dati.
SPIONAGGIO INFORMATICO **(Cyber Espionage) e** ***HACTIVISMO*** **(Hactivism)**	Sono le operazioni atte a perseguire obiettivi sociali e politici attraverso la pirateria informatica.
SOFTWARE MALEVOLI **(Malware - Ransomware)**	Possono "infettare" i sistemi aziendali e insediarsi a fronte della vulnerabilità della infrastruttura IT dell'azienda in termine di applicazioni e sistemi operativi utilizzati oppure semplicemente perché un dipendente ha cliccato su un link web o ha aperto in lettura una mail sospetta.
ATTACCHI DDoS	Si riferiscono ad attacchi informatici perseguiti da più parti del mondo, verso un singolo obiettivo, con l'intento di impedirne l'operatività.
SPIONAGGIO TELEFONICO **(Phone Hacking)**	Si riferisce alle attività di intercettazione e ascolto di chiamate telefoniche o messaggi vocali, senza l'ottenimento del consenso delle parti coinvolte nella conversazione telefonica.
GIORNO-ZERO **(0-day)**	Gli *zero-day* sono tipi di attacchi informatici che sfruttano errori del software non ancora noti e per i quali non esistono le correzioni (*patch*). Se il pirata non è in grado di trovare un punto debole, può sperare di trovare un errore ancora ignoto e lanciare un attacco (*exploit*) in grado di sfruttare tale vulnerabilità.

Nella Tabella 8 che segue sono riportati dieci semplici suggerimenti che aiutano l'azienda a difendersi dagli attacchi informatici più comuni.

Tabella 8

SUGGERIMENTI PER DIFENDERSI DAGLI ATTACCHI INFORMATICI PIÙ COMUNI

1. Non lasciarsi indurre con l'inganno a fornire informazioni di natura riservata.	• Evitare di rispondere a email o telefonate che richiedono informazioni aziendali di natura confidenziale. • Tenere sempre presente che i malintenzionati riescono nel loro scopo perché sono convincenti. • Secondo le ultime informazioni, ultimamente in Canada i truffatori (*scammer*) stanno cercando di prelevare informazioni con l'inganno mediante chiamate di supporto tecnico fasulle. • Restare in guardia e riferire qualsiasi attività sospetta all'ufficio preposto.
2. Evitare di utilizzare un computer sprovvisto di protezione.	• Accedendo a informazioni di natura sensibile da un computer privo di protezione si mettono a rischio i dati visualizzati. • Esiste software malevolo che permette agli intrusi di spiare l'attività online quando si effettua l'accesso a siti privi di difese. • Se non si ha la certezza che il computer adoperato sia sicuro, evitare di utilizzarlo per accedere a dati aziendali o sensibili.
3. Evitare di lasciare in giro informazioni di natura sensibile.	• Evitare di lasciare sulla scrivania fogli stampati contenenti informazioni private; per un visitatore è facile gettare un occhio sulla vostra scrivania e poter leggere documenti di natura sensibile. • Mantenere la scrivania in ordine e i documenti sotto chiave, oppure distruggerli quando non sono più necessari; in questo modo l'ufficio assumerà un aspetto più organizzato e diminuiranno i rischi di fuga delle informazioni.
4. Bloccare computer e telefoni cellulari quando non sono in uso.	• Quando non sono in uso, bloccare sempre i computer e i telefoni cellulari. I dati con i quali avete a che fare sono importanti e bisogna assicurarsi che rimangano protetti. • Bloccare questi dispositivi mantiene sia le vostre informazioni personali che i dati e i contatti aziendali al sicuro da occhi indiscreti.
5. Restare in guardia e riferire qualsiasi attività sospetta.	• A volte le attività sospette non sono tanto ovvie quanto crediamo. • Un articolo recentemente pubblicato descrive il caso del manager di un supermercato a cui una signora misteriosa ha inviato una richiesta di amicizia su Facebook. Il manager ha accettato un «appuntamento» al quale si sono presentati due uomini che lo hanno immobilizzato e hanno rapinato il negozio. • Non ci si deve fidare di chi chiede informazioni senza essere conosciuto, specialmente su Internet. • Riferire qualsiasi attività sospetta al reparto IT.

6. Proteggere con password i file e i dispositivi di natura sensibile.	• I file di natura sensibile archiviati su computer, unità flash USB, smartphone, laptop, ecc... vanno sempre protetti da password. • Smarrire un dispositivo può accadere a chiunque ma, se il dispositivo è protetto da una password sicura, è possibile renderne più difficile la violazione e il conseguente furto dei dati.
7. Utilizzare sempre password difficili da dedurre.	• Molti si servono di password ovvie come "password," oppure sequenze di caratteri deducibili su una tastiera QWERTY, come ad es. "zaq12wsx". • Creare password complesse che includano lettere maiuscole e minuscole, numeri e persino punteggiatura. • Cercare di adoperare password diverse per i vari siti Web e computer. In questo modo, se uno di essi viene violato, gli altri account saranno al sicuro.
8. Non fidarsi di email e link sospetti.	• Gli hacker cercano di appropriarsi di elenchi di email aziendali; ciò è capitato recentemente a Toshiba. Gli indirizzi email aziendali sono preziosi per gli hacker, in quanto consentono loro di creare email fasulle provenienti da "persone reali". • Eliminare sempre le email sospette da mittenti sconosciuti; evitare di cliccare sui link sospetti o scaricare allegati da messaggi di posta elettronica ignoti. • Anche solamente aprire o visualizzare tali link può compromettere il computer a propria insaputa.
9. Evitare di connettere dispositivi personali senza l'autorizzazione.	• Evitare di connettere dispositivi personali come USB, lettori MP3 e smartphone senza l'autorizzazione aziendale; anche se appena acquistati possono contenere virus. • Questi dispositivi possono essere stati violati e possono contenere codice in attesa di avvio automatico non appena vengono connessi a un computer.
10. Evitare di installare programmi non autorizzati sui computer utilizzati al lavoro.	• Le applicazioni malevole si spacciano spesso per programmi legittimi come giochi, strumenti o persino software antivirus. • Cercano di indurre a infettare in maniera non intenzionale il computer o la rete.

La **sicurezza informatica** è responsabilità di tutti; ogni individuo dell'azienda rappresenta la prima linea di difesa contro i rischi di sicurezza. Anche le buone intenzioni, come ad esempio la creazione di espedienti (*work-around*) e scorciatoie per migliorare l'erogazione dei servizi, in grado di violare le politiche di sicurezza, possono portare a conseguenze impreviste e involontarie, tra cui violazioni della sicurezza e divulgazione di informazioni personali.

2.5 Garanzie da richiedere ai fornitori esterni (*outsourcer*)

Negli ultimi anni le trasformazioni avvenute nell'industria e nei servizi hanno imposto una corsa all'innovazione con un'accelerazione allo sviluppo di nuovi prodotti, soddisfacendo la clientela in termini di varietà, flessibilità e dinamicità con una drastica riduzione dei tempi di produzione (*time to market*), un'ottimizzazione della qualità del prodotto e una ricerca permanente della redditività in termini finanziari.
Tutto questo si riflette sulle imprese che per aver un vantaggio concorrenziale hanno posto la loro attenzione ed i loro sforzi sull'attività di base (*Core Competencies*) ricercando competenze specifiche all'esterno per tutte le altre attività.
Questa scelta strategica di ricorrere ad altre imprese per lo svolgimento di attività non fondamentali viene definita ***outsourcing***. Attraverso questo processo le aziende assegnano stabilmente a fornitori esterni (eventualmente con trasferimento dell'intero settore di attività), per un periodo contrattualmente definito, la gestione operativa di una o più funzioni in precedenza svolte all'interno.
Data la rilevanza della problematica della riservatezza e della protezione dei dati che le società di *outsourcing* devono rispettare è necessario disciplinarne tutti gli aspetti.
Oltre all'obbligo di riservatezza delle informazioni, è importate trattare tutte le norme relative alla protezione dei dati personali (Codice Privacy) chiedendo il consenso al trattamento e nominando il fornitore quale responsabile del trattamento. Sia i "Dati" che le "Informazioni" dovranno quindi essere protetti e salvaguardati contro le cause che ne possono pregiudicare l'**integrità,** la **funzionalità** e la **facilità d'uso**.
In base al tipo di servizio posto in essere potranno esserci misure di sicurezza a carico del committente o del fornitore. È importante attribuire alle parti le eventuali responsabilità derivanti da un errato trattamento dei dati.

Il fornitore chiamato a svolgere attività di servizi professionali o di sviluppo dovrà operare in modo che i risultati del lavoro svolto siano coerenti con le specifiche ricevute.
Le specifiche posso riguardare requisiti attinenti alla:

- sicurezza fisica, cioè controllo accessi, identificazione delle persone ecc..
- sicurezza logica, cioè misure atte alla salvaguardia del sistema e dei dati in esso contenuti quali, ad esempio, software di antintrusione (*firewall*), sistemi di rilevazione d'intrusione (*intrusion detection*), ecc..

È compito del cliente far sì che il fornitore riceva tutte le norme alle quali il personale che opera nell'esecuzione delle attività, sancite dal contratto, dovrà attenersi garantendone l'**integrità,** la **riservatezza** e la **disponibilità**.

2.6 Conformità normativa (*Compliance*)

La conformità normativa (*Compliance*) è un'attività che individua, valuta, supporta, controlla e riferisce in merito al rischio di:

- sanzioni legali o amministrative,
- perdite operative,
- deterioramento della reputazione aziendale,
- leggi,
- regolamenti,
- procedure e codici di condotta.

La **conformità normativa** ha infatti un'ottica prevalentemente preventiva nel presidiare rischi di carattere legale e reputazionale.

Indipendentemente dalle dimensioni, nelle aziende si assiste al costante progresso e utilizzo delle tecnologie IT e ciò è accompagnato da un'evoluzione normativa e giurisprudenziale che negli ultimi anni ha avuto notevoli sviluppi. **È sempre più difficile gestire la conformità normativa (*Compliance*)**.

Diventa quindi fondamentale avere sotto controllo le normative che impattano direttamente o indirettamente l'azienda al fine di comprendere quali siano i rischi che l'azienda corre in caso di mancato rispetto degli obblighi di legge.

L'adozione di funzioni interne di Conformità Normativa (*Compliance*), Gestione del Rischio (*Risk Management*) e Controllo interno (*Internal Audit*), anche demandate ad aziende IT specializzate, dovrà essere tenuta in estrema considerazione dalle aziende che trattano dati riservati e/o sensibili dei propri clienti e/o dipendenti.

Capitolo 3

LA GESTIONE del rischio

3.1 Come valutare i rischi

Minacce e Vulnerabilità

Per condurre un'attività di Analisi dei Rischi in Informatica (*IT Risk Analysis*) è indispensabile individuare le minacce e le vulnerabilità che possono interessare i sistemi informatici aziendali.
Di fatto, una minaccia è costituita da tutti gli eventi in grado di provocare un danno agli apparati tecnologici mediante lo sfruttamento di una o più vulnerabilità, ossia di falle tecnologiche, organizzative o fisiche.

Ambito tecnologico

Le minacce di questo tipo possono intaccare riservatezza, integrità e disponibilità di sistemi e informazioni, sfruttando le vulnerabilità specifiche degli apparati IT. Accessi non autorizzati, furto di informazioni, blocco o danneggiamento di basi dati sono solo alcuni esempi tipici di minacce a cui i sistemi informatici sono esposti. Al fine di ridurre il rischio di attacchi di natura tecnologica, è indispensabile mettere in campo **tecniche di controllo proattivo** (come, ad esempio, strumenti per il controllo dei sistemi e delle applicazioni web), **attivo** (quali, ad esempio, apparati per il monitoraggio delle infrastrutture di rete) e **attività di verifica ex post** (come l'analisi dei *log* relativi ad accessi o elaborazioni informatiche).

Ambito organizzativo

I sistemi informatici, di fatto, costituiscono l'apparato tecnologico a supporto dei processi aziendali. La protezione delle informazioni deve essere garantita anche attraverso una corretta implementazione di procedure specifiche che, qualora mancanti, renderebbero ininfluenti le contromisure definite nell'ambito tecnologico.
Aspetti legati alla corretta definizione di principi, quali la segregazione dei compiti o il minimo privilegio, sono tra i più comuni nell'ambito di una sicura implementazione dei processi aziendali.
La **corretta valutazione dei processi** e il grado di protezione organizzativa che va loro riservata sono il risultato di una specifica attività di analisi, volta a definire la criticità degli stessi.

Ambito fisico

Nonostante l'uso sempre crescente di tecnologie offerte come servizi esternalizzati, la protezione delle risorse fisiche deve essere opportunamente considerata nei processi di gestione e valutazione del rischio.
Accadimenti negativi possono essere legati ad eventi naturali straordinari (es. inondazioni, terremoti) piuttosto che relativi ad intervento umano volontario o involontario (come furto, sabotaggio, distruzione di apparati, imperizia).
La protezione contro questa tipologia di minacce deve considerare aspetti logistici ed organizzativi, come la realizzazione di misure di controllo degli accessi fisici (e relative politiche) alle aree aziendali sensibili e l'adozione di misure di sicurezza contro eventi naturali, come idonei impianti antincendio e antiallagamento ed eventuali siti di recupero (*recovery*) opportunamente dislocati.

Valutazione dei rischi

Le minacce, informatiche e non, che si possano concretizzare in relazione alle vulnerabilità individuate, devono essere opportunamente mitigate, indirizzando gli interventi correttivi in modo attento e prioritario.

A tal proposito, occorre adottare metodi di valutazione del rischio, al fine di determinare una scala di impatti e definire così un ordine ragionato di interventi ad eliminazione o mitigazione del rischio.

- La valutazione dei rischi viene condotta mediante alcune macro fasi, quali:
  l'identificazione dei rischi, a seguito di attività di valutazione della vulnerabilità (*vulnerability assessment*), interviste, analisi dei dati storici, etc.;
- la stima degli eventi rischiosi, intesa come la valutazione numerica della relazione tra probabilità di accadimento ed impatto sui processi e/o sui beni aziendali, rappresentata comunemente tramite matrice (vedi figura qui sotto).

MATRICE PER IL CALCOLO DEL RISCHIO

	PROBABILITÀ			
IMPATTO	**Improbabile**	**Possibile**	**Probabile**	**Quasi certo**
Catastrofico	**Moderato**	**Alto**	**Critico**	**Critico**
Rilevante	**Moderato**	**Moderato**	**Alto**	**Critico**
Moderato	**Basso**	**Moderato**	**Moderato**	**Alto**
Marginale	**Basso**	**Basso**	**Moderato**	**Moderato**

L'analisi del rapporto tra probabilità ed impatto degli eventi rischiosi, unitamente al livello di propensione al rischio ed agli obiettivi strategici dell'azienda in termini di gestione del rischio *(Risk Management*), definisce i tempi (priorità di intervento) e le modalità di copertura (riduzione, diversificazione, trasferimento del rischio, etc).

3.2 Come affrontare i rischi

Rischi informatici e business

Il rischio è presente in tutte le attività che si svolgono in azienda e nella vita privata; basti pensare al rischio di infortuni, furti, gravi anomalie degli impianti di produzione, etc.
Le valutazioni del rischio riguardano inevitabilmente, e sempre più, anche la sicurezza informatica per le evidenti conseguenze che carenti misure di sicurezza nei servizi informatici aziendali o esternalizzati (in *outsourcing*) possono avere sul business o sulla conformità (*Compliance*) alle leggi (es. Privacy).
Le componenti fondamentali delle sicurezza delle informazioni (sicurezza informatica e sicurezza di trattamenti di informazioni riportate su documenti "cartacei") sono tre:
- **riservatezza** delle informazioni (i dati devono esser accessibili solo a persone autorizzate);
- **disponibilità** delle informazioni (i dati devono essere sempre disponibili);
- **integrità** delle informazioni (i dati devono essere "esatti")

La gestione del rischio

Gestire il rischio significa avere la consapevolezza delle misure di protezione adottate dall'azienda relative alla sicurezza delle informazioni (tecnologiche, organizzative, procedurali), misure che hanno una crescente rilevanza per il business e per la conformità (*compliance*) alle leggi; basti pensare al nuovo Regolamento Europeo EU 2016/679, che prevede specifici adempimenti obbligatori relativi alle valutazioni di rischio nel trattamento di dati personali.

La gestione del rischio[1] prevede le seguenti fasi principali:
- identificare i rischi (*risk analysis*);
- valutare i rischi (*risk assessment*);
- gestire i rischi per ricondurli ad un livello accettabile (*risk mitigation*).

Il calcolo del rischio[2] relativo alla sicurezza delle informazioni, per le tre componenti citate (riservatezza, disponibilità e integrità), richiede di considerare, a fronte delle possibili minacce alla sicurezza delle informazioni, tre elementi:
- probabilità di accadimento delle minacce;
- impatto (danni economici di business, di immagine, di compliance, etc) nel caso di accadimento delle minacce;
- vulnerabilità delle misure di sicurezza in atto per contrastare le minacce (contromisure).

Accettabilità del rischio

Calcolato il rischio, è fondamentale confrontarlo con i criteri di accettabilità del rischio condivisi con la Direzione aziendale. Se i valori di rischio non rispettano i criteri di accettabilità definiti, è necessario condividere la situazione con la Direzione aziendale, promuovendo le azioni più opportune, quali, ad esempio, progetti di miglioramento delle contromisure di informatica in atto (tecnologiche, organizzative, procedurali).

Cosa fare in pratica

Il primo passo è definire la metodologia aziendale da adottare per la gestione del rischio, facendo riferimento alle "migliori pratiche" (*best practices*) disponibili sul mercato, fra le quali le Norme ISO 27001[3] e ISO 27005[4], che possono essere un importante e concreto riferimento per lo svolgimento di una adeguata istruttoria di valutazione dei rischi informatici.
In relazione alle caratteristiche dei servizi informatici aziendali, per i quali è complesso identificare con precisione il valore economico del rischio, e considerando che una valutazione qualitativa non consente di esprimere con precisione le priorità degli interventi di mitigazione del rischio necessari, si suggerisce di utilizzare scale di valutazioni quantitative (Vedi Nota 2).

La valutazione dei rischi deve essere svolta almeno una volta l'anno e in occasione di rilevanti cambiamenti del sistema informativo aziendale, di natura infrastrutturale e/o applicativa.
In relazione alla dimensione e criticità del sistema informativo aziendale l'utilizzo di strumenti (*Tools*) che supportino il processo di gestione del rischio (*Risk Management*) può costituire un notevole aiuto in termini di tempo e accuratezza delle valutazioni che, è opportuno sottolineare, devono veder coinvolti non solo esperti di sicurezza IT, ma anche i responsabili della progettazione dei processi (*process owners*), le funzioni che curano la conformità alle leggi, i responsabili operativi e dello sviluppo di applicazioni IT, nonché i fornitori più coinvolti (*outsourcer, software house*, etc.).
Il supporto della consulenza e l'adozione della Norma ISO 27001 in modalità certificata possono essere due opportunità da valutare attentamente da parte del Management e dei Responsabili IT.

[1] *Vedi Norma ISO 31000, Risk management, che descrive i capisaldi delle attività di gestione del Rischio.*

[2] *Il rischio può essere un valore economico (ad esempio: rischio di 100.000 euro), oppure una valutazione qualitativa (ad esempio rischio medio nei confronti di una scala di valutazione qualitativa predefinita) o quantitativa (ad esempio confronti di una scala di valutazione quantitativa predefinita).*

[3] *ISO 27001, Information management security system, prevede una serie di contromisure ("Controls") utilizzabili per le valutazioni di rischio e per la realizzazione di progetti di mitigazione dei rischi.*

[4] *ISO 27005, Information security risk, elenca esempi di minacce alla sicurezza delle informazioni e indicazioni sulle modalità di calcolo del rischio.*

3.3 Gestione degli utenti

Gli utenti dei sistemi informatici aziendali devono rispettare misure di sicurezza "di base" riportate in altre sezioni del Vademecum (es. gestione delle password, salvataggio dei dati, consultazione "sicura" di allegati nelle mail, etc).
In questo capitolo si fa specifico riferimento agli utenti con account privilegiati, che, se non opportunamente "gestiti", consentono agli *hacker* di effettuare attacchi in modo semplice e veloce, lasciando poche tracce e, spesso, rendendo impossibile l'accesso a qualsiasi altro utente.
Premesso che all'interno di ogni azienda esiste almeno un account privilegiato in grado di fornire un accesso quasi illimitato a workstation, server, reti, dispositivi, database e applicazioni, è possibile distinguere diverse tipologie di account, come di seguito.

- **Amministratore locale**: account non personale (generico, utilizzato da più utenti) che fornisce un accesso di tipo amministrativo ad un terminale di qualsiasi tipo collegato ad una rete informatica; solitamente è utilizzato per effettuare operazioni di manutenzione della rete (*network*).

- **Amministratore di sistema** (oppure utente con privilegi): è tra le utenze più diffuse e fornisce ampi privilegi amministrativi su uno o più sistemi; generalmente è protetta da password complesse e sottoposta a monitoraggio.

- **Amministratore di dominio**: fornisce il massimo accesso a tutti i sistemi all'interno di una rete; in genere sono numericamente ridotti in quanto dotati di ampi poteri di controllo e dell'abilità di apportare modifiche a tutti gli account amministrativi al suo interno. La compromissione dell'account di un amministratore di dominio è solitamente considerata un'incidente della massima gravità, da gestire con le dovute precauzioni.

- **Account d'emergenza**: fornisce agli utenti un accesso amministrativo a sistemi sicuri in casi di emergenza.

- **Account di servizio**: è utilizzato da un'applicazione o da un servizio per interagire con un sistema operativo.

- **Account applicativo**: è utilizzato dalle applicazioni per accedere a database e fornire tale accesso ad altre applicazioni.

Le principali vulnerabilità relative agli account privilegiati riguardano le password, che spesso (troppo spesso) sono note a molte persone (incluso il personale che ha lasciato l'azienda), utilizzate per l'accesso a diversi sistemi e modificate raramente.
Senza un accurato controllo degli account, l'azienda è sottoposta a rischi la cui natura è tutt'altro che trascurabile: è per questo che l'adozione di misure di protezione degli account non può essere sottovalutata.
Indipendentemente dalle dimensioni dell'azienda e dalle risorse disponibili, è possibile individuare serie di "buone pratiche" applicabili per migliorare in modo incrementale la sicurezza delle informazioni aziendali.

Tabella 9

SOLUZIONI PER LA GESTIONE DEGLI UTENTI "PRIVILEGIATI"

SOLUZIONI DI BASE	• Predisporre un inventario delle utenze e ridurre al minimo indispensabile il numero di utenze dotate di privilegi: conoscere con esattezza il numero di utenti è il primo passo per una corretta gestione del rischio; una volta inventariati, gli account non necessari devono essere eliminati. • Non fornire privilegi agli account utente: occorre separare uso generale e uso amministrativo degli account, in modo da identificare eventuali abusi. L'adozione del principio del minimo privilegio è un passo fondamentale nel miglioramento della sicurezza aziendale. • Sviluppare e applicare un processo di "inserimento in azienda" (*on boarding*): i dipendenti devono comprendere le responsabilità relative all'utilizzo di account privilegiati e la creazione di tali utenze deve essere il risultato di un processo di autorizzazione chiaramente definito. • Rivedere costantemente gli account ed i privilegi, che devono essere modificati o disabilitati quando non più richiesti e creare un processo di "uscita dall'azienda" (*off boarding*): la disabilitazione deve riguardare tutti gli account privilegiati associati all'utente, avendo cura di modificare le password relative a eventuali utenze condivise accedute dal dipendente dimissionario. • Prestare attenzione alla gestione delle chiavi di accesso: non utilizzare le password deboli o prive di scadenza, proteggere in modo adeguato le credenziali "critiche" (che forniscono l'accesso ad account privilegiati) utilizzando adeguati sistemi di crittografia ed evitare di scriverle per non dimenticarle. • Utilizzare sempre utenze individuali, evitando l'utilizzo di utenze generiche o di gruppo: l'uso di account personali consente di tenere traccia delle attività svolte da ciascun dipendente.
SOLUZIONI AVANZATE	• Cambiamento automatico delle password per account privilegiati. • Utilizzo di password valide per un solo accesso o transazione (one-time password) o di soluzioni di autenticazione forte (*strong authentication*) quali, ad es. token, smart card, ecc. • Registrazione dei log delle attività effettuate da account privilegiati e utilizzo di sistemi di monitoraggio dell'attività svolta dagli utenti. • Controllo sull'uso degli account dotati di privilegi amministrativi per individuare eventuali comportamenti anomali. • Utilizzo di software di verifica e gestione delle password.

3.4 Aggiornamento dei sistemi

Una fase importante di una buona azione preventiva è rappresentata sicuramente da una buona cura nell'aggiornamento periodico dei propri sistemi informativi, sia esso automatico che manuale.
La scelta se automatizzarlo o meno è molto soggettiva; sicuramente se si hanno le competenze necessarie o si è seguiti da un tecnico o da un'azienda specializzata, vagliare di volta in volta i vari aggiornamenti prima di installarli consente di evitare possibili conflitti di compatibilità o problematiche minori riguardo alcune modifiche delle funzionalità che vengono man mano introdotte.
Per prima cosa bisogna aggiornare sicuramente i server ed i computer, indipendentemente dal sistema operativo usato (Windows, Linux, Mac o altro); un sistema aggiornato consente di mettersi al riparo da virus, hacker o semplicemente problematiche che man mano vengono scoperte e possono compromettere il corretto funzionamento degli apparati.

Moltissimi virus e attacchi di nuova generazione infatti fanno leva proprio su eventuali problemi (i cosiddetti *bug* di sistema) che consentono ad un software potenzialmente maligno di acquisire il controllo del nostro computer a nostra insaputa e manometterlo o comandarlo a loro piacimento.

Inoltre è importantissimo passare ad una nuova versione di sistema operativo o di software nel momento in cui la precedente versione viene dismessa e non più aggiornata dalla casa madre, in caso contrario ci si espone ancor di più a tutti quei rischi sopracitati, perché gli errori presenti nel software non verranno mai più risolti dal produttore.

Per citare un esempio, Windows XP risulta ancora presente in numerose realtà aziendali e professionali, anche se ancora potenzialmente in grado di funzionare, occorre abbandonarlo il prima possibile per un sistema operativo più recente, in quanto facilmente attaccabile da software maligni e virus che possono abilmente sfruttare falle di sistema che mai più verranno sistemate.

Oltre a server e computer è necessario tenere aggiornate allo stesso modo tutte le altre periferiche che compongono la rete quali: *firewall*, *switch*, apparati di videosorveglianza, multifunzione; tutti questi sistemi sono controllati da un software, che deve essere manutenuto e conseguentemente aggiornato in modo da garantire un corretto funzionamento.
Parimenti i sistemi antintrusione, *antispam* e *antivirus* non aggiornati diventano impotenti di fronte alle nuove minacce che quotidianamente si affacciano sulla rete internet.
Soprattutto per queste ultime tipologie di apparati non sempre è semplice e alla portata di tutti effettuarne una corretta manutenzione ed applicarne gli aggiornamenti software; se non si hanno le adeguate competenze informatiche si consiglia caldamente di rivolgersi ad un'azienda o ad un professionista qualificato, che possa seguire per intero i vostri apparati di rete e garantire una gestione a regola d'arte.

3.5 Protezione dai codici maligni

Possiamo definire un codice maligno (*malware*) come un software di qualsiasi genere creato con l'apposito scopo di causare danni più o meno gravi sul computer in cui viene eseguito.
Ne esistono di diverse tipologie e la diffusione aumenta di anno in anno in modo esponenziale; nella Tabella 10 che segue ne citiamo alcuni tra i più conosciuti e dannosi.

Tabella 10

TIPOLOGIE DI CODICI MALIGNI

PROGRAMMA PIRATA **(Virus)**	Software dannoso che infetta programmi installati sul computer al fine di replicarsi e causare danni più o meno visibili all'utente sia a livello software che hardware (causando per esempio surriscaldamenti o sovraccarichi di sistema).
CAVALLO DI TROIA **(Trojan)**	Software nascosto dentro altri programmi potenzialmente utili che normalmente vengono scaricati da internet dall'utente e che, una volta installati, installano anche il codice maligno che serve ad un potenziale attaccante per prendere il controllo del nostro computer, inoltrare dati sensibili o causare danni o malfunzionamenti generici.
PORTA DI SERVIZIO **(Backdoor)**	Spesso rappresentano uno dei principali codici maligni installati da virus e cavalli di troia. Essi creano una sorta di "porta sul retro" dei nostri sistemi, ossia un canale di accesso al computer su cui è installato, che aggira completamente tutte le politiche di sicurezza e che consente ad un potenziale attaccante di prendere il controllo della macchina senza l'autorizzazione del proprietario e senza che lui se ne accorga.
INTERCETTORE DELLA TASTIERA **(Keylogger)**	Software dannoso che si occupa di tenere traccia di tutto quello che viene digitato sulla tastiera del computer in cui si è installato e trasferirlo all'esterno.
PROGRAMMA SPIA **(Spyware)**	Software che spia le attività dell'utente e ne tiene traccia senza il suo consenso, per poi inviarle via internet ad organizzazioni che utilizzeranno tali dati per trarne profitto (per esempio con invio indesiderato di pubblicità mirata).

Tutti questi software possono finire sul nostro computer se non attiviamo le dovute misure di sicurezza e se non applichiamo delle regole base per l'utilizzo e la navigazione consapevole in internet.

È possibile infatti prendere un virus:

1. navigando su siti non sicuri,
2. aprendo allegati dannosi ricevuti via email,
3. scaricando ed installando programmi di dubbia provenienza,
4. utilizzando per la navigazione internet un computer dotato di software vecchio, non aggiornato, senza antivirus e senza firewall.

Moltissimi software maligni infatti sono efficaci solo su sistemi con bassa protezione e falle di sicurezza non corrette; dotarsi innanzitutto di un sistema aggiornato è la base per proteggersi dai loro attacchi.

Un software antivirus professionale (che può costare anche poche decine di euro) consente di rilevare e bloccare in tempo reale minacce e tentativi di attacco o installazione di software maligno sul nostro computer; se siamo in una rete con più computer sarebbe meglio averne uno che consenta una gestione centralizzata da far gestire ad un tecnico specializzato.

Un sistema firewall (o addirittura di rilevazione delle intrusioni) metterà i nostri sistemi al riparo anche da attacchi più diretti e mirati a prendere il controllo del nostro computer.
Se il computer è singolo e magari anche portatile, bisogna valutare la possibilità di attivare un firewall software direttamente sul computer, così da essere sempre protetti qualunque sia la rete informatica utilizzata; in mancanza di nulla anche semplicemente il firewall che avete in dotazione con il sistema operativo può essere sufficiente.

Per concludere quindi, oltre a sistemi software e hardware, non c'è nulla di meglio che una navigazione attenta e consapevole per mettersi al riparo da potenziali rischi.

3.6 Gestione dei siti web aziendali

I siti e le applicazioni Web sono un elemento cardine della comunicazione aziendale; attraverso questi strumenti è possibile promuovere l'immagine aziendale, presentare i prodotti o offrire servizi, fornire informazioni o vendere i propri prodotti.
La presenza nella rete comporta, però, l'assunzione di una chiara responsabilità: l'adozione di specifiche misure di sicurezza per minimizzare i rischi legati ad attacchi e frodi informatiche, che possono colpire sia l'infrastruttura del sito o l'applicazione Web, così come gli utenti che ne fanno uso. I rischi per gli utenti e per il business sono molteplici; eccone alcuni esempi:

- oscuramento del sito o dell'applicazione Web in seguito ad un attacco informatico;
- attacco informatico al sito o all'applicazione Web, finalizzato al furto delle informazioni.

Nella seguente Tabella 11 sono riportate le principali buone pratiche da adottare in sede di sviluppo di un sito o di un'applicazione Web, valide per tutte le aziende, ed anche per le PMI che trattano dati personali o business "critici".
L'adozione delle buone pratiche potrà essere attuata dalle aziende con risorse specialistiche interne o, in relazione alle competenze disponibili, con il supporto di esperti reperiti sul mercato.

Tabella 11

BUONE PRATICHE PER LO SVILUPPO DI UN SITO O DI UN'APPLICAZIONE WEB

VALUTAZIONE DEI RISCHI	I requisiti di sicurezza adottati devono essere commisurati alle criticità del sito, dell'applicazione Web e dei dati trattati: occorre valutare il rischio, considerando sia gli utenti dell'applicazione, sia le informazioni accessibili. Ugualmente importante è la scelta di un provider affidabile e di software sicuri.
SOFTWARE AGGIORNATI	Se si gestisce in prima persona il proprio sito Web è importante utilizzare sempre la versione più aggiornata del CMS (*Content Management System*) utilizzato; in questo modo si evita che le vulnerabilità note possano essere sfruttate da eventuali *hacker*.

GESTIONE DELLE MAIL	Mai aprire link o allegati provenienti da mittenti di dubbia identità; tali contenuti possono contenere virus in grado di infettare il PC e/o sottrarre le credenziali di accesso all'applicazione o al sito Web aziendale.
AUTENTICAZIONE	Utilizzare password sicure, ricordando che le credenziali di accesso devono avere una scadenza ed essere periodicamente sostituite. Le informazioni di accesso, in particolare quelle di utenti e amministratori, devono essere adeguatamente protette (es. tramite crittografia) e non devono essere registrate su database facilmente accessibili. È bene impostare un blocco automatico dell'accesso dopo un dato numero di tentativi falliti.
AUTORIZZAZIONE E ACCESSO	I privilegi di accesso devono essere commisurati al ruolo e alle attività svolte dall'utente. Occorre verificare che gli utenti non possano accedere a contenuti a loro preclusi (es. informazioni riservate accessibili tramite URL, password, chiavi crittografiche, connessioni a database, ecc.).
GESTIONE DELLE SESSIONI ***(Session management)***	La gestione delle sessioni di attività consente di tener traccia dell'utente autenticato in modo da riconoscerlo durante la navigazione. In altri termini, ogni volta che un utente si autentica nel sito o nell'applicazione Web gli viene fornito un ID valido per tutta la durata della navigazione nell'area protetta. L'ID deve essere univoco per ciascun utente e fornito in seguito ad un processo di autenticazione.
COOKIE	I cookie sono utilizzati per facilitare i meccanismi di autenticazione e di navigazione: essi memorizzano una serie di informazioni utili alla navigazione (es. lingua e aspetto delle pagine Web, dati di navigazione, ecc.). Poiché i cookie sono trasmessi in chiaro, all'interno di essi non devono essere presenti dati sensibili. I cookie contenenti informazioni critiche devono essere protetti mediante crittografia.
GESTIONE SICURA DI INPUT E OUTPUT	Ogni software necessita di un input corretto per poter produrre dell'output corretto; detto ciò, è fondamentale verificare l'input, in particolare quello proveniente da fonti non sicure (es. utenti). La validazione (e il filtraggio) dell'input consente di verificare che i dati immessi siano sicuri prima del loro utilizzo da parte dell'applicazione; in questo modo è possibile prevenire alcune vulnerabilità che potrebbero essere sfruttate per compiere specifici attacchi. Allo stesso modo, è importante gestire correttamente gli output dell'applicazione sviluppata, i quali potrebbero contenere parte dei dati immessi come input o nei casi peggiori, codici maligni.
REVISIONE DEL CODICE (CODE REVIEW) E CONTROLLI DI SICUREZZA	Il codice sorgente dei programmi informatici deve essere esaminato per verificare che non siano presenti vulnerabilità che consentano ad un *hacker* di svolgere azioni dolose (es. accessi ad informazioni critiche, frodi, etc). Al riguardo sono disponibili sul mercato specifici standard per svolgere tali verifiche (es. *OWASP-Top ten vulnerabilities*). È inoltre di fondamentale importanza fare un uso corretto di *firewall* e software *antimalware* per monitorare il traffico in ingresso e in uscita, rilevare eventuali attacchi e notificarli in modo tempestivo.

PROTEZIONE CRITTOGRAFICA	Bisogna proteggere le informazioni (statiche e in transito) valutate critiche in sede di valutazione dei rischi tramite la crittografia. Occorre utilizzare chiavi crittografiche adeguate in termini di algoritmo utilizzato e di dimensione (maggiore è la lunghezza della chiave, maggiore è la sicurezza della stessa), proteggendole da accessi non autorizzati.
GESTIONE DELLE ECCEZIONI	I messaggi di errore devono essere strutturati in modo da non consentire, ad un eventuale attaccante, di dedurre informazioni che potrebbero essere sfruttate a suo vantaggio.
BACKUP, LOGGING E AUDITING	Effettuare periodicamente copie di sicurezza (*backup*), le quali devono essere adeguatamente protette e testate. È buona norma registrare (*logging*) e verificare (*auditing*) periodicamente le seguenti attività: eventi di autenticazione e di autorizzazione, attività degli amministratori, cancellazione o modifica dei dati o dei permessi. I *log* rappresentano informazioni critiche e devono essere adeguatamente protetti contro accessi e/o modifiche non autorizzate.

3.7 Gestione della navigazione sul web

Internet è considerata il principale vettore di attacchi informatici. Nella Tabella 12 che segue sono riassunte le principali "buone pratiche" da utilizzare per minimizzare i rischi legati alla navigazione Web.

Tabella 12

BUONE PRATICHE PER LA NAVIGAZIONE WEB

CONNESSIONI SICURE	Prima di procedere alla navigazione, assicurarsi che la connessione sia affidabile. A tal fine: • impostare sul proprio router/modem una password sicura subito, evitando di utilizzare il nome utente e la password fornite dal produttore; • evitare di collegarsi a reti pubbliche o prive di password, soprattutto quando internet deve essere utilizzato per operazioni che richiedono un certo grado di sicurezza (es. invio o ricezione di documenti aziendali, operazioni bancarie, ecc.).
SCELTA DEL BROWSER	Fondamentale è la scelta del browser; diverse piattaforme offrono diverse opzioni di protezione, che possono (e devono) essere attivate per aumentare la sicurezza dell'utente durante la navigazione.
AGGIORNAMENTO E CORREZIONI (Patch)	La maggior parte degli attacchi informatici sfrutta le vulnerabilità dei sistemi operativi e dei programmi installati sui dispositivi destinatari (*target*); per questo motivo occorre prestare attenzione agli aggiornamenti di sicurezza del software installato (es. sistema operativo, browser, plug-in, ecc.). È buona norma configurare il proprio computer e, più in generale, tutti i dispositivi connessi alla rete, in modo che scarichino e installino automaticamente le correzioni di sicurezza.

REGOLE DI NAVIGAZIONE

Durante la navigazione, prestare attenzione alla pagina Web visitata. In tal senso verificare che:

- nella barra degli indirizzi, il collegamento inizi con https:// invece di http://;
- nella barra di stato del browser sia presente la classica icona a forma di lucchetto.

L'insieme di questi elementi indica che il sito è sicuro e utilizza sistemi di cifratura.
Nell'utilizzare i *Social Network* è buona norma limitare la visione delle informazioni personali alle sole persone con cui si desidera condividerle, prestando attenzione ai contenuti pubblicati.
Nel caso in cui dovessero apparire pop-up inattesi (es. segnalazioni della presenza di virus sul computer), la prima regola è **evitare di aprire il link e non autorizzare eventuali download**.
Ove possibile è bene utilizzare account con limitazioni (es. divieto di modifica delle impostazioni di sistema o di installare programmi); in questo modo, un eventuale *malware* capace di sfruttare le vulnerabilità del browser utilizzato non sarebbe in grado di infettare il vostro dispositivo.

PASSWORD SICURE

Ogni account deve essere protetto mediante chiavi di accesso sicure e difficili da dedurre. È bene rispettare le seguenti buone norme per la scelta delle proprie password:

1. evitare di utilizzare nomi di persone o date di nascita;
2. utilizzare nomi di fantasia non presenti in dizionari: in questo modo sarebbe particolarmente complicato utilizzare "attacchi a dizionario" per violare il sistema;
3. non utilizzare password contenenti caratteri sequenziali o ripetuti;
4. la chiave d'accesso deve essere sufficientemente lunga (9 caratteri);
5. utilizzare combinazioni contenenti caratteri normali, speciali, maiuscole e numeri;
6. cambiare le proprie password a intervalli regolari (almeno ogni 3 mesi), evitando di scegliere chiavi d'accesso simili a quelle utilizzate in precedenza (3 versioni);
7. scegliere password facilmente memorizzabili, evitando di scriverle;
8. non usare risposte eccessivamente semplici o facili da individuare nelle opzioni "Domanda segreta".

Una soluzione alternativa alle password tradizionali è l'utilizzo di una frase di accesso (*passphrase*) composta da un numero elevato di caratteri molto meno individuabile rispetto ad una password.
I criteri per la scelta di una frase d'accesso robusta sono i seguenti:

- lunghezza sufficiente a rendere la frase di difficile individuazione (almeno 20-30 caratteri);
- non utilizzare parole o frasi reperibili in un dizionario, oppure celebri;
- utilizzare combinazioni contenenti caratteri normali, speciali, maiuscole e numeri;
- scegliere frasi di accesso facilmente memorizzabili, evitando di scriverle;
- evitare di "salvare" le password sul dispositivo utilizzato.

ACCESSO A SITI INDESIDERATI	In un contesto aziendale può essere necessario impedire agli utenti di accedere a siti Internet non adeguati, dai contenuti offensivi o che potrebbero mettere a repentaglio la sicurezza e la reputazione aziendale; ciò è possibile utilizzando un software per il filtraggio del Web o configurando il proprio browser in modo da permettere l'accesso ai soli siti sicuri, impedendo l'ingresso in quelli classificati come "sconvenienti".
FIREWALL E ANTIMALWARE	Prima di procedere con la navigazione, è bene assicurarsi che sul dispositivo sia installato e attivo un software *anti-malware* in grado di rilevare e disabilitare eventuali programmi dannosi contenuti in email o siti Web non sicuri. I software di sicurezza dovrebbero essere installati come primi programmi in esecuzione e utilizzati per effettuare una scansione completa del sistema con cadenza almeno settimanale. Occorre utilizzare un *firewall* in grado di proteggere le informazioni critiche (aziendali o personali) e impedire eventuali scambi di dati non autorizzati. Tutte le applicazioni citate in precedenza devono essere mantenute attive e aggiornate.

3.8 Gestione della posta elettronica

La posta elettronica è sicuramente il mezzo di comunicazione, asincrono, più diffuso ed è in crescita continua nel mondo business. Cresce per la sempre maggiore numerosità di utenti e lo fa anche soppiantando l'ormai obsoleto fax e resistendo agli assalti sferrati dalla comunicazione in tempo reale (es. WhatsApp). E' un modo di comunicare apparentemente elementare da usare e viene spesso utilizzata con "disinvoltura" eccessiva e senza badare adeguatamente agli effetti sgraditi che i comportamenti non corretti comportano. Cercheremo qui di schematizzare i rischi e le indicazioni utili per un buon utilizzo ed i motivi per i quali, non sembri strano, riteniamo opportuno **insegnare** agli operativi ad usare al meglio questo strumento. La posta elettronica ha, infatti, nella sua semplicità d'uso e nell'apparente assenza di costo diretto di utilizzo i propri nemici storici. Saperla usare bene non è quindi meramente un fatto tecnico, ma comporta un insieme di regole di comportamento e di informazioni anche legali che di solito sono, a dir poco, sottovalutate.
Esaminiamo di seguito la posta elettronica funzionalmente.

- **Comporre** un messaggio significa predisporre la trasmissione di un insieme di informazioni, talvolta di grande valore, ad un insieme di individui, interni o esterni all'azienda del mittente, con i quali il mittente ha relazioni di tipo diverso. Le informazioni stesse possono essere o non essere:
  - confidenziali (riservate);
  - impegnative (aspetto legale/contrattuale della mail);
  - redatte in modo formalmente corretto e rispettoso delle convenzioni;
  - mandate con ricevuta di ritorno;
  - trasmesse in copia conoscenza nascosta.
- **Ricevere** un messaggio comporta in primis la difesa (aiutata dal sistema informatico o esercitata come discernimento personale) di sé stessi e del proprio tempo lavorativo dal grave fenomeno dello *spam*[6], e peggio ancora del *ransomware*[7], e solo dopo inizia il processo aziendale di interpretazione del messaggio e la sua attuazione o comunque gestione.
- **Rispondere** ad un messaggio comporta il rispetto di una serie di norme, obblighi e responsabilità, troppo poche volte esplicitati, spesso solo tratteggiati; basti pensare alla scelta tra la risposta a tutti e la risposta al solo mittente così come l'improvvida aggiunta di un destinatario durante uno scambio già in corso.
  Fra questi obblighi citiamo solo il più tristemente noto e causa di stress: rispondere in fretta, tipicamente non oltre una giornata lavorativa.

Come si vede quello che sembrava il nostro compito più banale della giornata, spesso svolto con lo smartphone o il tablet nei ritagli di tempo, se correttamente considerato dal punto di vista funzionale, diviene tutt'altro che banale.

[6] *Posta non desiderata (non richiesta) inviata, nel migliore dei casi, per pubblicizzare un prodotto o servizio.*

[7] *Ransomware significa prodotto informatico finalizzato ad estorcere un riscatto in vari modi, tra cui, ad esempio, criptando i dati e vendendo la relativa chiave di cifratura al danneggiato.*

E non abbiamo argomentato nulla di "tecnologico": la tecnologia infatti può soltanto supportare il processo e renderlo più comodo e facile ma non sostituirci. Ad esempio un ottimo *mail gateway*[8] proteggerà, riducendo il numero di seccature e rischi, ma, alla fine, c'è sempre un umano che deve prendere delle decisioni su messaggi normali e spesso anche su **qualche**, si spera pochi, messaggio infetto o rischioso che il *mail gateway* non ha fermato. Sia gli aspetti funzionali che la funzione di estremo difensore devono essere ben **insegnati** e compresi, pena la crescita esponenziale dei rischi che sono in capo al soggetto e all'impresa. Un solo esempio, per riflettere: un alberello natalizio (1MB di immagine in fondo non è tanto) inviato, anni fa, come immagine augurale da un ignaro impiegato a tutti i membri della rubrica (*directory*) aziendale (4000 persone) di una multinazionale con ricevuta di ritorno. Il traffico generato rischiò di creare seri problemi all'infrastruttura informatica aziendale di una catena della GDO!

Tabella 13

GESTIONE DELLA POSTA ELETTRONICA E MISURE DI SICUREZZA

FORMAZIONE E SENSIBILIZZAZIONE DEI DIPENDENTI	La formazione e la sensibilizzazione dei dipendenti è fondamentale per gestire "in sicurezza" la posta elettronica; è necessario coinvolgere i dipendenti per aumentare la loro consapevolezza sui rischi di compromissione delle informazioni aziendali e personali.
MISURE ORGANIZZATIVE	• Normare gli utilizzi (es. divieto di uso privato dell'email poiché la promiscuità avvantaggia i *malware*). • Formare ed informare circa le responsabilità e le regole da rispettare e le particolarità aziendali. • Chiarire la perseguibilità individuale in caso di danni dolosi o colposi. • Assicurare la corretta conformità della gestione delle informazioni distribuite via mail secondo le norme e gli usi anche internazionali (ad esempio, in Germania, la signature[9] DEVE per legge informare su chi è il CEO della società scrivente al momento della spedizione). • Normare le posizioni aziendali che possono "firmare" mail impegnative. • Assicurare la conoscenza delle leggi e delle politiche in vigore tramite formazione aziendale. • Conservare la posta elettronica per DIECI anni, come la normale corrispondenza, e possibilmente avere modo di smascherare le cancellazioni, dolose o colpose, di messaggi, anche a distanza di tempo. • Decidere tra casella di posta elettronica (*mailbox*) con indirizzi di ufficio o personali (quelli personali meritano riflessioni aggiuntive).
MISURE "MINIME" DI SICUREZZA	• Proteggere la posta elettronica da usi impropri con tutti i sistemi disponibili e obbligare al cambiamento frequente delle password. • Avere copie di sicurezza (backup) frequenti: il *ransomware* passa dalla posta ma i danni li fa a tutto il sistema e non solo al dispositivo colpito. • Utilizzare *firewall* e software di *mail gateway* adeguati per proteggere il proprio dispositivo da collegamenti non sicuri, virus e altre tipologie di attacco. • Aggiornare puntualmente tutti i sistemi coinvolti.
MISURE AGGIUNTIVE DI SICUREZZA	• Effettuare una cifratura completa dei dispositivi personali: se le password fossero violate, la cifratura dei dati costituirebbe un secondo livello di sicurezza. La crittografia deve essere applicata ai dati in transito, a quelli statici, alle memorie interne e a quelle esterne. • Impiegare un *mail gateway* evoluto e dotato di blocco dell'accesso a pagine web con funzioni maligne (*url sandboxing*): il sistema verifica la bontà dell'indirizzo web (URL o *Uniform Resource Locator*) prima di renderlo disponibile all'utente. • In casi estremi impiegare una lista dei domini dei corrispondenti autorizzati, che azzera il rischio di link fraudolenti.

[8] *Mail Gateway è l'insieme dei sistemi che proteggono da spam e ransomware, come tutte le difese è migliore quanto più è aggiornato; e comunque NON è infallibile.*

[9] *Il testo in calce contenente gli estremi del mittente ed eventuali loghi o messaggi di marketing, da non confondere con la firma elettronica che è invece un prodotto informatico idoneo per garantire l'autenticità del messaggio.*

3.9 Gestione del *Social Network*

La sicurezza delle informazioni deve essere garantita anche mediante l'uso consapevole di servizi legati alle "reti sociali" (*Social Networking*). L'utilizzo non corretto di queste piattaforme da parte dei dipendenti potrebbe esporre l'azienda a minacce e a danni economici diretti e/o indiretti.

Le principali minacce nell'ambito dei *Social Network* possono riguardare il furto delle identità digitali, l'ottenimento di informazioni sensibili o la profilazione dell'utente tramite attività di "*social engineering*", ossia l'analisi dei comportamenti dell'utente al fine di determinare dettagli utili per un eventuale tentativo di accesso e modifica di un sistema informatico (*hacking*).
La pubblicazione sui *Social Network* deve sempre preservare la riservatezza dei dati, nonché la reputazione dell'azienda.
È indispensabile quindi prestare attenzione e rispettare alcuni pratici accorgimenti:

- verificare il "pubblico" con il quale il contenuto viene condiviso, limitando a seconda dei casi, la visibilità a determinate categorie / gruppi di utenti;
- evitare l'utilizzo di account personali per la pubblicazione di contenuti nell'ambito della propria attività lavorativa;
- verificare le impostazioni sulla privacy (dati personali condivisi, connessioni attive sul proprio account, etc.), utilizzando le specifiche funzionalità messe a disposizione dal portale *Social*;
- accettare richieste di collegamento solo da contatti realmente conosciuti o comunque certificati;
- gestire le credenziali di accesso ai social rispettando le politiche aziendali o comunque le principali "buone pratiche" per la gestione sicura delle password (cambiarle spesso, utilizzando termini non comuni, accompagnati da caratteri speciali / numeri, etc.)

3.10 Gestione del personal computer dell'azienda

I Personal Computer (insieme ad altri dispositivi mobili, anche personali) costituiscono il punto di accesso ai sistemi informativi aziendali da parte degli utenti. Per questo devono essere gestiti e protetti per impedire intrusioni da parte di persone non autorizzate (interne o esterne all'azienda) e la conseguente sottrazione, manipolazione o distruzione di dati, sia presenti sui PC stessi, sia sui server ad essi collegati.

Per poter avviare una efficace gestione del parco PC è necessario disporre di un inventario completo della dotazione di hardware e software e della loro assegnazione agli utenti; la gestione dei PC potrà efficacemente essere integrata con altri processi aziendali (acquisti, magazzini, cespiti, gestione spazi...) ma ove ciò fosse eccessivamente oneroso può anche vivere come attività autonoma che scambia dati con altri processi. L'ingresso in azienda di un PC (e relative periferiche come monitor, stampanti, memorie esterne) comporta la registrazione a magazzino e la sua successiva assegnazione a singoli utenti, reparti o commesse; anche nel caso di assegnazioni non nominative andrà individuata una persona di riferimento. Normalmente l'assegnazione prevede un processo di richiesta e autorizzazione che può essere connesso alla gestione degli strumenti informatici. Per i PC fissi sarà indicata la collocazione fisica ma anche per i PC portatili va segnata una collocazione principale.

Alla registrazione di ogni PC saranno poi assegnate le relative periferiche e le licenze di software legittimamente acquistato ed assegnato a quel PC; il personale tecnico sarà autorizzato ad installare solo i programmi che risultano assegnati a quella postazione; per rispettare la proprietà intellettuale e la sicurezza informatica, gli utenti finali non saranno autorizzati ad installare o rimuovere autonomamente alcun software, neanche nel caso in cui dispongano dei privilegi tecnici che lo consentirebbero.

Rigorosi controlli andranno effettuati su tale aspetto. Il normale processo di movimentazione e riassegnazione delle risorse informatiche (PC, periferiche e programmi) deve essere gestito e registrato nel sistema di gestione. Il servizio di assistenza tecnica per poter gestire le chiamate da parte degli utenti (e gli interventi richiesti dalla Direzione Sistemi) dovrà avere accesso all'anagrafica delle risorse informatiche assegnate e poterla modificare in caso di installazioni o disinstallazioni autorizzate.

L'esperienza insegna tuttavia che, anche con le migliori intenzioni e con un'organizzazione di ferro, il mondo reale tende a disallinearsi progressivamente dalla sua rappresentazione all'interno dei sistemi di gestione.
Non va quindi trascurata la necessità di inventari periodici sul campo (manuali o con appositi strumenti automatici) per confermare o eventualmente aggiornare la presenza, collocazione ed assegnazione dei PC e del loro corredo; tali inventari dovranno contemplare sia gli uffici o unità produttive che i magazzini di ingresso, lavorazione, transito o uscita in cui si possano trovare temporaneamente i PC.

L'azienda definirà un Regolamento sull'utilizzo (eventualmente anche personale) dei PC aziendali, che escluda comunque l'installazione autonoma di software non autorizzato e la modifica dei parametri di configurazione e di sicurezza; dovrà poi darne adeguata diffusione agli utenti ed effettuare gli opportuni controlli, nel rispetto della normativa Privacy e di quella sul lavoro.

3.11 Sicurezza Mobile e *Bring your own device* (BYOD)

Smartphone, PC portatili e Tablet sono strumenti di larga diffusione in azienda, in quanto favoriscono la condivisione di informazioni fra colleghi, clienti, fornitori e altre persone, che possono essere coinvolte in attività "legate" al business aziendale. L'elemento che accomuna tali strumenti è il fatto che sono in pratica dei computer, con le problematiche di sicurezza informatica che caratterizzano tali strumenti.

Il termine *Bring Your Own Device* (BYOD) [in italiano "porta il tuo dispositivo"] identifica l'insieme delle politiche e soluzioni tecnico-organizzative aziendali che permettono di utilizzare in sicurezza i propri dispositivi personali anche per attività lavorative.
La pratica del BYOD può generare benefici per l'azienda e il dipendente, come:

- la riduzione dei costi legati all'acquisto, alla manutenzione, alla gestione e all'aggiornamento di dispositivi mobili che devono essere forniti a ciascun membro dell'azienda;
- il miglioramento della produttività personale, dell'innovazione aziendale, della flessibilità dei dipendenti e della loro soddisfazione, grazie alla possibilità di accedere alle risorse e alle informazioni aziendali in mobilità, utilizzando un solo strumento per lavoro e vita privata.

A questi benefici si affiancano una serie di rischi che non devono essere sottovalutati. L'ampia diffusione dei dispositivi mobili rende questi ultimi un obiettivo chiave dei criminali informatici, che mirano a sfruttare le vulnerabilità delle aziende, che permettono l'utilizzo sul lavoro di dispositivi personali senza un adeguato sistema di sicurezza, fra le quali:

- uso promiscuo e contemporanea presenza di informazioni personali e aziendali sullo stesso dispositivo; la conseguenza è la perdita di controllo sulle informazioni aziendali gestite attraverso dispositivi personali;
- facilità di furto o smarrimento dei dispositivi personali, in particolare smartphone e tablet;
- vulnerabilità tecniche dei dispositivi: questi ultimi sono progettati per uso privato (fascia *consumer*), prestando poca attenzione all'infrastruttura di sicurezza a favore della facilità di utilizzo.

Le minacce che possono sfruttare le vulnerabilità elencate in precedenza sono diverse:

- *malware* (es. virus, trojan, spyware, ecc.): la compromissione di un dispositivo mobile può portare alla perdita, al furto, alla compromissione o alla divulgazione di informazioni confidenziali (personali o aziendali);
- *phishing* (truffa informatica tramite email recante il logo contraffatto di una banca o di grande azienda) e attacchi *hacker*: sfruttando le vulnerabilità legate al comportamento umano o la scarsa sicurezza degli ambienti di connessione dei dispositivi mobili è possibile sottrarre informazioni gestite attraverso dispositivi personali.

L'adozione di un adeguato programma BYOD (e la conseguente regolamentazione di queste pratiche) consente di minimizzare i rischi legati all'utilizzo di dispositivi personali sul luogo di lavoro, mantenendo inalterati i benefici per l'azienda.
Un'efficace strategia BYOD dovrebbe comprendere le attività e le contromisure riassunte nella Tabella 14, le quali devono essere coerenti con la criticità delle informazioni da proteggere.
È bene precisare che la scelta di adeguate misure di sicurezza può richiedere il coinvolgimento di consulenti specializzati nelle tematiche trattate.

Tabella 14

GESTIONE DEI DISPOSITIVI MOBILI E MISURE DI SICUREZZA

FORMAZIONE E SENSIBILIZZAZIONE DEI DIPENDENTI	La formazione e la sensibilizzazione dei dipendenti è fondamentale per gestire "in sicurezza" la soluzione BYOD; è necessario coinvolgere i dipendenti per aumentare la loro consapevolezza sui rischi di compromissione delle informazioni aziendali e personali.
MISURE ORGANIZZATIVE	• Individuare i rischi introdotti dal BYOD ed effettuare una mappatura delle informazioni che possono essere accedute tramite dispositivi personali. • Determinare ruoli e responsabilità per la sicurezza e la corretta gestione dei dispositivi mobili, considerando l'amministrazione centralizzata degli stessi. • Inventariare i dispositivi che hanno privilegi di accesso alle informazioni e alle risorse aziendali, registrandone le informazioni chiave (es. modello, numero di serie, sistema operativo, ecc.).
MISURE "MINIME" DI SICUREZZA	• Gestire i privilegi di accesso alla rete aziendale tramite dispositivi BYOD. • Utilizzare password sicure su tutti i dispositivi. • Utilizzare *firewall* e software *antivirus* e/o *antimalware* per proteggere il proprio dispositivo da applicazioni non sicure, virus e altre tipologie di attacco. • Aggiornare con costanza il software e installare le correzioni (*patch*) che possono migliorare la sicurezza dei dispositivi personali. • Effettuare copie di sicurezza (*backup*) regolari dei dati.
MISURE AGGIUNTIVE DI SICUREZZA	• Effettuare una cifratura completa dei dispositivi personali: se le password fossero violate, la cifratura dei dati costituirebbe un secondo livello di sicurezza. La crittografia deve essere applicata ai dati in transito, a quelli statici, alle memorie interne e a quelle esterne. • Installare applicazioni sicure: ciò può essere facilitato formalizzando una lista del software approvato (*whitelist*) e/o di quello vietato (*blacklist*) dall'azienda. • Utilizzare tecnologie VPN - SSL (*Virtual Private Network - Secure Sockets Layer*): queste soluzioni consentono la creazione di un vero e proprio "tunnel" cifrato che aumenta sensibilmente i livelli di sicurezza delle informazioni accedute tramite dispositivi personali.

3.12 Creazione e gestione della rete locale e wireless in sicurezza

Cosa è la rete locale (o LAN, o *Local Area Network*)

Si premette che, in questo contesto e se non altrimenti specificato, LAN e Rete Wireless (o WiFi) sono sinonimi.
È la componente di rete interna alla propria organizzazione, solitamente riferita ad una singola "località ristretta", intendendo con ciò un ufficio, un edificio, un campus di più edifici.
Se due o più reti locali sono collegate fra loro attraversando in qualunque modo suolo pubblico, esse non costituiscono una singola LAN, ma più reti locali (proprie!) fra loro interconnesse.

È la componente di rete più importante dal punto di vista aziendale, perché:

- è l'unica componente veramente sotto il proprio diretto controllo e quindi, purtroppo, sotto la propria responsabilità,
- collega fra loro i diversi dispositivi (PC, server, stampanti, dischi...) poiché un sistema isolato è inutile,
- è il primo anello di collegamento ad internet e quindi deve funzionare bene, essere sicuro e sotto controllo.

Una LAN può essere costruita su diverse tecnologie, anche mischiate fra loro. Ne esistono tante, ma nella stragrande maggioranza dei casi, oggi i dispositivi locali sono connessi fra loro con queste due principali tecnologie: (a) cavi Ethernet, (b) radio (detto wireless, noto anche come WiFi).
Quindi la LAN è interconnessa ad Internet con altre tecnologie (fibra, adsl, radio, ...) non di interesse in questo paragrafo.
Dal punto di vista della sicurezza, i collegamenti via cavo Ethernet sono preferibili, perché un canale radio è per sua natura un canale aperto, anche se poi proteggibile in vari modi, ad esempio tramite la crittografia.
Ormai, però, i collegamenti WiFi sono, nella maggioranza dei casi, inevitabili: per convenienza economica e per collegare i dispositivi mobili come tablet e smartphone che proliferano in azienda.
Nel costruire e gestire la LAN, o nel chiedere al proprio fornitore di fiducia di farlo, bisogna in particolare focalizzarsi su questi aspetti chiave:

- è la propria rete locale ed è sotto la propria responsabilità: non ci sono altri responsabili;
- bisogna avere un approccio minimalista: quel che non c'è non costa, non si guasta, non fallisce, non è attaccabile;
- è giusto proteggere la rete dalle minacce esterne, ma anche dalle minacce interne;
- i *firewall* sono oggetti necessari, ma non sufficienti: non bisogna pensare in termini di "ho il *firewall*, sono a posto";
- la configurazione di fabbrica dei firewall o di ogni altro dispositivo deve essere riconfigurata;
- i canali radio (WiFi o ponti radio) sono canali aperti per definizione: bisogna proteggerli con chiavi crittografiche;
- se si interconnettono più LAN proprie attraversando suolo pubblico bisogna crittografare la connessione, per esempio con "tecnologie VPN";
- le chiavi WiFi e la password di accesso ai *firewall* e ad altri dispositivi di sicurezza vanno cambiate regolarmente;
- il **monitoraggio è fondamentale e costoso**: firewall ed altri dispositivi (proxy, punti di accesso WiFi e VPN) generano *log* e allarmi, ma se nessuno li raccoglie ed analizza, può accadere di aver subito un attacco senza esserne coscienti; monitorare la rete comunque costa meno che subire un attacco e non saperlo o saperlo troppo tardi;
- conviene isolare la propria LAN da internet con minimo due firewall: uno esterno (*outwall*) ed uno interno (*inwall*), possibilmente di diversa tecnologia.
  (internet) ====> [outwall] =======> [inwall] =========> (la propria LAN)

Poco importa che il *firewall* interno ripeta e riconfermi le stesse regole di quello esterno. Lo scopo di questa configurazione è di minimizzare i danni se un attacco al firewall esterno avesse successo.
In venticinque anni allo scrivente è capitato diverse volte di avere il firewall esterno compromesso e sempre senza nessuna conseguenza (tranne la perdita di tempo per ripristinare il *firewall* esterno).
Questo perché l'attaccante dopo aver "forato" il primo muro si è scontrato col secondo, ma il secondo muro, essendo di tecnologia diversa, ha resistito al tipo d'attacco che aveva compromesso il primo, essendo i due dispositivi monitorati, mentre l'attaccante cercava altri metodi per forare il secondo muro, l'attacco è stato rilevato e c'è stato agilmente tutto il tempo per fermarlo prima che potesse fare alcun tipo di danno.

Tabella 15

IMPLICAZIONI DI SICUREZZA NELLE RETI LOCALI

Problema	***Soluzione***
Responsabilità	***Progetto e gestione nel tempo della propria LAN***
• la propria LAN è ... la propria LAN! • l'azienda è l'unica responsabile di quel che succede nella propria rete locale; • non essere coscienti di cosa la propria LAN genera non sposta la responsabilità, anzi la peggiora* • ancor di più se genera danni a terzi che potrebbero (quindi lo faranno) chiedervene conto! *inversione dell'onere della prova (TU Privacy e art. 2050 del C.C. oggi, GDPR/Regolamento EU domani)	• Bisogna progettare bene e gestire nel tempo la propria LAN: ▪ è prima di tutto un proprio interesse, poi un proprio dovere; ▪ bisogna documentare tutto, perché l'onere della prova è proprio carico; • Bisogna progettare o far progettare la LAN su questi punti cardine: ▪ sicurezza della progettazione (vedasi il Regolamento Europeo); ▪ minimalismo: ▪ quel che non c'è non costa, non si guasta, non fallisce; ▪ minore è la complessità, maggiore è la facilità di gestione • protezione in tutte le direzioni: ▪ dall'esterno (internet) verso l'interno (LAN) ▪ dall'interno (LAN) verso l'esterno (internet) (v. anche par. su *IOT* e *Big Data*) ▪ e fra le diverse proprie LAN, se interconnesse; • I firewall sono oggetti necessari, ma non sufficienti • altri dispositivi potrebbero essere utili o necessari, da stabilire in fase di progetto se dovessero servire, visto che contrastano con l'approccio minimalista: ▪ forse, per esempio, proxy, VPN e monitor di rete; ▪ quasi certamente collettori di *log*.

Disordine	Ordine
• la propria LAN è … la propria LAN! • l'azienda è l'unica responsabile di quel che succede nella propria rete locale; • non essere coscienti di cosa la propria LAN genera non sposta la responsabilità, anzi la peggiora* • ancor di più se genera danni a terzi che potrebbero (quindi lo faranno) chiedervene conto!	• Bisogna adottare un approccio del tipo "è vietato ciò che non è permesso" (*deny by default*): ▪ disabilitare tutto, poi abilitare il necessario e sufficiente. • Tutti i dispositivi di rete, i server, i PC installati: ▪ vanno configurati correttamente all'inizio e nel tempo; ▪ vanno gestiti nel tempo e soprattutto, monitorati. • Quando si installa un nuovo dispositivo bisogna: ▪ cambiare la password di fabbrica; ▪ cambiare le chiavi crittografiche dei dispositivi WiFi; ▪ fornire password e chiavi non banali! • Ci si deve accertare che, per i protocolli/servizi da usare, i firewall garantiscano che tali protocolli rimangano all'interno della/e propria/e LAN. Potrebbero probabilmente servire alcuni protocolli verso l'esterno (internet): ▪ HTTP/HTTPS per accedere ai siti web di internet, ▪ POP/SMTP per inviare e ricevere la posta elettronica, ▪ SSH/FTP per accedere a propri sistemi remoti. • Bisogna cambiare le chiavi crittografiche e le password: ▪ almeno ogni sei mesi, meglio ogni tre; ▪ sicuramente ad ogni entrata/uscita di collaboratori. • Relativamente ai *log* è necessario: ▪ raccogliere i log generati da firewall, VPN, PC, server, WiFi, ecc. e conservarli per almeno sei mesi, possibilmente su un collettore separato e ben protetto; ▪ fare attenzione al dispositivo: se i *log* sono registrati localmente su un dispositivo compromesso, anche i *log* saranno compromessi insieme ad esso; ▪ ricordarsi che la mancanza del log comporta non avere prove e quindi non poter dimostrare alcunché; ▪ optare, se del caso, per acquisire tale servizio all'esterno (*As a Service*) da un fornitore (*provider*) che **non** sia: ▪ il vostro internet *service provider*, ▪ il vostro fornitore di servizi ICT, ▪ qualsiasi altro fornitore con conflitti di interesse.

*inversione dell'onere della prova (TU Privacy e art. 2050 del C.C. oggi, GDPR/Regolamento EU domani)

3.13 Gestione dei dispositivi di memorizzazione esterni

L'uso di supporti informatici per custodire ed elaborare le informazioni è diventata pratica diffusa nella società ad ogni livello: che i dati da preservare siano privati o lavorativi, svariate sono le soluzioni di archiviazione (hard disk, pen drive, memory card, smartphone, etc...) per trasferire le informazioni, elaborarle e ordinarle a fini conservativi.
Saper gestire i dispositivi di memoria esterni è diventato imperativo, diversamente si rischia di perdere irrimediabilmente dati, informazioni, appuntamenti, contatti preziosi per il lavoro e la vita quotidiana di ognuno di noi. Per sapere come comportarci e per evitare una perdita di dati, occorre sapere poche cose, tra cui assolutamente quali possono essere le tipologie di supporti e le loro connessioni.

I supporti più comuni usati per la memorizzazione dei dati sono:
- disco rigido, interno o esterno (o hard disk);
- chiavetta USB (o *pen drive*);
- schedina (o *memory card*);
- dispositivo contenente più dischi rigidi (o NAS).

Essi possono connettersi ai nostri Computer o Notebook direttamente tramite apposita porta (ad es. USB) oppure via:
- cavo USB;
- rete locale o LAN;
- rete Wi-Fi.

Ogni connessione è legata ad una o più tipologie di supporto.
Nelle successive Tabelle 16, 17 e 18 sono riportate, per ogni connessione, le caratteristiche e le criticità dei dispositivi di memorizzazione esterni ad essa collegabili.

Tabella 16
CONNESSIONE TRAMITE CAVO USB - VANTAGGI E CRITICITÀ

Tipologia di dispositivi	*Vantaggi/Criticità*
Generalmente sono dispositivi composti da un singolo disco rigido o da una chiavetta USB o da una schedina. Sono usati prevalentemente per avere una copia dei dati ed utilizzarli in movimento; per questo motivo sono piccoli e facilmente trasportabili. Le schedine, invece, sono utilizzate prevalentemente nelle macchine fotografiche. Relativamente ai dischi rigidi esistono dei dispositivi (NAS) con più dischi rigidi, sui quali gli stessi dati sono contemporaneamente memorizzati in copia, al fine di aumentarne la sicurezza. Tali soluzioni però, difficilmente sono trasportabili e generalmente vengono utilizzate esclusivamente sulla scrivania anche come "raccoglitore" unico dei dati o backup.	Il vantaggio principale dei supporti trasportabili è la loro maneggevolezza, che li rende uno strumento da utilizzare al lavoro, a casa e in movimento. Purtroppo le criticità di queste soluzioni sono molto alte, infatti non solo occorre provvedere correttamente al loro distacco dal computer, ma sono facilmente soggetti ad urti e cadute, che possono portare facilmente alla perdita dei dati. Si consiglia, quindi, di adottare questi supporti solo ed esclusivamente per spostare i dati e non come unico supporto di lavoro o *backup*. Altra criticità risiede nella condivisione con altri utenti, dei dati memorizzati, che può avvenire solo tramite il computer a cui sono collegati i supporti e solo quando è acceso. I NAS hanno il vantaggio di poter essere utilizzati sia come "raccoglitori" di dati che come supporti di *backup*, stando attenti a collocarli in posti ben ventilati e sicuri dalle cadute. Gli svantaggi riguardano la loro poca trasportabilità e, come per gli altri supporti, sono legati al loro corretto distacco dal computer al quale sono collegati e alla condivisione dei dati, che può avvenire esclusivamente a computer acceso. Gli svantaggi sono quelli già descritti per gli altri supporti, cui va aggiunta la loro poca trasportabilità.

Tabella 17

CONNESSIONE TRAMITE LAN (Rete locale) - VANTAGGI E CRITICITÀ

Tipologia di dispositivi	*Vantaggi/Criticità*
Tipici supporti di memorizzazione, che usano questa connessione, sono i NAS (*Network Attached Storage* cioè "Magazzino di Rete Collegato"), ovvero un dispositivo collegato alla rete locale aziendale, la cui funzione è quella di consentire agli utenti autorizzati di accedere e condividere file, lavori e cartelle. Generalmente sono composti da più dischi rigidi in varie configurazioni, ma possono anche essere formati da un solo supporto di memorizzazione. Necessitano di una porta LAN per il collegamento in rete.	Generalmente questa tipologia di supporti non è trasportabile sia per la loro grandezza che per il mezzo usato (cavo) per collegarlo alla LAN. Infatti tale collegamento ha senso se il dispositivo fa parte di una rete interna ad un ufficio o casa; a seconda del tipo di cavo e della scheda di rete usati si può raggiungere una velocità di trasferimento dei dati pari a 10 Gigabit al secondo. Questa caratteristica di non trasportabilità elimina tutte le problematiche derivanti dalle cadute e dagli urti accidentali; occorre però accertarsi di disporre il dispositivo in ambienti sicuri e ben arieggiati. Nel caso dei NAS i vantaggi aumentano in quanto la presenza di più dischi rigidi all'interno garantisce la continuità di lavoro anche in caso di rottura di un disco. Se, invece, il dispositivo ha un solo disco rigido allora è opportuno prendere tutte le precauzione viste al punto precedente. Il collegamento in LAN prevede la presenza o realizzazione di una infrastruttura di rete e le velocità di trasferimento dati, secondo la tipologia di cavo adottata e della scheda di rete, possono raggiungere velocità di 10 Gbit/s

Tabella 18

CONNESSIONE TRAMITE WIFI - VANTAGGI E CRITICITÀ

Tipologia di dispositivi	*Vantaggi/Criticità*
Questa tipologia di connessione, prevede il collegamento con il supporto di memorizzazione via etere, ovvero senza nessun collegamento diretto. Non è molto diffuso ed è distribuito solo da alcune case costruttrici. Generalmente questa tipologia di connessione è tipica di supporti singoli e non di supporti con architettura tipo NAS, con più dischi rigidi.	I vantaggi di tale tipo di collegamento sono esclusivamente riferibili al mancato utilizzo di cavi di collegamento; pertanto non ci sono i costi e la progettazione di un cablaggio di rete. Le criticità possono essere: • il limitato campo di copertura di una rete WiFi ed eventuali ostacoli o interferenze; • la limitazione di velocità di accesso al supporto, che non raggiunge mai quella con un collegamento via cavo; • il loro facile spostamento, che rende il supporto più soggetto ad urti o a cadute.

3.14 Gestione dei servizi gratuiti di *cloud storage*

I servizi di "conservazione di dati su internet" (*cloud storage*) consentono la memorizzazione di dati (documenti, immagini, file multimediali, etc.) e la relativa sincronizzazione tra più dispositivi. La semplicità nell'utilizzo, il costo contenuto (in diversi casi anche gratuito nelle versioni base) e l'integrazione con i più comuni servizi di terze parti hanno consentito la rapida diffusione di questa tecnologia.
Per un uso sicuro di questa tipologia di servizio è opportuno adottare gli accorgimenti di seguito annotati.

Credenziali e sessioni di sincronizzazione
Bisogna utilizzare password con un efficace livello di complessità e cambiarle in modo frequente, mantenendone la riservatezza.
Qualora disponibile, si deve verificare la titolarità delle sessioni web attive, terminando quelle non riconosciute e, inoltre, controllare costantemente i dispositivi collegati quali smartphone, tablet, PC e notebook, in modo da poter gestire tempestivamente il blocco della sincronizzazione.

Condivisione
La condivisione dei file deve avvenire utilizzando le specifiche funzionalità messe a disposizione dal servizio scelto mediante la definizione di più account personali sul medesimo servizio, evitando così l'utilizzo condiviso di un singolo account e beneficiando di funzionalità avanzate quali diritti diversificati in lettura / scrittura, revoca delle condivisioni, etc.

3.15 Organizzazione della sicurezza: politiche e procedure

Perché "organizzare" la sicurezza

I motivi principali sono:

- organizzare la sicurezza costa meno ed è più efficace che improvvisarla, anche se potrebbe apparire non intuitivo;
- è utile prima di tutto a se stessi;
- è uno strumento di distinzione ed è un valore aggiunto ai propri servizi, quindi una occasione di marketing,
- non ultimo, è un obbligo di legge: in particolare bisogna ricordarsi che l'onere della prova è a proprio carico!

Come "organizzare" la sicurezza

I due principali **strumenti** sono le "Politiche" (o *Policy*) e le "Procedure". C'è un preciso scopo nel definirli "strumenti" invece di "documenti". È vero che Politiche e Procedure sono contenute in documenti, ma il loro scopo non è di esistere ed essere semplicemente scritte (magari in ottimo italiano, inglese o "legalese").
Il loro scopo è **essere applicabili ed applicate**; si deve:

- dimenticare le fotocopie e/o i "taglia & incolla" di documenti altrui, perché ogni realtà aziendale ha le sue specificità,
- stabilire obiettivi **applicabili**, che ci si può permettere per budget e per natura della propria azienda;
- fissare gli strumenti con cui **rendere applicabili** gli obiettivi stabiliti: primo fra tutti il budget annuale dedicato alla sicurezza;
- definire di chi sia la responsabilità di **applicare**;
- definire come, da chi e riportando a chi sarà verificata la effettiva **applicazione** delle regole stabilite.

Attenzione al "fai-da-te" a meno che la sicurezza e la conformità non siano il proprio mestiere, nel qual caso difficilmente si starebbe leggendo questo documento.

Bisogna resistere alla facile tentazione di fare in proprio; sembra di risparmiare, ma così non è.
Al primo incidente serio ci si rende conto.
Bisogna fare attenzione ai "fotocopiatori" e/o "taglia & incollatori". Prima di scrivere una singola riga sulle Politiche e Procedure specifiche di un'impresa, un consulente assillerà e vorrà dettagli sulla missione ed organizzazione della stessa, sui budget, sulle tecnologie in uso attualmente ed in prospettiva e su tanto altro. Se non lo fa, bisogna cambiare consulente!

Differenza fra politiche e procedure

Per convenzione le politiche dettano obiettivi e politiche aziendali di tipo generale e da esse derivano delle procedure via via più di dettaglio, da quelle organizzative a quelle tecniche. A volte è difficile distinguere una Politica da una Procedura a causa del confine sfumato fra le due tipologie di strumenti.

Un buon criterio per distinguere le due è la sua durata nel tempo: meno frequenti sono le revisioni o gli aggiustamenti in funzione delle evoluzioni tecnologiche, meno è una Procedura e più è una Politica e viceversa. Una buona Politica può durare decenni senza revisioni, tranne che cambi la missione, natura o dimensione dell'azienda oppure la legislazione di riferimento.
Una politica o una procedura di tipo organizzativo dura molti anni, tranne che non si riorganizzi l'azienda; una procedura tecnica dura tanto quanto dura la relativa tecnologia in azienda.

Politiche e procedure (non documenti con scritte le politiche e le procedure)

Si ribadisce che i "documenti" su cui sono scritte le politiche e le procedure sono solo dei contenitori.
Avere delle politiche e procedure significa che:

- quello che è scritto nei documenti che contengono le politiche e le procedure sia applicabile ed applicato;
- sia noto a tutti in azienda sia in fase di prima stesura che in seguito in caso di revisioni;
- sia definito un budget per applicare quanto stabilito; questo fattore troppo spesso è sottostimato se non dimenticato;
- sia supportato da tutto il top management dell'azienda;
- i risultati siano controllati ed eventualmente si revisioni quel che non funziona o funziona male.

Non esiste un "insieme minimo" di politiche e sicurezza; dipende molto dalla natura della singola azienda.

Come linea guida si può considerare questo insieme:

- politiche generali, comprendenti obiettivi strategici, budget e norme di riferimento;
- politiche specifiche relativamente a: privacy, gestione accessi, uso corretto degli strumenti aziendali, continuità operativa (*business continuity*), gestione incidenti;
- procedure relative a: monitoraggio dei dispositivi, salvataggio e ripristino, ripristino da disastro (*Disaster Recovery*) rapporti con mezzi di comunicazione, autorità, clienti e fornitori.

Se l'azienda sviluppa o integra software o fornisce servizi ICT bisogna considerare l'opportunità di avere politiche e procedure specifiche relativamente alla sicurezza della progettazione (*security by design*).

Esempio di gerarchia delle politiche e delle procedure

La Politica Generale per la Sicurezza fissa obiettivi e politiche aziendali di tipo strategico che riguardano tutti in tutta l'azienda come, ad esempio:

- cosa i collaboratori possono e non possono fare con gli strumenti aziendali, quali stazioni di lavoro, rete, ecc.;
- la percentuale di budget aziendale riservato alla sicurezza rispetto al budget ICT o a quello complessivo;
- i principi di responsabilità individuale, come, ad esempio, se si vuole o meno che sia dovere di tutti riportare gli incidenti;
- i criteri di sicurezza e conformità con cui scegliere i propri fornitori, le tecnologie ed i relativi strumenti di gestione;
- le norme di riferimento, siano esse di legge, internazionali (ISO), di settore, o migliori pratiche (*best practice*).

Dalla Politica Generale derivano le Politiche più specifiche quali, per esempio:

- **Politica sulla Continuità Operativa (*Business Continuity*), da cui derivano, a cascata, la Politica Procedura di Recupero dal Disastro (*Disaster Recovery*) e la Procedura di Salvataggio e Ripristino (*Backup e Restore*);**
- **Politica sulla Gestione degli Accessi, da cui derivano la Procedura di Controllo Accessi e la Procedura di Monitoraggio.**

La Politica sulla Continuità Operativa (*Business Continuity*) fissa obiettivi e politiche per la specifica area quali:

- gli obiettivi di budget,
- gli obblighi derivanti da eventuali norme di legge, internazionali (ISO) o di riferimento per il settore,
- le indicazioni strategiche con cui s'intende ottenere la Continuità Operativa tramite, per esempio:
  - ridondanza fra diverse sedi,
  - accordo di mutuo soccorso con altri,
  - servizi offerti da un provider quali quelli di tipo "*As A Service*";
- gli obiettivi di recupero della operatività in caso di incidente bloccante, definiti in funzione delle esigenze aziendali o dei dettami del settore ed espressi in termini di 1 ora, 1 giorno, 1 settimana e non in termini di "al più presto" e/o "al meglio", che non costituiscono un criterio!

La Politica/Procedura di Recupero dal Disastro (*Disaster Recovery*) è un prerequisito per la Continuità Operativa; essa:

- deve essere congrua e coerente con la Politica sulla Continuità Operativa;
- a seconda di come è impostata, può essere considerata politica o procedura o qualunque scala di grigi fra le due.

La procedura di Salvataggio e Ripristino (*Backup e Restore*) costituisce un prerequisito per il Recupero dal Disastro (Disaster Recovery); essa:

- è molto tecnica e molto legata alle tecnologie scelte;
- è sicuramente una procedura e non una politica!

La Politica sulla Gestione degli Accessi fissa obiettivi e politiche nella specifica area della Gestione Accessi quali, per esempio:

- i criteri generali con cui si gestiscono (creano, modificano, sospendono, cancellano) gli accessi dei collaboratori ai sistemi;
- se, come, con quale frequenza e dettaglio gli accessi sono controllati e da chi.

La Procedura di Controllo Accessi è un prerequisito per la Gestione Accessi; essa non è solo tecnica e non riguarda solo l'ICT; infatti se l'obiettivo è chiudere un account in dieci minuti dalle dimissioni di un collaboratore o dalla chiusura di un contratto, bisogna coinvolgere l'Ufficio del Personale o l'Ufficio Acquisti; inoltre un sistemista deve sapere che un account è da chiudere per poterlo chiudere: banale? No!

La Procedura di Monitoraggio costituisce un altro prerequisito della Gestione Accessi e anche della Gestione Incidenti; essa è in parte tecnica ed in parte legale e, pertanto riguarda sia l'ICT che l'ufficio legale. Questa procedura stabilisce come raggiungere gli obiettivi dettati dalla politica per la "Gestione Accessi".

3.16 Gestione degli *outsourcer*: contratti e Service Level Agreement

La sicurezza nei contratti e SLA

Una questione cardinale della sicurezza è stabilire con chiarezza "chi fa cosa", perché, su cosa, come, dove, sotto la responsabilità di chi. Al vostro interno ciò è stabilito dalle proprie "Politiche e Procedure". Verso gli acquirenti di beni o servizi dall'esterno *(outsourcer)* e più in generale verso ogni tipologia di cliente, fornitore o partner lo strumento principe per stabilire "chi fa cosa" è il contratto e/o gli "Accordi sui Livelli di Servizio" (*Service Level Agreement o SLA*).
È una scelta aziendale decidere se contratto e SLA sono contenuti nello stesso documento o sono contenuti in due documenti separati, di cui lo SLA è un allegato al contratto. Ci sono buone ragioni per scegliere l'una o l'altra strada. Dipende da troppi fattori per propendere verso una soluzione piuttosto che l'altra: abitudini commerciali, organizzazione, dinamicità della tecnologia che sottende il contratto; se il contratto ha un ciclo di vita lungo e lo SLA un ciclo di vita corto, potrebbe essere conveniente averli in due documenti separati. Ai fini della sicurezza una soluzione vale l'altra.

Scopo e natura dei contratti e SLA nel contesto Sicurezza/Conformità

Come già detto delle Politiche e Procedure, i documenti materiali od immateriali su cui sono scritti Contratti e SLA sono solo contenitori. Il loro principale scopo è definire chi è responsabile di "fare cosa". È assolutamente importante che nei contratti e negli accordi di servizio (*SLA*) i compiti, i doveri e le responsabilità di ognuna delle parti siano ben definiti e chiari a tutti gli interessati. Questa chiarezza deve essere evidente da subito, non quando ci sarà da gestire un incidente e si perderà più tempo a discutere di "chi deve fare cosa" invece che farla o, peggio, si perderà tempo a cercare il colpevole invece della soluzione!

Caveat emptor (il compratore stia attento!)

I clienti devono fare attenzione a quello che i fornitori sono disposti a firmare pur di aggiudicarsi il contratto! E viceversa i fornitori a quanto i clienti sono disposti a "tirarli per il collo" pur di scaricare su di loro responsabilità al minor prezzo possibile.
Deve esserci una reciproca onestà intellettuale fra le parti o i contratti e gli Accordi di Servizio rimangono pezzi di carta da esibire in occasione di qualche litigio, senza generare alcun valore aggiunto in termini di sicurezza e conformità.

Nei contratti e/o negli accordi (*SLA*):

- bisogna stabilire **obiettivi raggiungibili**, che il cliente può permettersi per budget e per natura dell'Azienda e che il fornitore è in grado tecnologicamente ed organizzativamente di fornire ad un **prezzo giusto**;
- il Fornitore deve fissare gli strumenti (organizzativi e tecnologici) con cui **raggiungere gli obiettivi** stabiliti o, in altre parole, come fornirà al cliente quanto promesso;
- il Cliente deve definire come, da chi e riportando a chi sarà **verificato il raggiungimento** degli obiettivi stabiliti.

Di norma è il cliente o una terza parte da questi incaricata che dovrà verificare e non il fornitore stesso.

Chi definisce contratti e accordi (SLA)

Se il contratto in senso stretto è quasi esclusivamente una questione commerciale e tecnico-legale, la componente SLA richiede la partecipazione dei rispettivi reparti tecnici: in tal modo il Cliente può fare al Fornitore le domande giuste ed il Fornitore può dare al Cliente risposte oneste. I rapporti di forza fra le parti giocano un grande ruolo; se tali rapporti sono molto sbilanciati, si corre il rischio che il "grande e grosso" detti contratto e accordi (SLA) ed il "piccolo" li subisca, ma non dovrebbe essere così, soprattutto nel caso di accordi relativi alla sicurezza. Non conviene neanche al "grande e grosso", perché si potrebbe ritrovare un contratto o accordo ben formalizzati, ma con obiettivi difficilmente raggiungibili.

Contratti e accordi (*SLA*) non trasferiscono la responsabilità ultima di un trattamento dati

Il titolare di un trattamento di dati rimane in ultima istanza colui che è tenuto a rendere conto di ciò che fa con i dati davanti alla Legge. Poco importa che attraverso contratti e/o accordi alcune funzioni di sicurezza e conformità siano state delegate all'esterno.
Esempio: Mario Bianchi ha un contratto con Giorgio Venti anche "in senso lato", per esempio ha acquistato una qualunque cosa e ha consegnato i propri dati personali a Giorgio Venti. Se Bianchi contesta qualcosa, Venti non può rispondergli "rivolgiti al nostro fornitore esterno (*outsourcer*) X "Mario Bianchi il contratto (de jure o de facto poco importa) ce l'ha con Giorgio Venti e a quest'ultimo chiede conto di quel che è stato fatto coi suoi dati personali. Che poi Venti voglia chiedere spiegazioni o rifarsi sul suo fornitore esterno (*outsourcer*) X questo è un problema di Venti, non di Mario Bianchi.
Per questo principale motivo abbiamo scritto prima:
"il Cliente deve definire come, da chi e riportando a chi sarà verificato il raggiungimento degli obiettivi stabiliti".
È fortemente auspicabile che la verifica sia periodica e sistemica, per intercettare un, anche solo potenziale, incidente prima che possa fare danni, invece che a danno compiuto (*v. anche "Gestione Incidenti"*).
Per arrivare a questo risultato serve una Politica specifica. A seconda della dimensione e natura dell'azienda, la verifica periodica degli obiettivi di contratti e/o accordi può stare altrettanto bene nella "Politica Generale" o in una "Politica specifica" (v. par. su "Politica e Procedure").

Esempio di SLA relativo alla raccolta di eventi di log "*As A Service*"

Nel par. "Creazione e gestione della rete locale e *wireless* in sicurezza", abbiamo discusso dell'opzione di raccogliere i *log* generati dai sistemi e dispositivi della propria rete in modalità "servizio" ("*As A Service*"). Perché è un lavoro molto specialistico, complicato, tedioso, insidioso, da cui in Azienda molti, di solito, vorranno star ben lontani.
In questo esempio, la raccolta dei *log* è circoscritta ad una precisa sotto-casistica: i *log* degli Amministratori di Sistema, ma la struttura non cambierebbe se lo SLA riguardasse tutti i *log* (o anche un altro servizio). Notare come sia ben chiaro cosa il Fornitore stia promettendo, in quali tempi, *su cosa*, rispetto a quali norme, dove, autorizzato da chi e verso chi. E viceversa notare come sia chiaramente definito cosa rimane sotto la responsabilità del Cliente ed infine come siano chiarite le norme di riferimento per entrambi. **Un lavoraccio? Sì. Ma a lungo termine paga**.

Il Fornitore si prende carico di:

1. la acquisizione, installazione, gestione ed amministrazione degli strumenti (tool) tecnologic (hardware e software) necessari alla raccolta dei log dai sistemi del Cliente (i collettori);
2. il riconoscimento degli eventi di *log* rilevanti rispetto al Provvedimento del Garante della Privacy sugli Amministratori di Sistema, ovvero *logon*, *logoff* o *logfail* di un Amministratore (come definito nel Provvedimento), fino ad un massimo di X.XXX sistemi;
3. l'archiviazione a norma degli eventi di log di cui al punto 2: per 185 giorni, in almeno due sedi distanti fra loro non meno di 120 Km in linea d'aria; ogni evento sarà firmato elettronicamente dal Legale Rappresentante Z del Fornitore;
4. l'estrazione e messa a disposizione di tali eventi a chi ne abbia diritto o dovere in N ore lavorative dalla lecita richiesta de:
   - il Cliente stesso, attraverso i contatti di riferimento: X, Y e Z;
   - una autorità giudiziaria che abbia giurisdizione e titolo per fare tale richiesta;
   - chiunque sia stato autorizzato preventivamente dal Cliente (autorità di riferimento del Cliente: Direttori X e/o W);
5. 5.la difesa in ogni sede giudiziaria della integrità dei log archiviati e poi estratti nell'ambito delle Province di J e Q e presso il Garante;
6. la fornitura trimestrale, o dietro semplice ed informale richiesta del Cliente, di statistiche di servizio;
7. l'accettazione della nomina a Responsabile di questo Trattamento a tutti gli effetti del TU Privacy (successivamente del GDPR);
8. la garanzia di mantenere la riservatezza dei dati (personali e non) del Cliente anche successivamente alla conclusione del Servizio.

Il Cliente si prende carico di:

- fornire gli spazi tecnologici, l'energia ed i servizi di rete ed ambientali necessari agli strumenti tecnologici (collettori);
- fornire accesso ai locali tecnologici contenenti i collettori, entro X ore in orario lavorativo e Y ore in orario notturno o festivo, dietro semplice ed informale richiesta telefonica del Fornitore al supporto SSS raggiungibile H24 telefonicamente al 800-xxx-xxxxx;
- generare gli eventi di log presso i sistemi sorgente dal Cliente stesso amministrati, secondo le indicazioni tecniche del Fornitore.

Norme di riferimento per entrambe le parti (accessibili e note a Cliente e Fornitore):

1. del Cliente: "Politica di sicurezza generale" n. X , "Politica di accesso ai locali tecnologici" n. Y e "Politica di monitoraggio" n. Z;
2. del Fornitore: "Politica di amministrazione remota" n. J, "Politica e procedure di salvataggio e ripristino" n. S;
3. il Provvedimento del Garante della Privacy sugli Amministratori di Sistema;
4. le norme di Pubblica Sicurezza alla data e loro future modifiche e/o integrazioni per la durata del contratto;
5. l'attuale Testo Unico sulla Privacy e, a far data dal 25-05-2018, il Regolamento Europeo sulla Protezione dei Dati (GDPR).

3.17 Sicurezza ICT ed impianti primari

Vista la fragilità intrinseca delle attrezzature elettroniche che gestiscono i nostri dati, resta da stabilire quali possono essere le criticità e quali sono le procedure o le contromisure da utilizzare per aver cura e mettere in sicurezza l'hardware presente nei nostri uffici e di conseguenza i dati.

Interruzioni e disturbi elettrici

Non date per scontata la continua e regolare erogazione di energia elettrica! Senza energia elettrica tutti i vostri apparati tecnologici diventano inutili pezzi d'arredamento... senza energia non c'è nulla che trovate in questo vademecum o altrove che possiate fare.
La fornitura standard d'energia può subire momentanei sbalzi di tensione ben oltre i limiti di tolleranza, micro interruzioni per pochi millisecondi o secondi, interruzioni (blackout) di minuti od ore. Capita più spesso di quel che pensate. Anche quando passano inosservati, sono fra le principali cause di guasti hardware e corruzione o perdita di dati. A differenza di altri apparati elettrici, gli apparati informatici al ritorno dell'energia possono non riaccendersi, se si riaccendono non c'è garanzia che ripartano, se ripartono non è detto che tutti i dati siano ancora integri o disponibili.
Il principale danno è economico e produttivo. Mentre aspettate il ritorno dell'energia non lavorate. Alla ripartenza (quando e se ripartono...) dei sistemi, potrebbe servire l'intervento dei sistemisti per recuperare i dati (se recuperabili...).
La principale soluzione alle minacce di sbalzi di tensione e micro o macro interruzioni elettriche sono gli UPS (Uninterruptable Power Supply o Gruppi di Continuità). Hanno due funzioni: "puliscono" l'energia elettrica dalle micro interruzioni e sbalzi di tensione ed in caso di blackout forniscono energia elettrica per un periodo massimo che, a seconda dei modelli, va dai 10 minuti a molte ore.
Mettete l'energia elettrica in cima alla vostra lista di priorità, da essa dipende tutto il resto. Mettete sotto continituà elettrica tutti gli apparati della vostra rete (PC, server, dischi di rete, router, switch, ecc.). Se un solo anello della catena non funziona perché spento, guasto o corrotto, tutti gli altri dispositivi saranno si accesi, ma comunque inutili... Gli UPS vi servono. Non è questione di "se", ma di "come" e "quanto".
Quanta autonomia vi serve in caso di blackout? Dipende da due fattori: (a) la natura ed il settore d'attività della vostra Azienda e (b) se se siete o meno in zona storicamente (o per natura) soggetta a blackout prolungati. Se la risposta è superiore alle otto ore dovreste considerare di **affiancare** agli UPS i "gruppi elettrogeni" (argomento qui non approfondito). Gli UPS gestiscono sbalzi di tensione

e interruzioni elettriche fino ad un certo numero di ore, poi diventano anti-economici, i gruppi elettrogeni vi garantiscono elettricità per ore o giorni o settimane, ma ci mettono tempo a partire quindi servono comunque gli UPS per gestire sbalzi e micro interruzioni ed i primi minuti di blackout.
Affidatevi al vostro elettricista di fiducia per: (a) calcolare la potenza complessiva del o degli UPS che vi occorrono rispetto al tempo d'autonomia che avete stabilito, (b) decidere se è preferibile un unico UPS centralizzato o più distribuiti e se vi serve un gruppo elettrogeno, (c) la manutenzione periodica degli UPS e delle batterie in essi contenuti, batterie che non durano in eterno!
Affidatevi al vostro sistemista di fiducia affinché UPS e sistemi "si parlino": (a) i sistemi **devono** sapere che c'è un blackout, ognuno per comportarsi di conseguenza a seconda della propria natura, in modo di ripartire al ritorno dell'energia in modo "pulito" senza perdita o corruzione di dati.
UPS (ed eventualmente Gruppi di Continuità) sono le principali soluzioni. Chiedete al vostro elettricista di fiducia se siano opportune altre contromisure, qui non approfondite, quali: scaricatori, differenziali, trasformatori di isolamento o altro.

Temperatura e manutenzione

La temperatura è un altro fattore di rischio, poiché tutte le attrezzature elettroniche hanno un intervallo (*range*) termico nel quale funzionano correttamente e fuori del quale funzionano male o, addirittura, si rompono.
Ne consegue che, soprattutto nel caso dei server o dei NAS, che per loro struttura ed utilizzo non vengono mai spenti, è importante che gli spazi dedicati a queste attrezzature siano arieggiati e che la temperatura non sia mai troppo elevata o troppo bassa (in genere questi valori di escursione termica sono presenti sui manuali tecnici e vanno solitamente dai 10 ai 40 gradi Celsius).
In effetti i computer, i server, i NAS e le attrezzature varie usano un sistema di raffreddamento propriamente detto a "ventilazione forzata", il quale prevede una ventola anteriore che aspira l'aria fresca all'interno del telaio ed un'altra ventola posteriore che espelle l'aria calda; in tal modo i dischi fissi e l'elettronica non raggiungono mai temperature elevate.
Risulta ovvio che assume un'importanza vitale non solo il condizionamento dell'aria ma anche la manutenzione di queste ventole e delle griglie anteriori e posteriori, che, se bloccate da polvere ed impurità, impediscono la libera circolazione dell'aria.

Luoghi e posizione dei PC e supporti di memorizzazione esterni

Il posizionamento dei computer, dei supporti di memorizzazione esterni o dei server è estremamente importante per prevenire eventuali perdite di dati e fermo lavorativo. Luoghi ben arieggiati, asciutti e climatizzati sono quanto di meglio si può fare per aumentare la sicurezza e la durata delle attrezzature informatiche.
Nel caso in cui fossero presenti dati sensibili o dove la responsabilità dei dati avesse un valore estremamente alto, è assolutamente consigliabile destinare degli spazi dedicati e ad accesso controllato, nei quali applicare sensori di calore, climatizzatori ed in ultima analisi anche sistemi di rilevamento delle fiamme.

Manutenzione preventiva

Una cosa da tener ben presente è che oggi quasi tutte le attività dipendono strettamente dall'uso dei computer e delle relative attrezzature; in molti casi esso rappresenta lo strumento principale per ottemperare alle proprie mansioni o svolgere il proprio lavoro.
Così come un elettricista deve verificare il trapano elettrico, onde evitare di non poter svolgere il proprio lavoro, il contadino di aver effettuato il pieno al trattore ed affilato le lame dell'aratro, parimenti noi dobbiamo preoccuparci preventivamente di manutenere i nostri dispositivi; oltre al discorso già affrontato delle ventole, è possibile verificare con test specifici lo stato di salute dei dischi, delle schede e dei sistemi di copia dei dati (*backup*) etc.
Affidarsi a tecnici specializzati per fare controlli preventivi sullo stato di salute dei supporti o delle attrezzature, adottare delle politiche di controllo "visivo" e non sottovalutare rumori o informazioni di avviso (*alert*) che i vari sistemi ci inviano, è sicuramente il miglior modo per proteggere i nostri dati.

3.18 Gestione degli incidenti

Definizione di incidente

In questo contesto "sistema" è qualunque apparato hardware o software (firewall, server, pc, disco di rete, database, applicazione, ecc.) ed "incidente" qualunque evento anomalo che abbia il potenziale di impattare o davvero impatti la confidenzialità, integrità o disponibilità di:

- informazioni dell'azienda propria o altrui (per esempio di Clienti) custodite sotto la responsabilità della propria azienda,
- di sistemi propri o altrui sotto la propria responsabilità.

Non serve un danno per avere un incidente.

Anzi, è auspicabile che l'azienda si organizzi per rilevare e gestire gli incidenti al loro insorgere e, nella maggior parte dei casi, fermarli molto prima che provochino danni! Ma questo non sarà sempre possibile. Per quanto bravi si possa essere (fornitori compresi!) bisogna organizzarsi per gestire due tipologie di incidenti:

- incidenti in grado di provocare un danno: l'obiettivo sarà gestirli e fermarli prima che provochino il danno;
- incidenti che hanno già provocato un danno: l'obiettivo sarà mitigare il danno e gestirne al meglio le conseguenze.

Monitoraggio!

Difficile, ma non impossibile.
Se si verifica il furto di una bicicletta, prima o poi il proprietario si accorgerà di non avere più la bicicletta. Se viene forzata una serratura, prima o poi la vittima si accorgerà che essa è stata forzata. Questa logica non vale nel caso delle informazioni e delle reti. Dopo un furto di dati i dati sono ancora in possesso del legittimo proprietario! Dopo la forzatura di una porta di un *firewall* o di un sistema non c'è nulla che lasci traccia di ciò. Se invece l'attacco aveva il solo scopo di distruggere i dati e/o i sistemi (caso ormai raro) o per qualche forma di *ransomware*, allora si viene certamente a sapere dell'incidente… ma solo a danno compiuto!

Per accorgersi di un incidente, possibilmente **prima** che faccia danni, serve il monitoraggio.
Esso non complica più di tanto la gestione dei sistemi, costa meno di quel che si pensi ed è l'unica soluzione a tre questioni legali cardinali:

- provare chi e quando ha tentato o ha fatto il danno, in modo da poterlo perseguire legalmente;
- provare chi e quando ha tentato o ha fatto il danno, per difendersi dall'eventuale accusa di danni provocati a terzi (inversione dell'onere della prova!);
- provare chi e quando ha tentato di perpetrare il danno per poter rilevare incidenti **prima** che accadano o **dopo**.

Il GDPR prevede l'obbligo di dare comunicazione di un incidente (con danni), per farlo ci si deve accorgere che c'è stato!

Politiche e procedure

È una questione parzialmente tecnica e molto organizzativa.
Da un punto di vista tecnico bisogna dotarsi di sistemi di monitoraggio, *backup*, sistemi duplicati (*mirror*) e procedure di recupero (*restore*: il contrario del *backup*) affidabili; infatti troppe volte capita di non riuscire, in tutto od in parte, a recuperare dati da supporti di *backup* (dvd, cdrom, nastri, dischi di rete) perfetti, nel senso che contengono i dati e sono leggibili, ma da cui non era mai stato provato una volta a fare il recupero dei dati. Almeno una volta l'anno si deve provare un recupero per verificare che funzioni. Ci sono decine di buoni motivi perché non funzioni nonostante il supporto di *backup* contenga i dati e sia leggibile!

Fra i motivi principali:

- la compatibilità dei file system di sistemi diversi quali Microsoft, Linux, IOS, Apple, ecc.;
- essersi dimenticati di fare il *backup* di qualche file di sistema necessario a riportare il sistema allo stato precedente;
- aver fatto il *backup* di qualche file già corrotto, la cui versione corretta è già andata perduta perché non più presente nei *backup* disponibili.

Da un punto di vista organizzativo bisogna dotarsi di una politica e delle relative procedure in cui sia chiaro a tutti in azienda cosa fare (e non fare!) in caso di incidente. Soprattutto nel caso di incidenti che abbiano già provocato danni, troppe volte l'emozione, la paura, lo sconforto o la rabbia hanno il sopravvento.
Politiche e procedure ben scritte non cancellano queste emozioni, ma almeno le controllano prima che qualcuno faccia troppo poco o nulla o, assai peggio, faccia in totale buona fede troppo o quel che non è qualificato a fare.
Punti cardinali della vostra politica e relative procedure devono essere:

- dotarsi di criteri per classificare gli incidenti per importanza e per urgenza di soluzione; di norma prima si gestiscono gli incidenti urgenti ed importanti, poi quelli urgenti ed infine quelli importanti;
- definire chi gestisce le questioni tecniche, chi parla col legale, chi con la stampa, chi coi fornitori/clienti, chi non fa nulla;
- effettuare una esercitazione almeno una volta all'anno, facendo finta d'aver subito un incidente e verificando che le procedure funzionino; se qualcosa non funziona, bisogna capirne la ragione e, se del caso, revisionare le politiche e le procedure.

Tabella 19

RESPONSABILITÀ, POLITICHE E PROCEDURE DI GESTIONE DEGLI INCIDENTI

Problema	***Soluzione***
Responsabilità	***Politiche e procedure di gestione degli incidenti***
• L'azienda è responsabile: ▪ dei propri dati e sistemi, ▪ dei dati e sistemi sotto la sua custodia. • Non essere coscienti d'aver subito un incidente non sposta la propria responsabilità, anzi la peggiora* ▪ ancor di più se genera danni a terzi che potrebbero (quindi lo faranno) chiederne conto! • Il GDPR prevede che sia una responsabilità della propria azienda rivelare pubblicamente (*fare outing*) alcune tipologie: ▪ di incidenti, ▪ di dati coinvolti, ▪ di settore d'attività. *inversione dell'onere della prova (TU Privacy e art. 2050 del C.C. oggi, GDPR/Regolamento EU domani)	• Gestire gli incidenti: ▪ è prima di tutto un proprio interesse, poi un proprio dovere; ▪ è documentare tutto, perché l'onere della prova è a proprio carico! • Per gestire con efficacia ed efficienza gli incidenti occorrono adeguata politica e relative procedure: ▪ personalizzate sulla proprie realtà (niente copia & incolla!); ▪ che stabiliscano con assoluta chiarezza: ▪ chi non fa nulla! ▪ gli strumenti tecnologici e organizzativi in uso; ▪ i criteri per la classificazione degli incidenti; ▪ i criteri di gestione in base a tale classificazione. ▪ Gli incidenti si classificano principalmente in due macro categorie: ▪ quelli che potenzialmente potrebbero provocare danni: ▪ vanno individuati e fermati prima che lo facciano; ▪ quelli che hanno già provocato danni, per i quali bisogna minimizzare le conseguenze: ▪ tecniche; ▪ legali, ▪ commerciali (contrattuali), ▪ di immagine, ▪ economiche. • Per entrambe le categorie vanno ripristinati sistemi, dati o informazioni allo stato precedente all'incidente (v. oltre).

Gli incidenti sono silenziosi

- I dati propri o sotto la propria custodia possono essere:
  - danneggiati,
  - copiati,
  - cancellati,
  - alterati,
  - intercettati

senza rendersene mai conto, o rendendosene conto a danno compiuto!

Monitoraggio *(v. anche par. su Rete Locale):*

- A tutti i livelli:
  - rete, sistemi, banche dati, applicazioni, dispositivi di rete;
- in tutte le direzioni (non tutti i problemi vengono da fuori):
  - da fuori a dentro (Internet → sistemi propri),
  - da dentro a dentro (fra i propri sistemi);
- il monitoraggio costa, ma meno di quel che si pensi;
  - ci sono molti strumenti di pubblico dominio (*open source*);
  - rimane la questione delle persone dietro gli strumenti:
    - possono essere propri dipendenti o collaboratori,
    - si possono acquisire strumenti e monitoraggio come servizio (*As a Service*).

Minimizzazione delle conseguenze

A valere in caso di:

- incidente potenzialmente dannoso da fermare prima che faccia danno;
- incidente con danni e conseguenze da minimizzare;
- in entrambi i casi occorre documentare tutto perché:
  - incidente potenzialmente dannoso da fermare prima che faccia danno;
  - bisogna essere in grado di documentare:
    - come ci si è organizzati;
    - cosa si è effettivamente fatto.

Ripristino allo stato precedente di sistemi e dati

Servono politiche e procedure di salvataggio e ripristino (*backup* e *restore*) che:

- comprendano la configurazione dei sistemi;
- funzionino (non solo i salvataggi, ma anche i ripristini);
- siano per quanto possibile automatiche (o non si fanno);
- non salvino dati danneggiati o corrotti;
- mantengano uno storico di almeno tre mesi (meglio sei);
- portino ad un punto di ripristino il più vicino possibile nel tempo rispetto al momento dell'incidente.

Servono trasparenza ed elasticità, per cui:

- se c'è qualcosa da denunciare all'autorità, va fatto;
- se c'è qualcosa da contestare a chicchessia, va fatto;
- se si è stati bravi a gestire un incidente non bisogna farne mistero:
  - il GDPR potrebbe comunque obbligare a rivelare pubblicamente (fare *outing*);
  - tanto vale farne una opportunità di comunicazione/marketing;
- si devono eseguire dei test almeno annuali, meglio se semestrali;
- si deve verificare che quanto pianificato funzioni o cambiarlo.

3.19 Garanzia della disponibilità delle informazioni

Al giorno d'oggi le aziende lavorano con informazioni digitali: tutto è memorizzato nei computer e nella rete; se le applicazioni per accedere a queste informazioni, per qualsiasi ragione, non sono disponibili l'azienda si ferma e non riesce più a lavorare.
Non si tratta di una possibilità remota: attacchi informatici, incidenti o errori umani possono mandare in fumo il lavoro di anni. Ecco quali sono i possibili scenari in caso di server fermi che non riescono a ripartire:

- l'azienda, pur essendo ferma, continua a pagare il personale anche se non lavora;
- non appena il sistema informatico riparte è necessario "rimettersi in pari" per recuperare il lavoro perso;
- se, durante il fermo, non si riesce a soddisfare la clientela, qualcuno potrebbe anche decidere di cambiare fornitore.

Per garantire quindi un "fermo aziendale" il più basso possibile, occorre adottare procedure, programmi e metodologie ben collaudate, che consentono di avere una continuità lavorativa ed una eventuale ripresa "post-fermo aziendale" la più rapida possibile.
Per garantire tutto ciò, occorre:

α buona assistenza o competenza informatica;

β software antivirus e anti-malware che prevengono eventuali attacchi da virus;

χ sistemi di controllo degli accessi o firewall, che non consentano l'accesso ad estranei alle informazioni

δ un sistema di copie di sicurezza (*backup*) differenziato, ovvero: giornaliero, settimanale e mensile, in modo da riuscire a recuperare sempre la copia più recente ed evitare di rifare il lavoro già svolto;

ε una corretta politica formativa ed informativa, che istruisca gli utilizzatori alla gestione del dato e all'effettuazione delle copie di sicurezza della propria postazione di lavoro;

ϕ una corretta politica di controllo delle copie di sicurezza; non di rado ci si accorge troppo tardi, che **non** si è fatto il *backup* di qualcosa di molto importante.

Per quanto riguarda il *backup*, le attuali soluzioni prevedono di effettuare le copie sia "in casa" che in *cloud*.
Le copie in "casa" si effettuano più velocemente e richiedono meno tempo nel ripristino dei sistemi in caso di indisponibilità dei dati. Va tenuto presente, però, che sono soggette alla stessa criticità delle altre infrastrutture informatiche in caso di furto, allagamento o incendio e possono essere "attaccate" come un qualsiasi computer, se non sono state correttamente configurate le politiche di accesso.
Le copie in cloud, forniscono maggiore garanzia dal punto di vista di mantenimento del dato, in quanto vengono mantenute da strutture (*Web Farm*) che ne garantiscono la disponibilità continua, salvaguardando il dato in caso di furti, incendi o allagamenti. Dal punto di vista del *backup*, necessitano di un buono e stabile collegamento internet, pena l'interruzione del *backup* e ovviamente, un tempo di ripristino più lento, in quanto i dati devono sempre e comunque transitare attraverso una linea internet.

3.20 Formazione e sensibilizzazione degli utenti

Una delle minacce più grandi per la sicurezza delle reti aziendali è rappresentata dagli stessi utenti che ne fanno parte.
Per questo motivo la sicurezza informatica (*cyber security*) non può essere delegata solo a chi si occupa di strategie di difesa.
E' importate sviluppare le capacità di risposta alle minacce, in modo da sviluppare cultura della sicurezza in ambito informatico.
La consapevolezza è un passo avanti rispetto alla conoscenza, si possono conoscere i rischi ma non per questo possiamo esserne consapevoli.

Occorre integrare conoscenza con esperienza, attraverso metodologie interattive. Coinvolgendo figure professionali con esperienza nel campo è possibile progettare degli interventi didattici per far comprendere gli impatti di un attacco informatico e la perdita di dati.
Sia a livello europeo che italiano sempre più si sottolinea l'importanza del ruolo della sensibilizzazione e della formazione su queste tematiche in continua evoluzione.

Il decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013 individua gli indirizzi operativi e le linee d'azione per la sicurezza informatica nazionale:

http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

Un programma di sensibilizzazione deve seguire un percorso che valorizzi il ruolo attivo di ciascun individuo nella protezione della sicurezza aziendale, in modo da definire un comportamento comune sul tema.
Una possibile proposta deve seguire gli obblighi dettati dal DL 193/03 vertendo principalmente sui tre aspetti:

- sicurezza, riservatezza, disponibilità e integrità dei dati,
- responsabilità per danni derivanti dall'accesso abusivo a sistemi informatici,
- furto di informazioni.

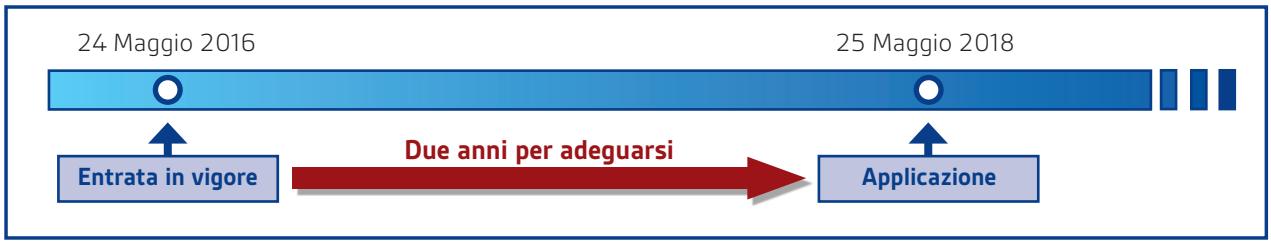
Capitolo 4

LE NORME vigenti in materia

4.1 Il Regolamento Europeo sulla Protezione dei Dati

Il Regolamento Generale sulla Protezione dei Dati Personali UE 679/2016 (*General Data Protection Regulation - GDPR*) ha l'obiettivo di tutelare i dati personali delle persone fisiche.

Il Regolamento è entrato in vigore il 24 maggio 2016; le aziende avranno tempo fino al 25 maggio 2018 per adeguarsi, data di effettiva applicazione del GDPR.



Sono tenuti a rispettare i requisiti imposti dal Regolamento: i Titolari del trattamento, ovvero le aziende che trattano dati personali dei propri dipendenti, clienti, fornitori, collaboratori, etc.

I principali adempimenti previsti dal Regolamento sono:

- aggiornamento delle informative e raccolta dei consensi per il trattamento dei dati personali, ove necessari;
- regolamentazione dei rapporti tramite nomina e/o contratto con i Responsabili del trattamento che trattano dati personali per conto del Titolare;
- nomina di un "Responsabile per la Protezione dei Dati" (*Data Protection Officer - DPO*) nei casi previsti dal Regolamento;
- valutazione d'impatto quando un trattamento comporta rischi per i diritti e le libertà degli interessati;
- adozione di misure di sicurezza adeguate al trattamento, alle finalità, ai costi di attuazione e ai rischi individuati;
- predisposizione del Registro delle attività di trattamento;
- rispetto dei principi di "protezione dei dati personali già dalla fase di progettazione" (*privacy by design*) e "raccolta e trattamento per difetto solo dei dati necessari alle finalità" (*privacy by default*).
- obbligo di notifica all'Autorità Garante e ai soggetti interessati, nei casi più a rischio, qualora si verifichi una violazione dei dati personali (*data breach*).

4.2 La legge sui cookie (*cookie law*)

I *cookie* sono piccoli file di testo che i siti visitati inviano al terminale (Computer, Tablet, Smartphone, Notebook) dell'utente, dove vengono memorizzati per raccogliere una serie di informazioni.
Possono essere:

- tecnici, se necessari per il funzionamento del sito;
  analitici, quando raccolgono informazioni sulle visite;
  di profilazione (*tracking cookie*), quando monitorano la navigazione dell'utente e raccolgono informazioni sui suoi gusti e abitudini di consumo per riproporre messaggi pubblicitari mirati.

Si distinguono ulteriormente in:

- *cookie* di prima parte, se installati direttamente dal sito stesso;
- *cookie* di terza parte, se installati da siti di terzi proprietari dei *cookie* (ad esempio quando un sito internet ospita annunci pubblicitari di terzi che registrano i click degli utenti).

Il provvedimento del Garante in materia di *cookie* dell'8 maggio 2014 individua le modalità per l'informativa e per l'acquisizione del consenso:

- banner informativo, appena si accede alla prima pagina (*homepage*) o ad altra pagina, contenente le informazioni principali sulle tipologie di cookie utilizzate e le modalità per acconsentire o negare il loro utilizzo;
- raccolta del consenso mediante azione volontaria dell'utente per il superamento del banner;
- informativa estesa (*Cookie policy*) che esplicita nel dettaglio le modalità e le finalità di trattamento esercitate mediante i cookie.

4.3 La legge sul crimine informatico (*Computer Crime*)

Il fattore tecnologico sempre più presente e costante nelle vite odierne ha portato, oltre che ad evidenti vantaggi, anche ad un incremento di nuove forme di reato: i crimini informatici (*Computer Crimes*).
In Italia il legislatore ha emanato le Leggi n. 547 del 23 dicembre 1993 e n. 48 del 18 marzo 2008 che introducono una serie di reati, c.d. informatici, all'interno del **Codice Penale**, quali:

- accesso abusivo ad un sistema informatico o telematico;
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- diffusione di programmi diretti a danneggiare o interrompere un sistema informatico;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche;
- danneggiamento di sistemi informatici o telematici;
- esercizio arbitrario delle proprie ragioni con violenza sulle cose;
- attentato a impianti di pubblica utilità;
- frode informatica;
- ingiuria e diffamazione su Internet.

Per la prevenzione di tali reati è necessaria l'adozione di misure di sicurezza tecniche, informatiche, organizzative e procedurali atte ad impedire l'accesso abusivo al sistema informatico, a minimizzarne i danni e ad eludere la conoscenza di informazioni e dati riservati a soggetti estranei malintenzionati.

4.4 Il Decreto Legislativo 231/2001

Il D.Lgs. 231/01 introduce l'applicazione di sanzioni amministrative nei confronti di società o enti responsabili di aver consentito o non impedito ai propri soggetti interni (sia figure apicali che dipendenti) di commettere un reato penale a favore e vantaggio dell'organizzazione stessa.

Ottemperare al D.Lgs. 231/01 è facoltativo per le aziende, salvo nei casi in cui le stesse operino per la Pubblica Amministrazione.

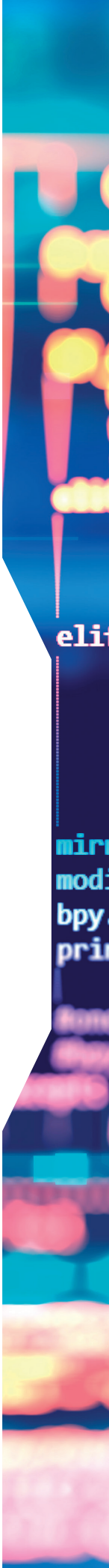
Tuttavia, quando si verifica un reato imputabile ad una società poter dimostrare di aver redatto e implementato un efficiente Modello Organizzativo 231 consente di ridurre o annullare la sanzione amministrativa applicabile.

I reati previsti dal Decreto 231/01 si suddividono in:

- delitti contro la pubblica amministrazione (ad es. corruzione, truffa, frode ai danni dello Stato);
- reati societari (false comunicazioni sociali, falso in prospetto, etc.);
- delitti in materia di terrorismo e di eversione dell'ordine democratico;
- delitti contro la personalità individuale (sfruttamento della prostituzione, pornografia minorile, etc.);
- abusi di mercato;
- pratiche di mutilazione degli organi genitali femminili;
- reati transnazionali (associazione per delinquere, traffico di sostanze stupefacenti, etc.);
- omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
- reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita;
- delitti informatici ed illecito trattamento dei dati (crimini informatici o *cyber crime*);
- delitti di criminalità organizzata;
- delitti contro l'industria e il commercio;
- delitti in materia di violazioni del diritto d'autore;
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- reati ambientali ed inquinamento del mare da parte delle navi;
- impiego di lavoratori stranieri irregolari.

Un Modello Organizzativo efficace volto a ridurre la responsabilità dell'azienda in caso di commissione di reati deve basarsi sui seguenti elementi fondamentali:

- mappatura delle attività a rischio per la realizzazione di un reato;
- procedure volte a definire le azioni di controllo atte a prevenire i rischi di reato;
- codice etico contenente i principi e le regole di comportamento da rispettare;
- costituzione di un Organismo di Vigilanza;
- attività di auditing;
- formazione per tutto il personale;
- sistema disciplinare atto a scoraggiare e punire l'inosservanza del Modello Organizzativo;
- continuo aggiornamento del Modello Organizzativo.



4.5 Il Codice dell'Amministrazione Digitale (CAD)

Il D.Lgs. n. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale - CAD) istituisce il diritto dei cittadini e delle imprese ad intrattenere rapporti con la PA (Pubblica Amministrazione) mediante l'uso di nuove tecnologie, al fine di facilitare le comunicazioni, ridurre i tempi e snellire i processi burocratici. Alcuni esempi di strumenti regolamentati nel Codice sono la Posta Elettronica Certificata, i documenti informatici e le firme elettroniche.

Il Codice si applica alle Amministrazioni pubbliche, alle Società interamente partecipate da enti pubblici o con prevalente capitale pubblico e ai privati gestori di servizi pubblici.
Le Pubbliche Amministrazioni sono pertanto tenute al rispetto del Codice dell'Amministrazione Digitale che impone tre fondamentali ambiti di intervento su cui operare:

- organizzazione interna che prevede un riallineamento dei processi aziendali per far fronte all'innovazione tecnologica e ai requisiti imposti;
- gestione dei rapporti con cittadini e imprese tramite mezzi telematici e non più cartacei;
- adozione di adeguati livelli di sicurezza informatica dei sistemi e delle infrastrutture.

L'obiettivo di raggiungere un adeguato livello di sicurezza informatica si ottiene attraverso misure di carattere organizzativo e tecnologico, quali ad esempio:

- livelli di autenticazione diversi in base ai ruoli ricoperti;
- tracciatura delle operazioni svolte sui sistemi;
- sistemi di prevenzione e blocco da accessi non autorizzati;
- sistemi idonei a garantire continuità operativa e recupero da disastro (*disaster recovery*);
- individuazione di soggetti con responsabilità in ambito ICT;
- formazione del personale interno.

Capitolo 5

STANDARD

internazionali per la gestione dei sistemi informativi[10]

5.1 ISO/IEC 27001:2013 - Sicurezza delle informazioni

Lo Standard Internazionale ISO/IEC 27001: 2013 è finalizzato a proteggere la riservatezza, l'integrità e la disponibilità delle informazioni di un'organizzazione tramite un insieme di processi, controlli e attività mirate alla analisi e alla gestione dei rischi a cui sono soggette.

Gli elementi principali di un efficace sistema di gestione per la sicurezza delle informazioni (*Information Security Management System* - ISMS) sono:

- analisi del contesto in cui opera l'azienda (fattori esterni, fattori interni, etc.);
- definizione dei ruoli, dei compiti, delle competenze e delle responsabilità dei soggetti che operano in azienda;
- attività di sensibilizzazione e formazione dei soggetti interni in materia di sicurezza delle informazioni;
- regolamentazione delle comunicazioni interne ed esterne all'azienda;
- processo di gestione dei cambiamenti a cui può essere soggetta l'organizzazione;
- individuazione, analisi e valutazione dei rischi;
- processo di trattamento dei rischi individuati al fine di ridurli o contenere le conseguenze;
- redazione di una politica della sicurezza (*security policy*);
- procedure specifiche per ogni processo attinente la sicurezza delle informazioni;
- adeguato insieme di controlli che comprendono misure tecniche, organizzative, fisiche e procedurali a garanzia di una reale sicurezza delle informazioni;
- attività di auditing e monitoraggio dell'efficacia del Sistema di Gestione;
- aggiornamento e miglioramento continuo del Sistema di Gestione.

5.2 ISO 22301:2012 - Gestione della continuità operativa

La Norma ISO 22301:2012 definisce i processi necessari per un Sistema di Gestione della Continuità Operativa. Garantire la continuità operativa di un'azienda significa predisporre, mantenere e aggiornare una serie di misure organizzative e tecniche necessarie sia per prevenire il verificarsi di eventi avversi sia per garantire, nel caso in cui si verifichino, il continuo svolgimento delle principali attività aziendali.

Per eventi avversi si intende qualsiasi evento in grado di compromettere l'operatività aziendale determinando, ad esempio, l'inaccessibilità della sede e dei locali aziendali, l'indisponibilità dei sistemi IT, del personale, dell'energia elettrica, etc.
L'obiettivo del BCM (*Business Continuity Management*) è quindi quello di consentire all'Azienda di continuare ad operare senza interruzioni anche se colpiti da un incidente (ad esempio guasto prolungato all'impianto elettrico).

[10] *NB: si tratta di norme di certificazione alle quali le aziende possono aderire su base volontaria*

L'output dell'intero processo è il Piano di Continuità Operativa (*Business Continuity Plan* o BCP) che racchiude:

- le misure da adottare per prevenire il verificarsi di eventi avversi;
- le strategia di ripristino e gli interventi necessari in risposta all'incidente o al guasto (*Disaster Recovery Plan*);
- le procedure per una gestione ottimale e ordinata dell'evento occorso e per una tempestiva risoluzione dell'emergenza;
- i ruoli e le responsabilità del personale aziendale nelle situazioni di crisi;
- gli strumenti necessari e la documentazione a supporto.

5.3 ISO/IEC 20000:2011 - Gestione dei servizi IT

Lo standard ISO/IEC 20000:2011 ha l'obiettivo di fornire i requisiti necessari affinché il sistema di gestione dei servizi IT possa essere conforme a standard di eccellenza.
La norma si applica alle aziende che forniscono servizi IT a soggetti terzi o alle società che possiedono un sistema informatico di medio-alta complessità e gestiscono internamente i servizi IT connessi.
I servizi IT in oggetto possono riguardare indistintamente sia sistemi hardware sia software.

I principali requisiti da rispettare in ogni fase del servizio possono essere riepilogati in:

- regolamentazione del servizio e dei livelli di servizio (SLA), sia nel caso di un fornitore che eroga tali servizi a terzi sia per servizi IT svolti da una divisione interna dell'organizzazione;
- reportistica (*reporting*) dei servizi erogati, con il dettaglio delle attività eseguite dal fornitore IT nei confronti del cliente o internamente all'organizzazione;
- adeguate garanzie di continuità e disponibilità del servizio;
- preventivazione iniziale dei costi, delle risorse, dei beni e dei mezzi da mettere a budget per l'erogazione dei servizi IT, a terzi o internamente all'organizzazione, e successiva consuntivazione;
- determinazione delle capacità e delle prestazioni che l'azienda è in grado di offrire in ambito IT a terzi o alla propria organizzazione (tipologia di servizi erogabili, requisiti, tempistiche, risorse, tecnologie, etc.);
- implementazione di una politica della sicurezza delle informazioni che prenda in considerazione i requisiti del servizio e tutti gli aspetti connessi:
  - controlli fisici, tecnici e amministrativi finalizzati a preservare la riservatezza, l'integrità e l'accessibilità del patrimonio informativo e a gestire i rischi connessi;
  - gestione tempestiva degli incidenti in base alle priorità aziendali;
  - requisiti di sicurezza da rispettare per lo sviluppo di software (identificazione e controllo delle versioni, conservazione separata delle configurazioni, stabilire la frequenza e la tipologia dei rilasci, etc.).

MISURE ORGANIZZATIVE	CDPR	Cookie	Cibercryme	231/01	CAD	27001	22301	20000
Identificazione ruoli e assegnazione responsabilità in ambito IT	●			●	●	●	●	●
Definizione di adeguati SLA con fornitori IT	●			●	●	●	●	●
Attività di formazione, sensibilizzazione e informazione nel confronto degli utenti	●	●	●	●	●	●	●	●
Sottoscrizione accordi di riservatezza con dipendenti e terzi	●		●	●	●	●	●	●
Monitoraggio dei sistemio e delle performance	●		●	●	●	●	●	●
Individuazione di budget annuali per incrementare il li vello di sicurezza ed efficenza dei sistemi IT	●		●	●	●	●	●	●
Adesione a gruppi specialistici e associazioni professionali che operano anche in ambito sicurezza delle informazioni	●		●	●		●	●	●

MISURE PROCEDURALI E DOCUMENTALI	CDPR	Cookie	Cibercryme	231/01	CAD	27001	22301	20000
Analisi dei rischi che incombono sui sistemi e sulle informazioni contenute	◆		◆	◆	◆	◆		◆
Insieme di politiche a garanzia del sistema informativo	◆		◆	◆	◆	◆		◆
Lettera di presa in carico degli strumenti assegnati agli utenti	◆					◆		
Inventario IT	◆					◆		
Regolamento aziendale sul corretto utilizzo degli strumenti da parte degli utenti	◆		◆	◆		◆		
Business Continuity Plan e Disaster Recovery Plan	◆				◆	◆	◆	◆
Informative e raccolta di consenso per clienti e utenti del sito internet	◆	◆						
Sistema disciplinare interno in caso di violazioni accertate				◆		◆		

MISURE ORGANIZZATIVE	CDPR	Cookie	Cibercryme	231/01	CAD	27001	22301	20000
Creazione profili utenti individuali e assegnazione permissions in base al ruolo e alle mansioni	▲		▲	▲	▲	▲		▲
Abilitazione accessi alle cartelle, ai programmi e ai file di rete solo agli utenti autorizzati per fini lavorativi	▲		▲	▲	▲	▲		▲
Accesso al sistema previo inserimento si password che rispettano gli standard di sicurezza	▲		▲	▲	▲	▲		▲
Utilizzo sistemi di cifratura di file e base dati	▲		▲	▲	▲	▲		▲
Separazione di ambienti sviluppo, test e produzione			▲			▲		▲
Sistemi di prevenzione e blocco relativamente a malware e virus (anivirus, Firewall, etc.)	▲		▲	▲	▲	▲		▲
Registrazione dei log degli accessi	▲		▲	▲	▲	▲		▲
Sistema di filtraggio e blocco per la navigazione in internet e per l'installazione di software non autorizzati	▲		▲	▲	▲	▲		
Sistemi di segnalazione e alert per gli eventi avversi occorsi al sistema	▲		▲	▲	▲	▲	▲	▲
Adeguate procedure di back up e di ripristino dati	▲			▲	▲	▲	▲	▲
Sistemi atti a garantire la continuità operativa in caso di malfunzionamenti tecnici	▲			▲	▲	▲	▲	▲
Dismissione sicura degli strumenti e cancellazione definitiva dei dati	▲		▲	▲	▲	▲		

MISURE FISICHE	CDPR	Cookie	Cibercryme	231/01	CAD	27001	22301	20000
Controllo accessi da parte di personale esterno	■					■	■	
Protezione degli accessi fisici alla sala CED e a locali riservati	■		■	■	■	■	■	■
Sistemi di protezione che garantiscono la continuità del servizio informatico in caso di interruzione dell'alimentazione	■				■	■	■	■
Costante manutenzione degli apparati	■				■	■	■	■
Non lasciare mai incustoditi dispositivi mobili	■		■	■		■